

# 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:

---

---

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
<hr/>			

**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	Immedi- ate/Scheduled				
Law Enforcement	Notify/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:

---

---

#### 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*