Cybersecurity Inspection & Real-Time Response Field Book

50 defensive skills for authorized inspection, hardening, monitoring, and incident response

Free and open-source first. Built for practical, real-time security operations.

Prepared for desktop use as a field-ready PDF

Generated: 2026-07-11 00:56

Use this book only for systems you own or are explicitly authorized to assess. The content is defensive by design: it focuses on visibility, prevention, containment, recovery, evidence, and governance.

Operating Doctrine

A strong cybersecurity inspection program does not begin with tools. It begins with authorization, asset knowledge, clear ownership, current evidence, and disciplined response decisions. This handbook gives you fifty repeatable skills for building and operating that program without depending on expensive platforms.

The response model is simple: prepare, detect, triage, contain, eradicate, recover, and improve. During a real event, the team should protect evidence, reduce attacker freedom, preserve business-critical services, and communicate facts without speculation.

This is not a promise that any organization can stop every attack. It is a practical operating system for increasing the chance that attacks are noticed early, contained quickly, investigated cleanly, and converted into stronger controls.

Phase	Primary question	Useful output
Prepare	Do we know the assets, owners, controls, and authority?	Scope, inventories, playbooks, contact tree
Detect	What signal changed and why does it matter?	Alert, log evidence, context, severity hypothesis
Triage	Is this benign, suspicious, or confirmed compromise?	Decision, initial timeline, next action
Contain	How do we reduce immediate risk with acceptable impact?	Isolation, account action, block, restriction
Eradicate	What access or weakness must be removed?	Patch, rebuild, rotation, persistence removal
Recover	How do we return safely and verify clean operation?	Restore, validation, monitoring, acceptance
Improve	What must change so this is less likely or less harmful?	Detection, control, training, architecture task

Free and Open-Source First Stack

Need	Tools to consider	Inspection value
SIEM and endpoint visibility	Wazuh, Elastic/OpenSearch, osquery	Collects alerts, endpoint data, and searchable evidence.
Network visibility	Zeek, Suricata, Arkime, Wireshark	Shows traffic behavior, DNS, flow, and packet-level clues.
Incident case management	TheHive, DFIR-IRIS, Timesketch	Keeps timelines, cases, actions, and evidence organized.
Vulnerability management	Greenbone CE, Trivy, Grype, OSV-Scanner	Finds infrastructure, container, and dependency risk.
Cloud posture	Prowler, ScoutSuite, Steampipe, CloudQuery	Checks cloud configuration, IAM, exposure, and drift.
Forensic triage	Velociraptor, GRR, Autopsy, YARA	Collects artifacts and supports endpoint investigations.
Automation	Shuffle, Cortex, StackStorm, Node-RED	Automates enrichment and repeatable response actions.
Secrets and code	Gitleaks, TruffleHog, Semgrep, Dependency-Track	Finds secrets, code issues, and supply-chain risk.

Contents

01	Authorization, Scope, and Rules of Engagement
02	Asset Inventory and Ownership
03	Defensive Network Discovery
04	External Exposure and Attack Surface Review
05	Identity Directory Inspection
06	MFA and Conditional Access Review
07	Privileged Access Management
08	Endpoint Security Posture
09	Patch and Vulnerability Management
10	Secure Configuration Baselines
11	Cloud Account and Project Inspection
12	SaaS Security Inspection
13	Email and Domain Protection
14	Web Application Security Inspection
15	API Security Inspection
16	Data Classification and Flow Mapping
17	Backup and Restore Inspection
18	Logging Coverage and Retention
19	SIEM Triage Operations
20	Endpoint Detection and Response Operations
21	Network Detection and Traffic Analysis
22	Threat Intelligence Intake
23	Detection Engineering
24	Incident Classification and Severity
25	Initial Triage and First 15 Minutes
26	Containment Strategy
27	Eradication and Root Cause Removal
28	Recovery and Return to Service
29	Ransomware Readiness and Response
30	Phishing Response
31	Business Email Compromise Response
32	Credential Theft Response
33	Web Intrusion Response
34	Cloud Compromise Response

35	Insider Risk Inspection
36	Third-Party and Supply Chain Risk
37	Secure Remote Access
38	Wireless Security Inspection
39	Mobile Device Security
40	IoT and Operational Technology Inspection
41	Vulnerability Remediation Governance
42	Security Metrics and Executive Signals
43	Evidence Handling and Legal Readiness
44	Crisis Communications
45	Tabletop Exercises and Simulations
46	Automation and SOAR Playbooks
47	AI-Assisted Security Operations
48	Continuous Control Monitoring
49	Purple Team and Validation Safety
50	Secure Software Delivery Inspection
51	Database and Storage Inspection
52	DNS, Certificates, and Trust Services
53	Network Segmentation and Zero Trust Checks
54	Security Awareness and Human Reporting
55	Physical Security and Device Handling
56	Real-Time Response Room Operations
57	Post-Incident Review and Improvement
58	90-Day Cyber Inspection Maturity Roadmap

Skill 01: Authorization, Scope, and Rules of Engagement

Mission: Make every inspection lawful, controlled, and useful before any technical work begins.

Inspection Checklist

- Confirm written authorization, business owner, technical owner, date window, and emergency contacts.
- Define in-scope assets, excluded assets, approved testing intensity, data handling limits, and stop conditions.
- Map the inspection to business services so findings describe operational risk, not only technical weakness.
- Record accepted assumptions, known maintenance windows, third-party dependencies, and regulatory constraints.
- Create a single evidence folder with immutable naming, chain-of-custody notes, and access restrictions.

Real-Time Signals

- A scan, alert, or response activity touches an asset not listed in scope.
- A business owner asks for testing to stop or a critical service starts degrading.
- Unexpected sensitive data appears in logs, screenshots, packet captures, or exported reports.
- A third party reports impact from the authorized inspection window.

Response Play

- Pause the specific activity that created uncertainty and preserve the current notes and tool output.
- Notify the named owner and incident lead with time, asset, activity, and observed impact.
- Reduce inspection intensity or narrow the asset set until the scope question is resolved.
- Document the decision, approver, and any compensating controls before continuing.
- After the inspection, add scope lessons to the next rules-of-engagement template.

Free/open tooling: ProjectLibre, OnlyOffice, Cryptomator, Git, OpenTimestamps.

Evidence to save: Signed authorization, asset list, contact tree, inspection window, exception log, and final scope statement.

Quality bar: No inspection activity occurs outside documented authorization, and every exception has an owner-approved decision.

Skill 02: Asset Inventory and Ownership

Mission: Build a living map of systems, people, services, and data before judging security posture.

Inspection Checklist

- Collect inventories from cloud accounts, identity providers, endpoint tools, network devices, CMDB exports, and finance records.
- Tag each asset with owner, environment, business service, data class, exposure, criticality, and last-seen time.
- Compare authoritative inventories against observed assets from passive network logs and endpoint telemetry.
- Identify unknown, duplicate, stale, unmanaged, and ownerless assets for cleanup or enrollment.
- Prioritize systems that are internet-facing, privileged, regulated, revenue-critical, or hard to rebuild.

Real-Time Signals

- A new host, cloud resource, service account, or public endpoint appears without owner metadata.
- An asset stops reporting telemetry or changes network location unexpectedly.
- Critical systems show missing backups, missing EDR, or no named technical owner.
- Cloud resources are created outside approved accounts, regions, projects, or naming patterns.

Response Play

- Quarantine or limit exposure for unknown assets until ownership and purpose are confirmed.
- Assign a temporary owner and ticket the permanent owner, lifecycle state, and required controls.
- Enroll the asset into logging, endpoint protection, vulnerability management, and backup coverage.
- Review recent activity for signs of misuse if the asset was exposed or unmanaged.
- Update inventory rules so similar future assets are automatically tagged and routed.

Free/open tooling: Snipe-IT, Ralph, osquery, Nmap, AWS Config, CloudQuery.

Evidence to save: Inventory export, unknown-asset list, owner assignments, telemetry coverage report, and cleanup tickets.

Quality bar: At least 98 percent of active assets have an owner, criticality, exposure status, and current telemetry timestamp.

Skill 03: Defensive Network Discovery

Mission: Understand live network services without disrupting production or drifting into unauthorized testing.

Inspection Checklist

- Start from approved CIDR ranges, VLANs, VPN pools, cloud VPCs, and known external IP addresses.
- Use low-intensity discovery first, then validate high-value services with targeted checks during approved windows.
- Identify externally reachable management ports, forgotten services, unexpected protocols, and unencrypted administrative paths.
- Cross-check observed hosts with DHCP, DNS, firewall, EDR, and asset inventory records.
- Document network segments that contain sensitive systems but lack clear ownership or monitoring.

Real-Time Signals

- A new listening service appears on a high-value server or internet-facing address.
- An internal host starts exposing administrative protocols beyond its expected segment.
- Discovery results change sharply after business hours or after a deployment.
- An unmanaged device appears in a restricted subnet or VPN address range.

Response Play

- Validate whether the service is approved, patched, encrypted, and restricted to expected sources.
- Block or restrict accidental exposure through firewall, security group, or access-list changes.
- Open an owner ticket for service justification, hardening, and monitoring coverage.
- Review relevant logs for access during the exposure window.
- Add the service pattern to continuous discovery and drift detection.

Free/open tooling: Nmap, RustScan, Zeek, NetBox, Arkime, Wireshark.

Evidence to save: Approved ranges, discovery output, service-owner map, change tickets, and before-after exposure snapshots.

Quality bar: Every open service on critical networks has a documented owner, purpose, restriction, and monitoring source.

Skill 04: External Exposure and Attack Surface Review

Mission: Find what the internet can reach and reduce avoidable exposure before adversaries benefit from it.

Inspection Checklist

- Inventory public DNS records, certificates, IP ranges, cloud load balancers, SaaS portals, and partner-hosted systems.
- Look for expired certificates, dangling DNS, forgotten staging apps, default pages, exposed admin panels, and weak redirects.
- Check whether public services require TLS, modern ciphers, secure headers, WAF rules, and rate limits where appropriate.
- Confirm that sensitive endpoints are protected by identity-aware access, VPN, allow lists, or private connectivity.
- Tie each exposed service to an owner, deployment source, support runbook, and vulnerability management workflow.

Real-Time Signals

- A new domain, certificate, bucket, load balancer, or public IP appears without a change record.
- A sensitive service becomes reachable from the internet or outside expected countries.
- Certificate transparency logs show unexpected names under the organization domain.
- Security headers, TLS posture, or WAF behavior changes after a release.

Response Play

- Confirm the service owner and business need for public exposure.
- Restrict access, remove stale records, rotate exposed secrets, or take down forgotten services.
- Review web, proxy, DNS, and identity logs for suspicious access during the exposure window.
- Add ownership, monitoring, and expiration metadata to the public asset inventory.
- Run a post-remediation verification from an external network.

Free/open tooling: OWASP Amass, crt.sh, Security Headers, Mozilla Observatory, Shodan CLI, Censys CLI.

Evidence to save: Public asset inventory, DNS and certificate findings, owner approvals, restriction changes, and validation screenshots.

Quality bar: All public assets are owner-tagged, monitored, patched, and justified, with stale exposure closed within SLA.

Skill 05: Identity Directory Inspection

Mission: Inspect identities as the control plane of modern security.

Inspection Checklist

- Review users, groups, roles, applications, service principals, break-glass accounts, and guest identities.
- Find stale accounts, shared accounts, weak recovery paths, excessive group nesting, and users without managers.
- Compare privileged groups with HR records, ticket approvals, and actual job duties.
- Validate joiner, mover, leaver, contractor, and emergency access procedures.
- Confirm that identity events are logged into the detection platform with enough detail for investigation.

Real-Time Signals

- A privileged group changes membership outside the approved workflow.
- A dormant identity authenticates, registers MFA, or creates tokens.
- A guest account gains access to sensitive groups, apps, or files.
- Authentication failures spike against executives, admins, or service accounts.

Response Play

- Disable or step-up-risky identities while preserving sign-in, audit, and change logs.
- Verify the user, manager, ticket, device, and business justification for the access.
- Rotate credentials and revoke sessions or tokens when compromise cannot be ruled out.
- Remove unnecessary group memberships and document the least-privilege state.
- Tune alerts for group changes, inactive reactivation, impossible travel, and token abuse indicators.

Free/open tooling: BloodHound Community Edition, Azure AD Exporter, LDAP queries, Wazuh, Sigma rules.

Evidence to save: Identity export, privileged membership review, stale-account list, access tickets, and remediation approvals.

Quality bar: Privileged identities are justified, MFA-protected, logged, and reviewed at least monthly.

Skill 06: MFA and Conditional Access Review

Mission: Make authentication resilient against password theft, phishing, and risky access patterns.

Inspection Checklist

- Measure MFA coverage by user type, admin role, application, geography, and device trust state.
- Find exclusions, legacy authentication, weak recovery methods, SMS reliance, and unmanaged device bypasses.
- Review conditional access policies for privileged roles, sensitive apps, high-risk sign-ins, and impossible travel.
- Check whether break-glass accounts are protected, monitored, and tested without routine use.
- Validate user enrollment experience and support paths so security controls do not collapse under pressure.

Real-Time Signals

- MFA fatigue, repeated push prompts, or authentication from a new country after password success.
- Legacy protocols authenticate against accounts that should require modern MFA.
- An admin account signs in from an unmanaged device or unusual network.
- A conditional access policy changes or is disabled without approval.

Response Play

- Revoke sessions, require password reset, and force phishing-resistant MFA registration for affected identities.
- Block legacy protocols and apply emergency conditional access rules to high-risk groups.
- Review sign-in logs, device state, token issuance, and application consent events.
- Notify users with clear instructions and verify helpdesk identity-proofing steps.
- Convert repeated incidents into policy improvements and targeted user training.

Free/open tooling: Microsoft Entra logs, Google Workspace reports, Wazuh, Sigma, Aegis Authenticator.

Evidence to save: MFA coverage report, policy export, exception list, sign-in evidence, and emergency change record.

Quality bar: All privileged and sensitive access requires phishing-resistant or strong MFA with monitored exceptions.

Skill 07: Privileged Access Management

Mission: Reduce standing privilege and make every powerful action visible, temporary, and accountable.

Inspection Checklist

- Inventory local admins, domain admins, cloud admins, database admins, SaaS admins, and CI/CD secret owners.
- Identify shared privileged accounts, permanent assignments, weak approval trails, and unused admin rights.
- Review privilege escalation paths through groups, service accounts, delegated roles, and automation platforms.
- Confirm admin workstations, hardened browsers, session logging, and just-in-time elevation where available.
- Test emergency access procedures without exposing secrets or bypassing audit requirements.

Real-Time Signals

- A new admin role appears, especially outside business hours or without a ticket.
- Privileged credentials are used from a normal workstation, unknown device, or unexpected country.
- A service account receives interactive login activity.
- Audit logging for privileged activity is disabled, reduced, or stops forwarding.

Response Play

- Remove or suspend unexpected privilege and preserve audit trails before deeper changes.
- Rotate affected credentials and revoke active privileged sessions.
- Review administrative actions during the suspicious window for persistence, data access, and policy changes.
- Move recurring admin tasks into approved just-in-time or workflow-based access.
- Add detections for privilege creation, role assignment, audit changes, and service account misuse.

Free/open tooling: Keycloak, FreeIPA, OpenBao, HashiCorp Vault Community, BloodHound CE, Wazuh.

Evidence to save: Privileged access inventory, approval trail, role assignment logs, rotation record, and session evidence.

Quality bar: Standing privileged access is minimized, reviewed frequently, and tied to named individuals or approved automation.

Skill 08: Endpoint Security Posture

Mission: Keep laptops, servers, and workstations visible, hardened, and ready for investigation.

Inspection Checklist

- Measure endpoint coverage for EDR, disk encryption, firewall, patching, device control, and logging.
- Review high-risk endpoints: executives, admins, developers, finance, remote users, and shared workstations.
- Check baseline configuration for local admins, scripting controls, macro handling, browser hardening, and USB policy.
- Validate that endpoint telemetry includes process, network, file, login, persistence, and alert events.
- Find stale agents, duplicated hostnames, unmanaged servers, and endpoints missing recent check-ins.

Real-Time Signals

- Endpoint protection stops, downgrades, or loses contact with the management plane.
- A workstation creates unusual child processes from office apps, browsers, archives, or scripting engines.
- New persistence, scheduled tasks, services, or startup items appear without deployment context.
- Admin tools run on a non-admin workstation or from unusual directories.

Response Play

- Isolate the endpoint through approved tooling or network controls if compromise is plausible.
- Preserve volatile details, alert timeline, user context, and relevant files before wiping or rebuilding.
- Collect triage data with a standard script or forensic collector appropriate to the environment.
- Reset credentials used on the host if token or credential theft is possible.
- Reimage or remediate according to severity, then verify control coverage before returning the device.

Free/open tooling: Wazuh, osquery, Velociraptor, GRR Rapid Response, ClamAV, YARA.

Evidence to save: Coverage report, agent health list, endpoint timeline, isolation record, triage package, and rebuild notes.

Quality bar: Critical endpoints maintain healthy telemetry and can be isolated, triaged, and restored within the response SLA.

Skill 09: Patch and Vulnerability Management

Mission: Turn vulnerability data into risk-ranked remediation that actually lands.

Inspection Checklist

- Collect vulnerability data from authenticated scans, cloud posture tools, container scans, dependency scans, and EDR.
- Rank findings by exploitability, exposure, business criticality, compensating controls, and active threat reporting.
- Separate true remediation from accepted risk, false positives, compensating controls, and planned decommissioning.
- Check patch coverage for operating systems, browsers, VPN, firewalls, hypervisors, databases, and developer tooling.
- Measure remediation cycle time by severity, asset owner, environment, and recurring root cause.

Real-Time Signals

- A critical vulnerability affects an internet-facing or privileged system.
- A vendor publishes active exploitation details for software used by the organization.
- A vulnerability remains open beyond SLA without risk acceptance.
- A patch causes operational failures or repeat rollback on a critical service.

Response Play

- Confirm exposure, affected versions, available patches, mitigations, and service owner.
- Apply emergency mitigation where patching cannot happen immediately.
- Search logs for indicators of exploitation without relying on a single indicator source.
- Patch or decommission affected systems, then perform targeted validation.
- Run a retrospective on delayed patch paths and update the remediation workflow.

Free/open tooling: Greenbone Community Edition, OpenVAS, Trivy, Grype, OSV-Scanner, Wazuh SCA.

Evidence to save: Scan reports, risk ranking, owner tickets, mitigation proof, patch validation, and SLA dashboard.

Quality bar: Critical exposed vulnerabilities are mitigated or remediated within defined emergency SLA.

Skill 10: Secure Configuration Baselines

Mission: Make secure defaults measurable across operating systems, cloud services, databases, and network devices.

Inspection Checklist

- Select baseline sources such as CIS Benchmarks, vendor hardening guides, and internal architecture standards.
- Compare production configurations against approved baselines with exceptions tracked by owner and expiration.
- Prioritize logging, authentication, encryption, network restriction, secret handling, and administrative access controls.
- Review drift after deployments, image updates, infrastructure changes, and emergency fixes.
- Turn repeated misconfiguration into templates, policy-as-code, or golden images.

Real-Time Signals

- A baseline control changes from pass to fail after a release or manual change.
- Encryption, audit logging, MFA, or network restriction is disabled on a sensitive asset.
- A new system is built from an old image or unapproved template.
- Exceptions accumulate without owners, end dates, or compensating controls.

Response Play

- Determine whether the drift is intentional, accidental, or suspicious.
- Restore the approved baseline through configuration management or emergency change.
- Preserve change logs and administrator actions for sensitive control failures.
- Open root-cause work for image, pipeline, or policy gaps that allowed recurrence.
- Update baseline tests so the control fails early in development or deployment.

Free/open tooling: OpenSCAP, Lynis, InSpec, Ansible, Prowler, ScoutSuite.

Evidence to save: Baseline selection, scan output, exception register, remediation commits, and drift trend.

Quality bar: High-risk baseline failures are detected quickly and exceptions expire unless re-approved.

Skill 11: Cloud Account and Project Inspection

Mission: Inspect cloud environments as dynamic control planes where identity, network, data, and automation meet.

Inspection Checklist

- Inventory accounts, subscriptions, projects, regions, VPCs, public services, IAM roles, and security tooling.
- Review root accounts, billing access, cloud admin roles, service principals, key rotation, and cross-account trust.
- Check storage exposure, logging coverage, encryption defaults, network boundaries, and workload identity patterns.
- Validate security services such as activity logs, guardrails, configuration recorders, threat detection, and backup.
- Look for unmanaged regions, unused access keys, default networks, public databases, and broad wildcard permissions.

Real-Time Signals

- CloudTrail, audit logs, or equivalent control-plane logging is disabled or stops delivering.
- A new public IP, storage bucket, database, or admin role appears without change context.
- Access keys are created for privileged users or used from unexpected networks.
- Security group, firewall, or route changes expose sensitive workloads.

Response Play

- Preserve control-plane logs and configuration snapshots before changing suspect resources.
- Restrict public exposure and revoke or rotate risky credentials.
- Review role assumptions, API actions, network flow logs, and data access for the affected window.
- Re-apply baseline guardrails and confirm security services are healthy.
- Turn lessons into policy-as-code and automated drift alerts.

Free/open tooling: Prowler, ScoutSuite, CloudQuery, Steampipe, Cloud Custodian, OpenTofu.

Evidence to save: Cloud inventory, IAM review, config snapshots, public exposure list, log health proof, and remediation records.

Quality bar: Every cloud account has active logging, clear ownership, least-privilege access, and monitored public exposure.

Skill 12: SaaS Security Inspection

Mission: Bring SaaS applications into the same inspection discipline as infrastructure.

Inspection Checklist

- Inventory SaaS apps, owners, data classes, SSO status, guest access, admin roles, integrations, and retention settings.
- Review external sharing, public links, OAuth grants, API tokens, marketplace apps, and inactive users.
- Check whether audit logs are enabled, retained, exported, and searchable during incidents.
- Validate backup or export options for business-critical SaaS data.
- Map sensitive SaaS workflows such as finance approval, customer data access, legal files, and HR records.

Real-Time Signals

- A user grants a high-permission OAuth app or creates a long-lived API token.
- Public file links or external sharing spike for sensitive repositories.
- An admin role changes or a dormant account accesses a SaaS application.
- Audit log export fails, retention drops, or search access disappears.

Response Play

- Revoke suspicious grants and tokens, then preserve the audit log and affected object list.
- Suspend or step-up the identity if account compromise is possible.
- Identify files, records, or workflows touched during the suspicious session.
- Notify the app owner and legal/privacy stakeholders when sensitive data may be involved.
- Tighten sharing defaults, app consent, and admin review cadences.

Free/open tooling: SaaS app audit exports, GAM, rclone, CyberDrain scripts, Wazuh, Sigma.

Evidence to save: SaaS inventory, OAuth grant list, sharing review, audit exports, response tickets, and owner approvals.

Quality bar: Critical SaaS apps use SSO, MFA, audit export, named ownership, and controlled third-party integrations.

Skill 13: Email and Domain Protection

Mission: Reduce phishing, spoofing, mailbox abuse, and business email compromise risk.

Inspection Checklist

- Review SPF, DKIM, DMARC, MX records, inbound filtering, outbound controls, and lookalike domain monitoring.
- Measure mailbox audit logging, forwarding rules, delegated access, application passwords, and external sender labels.
- Inspect executive, finance, HR, and support mailboxes for stronger controls and response playbooks.
- Check phishing reporting flow from user button to triage queue to feedback loop.
- Validate retention and search capability for headers, message trace, attachments, and mailbox actions.

Real-Time Signals

- New inbox rules forward or hide messages, especially with finance or security keywords.
- A mailbox logs in from an unusual location and sends external messages rapidly.
- DMARC reports show unauthorized sources sending as the domain.
- Users report similar messages, credential pages, or invoice changes in a short window.

Response Play

- Preserve headers, message trace, mailbox audit logs, and reported samples.
- Disable malicious forwarding, revoke sessions, reset credentials, and review OAuth grants.
- Search and purge malicious messages through approved mail administration workflows.
- Notify affected users and verify financial transaction changes through out-of-band channels.
- Tune filtering, domain authentication, and user reporting feedback after the incident.

Free/open tooling: DMARCian reports, parsedmarc, GoPhish for training, MailHeader analyzers, Sigma, Wazuh.

Evidence to save: DNS records, DMARC aggregate data, mailbox audit logs, sample messages, purge record, and user notifications.

Quality bar: DMARC is enforced, mailbox audit is searchable, and reported phishing reaches triage within minutes.

Skill 14: Web Application Security Inspection

Mission: Inspect web applications for exposure, secure defaults, data handling, and operational readiness.

Inspection Checklist

- Confirm ownership, environments, authentication model, sensitive data paths, deployment pipeline, and support runbook.
- Review TLS, headers, session settings, rate limits, authentication flows, authorization boundaries, and error handling.
- Run safe authenticated checks in staging or approved windows using conservative scan profiles.
- Inspect dependencies, secrets, debug routes, admin functions, file uploads, and logging coverage.
- Map findings to OWASP categories and business impact instead of only technical labels.

Real-Time Signals

- A release exposes debug output, admin routes, stack traces, or a staging environment.
- Authentication or authorization errors increase after deployment.
- Web logs show unusual request patterns against sensitive endpoints.
- A dependency or framework advisory affects an internet-facing application.

Response Play

- Roll back, disable the vulnerable feature, or apply a targeted mitigation based on severity.
- Preserve web, application, WAF, identity, and deployment logs for the affected window.
- Check for data access, account changes, file uploads, and suspicious admin activity.
- Patch code or configuration, redeploy through normal controls, and verify with a focused retest.
- Add regression tests or security checks to the pipeline.

Free/open tooling: OWASP ZAP, Semgrep, Trivy, Gitleaks, Mozilla Observatory, Security Headers.

Evidence to save: Application inventory, scan reports, dependency output, logs, fix commits, and retest proof.

Quality bar: Critical web findings are mitigated quickly and recurring classes are blocked in CI/CD.

Skill 15: API Security Inspection

Mission: Protect APIs as machine-facing business interfaces with explicit contracts and abuse controls.

Inspection Checklist

- Inventory public, partner, internal, and admin APIs with owners, consumers, authentication, and data classification.
- Review schema validation, authorization checks, rate limiting, object-level access, token scopes, and error responses.
- Validate token lifetime, rotation, storage, revocation, and audience restrictions.
- Check logs for caller identity, endpoint, decision, latency, status code, and trace correlation.
- Inspect API gateways, service meshes, and serverless functions for drift from approved policies.

Real-Time Signals

- A caller exceeds normal request volume, error rates, or sensitive endpoint access.
- Tokens are used from unexpected IP ranges, regions, or automation contexts.
- New endpoints appear without schema, ownership, or gateway policy.
- Repeated authorization failures target the same object type or account set.

Response Play

- Throttle, block, or revoke suspicious callers while preserving gateway and application logs.
- Identify affected objects, tenants, accounts, or records using trace IDs and data access logs.
- Patch authorization, validation, or gateway policy gaps through controlled deployment.
- Rotate secrets and tokens where leakage or abuse is plausible.
- Add contract tests and anomaly alerts for the specific failure mode.

Free/open tooling: OWASP ZAP, Schemathesis, 42Crunch community tools, OpenAPI validators, Kong OSS.

Evidence to save: API inventory, OpenAPI specs, gateway policies, token review, logs, rate-limit events, and fix validation.

Quality bar: Sensitive APIs enforce least-privilege tokens, object authorization, schema validation, and useful audit logs.

Skill 16: Data Classification and Flow Mapping

Mission: Know what data exists, where it moves, and how quickly exposure can be contained.

Inspection Checklist

- Define practical data classes such as public, internal, confidential, regulated, credentials, and customer secrets.
- Map data stores, SaaS repositories, backups, exports, logs, analytics tools, and third-party transfers.
- Identify high-risk flows: production data in development, public links, unmanaged exports, and over-retained logs.
- Review encryption, access controls, retention, deletion, masking, and DLP coverage by data class.
- Tie data owners to business processes so incident decisions have accountable leadership.

Real-Time Signals

- Sensitive data appears in logs, tickets, chat, analytics, test data, or public storage.
- Large exports occur outside normal roles, hours, or destinations.
- A new integration receives regulated or confidential data without review.
- Data retention exceeds legal, contractual, or business requirements.

Response Play

- Restrict access to exposed locations and preserve audit logs before deletion.
- Identify data subjects, volume, fields, recipients, and duration of exposure.
- Notify privacy, legal, business owner, and security leadership according to severity.
- Remove, rotate, or reissue exposed secrets and credentials immediately.
- Update controls so sensitive data cannot repeat the same path silently.

Free/open tooling: OpenDLP, TruffleHog, Gitleaks, S3Scanner, OpenMetadata, Amundsen.

Evidence to save: Data map, classification rules, access review, export logs, exposure timeline, and remediation proof.

Quality bar: High-risk data stores have owners, access review, retention rules, encryption, and incident-ready audit trails.

Skill 17: Backup and Restore Inspection

Mission: Prove the organization can recover cleanly after ransomware, deletion, corruption, or cloud mistakes.

Inspection Checklist

- Inventory backups by system, owner, schedule, retention, location, encryption, immutability, and restore priority.
- Verify that identity systems, critical SaaS data, databases, configuration repositories, and secrets stores are included.
- Test restore processes regularly, including partial restore, full service rebuild, and isolated recovery.
- Check backup access controls so attackers cannot delete or encrypt backups using normal admin paths.
- Measure recovery time objective and recovery point objective against business expectations.

Real-Time Signals

- Backup jobs fail, run unusually fast, change destination, or stop reporting.
- Retention, immutability, or encryption settings are altered outside change control.
- Large deletion or encryption events occur on production systems.
- Restore tests fail or take longer than the business impact tolerance.

Response Play

- Protect backup systems first: isolate management interfaces and freeze retention changes.
- Preserve evidence from affected systems before broad restore activity where feasible.
- Select a clean restore point based on compromise timeline and integrity checks.
- Restore into an isolated environment, validate, then reconnect through controlled steps.
- Update backup design based on the gap that slowed or endangered recovery.

Free/open tooling: Restic, BorgBackup, Duplicati, UrBackup, rclone, MinIO object lock.

Evidence to save: Backup inventory, restore test results, access review, retention proof, recovery timeline, and validation checklist.

Quality bar: Critical services have tested, protected, and monitored backups that meet agreed recovery objectives.

Skill 18: Logging Coverage and Retention

Mission: Make sure investigations have the evidence they need before an incident begins.

Inspection Checklist

- List required log sources: identity, endpoint, DNS, proxy, VPN, firewall, cloud control plane, SaaS, email, and apps.
- Check field quality, time synchronization, source health, retention, normalization, and search permissions.
- Verify logs from privileged actions, authentication, data access, administrative changes, and security control changes.
- Map log sources to likely incident types so response teams know what evidence exists.
- Test whether a recent user, host, domain, IP, file hash, and cloud API action can be searched quickly.

Real-Time Signals

- A log source stops forwarding, changes format, or drops critical fields.
- Retention falls below incident response, legal, or regulatory requirements.
- Time skew makes timelines unreliable across systems.
- Analysts cannot search logs needed for a high-priority incident.

Response Play

- Restore forwarding and preserve any local source logs before rotation removes them.
- Escalate critical blind spots to system owners and security leadership.
- Backfill logs where possible and clearly document unrecoverable gaps.
- Add health monitoring for log freshness, volume, parsing, and retention.
- Update incident playbooks to reflect actual evidence sources.

Free/open tooling: Wazuh, Elastic Stack, OpenSearch, Grafana Loki, Vector, Fluent Bit.

Evidence to save: Log source matrix, health dashboard, retention settings, parser tests, and sample search results.

Quality bar: Critical log sources are searchable, time-aligned, retained, and monitored for delivery health.

Skill 19: SIEM Triage Operations

Mission: Turn alerts into fast, consistent decisions with context, severity, and evidence.

Inspection Checklist

- Review alert queue structure, severity definitions, ownership, escalation paths, and closure reasons.
- Check that common alerts include identity, asset criticality, MITRE tactic, raw evidence, and suggested next steps.
- Measure false positives, duplicate alerts, missed context, and time from alert to analyst decision.
- Validate that high-severity alerts create incident records and notify the correct responders.
- Sample closed alerts to confirm evidence supports the decision.

Real-Time Signals

- High-severity alerts sit untriaged beyond SLA.
- Analysts close alerts without enough context or consistent reasoning.
- Alert volume spikes after a rule change, product update, or attack campaign.
- A detection source goes silent while related telemetry remains active.

Response Play

- Stabilize the queue by grouping related alerts and assigning an incident lead.
- Collect minimum triage facts: who, what, where, when, why plausible, and business impact.
- Escalate confirmed or likely compromise using the severity matrix.
- Tune noisy rules after preserving examples and analyst notes.
- Capture lessons into rule metadata, enrichment, and training examples.

Free/open tooling: Wazuh, Elastic Security, OpenSearch Security Analytics, Sigma, TheHive, Timesketch.

Evidence to save: Alert samples, triage notes, escalation records, rule metadata, tuning changes, and SLA metrics.

Quality bar: High-severity alerts receive consistent analyst decisions within agreed response time.

Skill 20: Endpoint Detection and Response Operations

Mission: Use endpoint telemetry to quickly distinguish benign activity from real compromise.

Inspection Checklist

- Verify EDR deployment, policy health, tamper protection, isolation capability, and analyst permissions.
- Review detection coverage for execution, persistence, privilege escalation, credential access, discovery, and exfiltration behaviors.
- Check whether endpoint alerts are enriched with user, asset criticality, vulnerability, and recent change context.
- Test safe response actions such as host isolation, file collection, process tree review, and timeline export.
- Inspect allow lists, exclusions, and suppressed detections for risky drift.

Real-Time Signals

- EDR agent tampering, unexpected service stop, or telemetry drop on a critical host.
- A suspicious process chain starts from email, browser, archive utility, script host, or remote management tool.
- Credentials, browser data, or sensitive files are accessed by an unusual process.
- An endpoint communicates with rare domains or infrastructure after suspicious execution.

Response Play

- Isolate the host when business impact permits and compromise is plausible.
- Export alert details, process tree, network connections, user sessions, and recent file changes.
- Collect triage artifacts and preserve suspicious files for controlled analysis.
- Reset credentials, revoke sessions, and hunt for the same indicators across the fleet.
- Document containment, remediation, and return-to-service criteria.

Free/open tooling: Wazuh, Velociraptor, osquery, YARA, Sysmon, Fleet.

Evidence to save: EDR policy export, alert timeline, host isolation record, collected artifacts, and fleet hunt results.

Quality bar: Compromised endpoints can be identified, isolated, investigated, and returned to service with auditable steps.

Skill 21: Network Detection and Traffic Analysis

Mission: See suspicious movement, command channels, data transfer, and policy violations at network level.

Inspection Checklist

- Identify key network sensors, span points, cloud flow logs, DNS logs, proxy logs, and firewall telemetry.
- Review visibility for north-south traffic, east-west traffic, privileged segments, VPN, and cloud workloads.
- Baseline normal DNS, HTTP, TLS, SMB, RDP, SSH, database, and data transfer patterns.
- Check detections for beaconing, rare destinations, lateral movement, scanning, tunneling, and unusual data volume.
- Validate packet capture retention and analyst access for high-priority segments.

Real-Time Signals

- A host contacts rare infrastructure, newly observed domains, or suspicious autonomous systems.
- Internal scanning or authentication attempts cross normal segment boundaries.
- Data transfer volume rises toward unapproved destinations or storage services.
- DNS queries show tunneling-like patterns, unusual entropy, or sudden volume increases.

Response Play

- Confirm the asset owner, process context, user, and recent changes behind the traffic.
- Block or rate-limit suspicious destinations while preserving flow records and packet samples.
- Correlate with endpoint and identity telemetry before broad containment.
- Hunt for related traffic patterns across neighboring hosts and time windows.
- Convert confirmed cases into tuned network detections and segmentation improvements.

Free/open tooling: Zeek, Suricata, Arkime, Wireshark, RITA, ntopng.

Evidence to save: Sensor map, flow samples, DNS logs, packet captures, firewall changes, and hunt notes.

Quality bar: Critical network paths have telemetry that supports detection, investigation, and containment decisions.

Skill 22: Threat Intelligence Intake

Mission: Use external intelligence to sharpen defense without flooding teams with low-value indicators.

Inspection Checklist

- Define intelligence requirements around industry threats, geography, technologies, executives, brands, and vendors.
- Review sources for reliability, timeliness, confidence, relevance, and legal use.
- Separate strategic trends, operational advisories, tactical indicators, and vulnerability intelligence.
- Check the path from intelligence intake to detection rules, hunts, blocking, patching, and leadership briefings.
- Measure expired indicators, duplicate feeds, false positives, and intelligence that created real action.

Real-Time Signals

- A credible advisory names technology or vendors used by the organization.
- Brand, executive, or domain impersonation appears in public reports.
- Indicators match internal logs, even at low volume.
- A new campaign targets the organization's region, sector, or customer type.

Response Play

- Validate relevance against asset inventory and exposure data.
- Search internal telemetry for matches before blocking broad indicator sets.
- Create focused detections, hunts, or hardening tasks with owner and expiration.
- Brief leadership when intelligence changes business risk or response posture.
- Retire stale indicators and record whether the intelligence produced action.

Free/open tooling: MISP, OpenCTI, Yeti, Abuse.ch feeds, AlienVault OTX, Sigma.

Evidence to save: Intelligence requirements, source list, indicator matches, actions taken, and expiration records.

Quality bar: Threat intelligence produces measurable detection, hunting, hardening, or decision value.

Skill 23: Detection Engineering

Mission: Create durable detections that are testable, contextual, and tied to real attacker behaviors.

Inspection Checklist

- Map detections to MITRE ATT&CK tactics, relevant assets, required logs, and known blind spots.
- Review rule logic, data source assumptions, severity, false-positive notes, and response guidance.
- Test detections with safe simulations or historical examples before production rollout.
- Track rule versioning, owners, tuning decisions, suppression logic, and review cadence.
- Measure alert value: true positives, useful hunts, false positives, and missed incidents.

Real-Time Signals

- A detection relies on a log source that stopped or changed format.
- A rule produces noisy alerts without actionable context.
- A new threat behavior is relevant but has no internal detection coverage.
- An incident reveals a detection gap or a rule that fired too late.

Response Play

- Write or update detection logic with clear assumptions and sample evidence.
- Backtest against historical logs and review false positives with service owners.
- Deploy gradually where possible and monitor alert quality.
- Add analyst guidance that explains first questions and likely benign causes.
- Document the detection gap and close it through logging, parsing, or control changes.

Free/open tooling: Sigma, YARA, Suricata rules, DetectionLab, Chainsaw, Hayabusa.

Evidence to save: Rule repository, test results, sample alerts, tuning notes, and coverage matrix.

Quality bar: High-priority attack behaviors have tested detections with owners, context, and measurable quality.

Skill 24: Incident Classification and Severity

Mission: Classify events consistently so response speed matches business risk.

Inspection Checklist

- Define severity levels using impact, likelihood, data sensitivity, asset criticality, containment state, and public exposure.
- Create criteria for security event, suspicious activity, confirmed incident, crisis, and disaster recovery activation.
- Align severity with escalation contacts, communication cadence, legal review, and leadership notification.
- Review past incidents for severity drift, delayed escalation, or over-escalation.
- Make classification fast enough for real-time response but flexible enough for new evidence.

Real-Time Signals

- An event touches regulated data, privileged identities, production systems, or public trust.
- Containment is uncertain, attacker access may still be active, or evidence is disappearing.
- Multiple business units, countries, customers, or vendors may be affected.
- Media, customer, regulator, or law enforcement attention is likely.

Response Play

- Assign an initial severity within the first decision window and name an incident commander if needed.
- Record the evidence behind the severity and what would raise or lower it.
- Trigger the matching escalation, communication, and legal/privacy workflows.
- Reassess severity at each major evidence change or response milestone.
- After closure, compare actual impact to initial severity and improve criteria.

Free/open tooling: TheHive, DFIR-IRIS, RTIR, Jira, Matrix/Element, Mattermost.

Evidence to save: Severity matrix, incident record, escalation timeline, impact assessment, and reclassification notes.

Quality bar: Severity decisions are fast, documented, consistently applied, and tied to response commitments.

Skill 25: Initial Triage and First 15 Minutes

Mission: Stabilize the first minutes of an incident with facts, ownership, and controlled action.

Inspection Checklist

- Confirm the alert source, affected user or asset, time window, business criticality, and current activity.
- Check whether the alert is isolated, spreading, recurring, or tied to a known change.
- Identify evidence at risk of rotation, deletion, or overwriting.
- Define the next decision: dismiss, monitor, escalate, contain, or declare incident.
- Make sure the responder knows who can approve containment that affects business operations.

Real-Time Signals

- The activity is ongoing or attacker access may still be active.
- A privileged identity, production service, customer data, or security control is involved.
- Multiple independent signals point to the same user, host, or service.
- Evidence suggests data access, persistence, lateral movement, or credential theft.

Response Play

- Start an incident log with timestamped actions and evidence references.
- Preserve high-value logs, alert details, screenshots, and system state quickly.
- Assign roles: incident lead, technical lead, communications lead, and scribe for major cases.
- Take reversible containment first when it meaningfully reduces risk.
- Set the next update time and decision checkpoint.

Free/open tooling: TheHive, Timesketch, Velociraptor, Wazuh, osquery, Mattermost.

Evidence to save: Initial alert, triage worksheet, incident log, first timeline, containment decision, and owner notifications.

Quality bar: Within 15 minutes, high-priority events have an owner, initial severity, preserved evidence, and next action.

Skill 26: Containment Strategy

Mission: Limit attacker freedom while protecting evidence and business continuity.

Inspection Checklist

- Predefine containment options for endpoints, identities, networks, cloud accounts, SaaS apps, and data stores.
- Understand which containment actions are reversible, disruptive, evidence-destructive, or approval-sensitive.
- Map authority for isolating hosts, disabling accounts, blocking IPs, revoking tokens, and shutting down services.
- Practice containment decision-making in tabletop scenarios with technical and business leaders.
- Review past incidents for delays caused by unclear approval or fear of business impact.

Real-Time Signals

- Attacker activity is ongoing or likely to resume with current access.
- Credential theft, persistence, lateral movement, or data staging is observed.
- Containment delay increases risk to regulated data or critical operations.
- Security controls are being disabled or evaded.

Response Play

- Choose the narrowest containment action that meaningfully reduces immediate risk.
- Preserve evidence and record the business tradeoff before disruptive actions.
- Coordinate identity, endpoint, network, cloud, and application containment as one plan.
- Monitor for attacker adaptation after containment is applied.
- Move from emergency containment to stable controls as soon as practical.

Free/open tooling: Wazuh, Velociraptor, pfSense, OPNsense, Cloud Custodian, TheHive.

Evidence to save: Containment decision log, approval record, technical changes, observed attacker reaction, and business impact notes.

Quality bar: Containment actions are timely, proportionate, reversible where possible, and documented.

Skill 27: Eradication and Root Cause Removal

Mission: Remove attacker access and the conditions that allowed compromise.

Inspection Checklist

- Identify initial access, persistence, compromised credentials, affected systems, exploited weaknesses, and control failures.
- Separate symptom cleanup from root-cause removal.
- Review accounts, tokens, keys, scheduled tasks, services, startup items, firewall changes, and cloud roles.
- Validate clean rebuild paths, patch availability, configuration changes, and credential rotation requirements.
- Track eradication work as tasks with owners, evidence, and verification steps.

Real-Time Signals

- The same alert returns after containment or rebuild.
- Persistence or unauthorized access remains after initial cleanup.
- The initial access weakness still exists on similar systems.
- Credential or token scope is broader than first understood.

Response Play

- Remove persistence and unauthorized changes using documented, reviewable actions.
- Patch, harden, rotate, rebuild, or decommission affected components according to root cause.
- Hunt for the same root cause across assets, accounts, and environments.
- Verify eradication with independent telemetry and owner signoff.
- Record prevention work that must be completed after emergency response.

Free/open tooling: Velociraptor, osquery, YARA, OpenSCAP, Ansible, Trivy.

Evidence to save: Root-cause analysis, eradication tasks, credential rotation proof, rebuild records, and hunt results.

Quality bar: No system returns to service until root-cause removal and verification criteria are met.

Skill 28: Recovery and Return to Service

Mission: Restore business safely with validation, monitoring, and clear acceptance criteria.

Inspection Checklist

- Define recovery criteria for each service: clean state, patched state, credentials, backups, monitoring, and owner approval.
- Plan phased recovery for identity, network, endpoints, applications, databases, and third-party integrations.
- Validate restored systems in isolation before reconnecting to production dependencies.
- Set heightened monitoring for the recovery window.
- Confirm customer, legal, and business communications are aligned with actual service state.

Real-Time Signals

- Recovered systems show recurring alerts, failed integrity checks, or missing controls.
- Users report service anomalies after restoration.
- Data consistency checks fail or downstream integrations behave unexpectedly.
- The business pressures teams to reconnect before security criteria are met.

Response Play

- Recover the minimum viable service first, then expand capability through controlled stages.
- Verify identity, patch, logging, backup, and network restrictions before reconnecting.
- Monitor aggressively for repeated attacker behavior or restoration errors.
- Record acceptance by technical owner, business owner, and incident lead.
- Schedule after-action work for long-term improvements.

Free/open tooling: Restic, BorgBackup, Ansible, Wazuh, Grafana, OpenSearch.

Evidence to save: Recovery plan, validation checklist, restored version, monitoring dashboard, and owner acceptance.

Quality bar: Services return only after security and business validation, with heightened monitoring in place.

Skill 29: Ransomware Readiness and Response

Mission: Prepare for destructive events with fast containment, protected backups, and decision clarity.

Inspection Checklist

- Review ransomware-specific coverage for backups, endpoint isolation, privileged access, segmentation, logging, and crisis roles.
- Identify systems where encryption, deletion, or downtime would create the highest business impact.
- Test restore from immutable or isolated backups for critical services.
- Review playbooks for ransom contact, legal involvement, insurer notification, and law enforcement considerations.
- Pre-stage communications for staff, customers, vendors, and leadership without making promises ahead of facts.

Real-Time Signals

- Mass file renames, encryption-like activity, deletion of backups, or shadow copy tampering.
- EDR alerts on known destructive behaviors or unauthorized remote administration.
- Multiple users lose access to shared files or see ransom notes.
- Backup or security tooling is disabled before file impact becomes visible.

Response Play

- Isolate affected segments and protect backup infrastructure immediately.
- Preserve evidence but prioritize stopping spread when destructive activity is ongoing.
- Disable compromised credentials and review remote access paths.
- Determine clean restore points and rebuild priority with business leadership.
- Communicate through the crisis process and document every major decision.

Free/open tooling: Wazuh, Velociraptor, Zeek, Restic, BorgBackup, TheHive.

Evidence to save: Impact map, containment timeline, backup integrity proof, credential actions, and recovery decisions.

Quality bar: The organization can isolate spread and begin clean recovery without depending on attacker cooperation.

Skill 30: Phishing Response

Mission: Turn user reports and mail alerts into quick containment of messages, credentials, and sessions.

Inspection Checklist

- Review phishing report intake, triage ownership, message search, purge workflow, and user feedback.
- Validate mailbox audit logging, sign-in logs, OAuth grants, forwarding rules, and message trace retention.
- Check training alignment with real themes: invoices, file shares, MFA prompts, HR notices, and executive requests.
- Measure time from first report to analyst decision and message removal.
- Ensure credential-entry cases trigger identity response, not only message cleanup.

Real-Time Signals

- Multiple users report similar messages or links.
- A user clicked a link and then had unusual sign-ins, MFA prompts, or mailbox changes.
- The sender impersonates a vendor, executive, or internal workflow.
- Attachments or links lead to suspicious file delivery or credential pages.

Response Play

- Preserve full headers, body, attachments, URLs, and message trace.
- Search and remove matching messages through approved administrative tools.
- Revoke sessions, reset passwords, and review MFA and OAuth state for affected users.
- Block confirmed malicious domains, senders, or file hashes with expiration review.
- Give users concise feedback so reporting behavior improves.

Free/open tooling: parsedmarc, CyberChef, URLhaus, PhishTool Community, TheHive, Wazuh.

Evidence to save: Reported sample, message trace, affected recipients, purge result, identity review, and user communication.

Quality bar: Reported phishing is triaged, contained, and fed back into controls quickly.

Skill 31: Business Email Compromise Response

Mission: Protect money movement, sensitive communication, and trust when mailbox abuse is suspected.

Inspection Checklist

- Review finance workflows for out-of-band verification, approval segregation, and emergency payment holds.
- Inspect mailbox forwarding, delegated access, inbox rules, OAuth grants, recent sign-ins, and sent items.
- Identify high-risk roles: executives, finance, procurement, HR, payroll, and customer success.
- Validate contact paths to banks, payment processors, vendors, legal, and leadership.
- Measure how quickly finance can freeze or verify suspicious transactions.

Real-Time Signals

- Payment instructions change by email without known process.
- Mailbox rules hide replies, invoices, bank terms, or security notices.
- An account sends messages while sign-ins come from unusual locations.
- Vendors or customers report unexpected invoice, payroll, or account changes.

Response Play

- Secure the mailbox: revoke sessions, reset credentials, remove malicious rules, and review OAuth grants.
- Preserve mailbox audit, message trace, sent items, deleted items, and sign-in logs.
- Contact finance, bank, and impacted partners through trusted out-of-band channels.
- Trace messages and transactions to identify affected recipients and potential losses.
- Update payment verification and mailbox monitoring based on findings.

Free/open tooling: Mailbox audit exports, TheHive, Timesketch, parsedmarc, Wazuh, Sigma.

Evidence to save: Mailbox timeline, suspicious rules, transaction details, partner notifications, and recovery actions.

Quality bar: BEC cases trigger both identity containment and financial verification within minutes.

Skill 32: Credential Theft Response

Mission: Assume stolen credentials can become active sessions, tokens, and downstream access.

Inspection Checklist

- Review where credentials live: browsers, password managers, scripts, CI/CD, cloud keys, service accounts, and secrets stores.
- Map session revocation, token invalidation, password reset, key rotation, and application-specific credential paths.
- Check detections for suspicious sign-in, token creation, OAuth grant, impossible travel, and password spray.
- Identify high-blast-radius credentials and compensating controls.
- Practice rotation for secrets that are hard to change under pressure.

Real-Time Signals

- Successful login follows phishing, malware, password spray, or impossible travel.
- New tokens, app passwords, OAuth grants, or API keys appear after suspicious authentication.
- Credentials are found in code, logs, tickets, chat, or exposed storage.
- A service account authenticates interactively or from a new location.

Response Play

- Revoke sessions and rotate credentials, keys, and tokens according to blast radius.
- Review recent access to sensitive apps, cloud accounts, SaaS data, and code repositories.
- Hunt for the same exposed credential across logs and repositories.
- Remove credential material from exposed locations and preserve evidence.
- Strengthen MFA, secret scanning, and least-privilege controls to reduce repeat risk.

Free/open tooling: Gitleaks, TruffleHog, OpenBao, Vault Community, Wazuh, Sigma.

Evidence to save: Credential source, affected identities, revocation proof, access review, and rotation record.

Quality bar: Stolen or exposed credentials are revoked, rotated, and investigated across all reachable systems.

Skill 33: Web Intrusion Response

Mission: Respond to suspected web compromise without losing application, data, and deployment evidence.

Inspection Checklist

- Pre-map application logs, web server logs, WAF logs, database logs, deployment history, and admin actions.
- Know how to place the application in maintenance mode, read-only mode, or restricted access.
- Review file integrity monitoring, dependency inventory, secret storage, and emergency rollback paths.
- Confirm who can approve downtime, data access review, and customer communication.
- Practice tracing a request from edge to application to database.

Real-Time Signals

- Unexpected admin actions, file changes, data export, unusual errors, or WAF alerts.
- Application secrets, environment variables, or configuration files may be exposed.
- A new process, cron job, plugin, or uploaded file appears on a web server.
- Database queries or object access spike around suspicious requests.

Response Play

- Preserve edge, WAF, web, application, database, and deployment logs.
- Restrict access or roll back vulnerable releases while maintaining evidence.
- Rotate secrets and credentials that may be reachable from the application.
- Identify affected users, records, files, and administrative actions.
- Patch root cause, validate with focused tests, and increase monitoring after restoration.

Free/open tooling: OWASP ZAP, Wazuh FIM, ModSecurity CRS, GoAccess, Timesketch, Semgrep.

Evidence to save: Request timeline, deployment diff, file integrity events, data access logs, and remediation proof.

Quality bar: Web incidents preserve enough evidence to determine entry point, affected data, and clean recovery state.

Skill 34: Cloud Compromise Response

Mission: Handle suspicious cloud activity with control-plane evidence, credential containment, and configuration recovery.

Inspection Checklist

- Pre-map cloud logs, identity federation, role assumptions, access keys, network flow logs, and resource inventory.
- Document emergency controls for disabling keys, revoking sessions, restricting roles, and isolating workloads.
- Review backup, snapshot, and infrastructure-as-code recovery paths.
- Identify accounts that hold security logs, billing, root access, and organization-wide policy control.
- Practice tracing an API action to user, role, source, resource, and business owner.

Real-Time Signals

- Suspicious API calls create users, keys, roles, firewall changes, snapshots, or public exposure.
- Cloud logging is disabled, altered, or redirected.
- Resources appear in unusual regions or accounts.
- Billing spikes, crypto-mining patterns, or unexpected compute fleets appear.

Response Play

- Preserve control-plane logs and snapshots of affected configurations.
- Revoke risky credentials, restrict roles, and block suspicious network paths.
- Identify every resource touched by the suspicious identity or role session.
- Restore known-good configurations through infrastructure-as-code where possible.
- Review organization guardrails and detection gaps that allowed the activity.

Free/open tooling: Prowler, CloudTrail Lake alternatives, Steampipe, CloudQuery, Cloud Custodian, TheHive.

Evidence to save: API timeline, IAM changes, resource diff, credential actions, guardrail status, and restored configuration.

Quality bar: Cloud incidents can be scoped by API timeline and contained through identity and policy controls.

Skill 35: Insider Risk Inspection

Mission: Detect and handle trusted-user risk with fairness, privacy, and strong evidence standards.

Inspection Checklist

- Define insider risk scenarios with legal, HR, privacy, and security leadership.
- Review access to sensitive repositories, privileged systems, customer data, source code, and financial records.
- Check controls for joiner, mover, leaver, conflict-of-interest roles, and high-risk terminations.
- Measure unusual data access, mass downloads, permission changes, and policy bypass attempts.
- Ensure investigations have proportionality, need-to-know access, and documented approval.

Real-Time Signals

- Large or unusual data access by a user without business context.
- Permission changes, export behavior, or file sharing increases around resignation or role change.
- Sensitive data moves to personal email, unmanaged devices, or unapproved storage.
- A user attempts to disable logging, bypass DLP, or use unauthorized tools.

Response Play

- Preserve evidence discreetly and involve authorized HR/legal stakeholders early.
- Avoid accusatory language until facts are reviewed and context is understood.
- Restrict access proportionately if ongoing risk is credible.
- Document business justification, data touched, and policy violations with clear timestamps.
- After resolution, improve access governance and least privilege.

Free/open tooling: Wazuh, OpenSearch, SaaS audit logs, DLP exports, TheHive, Timesketch.

Evidence to save: Approval record, audit timeline, access review, data movement evidence, and decision log.

Quality bar: Insider risk cases are evidence-led, privacy-aware, and handled through approved governance.

Skill 36: Third-Party and Supply Chain Risk

Mission: Inspect the security posture of vendors, integrations, dependencies, and outsourced operations.

Inspection Checklist

- Inventory vendors by service, data access, network access, criticality, contract owner, and renewal date.
- Review security obligations, breach notification terms, audit rights, data location, and subcontractor use.
- Inspect integrations: API scopes, OAuth grants, SSO, SCIM, webhooks, service accounts, and shared secrets.
- Monitor software dependencies, container images, build pipelines, and vendor advisories.
- Plan offboarding and emergency disconnect for critical vendors.

Real-Time Signals

- A vendor announces a breach, vulnerability, outage, or suspicious support access.
- A third-party integration requests broader permissions or creates unexpected tokens.
- A dependency advisory affects production code or build systems.
- Vendor accounts access data outside normal patterns.

Response Play

- Identify affected data, systems, integrations, and business processes.
- Restrict or rotate third-party access based on risk and operational dependency.
- Request vendor evidence and timeline through contract and incident channels.
- Search internal logs for vendor account activity during the risk window.
- Update vendor risk rating, controls, and renewal requirements.

Free/open tooling: OWASP Dependency-Track, Syft, Grype, Trivy, OSV-Scanner, OpenCTI.

Evidence to save: Vendor inventory, contract clauses, integration scopes, advisory review, access logs, and risk decision.

Quality bar: Critical vendors and integrations have known access, monitoring, exit paths, and incident contacts.

Skill 37: Secure Remote Access

Mission: Inspect VPN, zero-trust access, remote admin, and contractor pathways before attackers do.

Inspection Checklist

- Inventory VPNs, remote desktop gateways, admin portals, bastions, SSH paths, and vendor access methods.
- Review MFA, device trust, geo rules, split tunneling, session recording, idle timeout, and account lifecycle.
- Check exposed remote access services against patch level and vendor advisories.
- Validate logs for user, device, source, destination, session duration, and admin actions.
- Review emergency disable procedures for compromised accounts or vulnerable gateways.

Real-Time Signals

- Remote access from unusual countries, devices, impossible travel, or dormant accounts.
- Repeated failed logins followed by success.
- A remote access gateway has a critical advisory or active exploitation report.
- Admin protocols are reachable without expected access broker controls.

Response Play

- Disable or restrict suspicious sessions and accounts while preserving remote access logs.
- Patch or mitigate vulnerable gateways urgently, especially if internet-facing.
- Review accessed hosts, files, and administrative actions during suspicious sessions.
- Rotate credentials and enforce stronger MFA for affected groups.
- Tighten remote access policy and remove unused pathways.

Free/open tooling: OpenVPN, WireGuard, Teleport Community, Guacamole, Wazuh, Zeek.

Evidence to save: Remote access inventory, policy export, session logs, patch state, and containment actions.

Quality bar: Remote access is MFA-protected, logged, least-privilege, patched, and rapidly disableable.

Skill 38: Wireless Security Inspection

Mission: Confirm wireless networks do not become unmanaged bridges into sensitive systems.

Inspection Checklist

- Inventory SSIDs, authentication methods, guest networks, controller access, certificates, and network segmentation.
- Review WPA configuration, enterprise authentication, shared keys, rotation schedule, and rogue access point monitoring.
- Check whether guest wireless is isolated from internal systems and management planes.
- Validate controller logging, admin MFA, firmware updates, and backup configuration.
- Review physical areas where wireless coverage extends beyond expected boundaries.

Real-Time Signals

- A rogue or evil-twin-like SSID appears near facilities.
- Guest network traffic reaches internal services.
- Controller configuration changes without approval.
- Shared wireless credentials are posted, reused, or not rotated after staff changes.

Response Play

- Disable or isolate suspect SSIDs and preserve controller logs.
- Rotate shared keys or certificates when exposure is likely.
- Trace connected devices and validate whether any internal access occurred.
- Update segmentation and monitoring rules for wireless networks.
- Document physical and administrative corrective actions.

Free/open tooling: Kismet, Wireshark, FreeRADIUS, OpenWISP, Wazuh, NetBox.

Evidence to save: SSID inventory, controller config, authentication logs, segmentation proof, and rogue AP findings.

Quality bar: Wireless access is authenticated, segmented, monitored, and governed like any other network entry point.

Skill 39: Mobile Device Security

Mission: Protect phones and tablets that hold identity tokens, email, files, and approval workflows.

Inspection Checklist

- Inventory corporate and BYOD devices with enrollment state, OS version, encryption, lock settings, and app policy.
- Review access to email, SaaS, VPN, password managers, MFA apps, and executive communication.
- Check device compliance rules, jailbreak/root detection, lost-device procedures, and remote wipe authority.
- Validate mobile phishing reporting and secure browser controls where available.
- Inspect whether sensitive data can be copied to unmanaged apps or personal storage.

Real-Time Signals

- A device becomes noncompliant but still accesses sensitive apps.
- A lost or stolen device belongs to a privileged or high-risk user.
- Mobile sign-ins show impossible travel or unusual token behavior.
- Users report mobile phishing, MFA fatigue, or unexpected app prompts.

Response Play

- Revoke sessions and wipe or retire the device according to ownership model and policy.
- Reset credentials and re-register MFA when token exposure is plausible.
- Review recent app access, file downloads, and mailbox activity.
- Confirm the user has a clean replacement path that does not bypass controls.
- Improve compliance rules and user guidance based on incident findings.

Free/open tooling: Headwind MDM, MicroMDM, Wazuh, Aegis Authenticator, SaaS audit logs.

Evidence to save: Device inventory, compliance record, access logs, wipe/revoke proof, and user confirmation.

Quality bar: Mobile access to sensitive apps requires compliant devices, strong authentication, and rapid revocation.

Skill 40: IoT and Operational Technology Inspection

Mission: Inspect embedded, facility, industrial, and unmanaged devices with safety and uptime in mind.

Inspection Checklist

- Inventory cameras, printers, sensors, controllers, badge systems, building systems, lab devices, and industrial assets.
- Identify vendor support status, firmware, default credentials, remote access, protocols, and network placement.
- Use passive discovery first for fragile systems and coordinate active checks with operational owners.
- Review segmentation between IoT/OT networks, corporate networks, internet, and management systems.
- Document safety constraints, maintenance windows, and vendor dependencies.

Real-Time Signals

- An IoT or OT device communicates with unexpected external destinations.
- Default credentials, unsupported firmware, or exposed management interfaces are found.
- A device moves segments, changes firmware, or restarts unexpectedly.
- Operational staff report anomalies after network or security changes.

Response Play

- Coordinate with operational owners before containment that may affect safety or availability.
- Restrict network paths and management access rather than making risky device changes first.
- Preserve logs, firmware version, network captures, and vendor support details.
- Replace, patch, or isolate unsupported devices through a lifecycle plan.
- Update segmentation and monitoring for the device class.

Free/open tooling: Zeek, Wireshark, Nmap with approved profiles, NetBox, OpenPLC lab, Wazuh.

Evidence to save: Device inventory, network map, owner approvals, firmware status, capture samples, and segmentation changes.

Quality bar: IoT and OT assets are known, segmented, monitored, and changed only with operational approval.

Skill 41: Vulnerability Remediation Governance

Mission: Create accountability so risk does not remain trapped in reports.

Inspection Checklist

- Define severity, SLA, exception, ownership, and escalation rules for vulnerability findings.
- Connect scanners to ticketing, asset owners, service criticality, and remediation validation.
- Track repeated findings, reopen rates, false positives, accepted risks, and blocked remediation.
- Review executive reporting for trend, exposure, and business service risk.
- Ensure emergency vulnerability response has a separate fast lane.

Real-Time Signals

- Critical findings remain open after SLA or lack an owner.
- Remediation is marked complete without validation.
- Exceptions have no expiration or compensating control.
- The same vulnerability class reappears across teams or releases.

Response Play

- Escalate overdue critical risk through the service owner and leadership path.
- Validate remediation before closure and reopen incomplete fixes.
- Convert recurring issues into baseline, pipeline, image, or procurement changes.
- Review exceptions and retire those without current justification.
- Use metrics to improve root causes, not only to count findings.

Free/open tooling: DefectDojo, Faraday Community, Greenbone CE, Jira, OpenProject, Grafana.

Evidence to save: SLA policy, ticket exports, validation proof, exception register, and trend dashboard.

Quality bar: Vulnerabilities have owners, deadlines, evidence-backed closure, and executive-visible risk trends.

Skill 42: Security Metrics and Executive Signals

Mission: Show leadership the few signals that reveal whether cyber risk is improving or degrading.

Inspection Checklist

- Choose metrics tied to decisions: exposure, control coverage, response speed, recovery readiness, and unresolved critical risk.
- Avoid vanity metrics that reward alert volume, raw scan counts, or activity without risk reduction.
- Create service-level views for critical business processes.
- Review trends, thresholds, owners, and escalation triggers monthly.
- Include confidence and blind spots so leaders understand measurement quality.

Real-Time Signals

- Critical exposure grows while remediation slows.
- Logging, EDR, backup, or MFA coverage drops below target.
- Mean time to triage or contain worsens across high-severity events.
- Metrics look green while incidents reveal missing visibility.

Response Play

- Investigate metric drift as an operational signal, not a reporting problem.
- Assign owners for degraded controls and set recovery deadlines.
- Use incident lessons to add or retire metrics.
- Brief leadership on business impact, options, cost, and residual risk.
- Automate metric collection where possible to reduce manual reporting bias.

Free/open tooling: Grafana, Metabase, Superset, OpenSearch Dashboards, Steampipe, Evidence.dev.

Evidence to save: Metric definitions, source queries, dashboard screenshots, trend notes, and leadership decisions.

Quality bar: Security metrics drive decisions and clearly show control coverage, risk concentration, and response readiness.

Skill 43: Evidence Handling and Legal Readiness

Mission: Preserve investigation integrity so technical facts can support business, legal, and regulatory decisions.

Inspection Checklist

- Define evidence types: logs, disk images, memory captures, screenshots, messages, tickets, cloud exports, and artifacts.
- Review collection authority, privacy limits, chain of custody, storage encryption, and access restrictions.
- Set naming standards with time zone, source, collector, hash where applicable, and case ID.
- Confirm retention requirements for incidents involving customers, employees, regulated data, or litigation.
- Train responders on when to involve legal, privacy, HR, and outside counsel.

Real-Time Signals

- Evidence may be overwritten, deleted, altered, or exposed to too many people.
- An incident may involve regulated data, law enforcement, employee action, or customer notification.
- A responder wants to wipe or rebuild before preserving required facts.
- External parties request evidence without an approved process.

Response Play

- Preserve volatile and high-value evidence first with documented collection steps.
- Limit access to need-to-know responders and legal stakeholders.
- Hash exported files where practical and record custody transfers.
- Separate facts, analysis, assumptions, and decisions in the incident log.
- Review evidence handling after closure and fix process gaps.

Free/open tooling: Timesketch, Autopsy, Velociraptor, hashdeep, Cryptomator, TheHive.

Evidence to save: Chain-of-custody log, hashes, collection notes, access list, and legal/privacy decision records.

Quality bar: Evidence remains complete, traceable, protected, and usable for investigation and governance.

Skill 44: Crisis Communications

Mission: Communicate accurately under pressure without outrunning facts or creating avoidable confusion.

Inspection Checklist

- Define audiences: responders, executives, employees, customers, vendors, regulators, media, and law enforcement.
- Prepare templates for incident updates, holding statements, customer advisories, and internal guidance.
- Create approval paths for legal, privacy, leadership, and communications teams.
- Practice short update cycles with facts known, actions taken, next checkpoint, and what not to speculate on.
- Maintain out-of-band communication if email, chat, or identity systems are affected.

Real-Time Signals

- The incident affects customer trust, public services, regulated data, or employee safety.
- Rumors, screenshots, or external posts appear before official messaging.
- Teams are using compromised or unreliable communication channels.
- Executives need a decision before technical certainty is complete.

Response Play

- Establish a single source of truth and update cadence.
- Separate confirmed facts, current assessment, customer impact, and next steps.
- Use plain language and avoid blame, speculation, or unsupported precision.
- Keep responders focused by shielding them from duplicate executive requests.
- After closure, compare communications to actual findings and improve templates.

Free/open tooling: Mattermost, Matrix/Element, CryptPad, OnlyOffice, TheHive, Jitsi.

Evidence to save: Communication plan, approvals, sent messages, update cadence, Q&A; log, and post-incident review.

Quality bar: Stakeholders receive accurate, timely, approved updates that match the incident severity.

Skill 45: Tabletop Exercises and Simulations

Mission: Practice response decisions before the organization has to make them under real pressure.

Inspection Checklist

- Select scenarios based on actual risk: ransomware, cloud compromise, BEC, data exposure, vendor breach, and insider risk.
- Include technical teams, business owners, legal, privacy, communications, HR, and executives as appropriate.
- Test decisions, not trivia: severity, containment, customer impact, recovery, and leadership communication.
- Capture friction points, missing contacts, unclear authority, and evidence gaps.
- Convert exercise lessons into dated actions with owners.

Real-Time Signals

- Participants disagree on who can declare an incident or approve containment.
- Critical contacts, backup channels, or evidence sources are missing.
- Recovery assumptions differ from actual restore tests.
- Communications are delayed because facts and approval paths are unclear.

Response Play

- Pause the exercise only to clarify safety or scope, then continue realistic pressure.
- Record decisions, assumptions, missed data, and moments of confusion.
- Debrief immediately while details are fresh.
- Assign action items to playbook, control, training, or governance owners.
- Retest the highest-risk gaps in the next exercise.

Free/open tooling: TheHive, DFIR-IRIS, OpenProject, CryptPad, Jitsi, Draw.io.

Evidence to save: Scenario brief, participant list, decision log, gaps, action plan, and retest results.

Quality bar: Exercises produce measurable improvements in decision speed, role clarity, and response readiness.

Skill 46: Automation and SOAR Playbooks

Mission: Automate repeatable response work while keeping humans in control of risk decisions.

Inspection Checklist

- List high-frequency workflows: phishing triage, user disable, session revocation, host isolation, enrichment, and ticketing.
- Classify automation steps as observe, enrich, recommend, contain, or remediate.
- Require approval gates for disruptive, irreversible, or business-impacting actions.
- Review secrets, service accounts, audit logs, failure modes, and rollback paths for automation.
- Measure analyst time saved and incident outcomes, not just number of automated actions.

Real-Time Signals

- A manual response task is repeated often and has clear decision criteria.
- Automation runs without logging, owner, or failure alerting.
- A playbook action affects production without approval.
- Automation credentials have broad access or no rotation path.

Response Play

- Start with enrichment and evidence collection before automating containment.
- Add human approval for high-impact steps and log every action with case ID.
- Test playbooks on safe examples and staged environments.
- Monitor automation errors, partial failures, and unexpected side effects.
- Review permissions and rotate automation secrets like privileged accounts.

Free/open tooling: Shuffle, TheHive, Cortex, Node-RED, n8n community, StackStorm.

Evidence to save: Playbook inventory, approval gates, run logs, permission review, and failure tests.

Quality bar: Automation reduces response time without hiding decisions or increasing blast radius.

Skill 47: AI-Assisted Security Operations

Mission: Use AI to accelerate analysis while protecting secrets, privacy, and decision quality.

Inspection Checklist

- Define approved AI use cases: summarizing logs, drafting reports, clustering alerts, explaining detections, and checklist support.
- Restrict sensitive data, credentials, customer records, and regulated content from unapproved AI systems.
- Require human review for severity, containment, attribution, customer impact, and legal decisions.
- Track prompts, sources, assumptions, and outputs when AI materially supports an incident.
- Test AI outputs against known cases to understand hallucination and omission risk.

Real-Time Signals

- Analysts paste secrets, customer data, or raw incident evidence into unapproved tools.
- AI output is treated as fact without source verification.
- A summary omits key timeline events or changes severity language.
- Sensitive investigation data appears outside approved retention boundaries.

Response Play

- Stop unsafe data sharing and preserve records needed for privacy review.
- Verify AI-assisted findings against primary logs and artifacts.
- Mark AI-generated summaries as drafts until reviewed by an accountable human.
- Update prompt templates and data handling rules after mistakes.
- Use local or approved controlled environments for sensitive analysis where possible.

Free/open tooling: Local LLMs where approved, OpenSearch ML features, Jupyter, Ollama, Private notebooks.

Evidence to save: AI use policy, approved prompts, review notes, source references, and exception records.

Quality bar: AI improves speed and clarity without becoming an uncontrolled evidence or decision system.

Skill 48: Continuous Control Monitoring

Mission: Move from annual inspection to continuous assurance for the controls that matter most.

Inspection Checklist

- Select controls that can be measured continuously: MFA, EDR, logging, backups, public exposure, encryption, and patch posture.
- Connect measurements to authoritative sources and business service ownership.
- Define thresholds, alert routing, exception handling, and evidence retention.
- Review control failures as operational events with owners and deadlines.
- Keep dashboards small enough that teams act on them.

Real-Time Signals

- A critical control drops below threshold or stops reporting.
- An exception expires without remediation or renewed risk acceptance.
- A business-critical service lacks evidence for one or more core controls.
- Manual reporting disagrees with automated telemetry.

Response Play

- Route the control failure to the owning team with evidence and deadline.
- Escalate repeated or critical failures through risk governance.
- Fix data quality issues when measurements cannot be trusted.
- Add missing assets and owners discovered through control monitoring.
- Use trends to plan engineering work that removes recurring failures.

Free/open tooling: Steampipe, CloudQuery, Grafana, OpenSearch, Prowler, osquery.

Evidence to save: Control catalog, queries, dashboards, exception register, and remediation history.

Quality bar: Core controls are continuously measured and failures trigger accountable remediation.

Skill 49: Purple Team and Validation Safety

Mission: Validate defenses with controlled exercises that improve detection without creating unmanaged risk.

Inspection Checklist

- Define validation goals, authorized techniques, data sources, schedule, and stop conditions.
- Coordinate with system owners and incident responders so exercises test process as well as tooling.
- Use safe simulations, atomic tests, or lab environments when production testing is risky.
- Measure whether detections fired, alerts reached analysts, context was sufficient, and response actions were clear.
- Turn validation failures into logging, detection, playbook, and control improvements.

Real-Time Signals

- A validation activity triggers unexpected business impact.
- A control fails silently or an alert lacks enough evidence for triage.
- Responders mistake an exercise for an uncontrolled real incident without exercise governance.
- A planned technique exceeds authorization or safety limits.

Response Play

- Stop or reduce the activity if safety, scope, or operational impact becomes uncertain.
- Preserve exercise telemetry and responder notes.
- Label results clearly as validation, not evidence of hostile action.
- Fix gaps with owners and retest using the same success criteria.
- Update future rules of engagement based on lessons learned.

Free/open tooling: Atomic Red Team, Caldera in lab, DetectionLab, Sigma, TheHive, Wazuh.

Evidence to save: Rules of engagement, validation plan, detection results, responder notes, and improvement tickets.

Quality bar: Validation exercises improve real detection and response capability without uncontrolled impact.

Skill 50: Secure Software Delivery Inspection

Mission: Inspect code, pipelines, artifacts, and release controls as part of the security boundary.

Inspection Checklist

- Inventory repositories, owners, branch protections, CI/CD systems, artifact registries, deployment secrets, and release environments.
- Review secret scanning, dependency scanning, SAST, container scanning, code review, and protected branches.
- Check build provenance, artifact signing, deployment approvals, and separation between development and production.
- Inspect CI/CD service accounts and runners for excessive permissions or exposure.
- Validate rollback paths and emergency patch procedures.

Real-Time Signals

- Secrets appear in commits, build logs, artifacts, or issue trackers.
- Branch protection, review, or pipeline checks are disabled.
- A CI runner executes unexpected jobs or reaches sensitive networks.
- A release includes unreviewed dependency or configuration changes.

Response Play

- Rotate exposed secrets and remove them from history where required by policy.
- Preserve pipeline logs, commit details, artifact hashes, and deployment records.
- Disable compromised runners or tokens and review downstream deployments.
- Restore required protections and add regression checks.
- Brief engineering teams with the root cause and a prevention change.

Free/open tooling: Gitleaks, Trivy, Semgrep, Syft, Cosign, OWASP Dependency-Track.

Evidence to save: Repository inventory, scan outputs, pipeline logs, artifact metadata, and remediation commits.

Quality bar: Every production release passes defined security checks with traceable source and artifact evidence.

Skill 51: Database and Storage Inspection

Mission: Protect structured and unstructured data stores from accidental exposure and abusive access.

Inspection Checklist

- Inventory databases, object stores, file shares, data lakes, backups, replicas, and admin tools.
- Review public exposure, network access, encryption, authentication, authorization, audit logging, and retention.
- Identify shared accounts, stale admin grants, weak service account scopes, and unmanaged exports.
- Check query, object access, snapshot, and backup logs for investigation readiness.
- Validate restore and integrity checks for critical datasets.

Real-Time Signals

- A database or bucket becomes publicly reachable or broadly shared.
- Large exports, snapshots, or unusual queries happen outside normal workflows.
- Audit logging is disabled or retention is reduced.
- A privileged database account is used from an unusual host or tool.

Response Play

- Restrict access immediately and preserve audit logs and configuration state.
- Identify affected records, objects, accounts, and time window.
- Rotate credentials and review downstream systems that used the same secrets.
- Validate no unauthorized snapshots, replicas, or exports remain.
- Improve access patterns, logging, and approval workflow.

Free/open tooling: OpenMetadata, Amundsen, Prowler, ScoutSuite, rclone, Wazuh.

Evidence to save: Data store inventory, access review, audit logs, exposure timeline, and remediation proof.

Quality bar: Sensitive data stores are private by default, logged, encrypted, owner-tagged, and restore-tested.

Skill 52: DNS, Certificates, and Trust Services

Mission: Inspect the trust fabric that routes users, validates services, and reveals shadow assets.

Inspection Checklist

- Inventory zones, registrars, authoritative DNS, certificate authorities, certificate transparency, and automation accounts.
- Review domain locks, MFA, DNSSEC where appropriate, expiration, delegation, and administrator access.
- Find dangling records, wildcard records, stale subdomains, weak certificate lifecycle, and unmanaged names.
- Monitor certificate issuance for unexpected domains.
- Validate emergency access to DNS and certificate workflows during incidents.

Real-Time Signals

- A new certificate is issued for an unexpected hostname.
- DNS records change without a deployment or change record.
- A domain, certificate, or registrar account nears expiration or loses MFA.
- Traffic shifts to infrastructure not owned or approved by the organization.

Response Play

- Preserve DNS and registrar audit logs and identify the account used.
- Revert unauthorized records or certificates through approved emergency control.
- Rotate registrar, DNS, and certificate automation credentials if compromise is possible.
- Search for traffic, phishing, or data exposure related to the suspicious name.
- Improve monitoring for certificate transparency and zone drift.

Free/open tooling: crt.sh, Certbot, DNSControl, OctoDNS, Amass, dnstwist.

Evidence to save: Zone inventory, certificate list, registrar settings, change logs, and monitoring alerts.

Quality bar: Domains and certificates are owner-controlled, monitored, MFA-protected, and free of stale trust paths.

Skill 53: Network Segmentation and Zero Trust Checks

Mission: Limit blast radius by making access explicit, monitored, and justified.

Inspection Checklist

- Map segments by business function, data sensitivity, environment, and trust boundary.
- Review firewall rules, security groups, routes, identity-aware policies, and admin pathways.
- Find flat networks, broad any-any rules, legacy exceptions, and unmanaged east-west access.
- Validate that high-value systems require strong identity, device posture, and least-privilege network paths.
- Test segmentation with approved safe checks and owner coordination.

Real-Time Signals

- A host reaches a sensitive segment without expected identity or network control.
- Firewall or security group rules broaden after troubleshooting and are not reverted.
- Lateral movement indicators cross normal service boundaries.
- Temporary exceptions remain open beyond their approved window.

Response Play

- Restrict overbroad paths and preserve rule-change history.
- Confirm application dependencies before removing legacy rules.
- Prioritize segmentation for identity systems, backup systems, admin interfaces, and regulated data.
- Add monitoring for denied and allowed high-risk paths.
- Convert temporary access into workflow-based, expiring rules.

Free/open tooling: NetBox, Open Policy Agent, pfSense, OPNsense, Zeek, Nmap approved profiles.

Evidence to save: Network map, rule review, exception register, validation output, and change records.

Quality bar: Sensitive systems expose only justified paths with owner approval, monitoring, and expiration where needed.

Skill 54: Security Awareness and Human Reporting

Mission: Treat people as sensors and decision makers, not as the weakest link.

Inspection Checklist

- Review reporting channels for phishing, lost devices, suspicious calls, data exposure, and policy questions.
- Measure whether reports receive timely feedback and whether users trust the process.
- Align training with real incidents, role-specific risks, and current business workflows.
- Inspect executive, finance, HR, developer, and support training for tailored scenarios.
- Check that no one is punished for good-faith reporting.

Real-Time Signals

- Users bypass reporting because the process is slow, unclear, or punitive.
- Similar reports spike across teams or regions.
- High-risk roles repeatedly encounter the same social engineering themes.
- Employees share sensitive data through informal workarounds.

Response Play

- Acknowledge reports quickly and tell users what action was taken when possible.
- Escalate clusters of reports into incident triage.
- Convert real examples into short, respectful learning moments.
- Fix broken workflows that push users toward insecure behavior.
- Recognize useful reporting so the culture reinforces early warning.

Free/open tooling: GoPhish for training, Mattermost, TheHive, Formbricks, LimeSurvey, Moodle.

Evidence to save: Report metrics, feedback examples, training plan, role-specific materials, and improvement tickets.

Quality bar: Users report suspicious activity early and receive feedback that improves future decisions.

Skill 55: Physical Security and Device Handling

Mission: Include offices, devices, badges, paper, and visitor processes in cyber inspection.

Inspection Checklist

- Review badge access, visitor logs, server rooms, network closets, desk security, and device storage.
- Check lost-device reporting, hardware disposal, asset labels, screen locks, and sensitive document handling.
- Inspect whether public areas expose network ports, printers, unattended systems, or confidential displays.
- Validate handoff between facilities, HR, IT, and security for terminations and incidents.
- Review physical access logs during cyber incidents that involve local systems.

Real-Time Signals

- A lost laptop, badge, hardware token, or storage device belongs to a sensitive user.
- Physical access logs show unusual entry around a security event.
- Unmanaged devices are connected to internal ports.
- Sensitive paper or screens are visible in public or shared areas.

Response Play

- Revoke badges, certificates, sessions, and device access tied to the event.
- Preserve physical access logs, CCTV references where authorized, and asset records.
- Assess whether credentials, tokens, or data were exposed and rotate accordingly.
- Recover, wipe, or retire affected devices through documented process.
- Improve physical controls and staff guidance based on the incident.

Free/open tooling: Snipe-IT, NetBox, Wazuh, FreeIPA, OnlyOffice, Cryptomator.

Evidence to save: Asset record, badge logs, lost-device report, access revocation proof, and recovery decision.

Quality bar: Physical events that affect cyber risk trigger fast access revocation and evidence preservation.

Skill 56: Real-Time Response Room Operations

Mission: Run serious incidents with clear roles, rhythm, facts, and decisions.

Inspection Checklist

- Define incident commander, technical lead, communications lead, legal/privacy lead, business lead, and scribe roles.
- Prepare response room channels, bridge details, backup communication, access lists, and evidence locations.
- Use an update rhythm: current facts, current risk, actions completed, blockers, decisions needed, next checkpoint.
- Keep one incident log and one decision log to prevent confusion.
- Protect responders from side conversations and duplicate requests.

Real-Time Signals

- Multiple teams act without shared timeline or incident lead.
- Decisions are made verbally but not recorded.
- Executives or business owners lack clear status and repeatedly ask for updates.
- Responders are exhausted, context switching, or missing handoff notes.

Response Play

- Name the incident commander and scribe immediately for major incidents.
- Centralize updates in an approved channel and set the next briefing time.
- Record every material decision with owner, time, evidence, and tradeoff.
- Rotate roles for long incidents and brief incoming responders.
- Close the response room only after recovery, monitoring, and follow-up ownership are clear.

Free/open tooling: TheHive, Mattermost, Matrix/Element, Jitsi, CryptPad, OpenProject.

Evidence to save: Role assignments, incident log, decision log, briefing notes, action tracker, and handoff records.

Quality bar: Major incidents have one command structure, one source of truth, and predictable update cadence.

Skill 57: Post-Incident Review and Improvement

Mission: Turn incidents into durable security improvement without blame theater.

Inspection Checklist

- Review timeline, detection, triage, containment, eradication, recovery, communications, and business impact.
- Separate contributing factors from individual blame.
- Measure what worked, what failed, what was lucky, and what was unknown.
- Assign improvement items to controls, playbooks, detections, training, architecture, and governance.
- Track completion of post-incident actions until evidence shows risk reduction.

Real-Time Signals

- The same incident pattern repeats.
- Post-incident tasks remain open without owners or deadlines.
- Teams disagree about facts because evidence was incomplete.
- Leadership asks for lessons but no budget, priority, or ownership follows.

Response Play

- Hold the review soon after stabilization while facts are fresh.
- Build a timeline from primary evidence and clearly label assumptions.
- Choose a small number of high-leverage improvements with accountable owners.
- Publish an appropriate summary to stakeholders who need to learn from the event.
- Retest the most important fixes through monitoring or exercises.

Free/open tooling: Timesketch, TheHive, OpenProject, Grafana, CryptPad, Draw.io.

Evidence to save: Final timeline, root-cause notes, impact statement, action register, and verification evidence.

Quality bar: Every serious incident produces verified improvements that reduce recurrence or impact.

Skill 58: 90-Day Cyber Inspection Maturity Roadmap

Mission: Turn the book into a realistic first 90 days of defensive improvement.

Inspection Checklist

- Weeks 1-2: confirm scope, asset inventory, identity posture, public exposure, and critical service list.
- Weeks 3-4: close urgent exposure, enable missing logs, verify backups, and review privileged access.
- Weeks 5-6: build incident severity matrix, phishing/BEC playbooks, endpoint triage, and response room process.
- Weeks 7-9: deploy control monitoring for MFA, EDR, logging, backups, cloud exposure, and critical vulnerabilities.
- Weeks 10-13: run tabletop exercises, validate detections, fix gaps, and brief leadership on risk and next investment.

Real-Time Signals

- The organization cannot name critical assets or owners.
- Core controls have unknown coverage or manual-only reporting.
- Incident responders lack authority, evidence, or tested playbooks.
- Leadership sees cyber work as tasks rather than risk decisions.

Response Play

- Start with visibility and ownership before advanced tools.
- Fix internet-facing and privileged risks early.
- Create a lightweight daily/weekly operating cadence for remediation and response readiness.
- Use free and open-source tools where they fit, but assign owners for maintenance.
- End the 90 days with tested playbooks, metrics, and a prioritized roadmap.

Free/open tooling: Wazuh, TheHive, Velociraptor, Prowler, Greenbone CE, Grafana.

Evidence to save: 90-day plan, weekly milestones, control dashboard, tabletop report, and leadership briefing.

Quality bar: After 90 days, the organization has known assets, monitored core controls, and practiced response workflows.

Appendix A: Severity Matrix

Severity	Definition	Response target
SEV-1 Crisis	Active compromise or outage affecting critical services, regulated data, privileged control, or public trust.	Immediate command structure; updates every 30-60 minutes.
SEV-2 High	Likely compromise, exposed critical vulnerability, or limited data/security control impact.	Incident lead assigned; same-day containment plan.
SEV-3 Medium	Suspicious activity or confirmed weakness with bounded impact and no active attacker evidence.	Owner ticket, monitoring, and remediation deadline.
SEV-4 Low	Policy drift, low-risk finding, or informational weakness.	Backlog or scheduled improvement.

Appendix B: First-Hour Checklist

- Name the incident lead and scribe.
- Open a timestamped incident log and decision log.
- Preserve initial alert, logs, screenshots, affected identities, and affected assets.
- Assign initial severity and next reassessment time.
- Choose containment action and approval path.
- Notify business, legal/privacy, communications, and leadership according to severity.
- Set the next briefing time and stabilize the response channel.

Appendix C: Inspection Report Template

Section	What to include
Executive summary	Business risk, top findings, trend, and decisions requested.
Scope	Authorized assets, dates, exclusions, owners, and constraints.
Method	Tools, data sources, inspection depth, and safety limits.
Findings	Risk, evidence, affected assets, root cause, owner, and remediation.
Control coverage	MFA, EDR, logging, backups, patching, vulnerability, and cloud posture.
Incident readiness	Playbooks, contacts, evidence sources, response gaps, and recovery proof.
Roadmap	30/60/90 day actions with owners, cost, and risk reduction.

Appendix D: Minimum Daily Watchlist

- New public assets, certificates, DNS records, or cloud resources.
- Privileged role changes, suspicious sign-ins, and MFA anomalies.
- Critical exposed vulnerabilities and emergency vendor advisories.
- EDR health drops, tamper alerts, and suspicious process chains.
- Backup failures, retention changes, and restore-test status.
- High-severity SIEM alerts and untriaged user reports.

- SaaS sharing spikes, OAuth grants, and sensitive data exports.

Closing Note

Security improves when the same few disciplines become routine: know what exists, know who owns it, watch the controls that matter, respond quickly with evidence, and turn every incident into a stronger system. Use the fifty skills as a living operating manual, then adapt the checklists to your actual assets, people, and risk.