Overview & outcomes

Certified Implementation Specialist - Security Incident Response

KNOWLEDGE CHEATSHEET

RESPONSE OUTCOMES

Goals Business impact → **Team** Ownership → **Process** Consistency → **KPIs** Results

01 Security Incident Response Overview and Data Visualization 15%

Purpose and response team

- **Security Incident Response (SIR)** coordinates investigation and remediation to minimize the business impact of security incidents and imminent threats.
- **Security incident response team** duties include monitoring alerts, triage, response coordination, exercises, training and lessons learned. Everyone can report suspected incidents.
- **Implementation goals** start with customer outcomes, current processes and willingness to change. Agree ownership, escalation paths and measurable success criteria before automating.
- **Process maturity** grows through repeatable procedures, trained responders and automation of well-understood work. Dedicated coordination can shorten recovery and reduce its cost.

Records, dashboards and outcomes

- **Security Incident [sn_si_incident]** is the core response record. **Response Task [sn_si_task]** delegates a specific activity while retaining incident context.
- **CMDB relationships** connect affected configuration items (CIs) to business services. This context helps responders assess the impact of a technical compromise.
- **Analysts** need actionable incident detail; **security managers** need workload and response trends; **CIOs/CISOs** need business risk and overall security outcomes.
- **KPIs** should measure desired results: time to contain, time to remediate, backlog and recurrence. Define start/stop events consistently before comparing teams.
- **Leading indicators** track activities expected to improve results, such as exercise completion. **Lagging indicators** measure achieved outcomes, such as incident duration.

Intake & intelligence

Certified Implementation Specialist - Security Incident Response

KNOWLEDGE CHEATSHEET

THREAT CONTEXT

Intake Reports & tools → **Observables** Facts → **Intelligence** Context → **Response** Coordinated work

02 Security Incident Creation and Threat Intelligence 14%

Incident intake and catalog

- **Manual intake** includes the security incident form and Security Incident Catalog record producers. **Automated intake** includes integrations and inbound email actions.
- **Create Security Incident** on an IT incident raises a separate security response record. Preserve the relationship and apply security access controls to the resulting record.
- **Security Incident Catalog** exposes reporting choices suited to the customer. Record producers collect structured information; catalog configuration controls the choices presented.
- **Inbound email actions** evaluate conditions and scripts against received email. Parsing extracts values; field transforms map them into appropriate incident fields.

Observables, intelligence and ATT&CK

- **Observable** means a measurable fact such as an IP address, URL, domain or file hash. An **indicator of compromise (IoC)** adds threat context; an observable alone does not prove malicious activity.
- **Enrichment** adds reputation, ownership, endpoint details or threat context. **Sightings search** finds occurrences of an observable across connected sources to assess scope.
- **MITRE ATT&CK** organizes adversary behavior: tactics describe objectives, techniques describe methods, and sub-techniques add detail. Map observed evidence to behavior during investigation.
- **ATT&CK audiences** include analysts, threat-intelligence administrators and security leadership. The same mapped behavior supports investigation, configuration and coverage reporting.
- **MISP** exchanges structured threat intelligence. Its events group related intelligence, attributes hold details, tags classify information, and galaxies add contextual relationships.
- **MISP integration** can share incident observables as event attributes, update tags or galaxies, and associate extracted ATT&CK information with an incident. Apply sharing restrictions before publishing.

Major security incident coordination

- **Major security incident (MSI)** provides coordinated management for a significant event. Link related security incidents as **children** of the major incident.
- **Rollup framework** brings selected information from linked records into the major incident view. Child incident work remains associated with its own response tasks.

Intake & intelligence / Integrations

Certified Implementation Specialist - Security Incident Response

KNOWLEDGE CHEATSHEET

CONNECTED RESPONSE

Configure Connections → **Enrich** Evidence → **Respond** Actions → **Verify** Results

- **Major incident workspace** supports a manager coordinating status, tasks and communications across security, IT and business groups. Connected chat channels can support collaboration.
- **Summary reporting** communicates impact, response progress, decisions and remaining work. Incremental summaries focus on changes since the prior update; restrict report configuration to authorized workspace administrators.

03 Security Incident and Threat Intelligence Integrations 14%

Integration setup and APIs

- **Integration Configurations** is a starting point for prebuilt integrations. Check the **ServiceNow Store** for certified applications; assess shared community assets separately for support and suitability.
- **Integration methods** include REST and SOAP web services and directory integration through LDAP. Import and transform mechanisms map external fields into ServiceNow records.
- **REST methods:** GET reads, POST creates, PATCH partially updates, and DELETE removes a record. Endpoint authorization and record ACLs still apply.
- **REST API Explorer** helps construct and test API requests. Its **rest_api_explorer** role enables the tool; the test identity also needs permission for the target operation.
- **IntegrationHub** extends flows with reusable integration actions packaged as **spokes**. Configure connections, credentials and required capabilities before executing actions.
- **Automation entitlement** and installed plugins determine available capabilities. Confirm the contracted package and integration prerequisites when planning orchestration.

Investigation and response capabilities

- **Get Running Processes** retrieves endpoint processes. **Get Network Statistics** retrieves active network connections; these are enrichment actions for investigation.
- **Isolate Host** restricts endpoint communications. **Remove isolation** reverses that restriction. Confirm the endpoint, approval and business impact before containment.
- **Block actions** request enforcement in a connected control. **Watchlists** distribute observables for monitoring. Check execution results before treating the action as successful.
- **Microsoft Defender for Endpoint** supports host enrichment, enterprise searches and response actions such as isolation, antivirus scans and file quarantine through the configured integration.
- **CrowdStrike Falcon Sandbox** analyzes submitted artifacts; supported report enrichment can extract IoCs and ATT&CK techniques. A sandbox finding is evidence to evaluate in context.

Response management

Certified Implementation Specialist - Security Incident Response

KNOWLEDGE CHEATSHEET

CONTROL THE RESPONSE

- **Roles** — Authorized access
- **Assignment** — Suitable responders
- **Process** — State transitions
- **Tags** — Sharing policy

04 Security Incident Response Management 15%

Roles and separation of duties

- **sn_si** is the SIR application scope. **sn_si.admin** administers SIR, including territories and skills; platform administration and security-data administration are separate responsibilities.
- **sn_si.analyst** manages incidents. **sn_si.basic** provides underlying operational access; **sn_si.read** supplies read access; **sn_si.ciso** supports the CISO dashboard.
- **sn_si.external** supports collaboration subject to group and record access rules. Give non-SOC responders the access required for their assigned work and test visibility explicitly.
- **sn_si.integration_user** supports external creation and updates. Use a dedicated integration identity and grant only the permissions needed by its ingestion path.
- **Separation of duties** protects sensitive investigations and limits who can grant security roles. Group membership can convey inherited roles, so review both direct and group-based access.

Assignment, escalation and process

- **Assignment automation** matches incident needs to suitable responders using skills, territories or locations, time zones and availability. Maintain accurate responder and CI-location data.
- **Escalation rules** define when an incident needs additional attention and who receives it. Align conditions and notifications with severity, ownership and response targets.
- **Process Definition** controls the available incident states and transitions; **Process Selection** chooses the process to apply. Making a definition active is distinct from selecting it.
- **NIST Stateful** is the default process definition. Its available states depend on the current state; open definitions allow more flexible state selection.
- **Lifecycle:** Draft gathers information; Analysis investigates; Contain limits spread; Eradicate removes the cause; Recover validates operations; Review captures learning; Closed records completion.
- **Custom process definitions** combine a definition record with supporting scripted logic. Validate permitted transitions and automation behavior before applying them to active incidents.

Response management / Risk & review

Certified Implementation Specialist - Security Incident Response

KNOWLEDGE CHEATSHEET

PRIORITIZE AND LEARN

Context Business impact → **Calculate** Risk weights → **Review** Lessons learned → **Close** Record outcome

Security tags and information sharing

- **Security tags** attach classification metadata to supported security records, including incidents, response tasks, observables and IoCs. Groups organize related tags and can control multiple selection.
- **Tag groups** include Traffic Light Protocol, enrichment allow/deny lists and custom metatags. An allow-list classification affects analysis policy; it is not proof that an artifact is safe.
- **Traffic Light Protocol (TLP)** expresses how widely threat information may be shared. RED is tightly limited to recipients; AMBER limits distribution on a need-to-know basis; GREEN supports sharing within a defined community.
- **Restricted access** must be configured and enforced. Security tags can specify read/write roles when restriction is enabled; a descriptive label alone is not an authorization decision.

05 Risk Calculations and Post Incident Response 12%

Events, severity and calculators

- **Event** is an observable occurrence. An **alert** signals a condition needing attention; a **security incident** tracks investigation and response. Not every event warrants an incident.
- **Event Management [em_event]** holds incoming events used by supported alert and incident integrations. It differs from platform system events used for notifications and background processing.
- **External event data** should include a meaningful description, security classification and a node identifier that can resolve the affected CI, such as its name, IP address or sys_id.
- **Severity** reflects the seriousness of the incident, informed by affected assets and business services. **Priority** orders response work; **risk score** combines configured factors to support triage.
- **Calculators** set field values when conditions match. Calculator groups and their members have an execution order; within a group, the first matching calculator runs.
- **Business impact** connects technical findings to business value. Accurate CI, service and affected-user records improve the relevance of automated criticality and severity calculations.

Risk scores, review and closure

- **Risk Score Configuration** maps factor values to numeric weights. The arithmetic-mean calculation averages applicable configured weights; it does not simply add field choice numbers.
- **Business impact and priority** are inputs to the weight-based risk model; related user and service context can contribute. Change configuration weights to reflect organizational priorities.
- **Post-incident review (PIR)** captures lessons, process gaps and improvements. Use it for learning, organizational policy and compliance rather than blame.

Risk & review / Automation

Certified Implementation Specialist - Security Incident Response

KNOWLEDGE CHEATSHEET

PHISHING RESPONSE PIPELINE

Email — Report suspicious mail → **Phishing record** — Parse & classify → **Incident** — Transform & group → **Playbook** — Enrich & respond

- **Review evidence** can include questionnaires, key incident fields, activity history and relevant attachments. Assign follow-up actions with owners to turn findings into improvements.
- **Closure** requires appropriate closure information. Outstanding required PIR assessments must be completed or appropriately canceled; review active response work before closing.
- **PIR report** can be generated as a PDF attachment on the incident. Creating a draft knowledge article is a separate option for reusing lessons in future investigations.

06 Automation and Standard Processes 30%

Flows, actions and execution

- **Flow** combines a trigger with a sequence of actions and logic. Record creation or updates and schedules are common triggers; match trigger conditions to the intended security incidents.
- **Action** performs a reusable operation. A **subflow** packages reusable steps with defined inputs and outputs and is called by another flow or subflow.
- **Flow logic** includes conditions, For Each iteration and waiting for a condition. Design waits and branches so that incidents can progress when tasks finish or outcomes change.
- **Data pills** expose trigger records and prior action outputs for field mapping. Use the correct record or value type when passing information between steps.
- **Execution Details** shows action inputs, outputs and failures during testing. Validate trigger scope, permissions, credentials and error paths with representative incidents.
- **Security Operations Spoke** supplies security-related actions. Install and configure the required spoke before expecting its actions to appear in Flow Designer.

Playbooks, response tasks and runbooks

- **Playbook** coordinates the planned response for a threat scenario. Use a flow to create response tasks, collect outcomes and advance work through the incident lifecycle.
- **Automatic selection** depends on matching trigger conditions. **Analyst selection** uses the configured selection list; these are separate ways to start a playbook.
- **Selected Playbook list:** locate the Flow Designer playbook in **sys_hub_flow** and apply the **sir_playbook** tag so it is available for analyst selection.
- **Runbook** associates published knowledge instructions with matching response tasks. The knowledge article contains the steps; the flow controls task creation and sequencing.

Automation

Certified Implementation Specialist - Security Incident Response

KNOWLEDGE CHEATSHEET

PHISHING RESPONSE PIPELINE

Email — Report suspicious mail → **Phishing record** — Parse & classify → **Incident** — Transform & group → **Playbook** — Enrich & respond

- **Runbook conditions** can match the task short description. Keep the flow-created response task description aligned with that condition so the intended article appears.
- **Task outcomes** can drive branching, including yes/no decisions. Configure the response action outcome fields and wait for the relevant result before advancing dependent work.

User-reported phishing

- **Reporting mailbox** forwards suspicious messages to the platform ingestion address. Preserve the original message and attachment context so automated parsing can examine it.
- **User-reported phishing** separates the incoming email record from the security incident. Inbound processing creates a **Security Incident Phishing Email [sn_si_phishing_email]** record.
- **Transform Phishing Email to Security Incident** is the flow connecting phishing email processing to incident creation. Activate the appropriate configured flow and verify its trigger during setup.
- **Ingestion rules** control processing decisions; **duplication rules** detect repeated or related submissions. Aggregation reduces duplicate incident work while retaining reports.
- **Extracted observables** can include body URLs, domains and IP addresses, header IP addresses, and attachment names or hashes. Reporter identity and processing state are metadata.
- **Automated phishing response** can enrich observables, search for related messages and endpoints, and initiate containment through supported integrations. Review uncertain findings and scope before remediation.