The Cybersecurity Inspection and Real-Time Response Fieldbook

50 defensive skills for authorized inspections, live triage, containment, recovery, and resilient operations with free and open tooling

Defensive use only. Authorized systems only.

The Cybersecurity Inspection and Real-Time Response Fieldbook

Subtitle

50 defensive skills for authorized inspections, live triage, containment, recovery, and resilient operations with free and open tooling

Use Boundary

This is a defensive book for authorized cybersecurity inspection and incident response. It is written for owners, defenders, consultants, students, and operators who need to inspect systems they are allowed to protect. It intentionally avoids instructions for unauthorized access, exploitation, retaliation, or evasion. If an action could affect a third-party system, personal data, legal duties, or business continuity, involve the right owner, counsel, and executive decision-maker before acting.

What "Real-Time Response" Means

Real-time response means an organized defensive loop: detect, validate, contain, preserve, eradicate, recover, and improve. It does not mean panic, guessing, public blame, or attacking back. A mature team can disable a compromised account, isolate a host, block a domain, rotate a secret, pause a risky integration, collect evidence, restore a clean service, and brief leadership without losing the thread.

What "Free" Means

The book emphasizes free, community, or open-source options where possible: osquery, Wazuh, Suricata, Zeek, Sigma, YARA, Velociraptor, OpenCTI, MISP, TheHive, Trivy, Syft, Grype, Gitleaks, OpenVAS/GVM, OWASP ZAP, Semgrep Community, restic, BorgBackup, and native logs from operating systems, clouds, identity providers, and SaaS platforms. Some environments will still need commercial tooling, legal advice, insurance support, or specialist help. Free tools do not remove the need for authority, skill, and evidence discipline.

The Field Operating Loop

1. Govern: know who is allowed to decide, inspect, contain, and communicate.
2. Identify: know assets, owners, data, dependencies, and likely blast radius.
3. Protect: harden, patch, segment, back up, and reduce privilege before the crisis.
4. Detect: collect useful telemetry and test detections against realistic behavior.
5. Respond: contain inside the owned environment, preserve evidence, and coordinate.

6. Recover: restore clean service, validate business function, and watch closely.
7. Improve: convert every finding and incident into a control, detection, exercise, or policy update.

Severity Model

Severity	Meaning	First Response
SEV-1	Active compromise of critical service, privileged identity, regulated data, or destructive capability	Incident commander, executive contact, legal/privacy review, containment decision, evidence preservation
SEV-2	Confirmed compromise with bounded blast radius	Case owner, affected owner, containment within approved scope, targeted recovery
SEV-3	Suspicious activity or vulnerable exposure without confirmed compromise	Triage, owner notification, remediation ticket, detection tuning
SEV-4	Hygiene issue, policy gap, or low-risk misconfiguration	Backlog action, scheduled inspection, baseline update

Core Sources Used

- NIST Cybersecurity Framework 2.0: https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20
- NIST SP 800-61 Rev. 3 Incident Response Recommendations and Considerations: https://csrc.nist.gov/pubs/sp/800/61/r3/final
- CISA Federal Government Cybersecurity Incident and Vulnerability Response Playbooks: https://www.cisa.gov/resources-tools/resources/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks
- CISA Known Exploited Vulnerabilities Catalog: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- MITRE ATT&CK Enterprise Matrix: https://attack.mitre.org/matrices/
- OWASP Top 10: https://owasp.org/www-project-top-ten/
- OWASP Application Security Verification Standard: https://owasp.org/www-project-application-security-verification-standard/
- CIS Critical Security Controls v8.1: https://www.cisecurity.org/controls/v8-1
- Microsoft Security Baselines: https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines
- osquery Documentation: https://osquery.readthedocs.io/
- Sigma Specification: https://sigmahq.io/sigma-specification/

- Suricata: https://suricata.io/
- Wazuh Documentation: https://documentation.wazuh.com/current/getting-started/index.html
- Velociraptor: https://www.rapid7.com/products/velociraptor/
- OpenCTI Documentation: https://docs.opencti.io/latest/

Skill 01: Authority, Scope, and Legal Guardrails

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects permission boundaries, ownership, emergency authority, and lawful response. The main risk is scope drift and unauthorized action. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of permission boundaries, ownership, emergency authority, and lawful response.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.

6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that written authority exists.
- [ ] Confirm that owner is named.
- [ ] Confirm that decision rights are current.
- [ ] Confirm that exceptions expire.
- [ ] Confirm that legal and privacy contacts are known.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- NIST CSF 2.0 profiles
- CIS Controls v8.1
- ticketing system
- shared decision log
- risk register

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners

- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Govern, Identify. Map attacker behavior using MITRE ATT&CK language: Reconnaissance, Resource Development. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is scope drift and unauthorized action.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 02: Asset Inventory and Crown-Jewel Mapping

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects systems, data stores, owners, business criticality, and blast radius. The main risk is unknown exposure and poor prioritization. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of systems, data stores, owners, business criticality, and blast radius.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that asset has an owner.
- [ ] Confirm that business criticality is assigned.
- [ ] Confirm that internet exposure is known.
- [ ] Confirm that data classification is recorded.
- [ ] Confirm that monitoring coverage is visible.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- osquery
- Nmap in authorized ranges
- Amass for owned domains
- Snipe-IT
- Open-AudIT

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Identify. Map attacker behavior using MITRE ATT&CK language: Discovery. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is unknown exposure and poor prioritization.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 03: Identity and Access Inspection

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects accounts, groups, conditional access, MFA, passwordless options, and risky sign-ins. The main risk is credential compromise and privilege misuse. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of accounts, groups, conditional access, MFA, passwordless options, and risky sign-ins.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that MFA is enforced.
- [ ] Confirm that privileged paths are minimized.
- [ ] Confirm that stale accounts are removed.
- [ ] Confirm that service identities are owned.
- [ ] Confirm that risky sign-ins are reviewed.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.

5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- IdP audit exports
- Entra ID or Google Workspace logs
- BloodHound Community Edition in authorized AD
- KeePassXC
- OpenLDAP tooling

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Protect, Detect. Map attacker behavior using MITRE ATT&CK language: Credential Access, Initial Access. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.

- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is credential compromise and privilege misuse.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 04: Privileged Access Review

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects administrators, break-glass accounts, service principals, root accounts, and just-in-time access. The main risk is privilege escalation and admin takeover. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of administrators, break-glass accounts, service principals, root accounts, and just-in-time access.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that MFA is enforced.
- [ ] Confirm that privileged paths are minimized.
- [ ] Confirm that stale accounts are removed.
- [ ] Confirm that service identities are owned.
- [ ] Confirm that risky sign-ins are reviewed.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- IdP audit exports
- Entra ID or Google Workspace logs
- BloodHound Community Edition in authorized AD

- KeePassXC
- OpenLDAP tooling

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Govern, Protect. Map attacker behavior using MITRE ATT&CK language: Privilege Escalation, Persistence. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is privilege escalation and admin takeover.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 05: Endpoint Baseline and Hardening

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects workstation and server baseline state, security agents, local policies, and unsafe defaults. The main risk is malware execution and persistence. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of workstation and server baseline state, security agents, local policies, and unsafe defaults.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.

6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that agent health is current.
- [ ] Confirm that local admin is limited.
- [ ] Confirm that disk encryption is enabled.
- [ ] Confirm that logging is forwarded.
- [ ] Confirm that hardening drift is tracked.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- osquery
- Wazuh
- Velociraptor
- Lynis
- Windows Event Forwarding

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners

- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Protect, Detect. Map attacker behavior using MITRE ATT&CK language: Execution, Persistence. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is malware execution and persistence.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 06: Patch and Exposure Triage

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects missing patches, known exploited vulnerabilities, exposed services, and compensating controls. The main risk is weaponized public vulnerabilities. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of missing patches, known exploited vulnerabilities, exposed services, and compensating controls.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that KEV items are prioritized.
- [ ] Confirm that external exposure is known.
- [ ] Confirm that patch SLAs are visible.
- [ ] Confirm that exceptions have compensating controls.
- [ ] Confirm that fix evidence is retained.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- OpenVAS/GVM
- CISA KEV catalog
- Trivy
- Grype
- OWASP Dependency-Check

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Identify, Protect. Map attacker behavior using MITRE ATT&CK language: Initial Access, Exploitation. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is weaponized public vulnerabilities.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 07: Network Segmentation Inspection

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects zones, routes, firewalls, east-west traffic, management planes, and choke points. The main risk is lateral movement and uncontrolled spread. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of zones, routes, firewalls, east-west traffic, management planes, and choke points.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that management access is restricted.
- [ ] Confirm that egress is monitored.
- [ ] Confirm that east-west access is intentional.
- [ ] Confirm that IDS sensors see critical traffic.
- [ ] Confirm that deny rules are tested.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.

5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- Suricata
- Zeek
- Wireshark
- Arkime
- ntopng

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Protect, Detect. Map attacker behavior using MITRE ATT&CK language: Lateral Movement, Command and Control. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.

- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is lateral movement and uncontrolled spread.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 08: Perimeter and Remote Access Review

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects VPN, zero trust access, public services, DNS, certificates, WAF, and edge controls. The main risk is external intrusion and exposed management. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.

- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of VPN, zero trust access, public services, DNS, certificates, WAF, and edge controls.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that management access is restricted.
- [ ] Confirm that egress is monitored.
- [ ] Confirm that east-west access is intentional.
- [ ] Confirm that IDS sensors see critical traffic.
- [ ] Confirm that deny rules are tested.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- Suricata
- Zeek
- Wireshark
- Arkime
- ntopng

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Protect, Detect. Map attacker behavior using MITRE ATT&CK language: Initial Access, External Remote Services. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.

- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is external intrusion and exposed management.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 09: Cloud Account Security Inspection

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects cloud identity, organization policy, audit logs, public exposure, keys, and workload permissions. The main risk is cloud control-plane compromise. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of cloud identity, organization policy, audit logs, public exposure, keys, and workload permissions.

3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that root or owner accounts are protected.
- [ ] Confirm that audit logging is immutable.
- [ ] Confirm that public access is reviewed.
- [ ] Confirm that keys are rotated.
- [ ] Confirm that least privilege is enforced.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- Prowler
- ScoutSuite
- Cloud Custodian
- cloud provider audit logs
- Steampipe

Evidence to Preserve

- authorized scope and owner approval

- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Govern, Protect, Detect. Map attacker behavior using MITRE ATT&CK language: Cloud Account, Valid Accounts. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is cloud control-plane compromise.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 10: SaaS and Workspace Inspection

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects email suites, collaboration platforms, OAuth apps, sharing settings, audit logs, and tenant posture. The main risk is SaaS data leak and account takeover. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of email suites, collaboration platforms, OAuth apps, sharing settings, audit logs, and tenant posture.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that external sharing is controlled.
- [ ] Confirm that OAuth grants are reviewed.

- [ ] Confirm that admin roles are minimal.
- [ ] Confirm that audit logs are retained.
- [ ] Confirm that tenant settings match policy.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- tenant audit logs
- OAuth app reports
- admin center exports
- CASB-free reports where available
- MISP for indicators

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible

- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Protect, Detect. Map attacker behavior using MITRE ATT&CK language: Initial Access, Collection. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is SaaS data leak and account takeover.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 11: Email Security and Phishing Defense

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects mail authentication, mailbox rules, risky forwarding, reporting flows, and user resilience. The main risk is phishing, BEC, and malicious attachments. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of mail authentication, mailbox rules, risky forwarding, reporting flows, and user resilience.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that SPF, DKIM, and DMARC are aligned.
- [ ] Confirm that auto-forwarding is controlled.
- [ ] Confirm that reporting is easy.
- [ ] Confirm that mailbox audit is on.
- [ ] Confirm that payment-change workflow is verified.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.

3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- DMARC aggregate reports
- mailbox audit logs
- GoPhish for authorized training
- MXToolbox free checks
- TheHive case tracking

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Protect, Detect, Respond. Map attacker behavior using MITRE ATT&CK language: Phishing, Collection. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is phishing, BEC, and malicious attachments.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 12: Web Application Surface Inspection

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects auth flows, access control, input handling, headers, sessions, and deployment exposure. The main risk is web exploitation and data access. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of auth flows, access control, input handling, headers, sessions, and deployment exposure.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that auth and session controls are tested.
- [ ] Confirm that access control is verified.
- [ ] Confirm that dependencies are scanned.
- [ ] Confirm that logs include security events.
- [ ] Confirm that secrets are absent from code.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- OWASP ZAP in authorized tests
- Semgrep Community
- OWASP ASVS
- Trivy
- Syft

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Protect, Detect. Map attacker behavior using MITRE ATT&CK language: Initial Access, Exploit Public-Facing Application. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.

- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is web exploitation and data access.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 13: API Security Inspection

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects API inventory, authentication, authorization, rate limits, tokens, schema validation, and logs. The main risk is API abuse and token leakage. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of API inventory, authentication, authorization, rate limits, tokens, schema validation, and logs.
3. Mark what is normal, what is unknown, and what is immediately unsafe.

4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that auth and session controls are tested.
- [ ] Confirm that access control is verified.
- [ ] Confirm that dependencies are scanned.
- [ ] Confirm that logs include security events.
- [ ] Confirm that secrets are absent from code.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- OWASP ZAP in authorized tests
- Semgrep Community
- OWASP ASVS
- Trivy
- Syft

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate

- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Protect, Detect. Map attacker behavior using MITRE ATT&CK language: Initial Access, Collection. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is API abuse and token leakage.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 14: Vulnerability Management Cadence

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects intake, validation, prioritization, remediation ownership, exception handling, and reporting. The main risk is stalled remediation and risk blindness. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of intake, validation, prioritization, remediation ownership, exception handling, and reporting.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that KEV items are prioritized.

- [ ] Confirm that external exposure is known.
- [ ] Confirm that patch SLAs are visible.
- [ ] Confirm that exceptions have compensating controls.
- [ ] Confirm that fix evidence is retained.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- OpenVAS/GVM
- CISA KEV catalog
- Trivy
- Grype
- OWASP Dependency-Check

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access

- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Govern, Identify, Protect. Map attacker behavior using MITRE ATT&CK language: Reconnaissance, Initial Access. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is stalled remediation and risk blindness.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 15: Logging Coverage and Telemetry Quality

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full

access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects event sources, retention, time sync, parsing quality, and high-value alert visibility. The main risk is silent compromise and weak investigation. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of event sources, retention, time sync, parsing quality, and high-value alert visibility.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that each critical source logs.
- [ ] Confirm that time sync works.
- [ ] Confirm that parsing is reliable.
- [ ] Confirm that alerts have response notes.
- [ ] Confirm that detections are tested after changes.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.

2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- Wazuh
- Sigma
- Elastic or OpenSearch
- YARA
- ATT&CK Navigator

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Detect. Map attacker behavior using MITRE ATT&CK language: Defense Evasion, Discovery. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected,

and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is silent compromise and weak investigation.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 16: SIEM Detection Engineering

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects use cases, Sigma-style logic, ATT&CK mapping, tuning, response notes, and regression tests. The main risk is missed adversary behavior. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of use cases, Sigma-style logic, ATT&CK mapping, tuning, response notes, and regression tests.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that each critical source logs.
- [ ] Confirm that time sync works.
- [ ] Confirm that parsing is reliable.
- [ ] Confirm that alerts have response notes.
- [ ] Confirm that detections are tested after changes.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.

7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- Wazuh
- Sigma
- Elastic or OpenSearch
- YARA
- ATT&CK Navigator

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Detect, Respond. Map attacker behavior using MITRE ATT&CK language: Execution, Persistence, Lateral Movement. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is missed adversary behavior.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 17: Endpoint Detection and Response Operations

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects agent health, policy coverage, isolation rights, suspicious process trees, and response workflows. The main risk is endpoint compromise and delayed containment. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of agent health, policy coverage, isolation rights, suspicious process trees, and response workflows.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that agent health is current.
- [ ] Confirm that local admin is limited.
- [ ] Confirm that disk encryption is enabled.
- [ ] Confirm that logging is forwarded.
- [ ] Confirm that hardening drift is tracked.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- osquery
- Wazuh
- Velociraptor
- Lynis
- Windows Event Forwarding

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Detect, Respond. Map attacker behavior using MITRE ATT&CK language: Execution, Defense Evasion. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is endpoint compromise and delayed containment.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 18: Network Detection With IDS and NSM

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects DNS, HTTP, TLS, flow, IDS alerts, unusual egress, and command-and-control patterns. The main risk is covert traffic and lateral movement. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of DNS, HTTP, TLS, flow, IDS alerts, unusual egress, and command-and-control patterns.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.

7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that management access is restricted.
- [ ] Confirm that egress is monitored.
- [ ] Confirm that east-west access is intentional.
- [ ] Confirm that IDS sensors see critical traffic.
- [ ] Confirm that deny rules are tested.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- Suricata
- Zeek
- Wireshark
- Arkime
- ntopng

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Detect, Respond. Map attacker behavior using MITRE ATT&CK language: Command and Control, Exfiltration. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is covert traffic and lateral movement.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 19: Threat Intelligence Intake

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects source quality, indicators, TTPs, enrichment, relevance, and operationalization. The main risk is low-signal feeds and missed context. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of source quality, indicators, TTPs, enrichment, relevance, and operationalization.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that source credibility is scored.
- [ ] Confirm that indicators are aged.
- [ ] Confirm that TTPs matter more than raw IOCs.
- [ ] Confirm that intelligence maps to assets.
- [ ] Confirm that expired intel is removed.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- OpenCTI
- MISP
- CISA advisories
- ATT&CK
- abuse.ch community feeds

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Identify, Detect. Map attacker behavior using MITRE ATT&CK language: Resource Development, Command and Control. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is low-signal feeds and missed context.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 20: Attack Surface Monitoring

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects internet-facing assets, new domains, leaked services, certificates, cloud buckets, and shadow IT. The main risk is surprise exposure. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of internet-facing assets, new domains, leaked services, certificates, cloud buckets, and shadow IT.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that asset has an owner.
- [ ] Confirm that business criticality is assigned.
- [ ] Confirm that internet exposure is known.
- [ ] Confirm that data classification is recorded.
- [ ] Confirm that monitoring coverage is visible.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.

6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- osquery
- Nmap in authorized ranges
- Amass for owned domains
- Snipe-IT
- Open-AudIT

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Identify, Detect. Map attacker behavior using MITRE ATT&CK language: Reconnaissance, Initial Access. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.

- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is surprise exposure.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 21: Backup and Recovery Readiness

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects backup coverage, immutability, restore tests, RPO/RTO, identity dependencies, and recovery order. The main risk is failed recovery after destructive attack. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of backup coverage, immutability, restore tests, RPO/RTO, identity dependencies, and recovery order.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that restore was tested.
- [ ] Confirm that backup identity is protected.
- [ ] Confirm that immutability is enabled.
- [ ] Confirm that recovery order is documented.
- [ ] Confirm that business owner validates service.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- restic
- BorgBackup
- rclone
- immutable storage controls
- restore-test checklist

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Protect, Recover. Map attacker behavior using MITRE ATT&CK language: Impact. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is failed recovery after destructive attack.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 22: Ransomware Readiness and Response

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects early signals, containment decisions, backup protection, rebuild path, and executive communications. The main risk is ransomware spread and data extortion. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of early signals, containment decisions, backup protection, rebuild path, and executive communications.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.

7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that severity is assigned.
- [ ] Confirm that containment authority is clear.
- [ ] Confirm that evidence is preserved.
- [ ] Confirm that communications are controlled.
- [ ] Confirm that actions are tracked.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- TheHive
- Velociraptor
- Wazuh
- CISA playbooks
- shared war-room log

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Detect, Respond, Recover. Map attacker behavior using MITRE ATT&CK language: Impact, Exfiltration. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is ransomware spread and data extortion.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 23: Credential Theft Response

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects stolen passwords, session tokens, MFA fatigue, refresh tokens, and suspicious login trails. The main risk is account takeover and persistence. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of stolen passwords, session tokens, MFA fatigue, refresh tokens, and suspicious login trails.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that MFA is enforced.
- [ ] Confirm that privileged paths are minimized.
- [ ] Confirm that stale accounts are removed.
- [ ] Confirm that service identities are owned.
- [ ] Confirm that risky sign-ins are reviewed.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- IdP audit exports
- Entra ID or Google Workspace logs
- BloodHound Community Edition in authorized AD
- KeePassXC
- OpenLDAP tooling

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Detect, Respond. Map attacker behavior using MITRE ATT&CK language: Credential Access, Valid Accounts. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is account takeover and persistence.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 24: Business Email Compromise Response

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects mailbox rules, forwarding, payment changes, OAuth grants, login history, and stakeholder notification. The main risk is fraud, data theft, and account abuse. The goal

is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of mailbox rules, forwarding, payment changes, OAuth grants, login history, and stakeholder notification.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that SPF, DKIM, and DMARC are aligned.
- [ ] Confirm that auto-forwarding is controlled.
- [ ] Confirm that reporting is easy.
- [ ] Confirm that mailbox audit is on.
- [ ] Confirm that payment-change workflow is verified.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.

5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- DMARC aggregate reports
- mailbox audit logs
- GoPhish for authorized training
- MXToolbox free checks
- TheHive case tracking

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Detect, Respond, Recover. Map attacker behavior using MITRE ATT&CK language: Phishing, Collection. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.

- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is fraud, data theft, and account abuse.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 25: Malware Triage and Containment

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects suspicious binaries, persistence, process behavior, affected hosts, and isolation choices. The main risk is malware execution and spread. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.

- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of suspicious binaries, persistence, process behavior, affected hosts, and isolation choices.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that severity is assigned.
- [ ] Confirm that containment authority is clear.
- [ ] Confirm that evidence is preserved.
- [ ] Confirm that communications are controlled.
- [ ] Confirm that actions are tracked.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- TheHive
- Velociraptor

- Wazuh
- CISA playbooks
- shared war-room log

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Detect, Respond. Map attacker behavior using MITRE ATT&CK language: Execution, Persistence. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.

- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is malware execution and spread.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 26: Web Shell and Server Compromise Response

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects unexpected files, child processes, web logs, credentials, shells, and rebuild evidence. The main risk is server takeover and persistence. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of unexpected files, child processes, web logs, credentials, shells, and rebuild evidence.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.

5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that severity is assigned.
- [ ] Confirm that containment authority is clear.
- [ ] Confirm that evidence is preserved.
- [ ] Confirm that communications are controlled.
- [ ] Confirm that actions are tracked.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- TheHive
- Velociraptor
- Wazuh
- CISA playbooks
- shared war-room log

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results

- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Detect, Respond, Recover. Map attacker behavior using MITRE ATT&CK language: Persistence, Command and Control. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is server takeover and persistence.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 27: Cloud Key or Token Leak Response

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects exposed credentials, IAM impact, service use, audit trails, rotation, and blast-radius review. The main risk is cloud resource abuse and data access. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of exposed credentials, IAM impact, service use, audit trails, rotation, and blast-radius review.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that root or owner accounts are protected.

- [ ] Confirm that audit logging is immutable.
- [ ] Confirm that public access is reviewed.
- [ ] Confirm that keys are rotated.
- [ ] Confirm that least privilege is enforced.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- Prowler
- ScoutSuite
- Cloud Custodian
- cloud provider audit logs
- Steampipe

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access

- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Detect, Respond. Map attacker behavior using MITRE ATT&CK language: Credential Access, Exfiltration. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is cloud resource abuse and data access.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 28: Insider Risk and Data Exfiltration Response

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full

access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects unusual access, mass download, removable media, sanctioned channels, and HR/legal coordination. The main risk is data theft and policy breach. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of unusual access, mass download, removable media, sanctioned channels, and HR/legal coordination.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that data owner is known.
- [ ] Confirm that access is least privilege.
- [ ] Confirm that exports are logged.
- [ ] Confirm that encryption is verified.
- [ ] Confirm that retention matches policy.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.

2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- database audit logs
- DLP exports where available
- Apache Ranger
- OpenSearch dashboards
- rclone inventory

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Govern, Detect, Respond. Map attacker behavior using MITRE ATT&CK language: Collection, Exfiltration. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false

positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is data theft and policy breach.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 29: DDoS and Service Abuse Response

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects traffic baselines, provider escalation, rate limits, CDN/WAF tuning, and customer messaging. The main risk is availability loss and resource exhaustion. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of traffic baselines, provider escalation, rate limits, CDN/WAF tuning, and customer messaging.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that management access is restricted.
- [ ] Confirm that egress is monitored.
- [ ] Confirm that east-west access is intentional.
- [ ] Confirm that IDS sensors see critical traffic.
- [ ] Confirm that deny rules are tested.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.

7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- Suricata
- Zeek
- Wireshark
- Arkime
- ntopng

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Respond, Recover. Map attacker behavior using MITRE ATT&CK language: Impact. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is availability loss and resource exhaustion.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 30: Supply Chain and Dependency Inspection

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects dependencies, build systems, signatures, CI secrets, package sources, and vendor advisories. The main risk is dependency compromise. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of dependencies, build systems, signatures, CI secrets, package sources, and vendor advisories.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that auth and session controls are tested.
- [ ] Confirm that access control is verified.
- [ ] Confirm that dependencies are scanned.
- [ ] Confirm that logs include security events.
- [ ] Confirm that secrets are absent from code.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- OWASP ZAP in authorized tests
- Semgrep Community
- OWASP ASVS

- Trivy
- Syft

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Govern, Protect, Detect. Map attacker behavior using MITRE ATT&CK language: Supply Chain Compromise. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is dependency compromise.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 31: Container and Kubernetes Inspection

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects images, registries, RBAC, admission, network policy, secrets, runtime signals, and cluster logging. The main risk is container escape and cluster takeover. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of images, registries, RBAC, admission, network policy, secrets, runtime signals, and cluster logging.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.

6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that images are scanned.
- [ ] Confirm that RBAC is minimal.
- [ ] Confirm that secrets are mounted safely.
- [ ] Confirm that network policy is defined.
- [ ] Confirm that runtime alerts exist.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- Trivy
- kube-bench
- Falco
- Syft
- Kyverno policies

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners

- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Protect, Detect. Map attacker behavior using MITRE ATT&CK language: Privilege Escalation, Lateral Movement. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is container escape and cluster takeover.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 32: Database and Data Protection Inspection

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects data classification, encryption, roles, audit logs, backups, retention, and sensitive query behavior. The main risk is unauthorized data access. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of data classification, encryption, roles, audit logs, backups, retention, and sensitive query behavior.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that data owner is known.
- [ ] Confirm that access is least privilege.
- [ ] Confirm that exports are logged.
- [ ] Confirm that encryption is verified.

- [ ] Confirm that retention matches policy.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- database audit logs
- DLP exports where available
- Apache Ranger
- OpenSearch dashboards
- rclone inventory

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Protect, Detect. Map attacker behavior using MITRE ATT&CK language: Collection, Exfiltration. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is unauthorized data access.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 33: Secrets Management Inspection

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects keys, tokens, vaults, rotation, source-code leakage, environment variables, and deployment paths. The main risk is secret leakage and unauthorized access.

The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of keys, tokens, vaults, rotation, source-code leakage, environment variables, and deployment paths.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that secret location is known.
- [ ] Confirm that rotation owner is assigned.
- [ ] Confirm that code is scanned.
- [ ] Confirm that vault access is audited.
- [ ] Confirm that emergency rotation is rehearsed.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.

5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- Gitleaks
- TruffleHog OSS
- SOPS
- age
- Vault Community Edition

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Protect, Detect. Map attacker behavior using MITRE ATT&CK language: Credential Access. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.

- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is secret leakage and unauthorized access.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 34: Secure Configuration and Baselines

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects configuration drift, hardened templates, CIS/Microsoft baselines, exceptions, and evidence. The main risk is misconfiguration and avoidable exposure. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.

- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of configuration drift, hardened templates, CIS/Microsoft baselines, exceptions, and evidence.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that baseline is documented.
- [ ] Confirm that drift is measured.
- [ ] Confirm that exceptions are approved.
- [ ] Confirm that golden images are current.
- [ ] Confirm that change control includes security.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- CIS Benchmarks
- Microsoft Security Baselines

- Lynis
- OpenSCAP
- Ansible

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Govern, Protect. Map attacker behavior using MITRE ATT&CK language: Defense Evasion, Persistence. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.

- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is misconfiguration and avoidable exposure.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 35: Mobile and BYOD Inspection

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects device enrollment, app posture, encryption, lost-device handling, and conditional access. The main risk is mobile account and data exposure. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of device enrollment, app posture, encryption, lost-device handling, and conditional access.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.

5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that agent health is current.
- [ ] Confirm that local admin is limited.
- [ ] Confirm that disk encryption is enabled.
- [ ] Confirm that logging is forwarded.
- [ ] Confirm that hardening drift is tracked.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- osquery
- Wazuh
- Velociraptor
- Lynis
- Windows Event Forwarding

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results

- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Protect, Detect. Map attacker behavior using MITRE ATT&CK language: Initial Access, Collection. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is mobile account and data exposure.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 36: Physical Security and Hardware Trust

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects server rooms, device custody, secure disposal, removable media, and hardware provenance. The main risk is physical tampering and data loss. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of server rooms, device custody, secure disposal, removable media, and hardware provenance.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that written authority exists.

- [ ] Confirm that owner is named.
- [ ] Confirm that decision rights are current.
- [ ] Confirm that exceptions expire.
- [ ] Confirm that legal and privacy contacts are known.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- NIST CSF 2.0 profiles
- CIS Controls v8.1
- ticketing system
- shared decision log
- risk register

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access

- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Protect, Respond. Map attacker behavior using MITRE ATT&CK language: Impact. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is physical tampering and data loss.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 37: Third-Party and Vendor Security

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects supplier access, integration permissions, security contacts, contractual duties, and incident channels. The main risk is supplier-origin compromise. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of supplier access, integration permissions, security contacts, contractual duties, and incident channels.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that written authority exists.
- [ ] Confirm that owner is named.
- [ ] Confirm that decision rights are current.
- [ ] Confirm that exceptions expire.
- [ ] Confirm that legal and privacy contacts are known.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority

exists.

4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- NIST CSF 2.0 profiles
- CIS Controls v8.1
- ticketing system
- shared decision log
- risk register

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Govern, Identify, Respond. Map attacker behavior using MITRE ATT&CK language: Supply Chain Compromise. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is supplier-origin compromise.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 38: Policy, Governance, and Risk Register

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects decision rights, risk ownership, exception expiry, board reporting, and control accountability. The main risk is unowned cyber risk. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.

- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of decision rights, risk ownership, exception expiry, board reporting, and control accountability.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that written authority exists.
- [ ] Confirm that owner is named.
- [ ] Confirm that decision rights are current.
- [ ] Confirm that exceptions expire.
- [ ] Confirm that legal and privacy contacts are known.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- NIST CSF 2.0 profiles
- CIS Controls v8.1
- ticketing system
- shared decision log
- risk register

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Govern. Map attacker behavior using MITRE ATT&CK language: Resource Development. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.

- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is unowned cyber risk.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 39: Security Awareness and Reporting Culture

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects reporting channels, phishing drills, safe escalation, role-based training, and no-blame learning. The main risk is late reporting and human-factor failure. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of reporting channels, phishing drills, safe escalation, role-based training, and no-blame learning.

3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that written authority exists.
- [ ] Confirm that owner is named.
- [ ] Confirm that decision rights are current.
- [ ] Confirm that exceptions expire.
- [ ] Confirm that legal and privacy contacts are known.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- NIST CSF 2.0 profiles
- CIS Controls v8.1
- ticketing system
- shared decision log
- risk register

Evidence to Preserve

- authorized scope and owner approval

- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Govern, Protect. Map attacker behavior using MITRE ATT&CK language: Phishing. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is late reporting and human-factor failure.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 40: Incident Command and War Room Operations

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects roles, severity, rhythm, decision logs, communications, and action tracking. The main risk is confused response and duplicated work. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of roles, severity, rhythm, decision logs, communications, and action tracking.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that severity is assigned.

- [ ] Confirm that containment authority is clear.
- [ ] Confirm that evidence is preserved.
- [ ] Confirm that communications are controlled.
- [ ] Confirm that actions are tracked.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- TheHive
- Velociraptor
- Wazuh
- CISA playbooks
- shared war-room log

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access

- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Respond. Map attacker behavior using MITRE ATT&CK language: Impact. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is confused response and duplicated work.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 41: Evidence Handling and Chain of Custody

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full

access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects evidence integrity, timestamps, hashes, access controls, preservation orders, and handoff notes. The main risk is lost evidence and weak investigation. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of evidence integrity, timestamps, hashes, access controls, preservation orders, and handoff notes.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that collection scope is authorized.
- [ ] Confirm that time is synchronized.
- [ ] Confirm that hashes are recorded.
- [ ] Confirm that original evidence is protected.
- [ ] Confirm that analysis notes are reproducible.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.

2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- Velociraptor
- Autopsy
- Plaso/log2timeline
- Volatility
- hashdeep

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Respond. Map attacker behavior using MITRE ATT&CK language: Defense Evasion. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected,

and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is lost evidence and weak investigation.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 42: Live Triage Collection

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects volatile data, running processes, connections, log exports, endpoint artifacts, and collection scope. The main risk is evidence loss during active compromise. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of volatile data, running processes, connections, log exports, endpoint artifacts, and collection scope.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that collection scope is authorized.
- [ ] Confirm that time is synchronized.
- [ ] Confirm that hashes are recorded.
- [ ] Confirm that original evidence is protected.
- [ ] Confirm that analysis notes are reproducible.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- Velociraptor
- Autopsy
- Plaso/log2timeline
- Volatility
- hashdeep

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Detect, Respond. Map attacker behavior using MITRE ATT&CK language: Discovery, Defense Evasion. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.

- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is evidence loss during active compromise.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 43: Forensic Preservation and Timeline Analysis

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects disk images, log timelines, account events, process lineage, and corroboration. The main risk is uncertain root cause. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.

2. Build a current view of disk images, log timelines, account events, process lineage, and corroboration.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that collection scope is authorized.
- [ ] Confirm that time is synchronized.
- [ ] Confirm that hashes are recorded.
- [ ] Confirm that original evidence is protected.
- [ ] Confirm that analysis notes are reproducible.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- Velociraptor
- Autopsy
- Plaso/log2timeline
- Volatility
- hashdeep

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Respond, Recover. Map attacker behavior using MITRE ATT&CK language: Persistence, Lateral Movement. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is uncertain root cause.

- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 44: Eradication and Rebuild Decisions

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects removal confidence, golden images, credential rotation, persistence checks, and rebuild criteria. The main risk is reinfection and hidden persistence. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of removal confidence, golden images, credential rotation, persistence checks, and rebuild criteria.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that severity is assigned.
- [ ] Confirm that containment authority is clear.
- [ ] Confirm that evidence is preserved.
- [ ] Confirm that communications are controlled.
- [ ] Confirm that actions are tracked.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- TheHive
- Velociraptor
- Wazuh
- CISA playbooks
- shared war-room log

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Respond, Recover. Map attacker behavior using MITRE ATT&CK language: Persistence, Defense Evasion. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is reinfection and hidden persistence.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 45: Recovery Validation and Return to Service

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects clean restore, monitoring, business validation, user communications, and post-recovery watch. The main risk is unsafe return to production. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of clean restore, monitoring, business validation, user communications, and post-recovery watch.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that restore was tested.
- [ ] Confirm that backup identity is protected.
- [ ] Confirm that immutability is enabled.
- [ ] Confirm that recovery order is documented.
- [ ] Confirm that business owner validates service.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- restic
- BorgBackup
- rclone
- immutable storage controls
- restore-test checklist

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Recover. Map attacker behavior using MITRE ATT&CK language: Impact. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is unsafe return to production.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 46: Crisis Communications and Legal Coordination

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects internal updates, customer notices, regulator needs, counsel, insurance, and public statements. The main risk is trust damage and compliance gaps. The goal is to

reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of internal updates, customer notices, regulator needs, counsel, insurance, and public statements.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that written authority exists.
- [ ] Confirm that owner is named.
- [ ] Confirm that decision rights are current.
- [ ] Confirm that exceptions expire.
- [ ] Confirm that legal and privacy contacts are known.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.

5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- NIST CSF 2.0 profiles
- CIS Controls v8.1
- ticketing system
- shared decision log
- risk register

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Respond, Recover. Map attacker behavior using MITRE ATT&CK language: Impact. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.

- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is trust damage and compliance gaps.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 47: Metrics, Lessons Learned, and Control Improvement

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects MTTD, MTTR, dwell time, action closure, control gaps, and improvement backlog. The main risk is repeat incidents and shallow learning. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.

- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of MTTD, MTTR, dwell time, action closure, control gaps, and improvement backlog.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that written authority exists.
- [ ] Confirm that owner is named.
- [ ] Confirm that decision rights are current.
- [ ] Confirm that exceptions expire.
- [ ] Confirm that legal and privacy contacts are known.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- NIST CSF 2.0 profiles
- CIS Controls v8.1

- ticketing system
- shared decision log
- risk register

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Recover, Govern. Map attacker behavior using MITRE ATT&CK language: All Tactics. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.

- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is repeat incidents and shallow learning.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 48: Tabletop Exercises and Simulation

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects scenario design, decision drills, escalation, injects, observers, and improvement actions. The main risk is unpracticed response. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of scenario design, decision drills, escalation, injects, observers, and improvement actions.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.

5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that written authority exists.
- [ ] Confirm that owner is named.
- [ ] Confirm that decision rights are current.
- [ ] Confirm that exceptions expire.
- [ ] Confirm that legal and privacy contacts are known.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- NIST CSF 2.0 profiles
- CIS Controls v8.1
- ticketing system
- shared decision log
- risk register

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results

- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Govern, Respond, Recover. Map attacker behavior using MITRE ATT&CK language: All Tactics. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is unpracticed response.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 49: Automation and SOAR on a Budget

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects ticket routing, enrichment, containment approvals, repeatable playbooks, and audit trails. The main risk is manual delay and inconsistent action. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of ticket routing, enrichment, containment approvals, repeatable playbooks, and audit trails.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that automation has approval gates.

- [ ] Confirm that actions are logged.
- [ ] Confirm that rollback exists.
- [ ] Confirm that playbooks are tested.
- [ ] Confirm that false-positive risk is controlled.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.
2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- Shuffle
- TheHive
- Wazuh active response with approvals
- n8n self-hosted
- webhook audit logs

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access

- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Detect, Respond. Map attacker behavior using MITRE ATT&CK language: All Tactics. Create one human-readable detection note that says: what behavior is suspicious, which log source proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is manual delay and inconsistent action.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Skill 50: Real-Time Cyber Defense Operating Model

Defensive Use Boundary

Use this skill only for systems, accounts, networks, applications, and data that you own or are formally authorized to inspect and defend. This fieldbook does not authorize intrusion, retaliation, credential theft, exploitation of third-party systems, or hack-back activity. "Full

access" means pre-approved defensive authority inside the protected environment: isolate, block, revoke, rotate, preserve, rebuild, restore, and communicate.

What This Skill Protects

This skill protects the combined inspection, detection, response, recovery, and improvement loop. The main risk is fragmented security work. The goal is to reduce uncertainty quickly, protect people and data, and give responders a clean path from first signal to verified recovery.

Inspection Inputs

- Current scope, asset owner, business owner, and emergency contact.
- Relevant logs, configuration exports, inventories, and previous exceptions.
- Known business constraints, maintenance windows, and systems that cannot be interrupted without approval.
- A named response lead with authority to request containment and recovery actions.

15-Minute Inspection Pass

1. Confirm the written scope, systems, owners, and allowed response actions.
2. Build a current view of the combined inspection, detection, response, recovery, and improvement loop.
3. Mark what is normal, what is unknown, and what is immediately unsafe.
4. Prioritize findings by exploitability, blast radius, and business criticality.
5. Create one remediation ticket per owned action with due date, evidence need, and rollback note.
6. Add or tune at least one detection that would reveal the same issue in the future.
7. Close only after owner validation and a retained proof artifact.

Deep Inspection Checklist

- [ ] Confirm that weekly inspection runs.
- [ ] Confirm that alerts map to playbooks.
- [ ] Confirm that response roles are trained.
- [ ] Confirm that metrics are reviewed.
- [ ] Confirm that improvements close.

Real-Time Response Playbook

1. Validate the signal with at least two evidence points before declaring a major incident.

2. Assign an incident commander and create a single live action log.
3. Contain inside owned systems: isolate affected hosts, disable suspected accounts, block malicious destinations, revoke exposed tokens, or pause risky integrations when authority exists.
4. Preserve evidence before destructive changes whenever safety and business continuity allow.
5. Eradicate root cause by removing persistence, fixing vulnerable paths, rotating secrets, and rebuilding systems that cannot be trusted.
6. Recover by restoring clean service, increasing monitoring, and getting explicit business-owner validation.
7. Convert lessons into controls, detections, documentation, and a dated retest.

Free and Open Tool Stack

- NIST CSF 2.0 profile
- CISA playbooks
- ATT&CK Navigator
- OpenCTI
- weekly response scorecard

Evidence to Preserve

- authorized scope and owner approval
- timestamped screenshots or exports where appropriate
- configuration snapshots or read-only query results
- alert IDs, ticket IDs, and linked business owners
- decision log with who approved each disruptive action

Escalation Triggers

- customer data, regulated data, payment data, or credentials may be exposed
- an attacker may have administrator, root, owner, or token-level access
- critical service availability is degraded or destructive behavior is possible
- legal, contractual, insurance, law-enforcement, or regulator notification may be required
- containment could disrupt business operations or safety-critical services

Detection and Control Pattern

Map this skill to NIST CSF functions: Govern, Identify, Protect, Detect, Respond, Recover. Map attacker behavior using MITRE ATT&CK language: All Tactics. Create one human-readable detection note that says: what behavior is suspicious, which log source

proves it, which false positives are expected, and which responder action is allowed.

Deliverables

- Inspection summary with status: green, amber, red, or unknown.
- Remediation tickets with owner, due date, evidence required, and rollback note.
- Response action log if an active incident exists.
- Updated detection, playbook, baseline, or recovery note.

Metrics

- Time to verify signal.
- Time to containment decision.
- Percent of scoped assets with usable evidence.
- Number of expired exceptions removed.
- Number of control improvements closed after retest.

Practice Drill

- Run a 30-minute tabletop where the first symptom is fragmented security work.
- Force the team to make one containment decision with incomplete information.
- Record which data, tool, or permission was missing, then add it to the improvement backlog.

Free and Open Defensive Tool Stack

Use tools only in environments where you have permission. Prefer read-only collection during inspection, then documented and approved change actions during response.

Governance Stack

- NIST CSF 2.0 profiles
- CIS Controls v8.1
- ticketing system
- shared decision log
- risk register

Asset Stack

- osquery
- Nmap in authorized ranges

- Amass for owned domains
- Snipe-IT
- Open-AudIT

Identity Stack

- IdP audit exports
- Entra ID or Google Workspace logs
- BloodHound Community Edition in authorized AD
- KeePassXC
- OpenLDAP tooling

Endpoint Stack

- osquery
- Wazuh
- Velociraptor
- Lynis
- Windows Event Forwarding

Vulnerability Stack

- OpenVAS/GVM
- CISA KEV catalog
- Trivy
- Grype
- OWASP Dependency-Check

Network Stack

- Suricata
- Zeek
- Wireshark
- Arkime
- ntopng

Cloud Stack

- Prowler

- ScoutSuite
- Cloud Custodian
- cloud provider audit logs
- Steampipe

Saas Stack

- tenant audit logs
- OAuth app reports
- admin center exports
- CASB-free reports where available
- MISP for indicators

Email Stack

- DMARC aggregate reports
- mailbox audit logs
- GoPhish for authorized training
- MXToolbox free checks
- TheHive case tracking

Appsec Stack

- OWASP ZAP in authorized tests
- Semgrep Community
- OWASP ASVS
- Trivy
- Syft

Detection Stack

- Wazuh
- Sigma
- Elastic or OpenSearch
- YARA
- ATT&CK Navigator

Intel Stack

- OpenCTI
- MISP
- CISA advisories
- ATT&CK
- abuse.ch community feeds

Recovery Stack

- restic
- BorgBackup
- rclone
- immutable storage controls
- restore-test checklist

Incident Stack

- TheHive
- Velociraptor
- Wazuh
- CISA playbooks
- shared war-room log

Data Stack

- database audit logs
- DLP exports where available
- Apache Ranger
- OpenSearch dashboards
- rclone inventory

Container Stack

- Trivy
- kube-bench
- Falco
- Syft
- Kyverno policies

Secrets Stack

- Gitleaks
- TruffleHog OSS
- SOPS
- age
- Vault Community Edition

Baseline Stack

- CIS Benchmarks
- Microsoft Security Baselines
- Lynis
- OpenSCAP
- Ansible

Forensics Stack

- Velociraptor
- Autopsy
- Plaso/log2timeline
- Volatility
- hashdeep

Automation Stack

- Shuffle
- TheHive
- Wazuh active response with approvals
- n8n self-hosted
- webhook audit logs

Operations Stack

- NIST CSF 2.0 profile
- CISA playbooks
- ATT&CK Navigator
- OpenCTI
- weekly response scorecard

Incident Quickcards

First Five Minutes

- Start a single incident log with time zone, owner, severity, and hypothesis.
- Confirm authority before any disruptive action.
- Preserve the triggering alert, raw event, and first human interpretation.
- Name an incident commander, technical lead, communications lead, and evidence owner.
- Decide what can be safely contained now and what needs business approval.

Account Takeover

- Disable or suspend the suspected account if approved.
- Revoke sessions, refresh tokens, app passwords, OAuth grants, and risky device trust.
- Reset credentials from a clean admin path.
- Review mailbox rules, forwarding, delegated access, recent downloads, and privileged changes.
- Re-enable only after MFA, device posture, and owner validation.

Ransomware Signal

- Isolate affected endpoints or segments when approved.
- Protect backups and identity systems first.
- Preserve ransom notes, process trees, file samples, EDR alerts, and network indicators.
- Stop scheduled tasks, remote admin spread, and suspicious credential use.
- Restore only from clean backups and monitor for reinfection.

Exposed Secret

- Identify the secret type, owner, privileges, and systems that accepted it.
- Revoke or rotate the secret from a trusted path.
- Search logs for use before and after exposure.
- Check code, CI, artifacts, chat, tickets, and images for copies.
- Add a pre-commit, CI, or repository scanning control before closure.

Public Vulnerability

- Check whether the vulnerability is in CISA KEV or actively exploited by credible sources.

- Identify exposed assets and business owners.
- Apply patch, mitigation, isolation, or compensating control.
- Hunt for exploitation indicators from the earliest plausible exposure date.
- Retain evidence of fix and retest.

Source Recycling Map

The book uses official and primary sources as orientation references, then converts them into original defensive inspection modules. It does not reproduce source text. Teams should check the live source before production use because cybersecurity guidance, tooling, and threat conditions change.

NIST Cybersecurity Framework 2.0

- Use: Govern, Identify, Protect, Detect, Respond, and Recover outcomes for the book's operating model.
- URL: https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20

NIST SP 800-61 Rev. 3 Incident Response Recommendations and Considerations

- Use: Modern incident response structure, continuous readiness, and response improvement framing.
- URL: https://csrc.nist.gov/pubs/sp/800/61/r3/final

CISA Federal Government Cybersecurity Incident and Vulnerability Response Playbooks

- Use: Standardized identify, coordinate, remediate, recover, and track response workflow.
- URL: https://www.cisa.gov/resources-tools/resources/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks

CISA Known Exploited Vulnerabilities Catalog

- Use: Vulnerability triage based on known exploitation evidence.
- URL: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

MITRE ATT&CK Enterprise Matrix

- Use: Common adversary behavior language for detection and response coverage.
- URL: https://attack.mitre.org/matrices/

OWASP Top 10

- Use: Application risk categories for web inspection and secure development review.
- URL: https://owasp.org/www-project-top-ten/

OWASP Application Security Verification Standard

- Use: Application security verification requirements and test planning.
- URL: https://owasp.org/www-project-application-security-verification-standard/

CIS Critical Security Controls v8.1

- Use: Prioritized safeguards for enterprise cyber hygiene and control maturity.
- URL: https://www.cisecurity.org/controls/v8-1

Microsoft Security Baselines

- Use: Security configuration baseline concept for Microsoft estates.
- URL: https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines

osquery Documentation

- Use: Endpoint inspection and operating system instrumentation concepts.
- URL: https://osquery.readthedocs.io/

Sigma Specification

- Use: Portable detection-rule structure for SIEM and log analytics.
- URL: https://sigmahq.io/sigma-specification/

Suricata

- Use: Open-source network analysis and threat detection tooling.
- URL: https://suricata.io/

Wazuh Documentation

- Use: Free and open-source SIEM/XDR operating model reference.
- URL: https://documentation.wazuh.com/current/getting-started/index.html

Velociraptor

- Use: Open-source endpoint monitoring, DFIR, and incident response capability reference.

- URL: https://www.rapid7.com/products/velociraptor/

OpenCTI Documentation

- Use: Open-source cyber threat intelligence knowledge management reference.
- URL: https://docs.opencti.io/latest/