Activity 3: SOC Analyst Simulation

SentinelAI Response Cards (Grades 9-12)

These cards simulate SentinelAI SOAR platform responses for the SOC Analyst Simulation. Use them when live AI access isn't available—teams can draw cards at decision points during the incident response.

> **For Instructors**
>
> **How to use:**
> - Distribute cards at Phase 1 (Initial Triage), Phase 2 (Analysis), and Phase 3 (Response)
> - Cards reflect authentic SOAR platform output with explicit limitation notices
> - Teams should document how AI analysis informed—but didn't determine—their decisions
>
> **The goal:** Students experience enterprise-grade AI security analysis while recognizing that human judgment drives all critical decisions.

SentinelAI Analysis Reports

Initial Triage Report

SentinelAI Analysis Report #7291-A

Classification: CRITICAL **Confidence:** 94%

Pattern Analysis:

Lateral movement pattern indicates credential-based attack. Service account `svc_backup` shows authentication anomaly:

- Normal operation: 02:00-03:00 AM
- Current activity: 06:58-07:12 AM
- Statistical deviation: 99.7th percentile

Attack Chain Mapping (MITRE ATT&CK):

```
Initial Access (T1566.001) → Execution (T1204.002) →
Persistence (T1547.001) → Credential Access (T1078.002) →
Lateral Movement (T1021.002) → Collection (T1074.001) →
Command and Control (T1071.001)
```

Risk Assessment:

- 94% probability: Active compromise in progress
- Estimated impact if delayed 2 hours: 800GB additional data staging
- Potential OT system access via HVAC-CONTROLLER-01

LIMITATION NOTICE:

This analysis does not account for:

- Manufacturing production schedules
- Employee shift patterns
- Business-critical deadlines
- Stakeholder communication requirements

- Reputational impact assessment

Human decision authority required for all containment actions.

Threat Intelligence Correlation

SentinelAI Threat Intelligence Report

Query: Threat actor correlation for indicators

Attribution Assessment:

Indicators correlate with APT29/Cozy Bear with moderate-high confidence (78%).

Campaign Match:

MANUFACTURING-AUTUMN campaign targeting industrial sector (first observed September 2024).

Typical Objectives:

- Industrial espionage
- Supply chain intelligence
- Intellectual property theft
- Long-term persistent access

Expected TTPs:

1. Spearphishing with macro-enabled documents
2. Service account credential abuse
3. Data staging before exfiltration
4. Low-and-slow data transfer via encrypted channels

Prediction:

If this matches APT29 pattern, data exfiltration likely planned for nighttime hours when monitoring is reduced.

LIMITATION NOTICE:

Attribution is probabilistic. Sophisticated actors can false-flag. Business decisions should not rely solely on attribution confidence.

Response Recommendation

SentinelAI Response Recommendation

Recommended Actions (ranked by urgency):

1. **IMMEDIATE:** Authorize endpoint isolation for affected workstations
   - Impact: Manufacturing floor disruption
   - Risk if delayed: Additional lateral movement
2. **IMMEDIATE:** Reset service account credentials
   - Impact: Brief service interruption
   - Risk if delayed: Continued unauthorized access
3. **PRIORITY:** Network segmentation for OT systems
   - Impact: IT overhead increase
   - Risk if delayed: Potential OT compromise
4. **STANDARD:** Executive notification
   - Impact: Low
   - Risk if delayed: Trust erosion

WHAT I CANNOT ASSESS:

- Whether production deadlines justify delayed containment
- Impact on employee morale from sudden shutdowns
- Political dynamics between IT and operations leadership
- Legal implications of various response options
- Whether partial measures might be sufficient

I optimize for security metrics. You must optimize for organizational outcomes.

Educator Debrief Notes

After using these cards, facilitate discussion on:

SentinelAI strengths:

- Rapid MITRE ATT&CK framework mapping
- Threat intelligence correlation
- Pattern-based attack timeline reconstruction
- Quantified risk assessment and confidence levels

SentinelAI limitations:

- Cannot assess business context (production schedules, deadlines)
- Cannot understand organizational politics
- Cannot evaluate legal implications
- Cannot determine proportional response

Career connection:

Real SOC analysts at enterprise organizations use AI-powered SOAR platforms (CrowdStrike Falcon, Splunk SOAR, Microsoft Sentinel) with exactly these capabilities and limitations. Human-in-the-loop decision-making is industry standard.

Activity 3: SOC Analyst Simulation — SentinelAI Response Cards (9-12) Dr. Ryan Straight, University of Arizona