Deontae Carter, Ethan Brock, Emiliano Ceja, Jordan Marshall, Sierra Maldonado

Table of Contents

Deontae Carter, Ethan Brock, Emiliano Ceja, Jordan Marshall, Sierra Maldonado

Security Incident Plan SOP

Purpose:

The purpose of this Security Incident Plan Standard Operating Procedure (SOP) is to outline the steps to be followed in the event of a security incident. It provides guidelines for detecting, responding to, and mitigating security breaches effectively. This SOP ensures compliance with relevant security policies and standards.

Scope:

This SOP applies to all employees, contractors, and stakeholders responsible for the security of the organization's information systems.
Responsibilities:

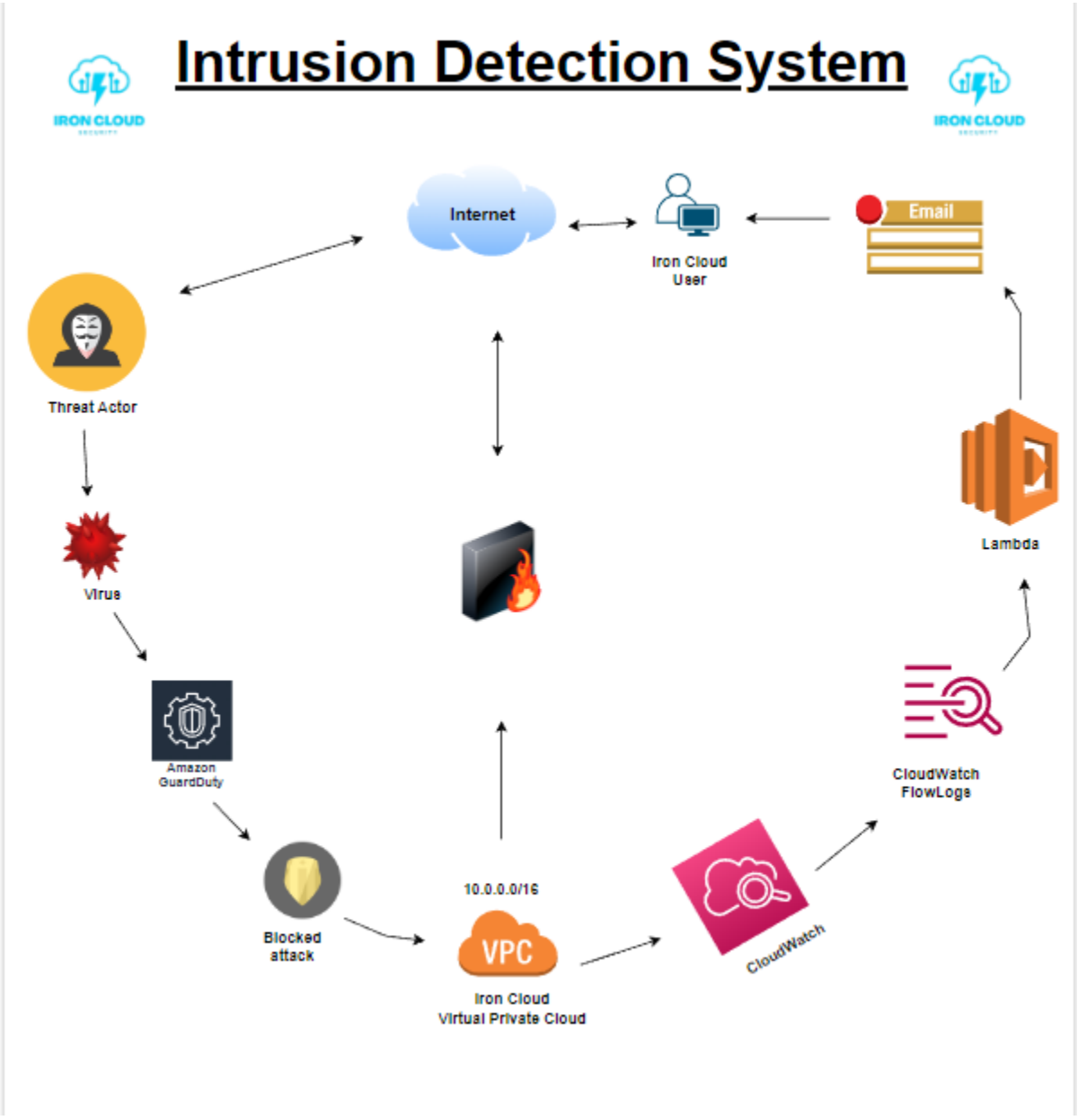
- Incident Response Team (IRT): Coordinate and manage the response to security incidents.
- IT Department: Implement and maintain security controls, monitoring tools, and system configurations.
- Security Department: Conduct regular security assessments, vulnerability scanning, and implement security awareness programs.

Prerequisites:

- Familiarity with security controls, monitoring tools, and incident response procedures.
- Access to relevant systems, documentation, and incident reporting channels.

Procedure:

Flow Chart:

1. 

Incident Detection and Reporting:

2. 2.1 Security Monitoring Tools:
    - Intrusion Detection Systems (IDS)
    - Security Information and Event Management (SIEM) solutions

Log analysis tools

- 2.2 Event Triggers:
- Unauthorized access attempts
- Unusual network traffic patterns
- Anomalies in user behavior
- System crashes or unavailability

Unusual log entries

- 2.3 Incident Reporting:
- Document incident details
- Assign unique incident reference number
- Assign incident owner from the Incident Response Team

Incident Response Process:

3. 3.1 Incident Identification and Classification:

Review incident details and classify based on severity and impact.

- 3.2 Incident Containment:

Take immediate action to isolate affected systems and limit further damage.

- 3.3 Incident Investigation:

Conduct a thorough investigation to determine the root cause and extent of the incident.

- 3.4 Incident Mitigation and Recovery:

Develop and implement a mitigation plan to restore affected systems and eliminate vulnerabilities.

- 3.5 Incident Communication:

Communicate updates and progress to relevant stakeholders.

- 3.6 Post-Incident Analysis and Lessons Learned:
- Conduct a post-incident analysis to identify areas for improvement and update security controls and procedures.

References:

- Ethan Denny’s SOP Template
- Chat GPT Assistance

Definitions:

- Policy: Broad, overarching guidance explaining the "why" behind actions.
- SOP: Detailed documentation explaining the "what, when, why" for specific procedures.
- Work Instructions: Step-by-step directions explaining the "how" for a particular task.

Revision History:

5/15/2023 -- "Security Incident Plan SOP" created by Emilio Ceja