Incident Response Guide for “Each1Teach1 Tech” Production SOC

1. Scope and purpose

Scope:

This Incident Response Guide covers the procedures and processes for handling and responding to security incidents within the SOC.

Purpose:

To detect, analyze, contain, eradicate, and recover from security incidents effectively and efficiently. To minimize the impact of security incidents on organizational assets and data. To ensure compliance with regulatory requirements and internal policies.

2. Roles and responsibilities

a. *SOC Manager:*

Oversee and coordinate incident response activities.

Approve incident response plans and procedures.

Ensure staff training and readiness.

b. *Cybersecurity analyst / Incident Responder:*

Detects and analyzes security events.

Create and manage incident tickets.

Implement containment and eradication measures.

Collaborate with external entities if required.

c. *IT Security Analyst (DevSecOps):*

Assist in incident detection and analysis.

Provide support for containment and eradication measures.

Document incident details and actions taken.

d. *Network Administrator:*

Assist in analyzing network-related security incidents.

Implement network-based containment measures.

Collaborate with Incident Responders and IT Security Analysts.

e. DevOps:

DevOps plays a pivotal role in a Security Operations Center (SOC) environment by seamlessly integrating security practices throughout the software development lifecycle. Through Continuous Security Integration (CSI), automated testing, and Infrastructure as Code (IaC), DevOps ensures the early identification of vulnerabilities, standardized security configurations, and automated compliance checks. Collaborating with security teams, DevOps fosters a DevSecOps culture, promoting shared responsibility for security across teams. Its involvement in incident response and monitoring includes the integration with Security Information and Event Management (SIEM) systems and the development of automated incident response playbooks. DevOps addresses container security, orchestrates secure container platforms, and contributes to ongoing security training for teams. By establishing feedback loops, participating in post-incident reviews, and automating patch management and security configurations, DevOps actively contributes to a more secure and resilient organizational infrastructure.

f. Legal and Compliance Officer:

Ensure compliance with legal and regulatory requirements.

Provide guidance on incident reporting and documentation.

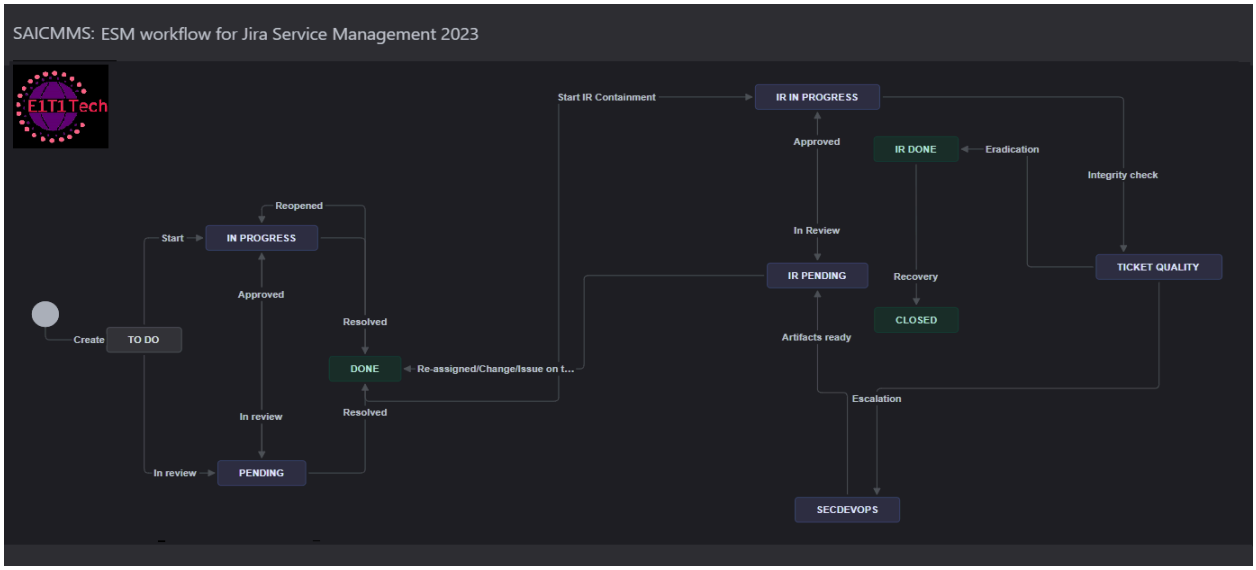
3. Guideline statement:

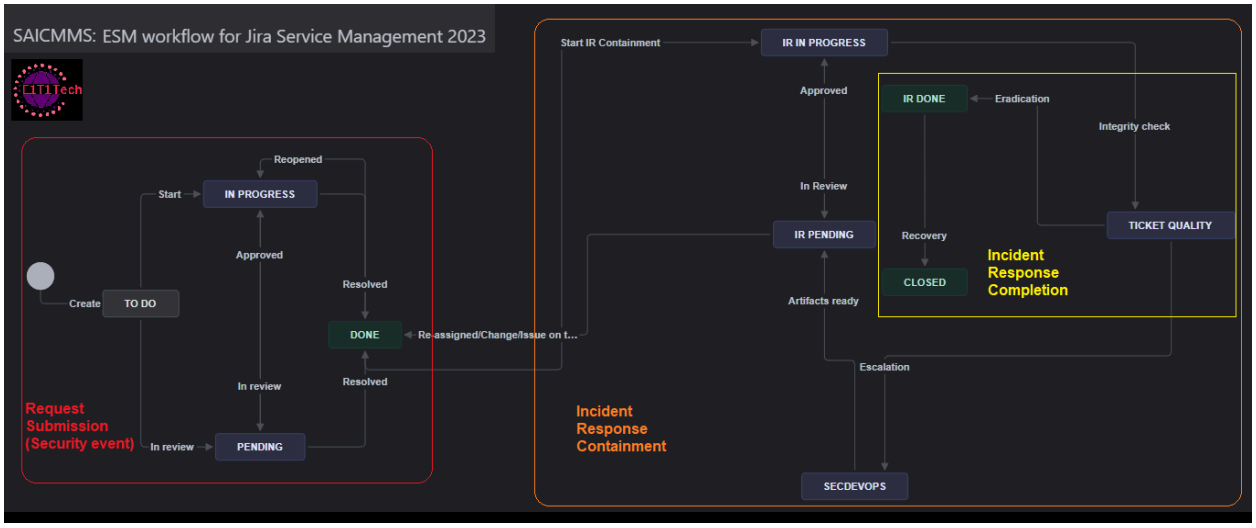
All security events, anomalies, and incidents must be promptly reported to the SOC for assessment and appropriate action.

The Incident Response Team will follow documented procedures to categorize, prioritize, and respond to incidents.

Regular training and drills will be conducted to ensure the readiness of the Incident Response Team, e.g. Tabletop exercise and scenarios.

Workflow:





4. REQUEST/SUBMIT SECURITY EVENT:

Create Ticket:

Incident Responder creates a ticket for reported security events.

Ticket status: "To Do."

Start or In Review:

If the incident is confirmed, change the ticket status to "In Progress."

If further analysis is required, change the ticket status to "Pending Review."

Pending Review:

If approved, change the ticket status back to "In Progress."

If not approved, mark the ticket as Pending or In progress.

Else the ticket is resolved and DONE.

The ticket may be marked as resolved if the review is satisfactory.

If approved, mark the ticket as resolved ("Done").

Reopened:

If flagged for an error, the ticket goes back to "In Progress."

5. RESPOND TO TICKET: (this part needs a lot of work)

Incident Responder and team take appropriate actions based on incident type.

Implement containment, eradication, and recovery measures.

Document all actions taken.

Verification- Verify that the raised ticket (artifacts, etc) corresponds with the alert in the SIEM tool.

Investigate- Investigate the underlying cause of the incident. Also validate if Source IP is malicious via (Malware Analyzer Ex.VirusTotal , Suricata or Abuse IPDB)

Determine- Determine the tactics (credential access, lateral movement, discovery, reconnaissance) threat actors used to gather the techniques (Ex. Password Guessing, Brute Force etc). In a nutshell we want to understand how the asset was breached.

Respond- Respond appropriately to the alert based on the tactics and techniques of the threat actors. Make sure the demographics (response time, _id, pre.decoder time, source ip address, agent id, etc) are correct and correspond with the artifacts within the raised ticket. Also attach artifacts, and make recommendations based on findings.

Example:

Security Event:

JID:SAICMMS:

Respond Date:

Reported Date:

Target IP Address:

Source IP Address:

Agent.id:

_id:

Soc analyst:

Manager/hostname:

Check Mitre ID:

First find time stamped:

Last find time stamped:

Incident Description:

Event of interest:

Evidence:

Response/Actions:

Verified User:

Priority:

Recommendations:

Follow-Up Actions:

Review:

Communication:

Legal: Consider any legal implications or requirements related to the incident.

Resolution and Closure:

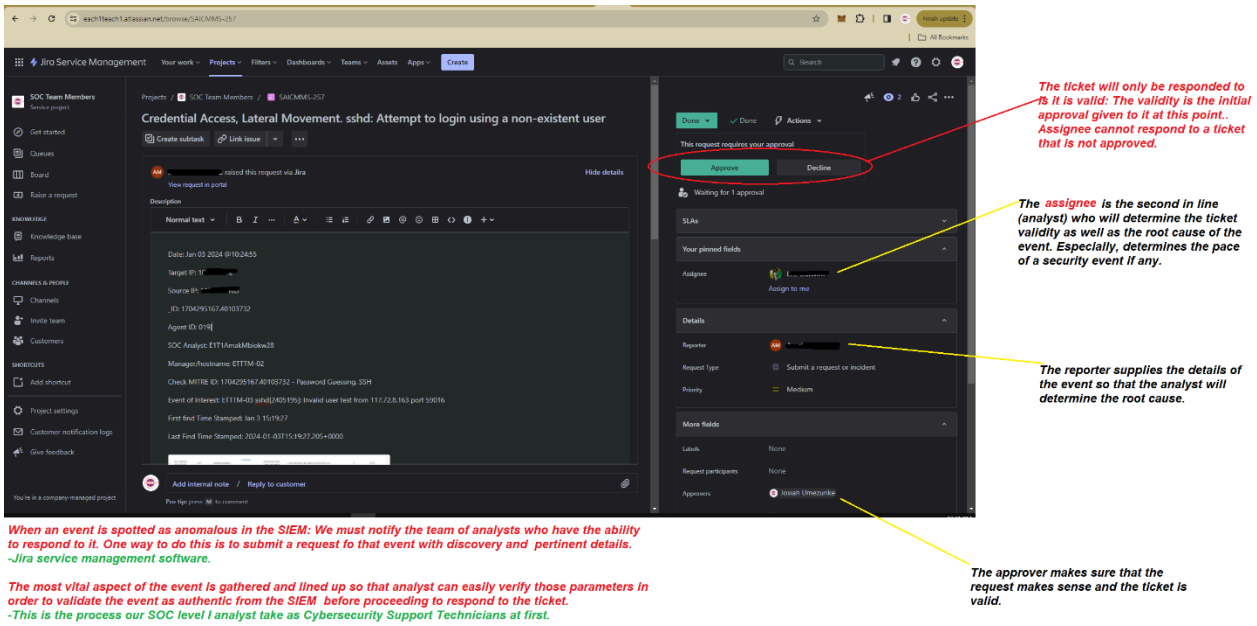
Incident Review and Lessons Learned:

Additional Comments:

ESM Jira service management software

We use Jira service management software.

Navigating Jira ticket:-



Summary: This gives you the highlight of the security event.

Description: Security details verification, validation covering the incident response phases

Approver: This is the team member with administrative rights capable of verifying ticket quality and the validity of the incident making sure that the incident is done according to the procedure provided.

Assignee: This is the team member that the approver or the reporter assigns the ticket for incident response.

Reporter: This is the security analyst or team member who monitored and detected the security event or incident. A reporter can not respond to a ticket they raised.

6. Operational considerations:

Regularly update incident response plans based on lessons learned.

Conduct post-incident reviews to identify areas for improvement.

Collaborate with external incident response teams and authorities when necessary.

Ensure all staff members are aware of their roles and responsibilities through ongoing training.

Conclusion:

This Incident Response Guide aims to provide a structured approach to handling security incidents within the SOC, fostering efficiency, collaboration, and continuous improvement.

Glossary of SOC & Incident Response Terms

A

Alert – A notification of suspicious activity (like a security guard's walkie-talkie reporting an open door).

Artifacts – Evidence left by an attacker (e.g., malware files, logs = fingerprints or broken locks).

ATT&CK Framework (MITRE) – A catalog of attacker tactics/techniques (like a burglar's playbook).

B

Brute Force Attack – Repeated login attempts to guess passwords (like a thief trying every key on a ring).

Containment – Isolating a threat to prevent spread (like locking a room where an intruder is hiding).

C

CSI (Continuous Security Integration) – Automating security checks in DevOps (like installing alarms during construction).

Compliance – Following laws/regulations (like a guard ensuring fire codes are met).

D

DevSecOps – Integrating security into DevOps (like building security cameras into a new facility's design).

Digital Perimeter – The boundary of a network (like a building's fences and gates).

E

EDR (Endpoint Detection & Response) – Tools to monitor devices for threats (like patrolling guards with bodycams).

Eradication – Removing a threat completely (like cleaning up after a break-in).

F

False Positive – A benign event flagged as malicious (like a guard mistaking a cat for an intruder).

I

IaC (Infrastructure as Code) – Managing systems via code (like blueprints for a building's security system).

Incident Response (IR) – The process of handling security breaches (like guards responding to an alarm).

J

Jira – Ticketing system for tracking incidents (like a guard's incident logbook).

L

Lateral Movement – An attacker moving through a network (like a thief exploring different rooms).

M

Malware – Malicious software (like a burglar's lockpick).

MITRE ATT&CK – A framework of attacker behaviors (see **ATT&CK**).

P

Playbook – Step-by-step response procedures (like a guard's manual for handling emergencies).

Post-Incident Review – Analyzing an incident to improve (like a guard debrief after a break-in).

R

Reconnaissance – Attackers researching targets (like a thief casing a building).

S

SIEM (Security Information & Event Management) – Centralized logging/alerting (like all security cameras feeding to one monitor).

SOC (Security Operations Center) – The team/tools monitoring threats (like a guard post).

T

Threat Actor – An attacker (like a burglar).

Ticket – A record of an incident (like a guard's written report).

V

VirusTotal – A tool to analyze suspicious files/URLs (like a guard running a background check).

Z

Zero-Day Exploit – A vulnerability with no known fix (like a thief using a never-seen-before trick).

Incident Response Guide 2024