Incident Response Lab Environment Setup and Playbook Development Project

Title: Ransomware Attack Simulation Targeting Confidential Football Play Data ($100M)

---

1. Project Concept

Objective:

Design and build an isolated lab environment that simulates a simple organizational network modeled after a professional football team. The primary goal is to simulate a ransomware attack targeting the confidentiality of digital football playbooks worth $100 million and to develop a detailed, standardized incident response playbook.

---

2. Lab Environment Design

2.1 Network Architecture (10.0.0.0/24)

```
┌──────────────────────────────────────────────────────────────
─┐
│                ISOLATED LAB NETWORK               │
│                 (10.0.0.0/24)                 │
├──────────────────────────────────────────────────────────────
─┤
│ Firewall (pfSense): 10.0.0.1                        │
│ Domain Controller (DC01): Windows Server, 10.0.0.10       │
│ File Server (FS01): Windows Server, 10.0.0.20            │
│ Web Server (WEB01): Linux, 10.0.0.30                 │
│ Mail Server (MAIL01): Linux, 10.0.0.40                │
│ Workstations (WS01/WS02): Windows 10, 10.0.0.101/102       │
│ SIEM (SIEM01): Linux, 10.0.0.50                    │
│ Vulnerability Scanner (VULN01): Kali Linux, 10.0.0.60      │
│ Attacker VM (ATTACKER): Kali Linux, 10.0.0.100           │
```

```
└──────────────────────────────────────────────────────────────────
─┘
```

2.2 Software Stack

- **SIEM Tools**: ELK Stack, Wazuh
- **Email & Web**: Postfix, Apache, DVWA
- **Endpoint Security**: Sysmon, Group Policy Audit
- **Attack Tools**: Metasploit, SET, custom ransomware binary

---

3. Threat Scenario

3.1 Description

A threat actor gains access to the admin workstation (WS02) via RDP brute force and deploys ransomware to encrypt all contents of the File Server (FS01), which houses the organization's most valuable asset: the digital football playbook repository. The attacker demands $10M ransom in exchange for the decryption key.

3.2 Objectives

- Breach confidentiality
- Encrypt data and disrupt operations
- Demand ransom for decryption

---

4. Incident Response Playbook

4.1 Phase 1: Preparation

- Define roles: IR Lead, Forensic Analyst, Comms, Legal
- Test backups and validate access to clean restore points
- Train staff on ransomware awareness
- Deploy detection signatures for encryption and C2 traffic

4.2 Phase 2: Detection & Analysis

- **Indicators**:
    - File extensions changed to `.playlock`
    - `README_LOCKED.txt` ransom note

    - CPU spike on FS01
- **Initial Response**:
    - SIEM alert from FS01
    - Verify through event logs and Sysmon

4.3 Phase 3: Containment

- Disconnect FS01 and WS02 from network
- Terminate attacker session
- Disable affected domain accounts
- Block known malicious IPs and domains

4.4 Phase 4: Eradication

- Remove ransomware binaries and scheduled tasks
- Restore system configurations
- Patch exploited vulnerabilities (e.g., RDP exposure)

4.5 Phase 5: Recovery

- Restore FS01 from secure backup
- Confirm data integrity and functionality
- Rejoin systems to network
- Re-enable users with strong credentials

4.6 Phase 6: Post-Incident

- Conduct lessons-learned session
- Update IR documentation
- Train users based on the findings
- Integrate scenario into regular tabletop exercises

---

5. Testing and Validation

5.1 Tabletop Exercise

- Walkthrough simulation of detection-to-recovery
- Evaluate team communication and technical effectiveness

5.2 Live Simulation

- Deploy ransomware in isolated VM

- Observe detection via SIEM
- Execute full containment and restore procedures

---

6. Outcome and Metrics

Metric	Target
MTTD (Detection)	< 15 minutes
MTTR (Recovery)	< 24 hours
File Recovery Accuracy	100%
Team Training Completion	100%
IR Plan Updates	Within 72 hours

---

7. Strategic Impact

- Safeguards high-value sports intellectual property
- Demonstrates cyber resilience capabilities
- Aligns with NIST 800-61 and ISO/IEC 27035 standards
- Enhances stakeholder and fan trust in security posture

---

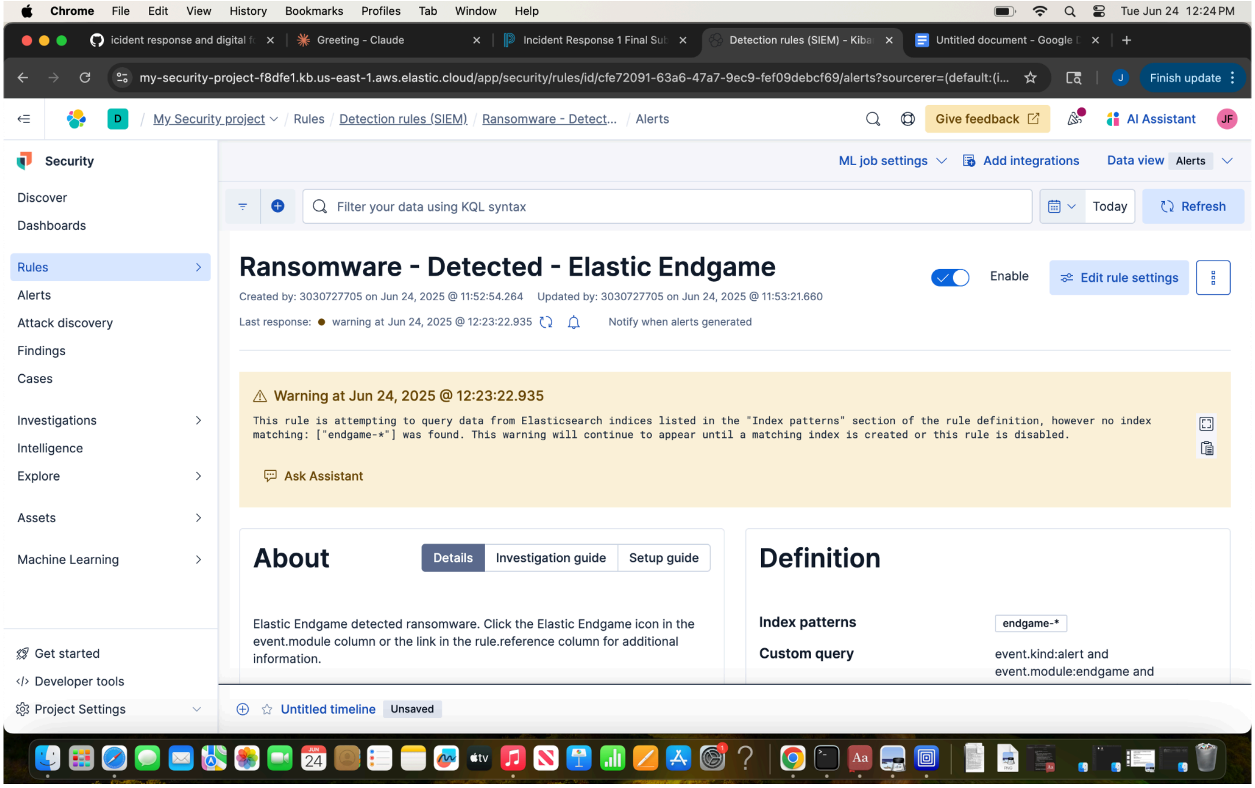
8. Deliverables

- Fully configured lab environment
- Network diagrams and system baselines
- End-to-end incident response playbook
- Recovery validation reports
- Training completion records

---

9. Conclusion

This project equips teams with the skills, tools, and framework necessary to detect, contain, and recover from a high-stakes ransomware incident. By focusing on the confidentiality of digital football playbooks, it demonstrates the real-world business impact of cyberattacks and underscores the importance of proactive incident response readiness.



my-security-project-f8dfe1.kb.us-east-1.aws.elastic.cloud/app/security/rules/id/cfe72091-63a6-47a7-9ec9-fef09debcf69/alerts?sourcerer=(default:(i...

Ransomware - Detected - Elastic Endgame

Created by: 3030727705 on Jun 24, 2025 @ 11:52:54.264 Updated by: 3030727705 on Jun 24, 2025 @ 11:53:21.660

Last response: ● warning at Jun 24, 2025 @ 12:23:22.935 Notify when alerts generated

Warning at Jun 24, 2025 @ 12:23:22.935

```
This rule is attempting to query data from Elasticsearch indices listed in the "Index patterns" section of the rule definition, however no index
matching: ["endgame-*"] was found. This warning will continue to appear until a matching index is created or this rule is disabled.
```

About

Elastic Endgame detected ransomware. Click the Elastic Endgame icon in the event.module column or the link in the rule.reference column for additional information.

Definition

Index patterns endgame-*

Custom query event.kind:alert and event.module:endgame and