

# SOC Analyst Simulation

## Enterprise Incident Response Worksheet (Grades 9-12)

**Name:** \_\_\_\_\_ **Date:** \_\_\_\_\_

**Role:** \_\_\_\_\_ **Team:** \_\_\_\_\_

### Mission Briefing

**Organization:** TechCorp Industries (2,500 employees, hybrid cloud)

**Your Role:** SOC Team, 7AM-3PM shift

**Alert:** SentinelAI has flagged CRITICAL alerts requiring human analysis and authorization.

### Phase 1: Initial Triage (10 minutes)

#### Evidence Package Review

**My assigned evidence package:** ☐ A: Network ☐ B: Auth ☐ C: Endpoint ☐ D: Threat Intel ☐ E: Business

#### Key indicators I identified:

Indicator	Significance	MITRE ATT&CK Mapping
-----------	--------------	----------------------

#### Initial assessment:

\_\_\_\_\_  
\_\_\_\_\_

#### SentinelAI Consultation

#### Query submitted:

\_\_\_\_\_

#### AI analysis summary:

\_\_\_\_\_

Confidence level: \_\_\_\_\_% Limitations acknowledged:

\_\_\_\_\_

**Critical Decision: Endpoint Isolation**

**SentinelAI recommends:** Full isolation of 47 manufacturing workstations

**Business impact:** \_\_\_\_\_

**Risk if delayed:** \_\_\_\_\_

**My recommendation:** ☐ Full isolation ☐ Partial ☐ Monitor only

**Rationale:**

\_\_\_\_\_

**Phase 2: Analysis and Scoping (15 minutes)**

**Attack Timeline Construction**

Time	Event	Source	Significance
------	-------	--------	--------------

\_\_\_\_\_

**Attack Chain Analysis**

**Initial Access:**

\_\_\_\_\_

**Execution:**

\_\_\_\_\_

**Persistence:**

\_\_\_\_\_

**Lateral Movement:**

\_\_\_\_\_

**Collection/Exfiltration:**

\_\_\_\_\_

## Scope Assessment

**Patient Zero:** \_\_\_\_\_

**Attack Vector:** \_\_\_\_\_

**Systems Compromised:** \_\_\_\_\_

**Data at Risk:** \_\_\_\_\_

**Attribution Confidence:** ☐ High ☐ Medium ☐ Low

**Likely Threat Actor:** \_\_\_\_\_

## Phase 3: Response Execution (15 minutes)

### Critical Decisions Matrix

Decision	Options	AI Input	Business Impact	Our Choice	Rationale
Endpoint Isolation	Full/Partial/None				
Network Segmentation	Activate/Monitor				
Credential Reset	Immediate/Scheduled				
Law Enforcement	No-tify/Wait				
Executive Escalation	Now/After containment				

## Complication Management

### Complication #1:

- Event: \_\_\_\_\_
- Impact on plan: \_\_\_\_\_
- Adaptation: \_\_\_\_\_

### Complication #2:

- Event: \_\_\_\_\_
- Impact on plan: \_\_\_\_\_
- Adaptation: \_\_\_\_\_

## Phase 4: Communications (10 minutes)

### Executive Flash Report

**TO:** CEO, CISO **FROM:** SOC Team **RE:** Security Incident - CRITICAL

### Summary:

\_\_\_\_\_  
\_\_\_\_\_  
**Current Status:**

\_\_\_\_\_  
**Business Impact:**

\_\_\_\_\_  
**Immediate Actions Taken:**

\_\_\_\_\_  
**Next Steps:**

\_\_\_\_\_  
**Operations Notification Draft**

**TO:** Manufacturing VP **RE:** System Availability

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
**Phase 5: After-Action Review**

**AI Partnership Evaluation**

**Where SentinelAI excelled:**

\_\_\_\_\_  
\_\_\_\_\_  
**Where human judgment was essential:**

\_\_\_\_\_  
**Decisions where AI and humans disagreed:**

\_\_\_\_\_  
**How we resolved disagreements:**

\_\_\_\_\_  
**Individual Role Reflection**

**My contribution to team response:**

**Skills I used from my Work Role:**

---

**What I would do differently:**

---

**Career Connection**

**This simulation relates to these NICE Framework Work Roles:**

---

**Required certifications for these careers:**

---

**What interested me most about this work:**

---

**Questions I have about SOC careers:**

---

*From “True Teamwork: Building Human-AI Partnerships” — NICE K12 2025 Dr. Ryan Straight,  
University of Arizona • [ryanstraight@arizona.edu](mailto:ryanstraight@arizona.edu)*