

# Activity 2: SOC Analyst Simulation

## Enterprise Incident Response with AI Partnership (Grades 9-12)

Dr. Ryan Straight

2025-12-07

### ! Instructor Overview

Students operate as a Security Operations Center (SOC) team responding to a realistic enterprise security incident. This simulation mirrors authentic SOC workflows where analysts coordinate with AI-powered Security Orchestration, Automation, and Response (SOAR) platforms. Students experience the NICE Framework's incident response work roles while developing critical thinking about human-AI collaboration in high-stakes situations.

**Duration:** 55-60 minutes **Grade Levels:** 9-12 **Group Size:** Teams of 4-5 students **Technology:** One device per student recommended; minimum one per team

### Learning Objectives

Students will:

- Execute **incident response procedures** aligned with industry frameworks (NIST, SANS)
- Operate within **NICE Framework Work Roles** during crisis response
- Leverage AI as a **SOC analyst partner** while maintaining human decision authority
- Analyze **technical indicators** and correlate evidence across multiple sources
- Practice **stakeholder communication** during active incidents
- Evaluate **AI recommendations** critically against organizational context

### CYBER.org Standards Alignment (9-12)

- **9-12.SEC.INFO:** Information security principles and incident response
- **9-12.SEC.DATA:** Data security and forensics fundamentals
- **9-12.SEC.NET:** Network security monitoring and analysis
- **9-12.DC.THRT:** Advanced threat analysis

### NICE Framework Alignment (v2.0.0)

**Primary Work Roles** (Protection and Defense category):

- Incident Response
- Defensive Cybersecurity
- Digital Forensics

**Supporting Work Roles:**

- Threat Analysis
- Vulnerability Analysis

## Simulation Environment

### TechCorp Industries Security Operations Center

**Organization Profile:** - Mid-size manufacturing company (2,500 employees) - IT infrastructure: Hybrid cloud (Azure/on-premises) - Security stack: CrowdStrike EDR, Splunk SIEM, Microsoft Defender - AI Capability: “SentinelAI” SOAR platform with automated detection and response

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

**Context:** SentinelAI has flagged a series of alerts requiring immediate human analysis and response. As the human operators, you must interpret AI findings, make critical decisions, and coordinate response across the organization.

**Key Constraint:** SentinelAI can detect patterns and recommend actions, but all containment, escalation, and communication decisions require human authorization.

## SOC Team Roles

### Incident Commander (IC)

**NICE: Incident Response** - Coordinates overall response effort - Makes final containment and escalation decisions - Manages communication with leadership - Balances technical response with business impact

### Lead Analyst

**NICE: Defensive Cybersecurity** - Performs deep technical analysis of indicators - Correlates data across multiple sources - Develops attack timeline and scope assessment - Works directly with SentinelAI for pattern analysis

### Threat Intelligence Analyst

**NICE: Threat Analysis (Protection and Defense)** - Researches threat actor TTPs - Provides context from threat intelligence feeds - Identifies attack campaign characteristics - Uses AI to correlate with known threat patterns

### Communications Specialist

**NICE: Related to Cybersecurity Management** - Drafts internal and external communications - Coordinates with legal and PR teams - Documents incident timeline - Prepares executive briefings

### Evidence Coordinator (Optional 5th role)

**NICE: Digital Forensics (Investigation)** - Ensures evidence preservation - Maintains chain of custody documentation - Coordinates with law enforcement if needed - Manages forensic data collection priorities

## The Incident

**Initial Alert: 7:12 AM**

**SentinelAI Priority: CRITICAL**

Multiple high-confidence alerts detected across manufacturing floor network segment:

ALERT CLUSTER #7291

Timestamp: 07:12:03 UTC

Severity: CRITICAL

Confidence: 94%

Indicators Detected:

- Lateral movement patterns (MITRE ATT&CK T1021)
- Unusual service account authentication (T1078.002)
- Large data staging activity on file server MFG-FS-01 (T1074)
- C2 beaconing to known malicious infrastructure (T1071)

Affected Systems:

- MFG-WORKSTATION-042 through MFG-WORKSTATION-089 (47 systems)
- MFG-FS-01 (file server, 2.3TB sensitive data)
- HVAC-CONTROLLER-01 (OT/IT bridge system)

Automated Actions Taken:

- Alert generation: COMPLETE
- Network traffic logging: ENABLED
- Endpoint isolation: AWAITING HUMAN AUTHORIZATION

Recommended Human Actions:

1. Authorize endpoint isolation (Impact: Manufacturing operations)
2. Activate incident response protocol
3. Escalate to CISO and Operations leadership

## Evidence Packages

### Evidence Package A: Network Logs

| TIME                                    | SRC_IP       | DST_IP        | PORT | PROTOCOL | BYTES | FLAGS     |
|---|--------------|---------------|------|----------|-------|-----------|
| 07:02:15                                | 10.50.42.102 | 10.50.42.103  | 445  | SMB      | 1.2MB | SYN       |
| 07:02:18                                | 10.50.42.102 | 10.50.42.104  | 445  | SMB      | 1.1MB | SYN       |
| 07:02:21                                | 10.50.42.102 | 10.50.42.105  | 445  | SMB      | 1.3MB | SYN       |
| [Pattern repeats for 47 workstations]   |              |               |      |          |       |           |
| 07:08:44                                | 10.50.42.102 | 185.234.XX.XX | 443  | HTTPS    | 256KB | ENCRYPTED |
| 07:08:47                                | 10.50.42.102 | 185.234.XX.XX | 443  | HTTPS    | 512KB | ENCRYPTED |
| 07:09:02                                | 10.50.42.102 | 185.234.XX.XX | 443  | HTTPS    | 1.1MB | ENCRYPTED |
| [Beaconing every ~20 seconds continues] |              |               |      |          |       |           |

### Evidence Package B: Authentication Logs

| TIMESTAMP | USER | SYSTEM | RESULT | METHOD |
|-----------|------|--------|--------|--------|
|-----------|------|--------|--------|--------|

|          |            |                     |         |          |
|----------|------------|---------------------|---------|----------|
| 06:58:22 | svc_backup | MFG-FS-01           | SUCCESS | Kerberos |
| 06:58:24 | svc_backup | MFG-WORKSTATION-042 | SUCCESS | Kerberos |
| 06:58:26 | svc_backup | MFG-WORKSTATION-043 | SUCCESS | Kerberos |

[Continues for all affected systems]

Note: svc\_backup account normally runs at 02:00 AM for nightly backups

Last password change: 847 days ago

Service account owner: IT Operations (no specific owner assigned)

## Evidence Package C: Endpoint Detection Data

MFG-WORKSTATION-042:

- Process: cmd.exe spawned by outlook.exe (07:01:44)
- File Drop: C:\Users\jsmith\AppData\Local\Temp\update.exe
- Hash: 3a4b5c6d7e8f... [MATCHES KNOWN THREAT: APT29 TOOLING]
- Registry: HKLM\Software\Microsoft\Windows\CurrentVersion\Run [PERSISTENCE]
- Network: Connection to 185.234.XX.XX:443 every 20 seconds

User jsmith:

- Role: Manufacturing Floor Supervisor
- Email received: 06:55:12 - Subject: "URGENT: Updated Shift Schedule"
- Attachment opened: 07:01:41 - schedule\_update.docm

## Evidence Package D: Threat Intelligence

IP: 185.234.XX.XX

- First seen: 2024-09-15
- Attribution: SUSPECTED APT29/Cozy Bear
- Campaign: MANUFACTURING-AUTUMN targeting industrial sector
- TTPs: Spearphishing → Service account abuse → Data staging → Exfiltration
- Past targets: Automotive, aerospace, manufacturing organizations
- Objective: Industrial espionage, supply chain intelligence

File Hash: 3a4b5c6d7e8f...

- Malware family: SUNSPOT variant
- Capabilities: Keylogging, credential harvesting, file staging
- Evasion: Living-off-the-land techniques, encrypted C2

## Evidence Package E: Business Context

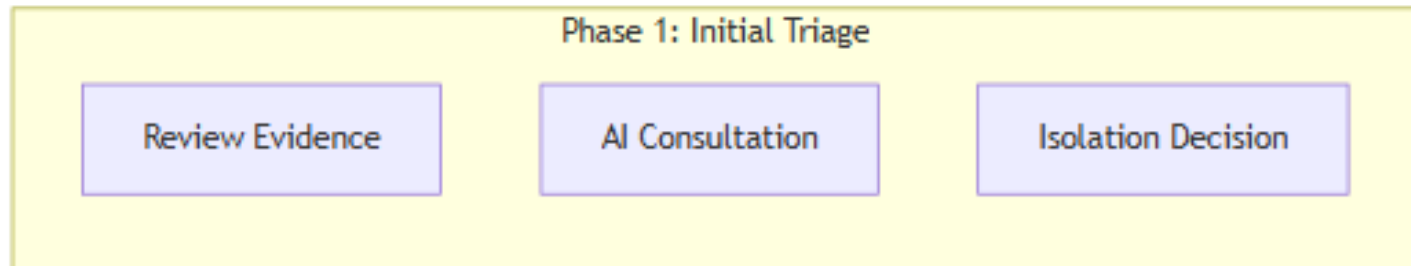
OPERATIONAL CONTEXT:

- Manufacturing floor runs 24/7, current shift change at 07:00
- MFG-FS-01 contains: Product designs, supplier contracts, pricing data
- HVAC-CONTROLLER-01 manages climate control for sensitive equipment
- Q4 production deadline in 2 weeks - high pressure environment
- Recent layoffs created employee morale concerns
- CEO presentation to board scheduled for Friday

PREVIOUS INCIDENTS:

- Phishing attempt blocked 3 weeks ago (similar TTP)
- Service account audit recommended 6 months ago (not completed)
- OT/IT segmentation project delayed due to budget

## Response Framework



### SOC Incident Response Workflow

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

**All Team Members:** 1. Review assigned evidence package 2. Document initial observations 3. Prepare briefing for team

#### SentinelAI Consultation (Lead Analyst):

“Analyze these network patterns [paste logs]. What attack progression do they indicate? Map to MITRE ATT&CK framework.”

“Compare this hash and IP against your threat intelligence. What campaign does this align with? What typically comes next in this attack chain?”

#### Key Decision Point:

- **Authorize endpoint isolation?** 47 manufacturing workstations offline = production impact
- SentinelAI recommends: YES (93% confidence attack in progress)
- Human consideration: Shift change happening, 200 workers need workstations

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

##### Lead Analyst Tasks:

- Build attack timeline
- Identify patient zero and attack vector
- Assess scope of compromise
- Determine if data exfiltration occurred

##### Threat Intel Tasks:

- Research APT29 TTPs
- Identify likely objectives
- Predict next attack phases
- Assess attribution confidence

##### IC Tasks:

- Prioritize response actions
- Assess business impact of containment options
- Prepare leadership notification
- Coordinate team activities

#### Communications Tasks:

- Draft executive summary
- Prepare manufacturing leadership notification
- Document decision log
- Track timeline

### Phase 3: Response Execution (15 minutes)

#### Critical Decisions Required:

| Decision             | Options                     | AI Recommendation | Business Impact          | Risk if Delayed         |
|----------------------|-----------------------------|-------------------|--------------------------|-------------------------|
| Endpoint Isolation   | Full /<br>Partial /<br>None | Full isolation    | High - production stops  | Very High - data loss   |
| Network Segmentation | Activate /<br>Monitor       | Activate          | Medium - IT overhead     | High - lateral movement |
| Credential Reset     | Immediate /<br>Scheduled    | Immediate         | Medium - user disruption | Critical - persistence  |
| Law Enforcement      | Notify /<br>Wait            | Wait for scope    | Low                      | Medium - evidence       |
| Executive Escalation | Now /<br>After containment  | Now               | Low                      | Medium - trust          |

#### Team must document:

- Decision made
- Rationale
- AI input considered
- Human factors that modified AI recommendation

### Phase 4: Communication (10 minutes)

#### Draft required communications:

##### 1. Executive Flash Report (for CEO/CISO)

- Incident severity and scope
- Immediate actions taken
- Business impact assessment
- Next steps and timeline

## 2. Operations Notification (for Manufacturing VP)

- Operational impact
- Workaround procedures
- Expected resolution timeline

## 3. IT Staff Directive

- Technical containment actions
- Evidence preservation requirements
- Coordination instructions

## Phase 5: Debrief (10 minutes)

### Team Discussion:

#### 1. What did SentinelAI do well?

- Pattern detection speed
- Threat intelligence correlation
- Attack chain mapping
- Risk quantification

#### 2. Where did human judgment matter most?

- Business context interpretation
- Stakeholder communication
- Trade-off decisions
- Ethical considerations

#### 3. What would happen without AI?

- Detection delay (hours vs. minutes)
- Analysis depth limitations
- Correlation challenges
- Response speed impact

#### 4. What would happen without humans?

- Context-blind automation
- Business disruption from over-response
- Stakeholder communication gaps
- Ethical oversight absence

## Assessment Rubric

| Criterion                 | Developing (1-2)          | Proficient (3)                           | Advanced (4)   |
|---------------------------|---------------------------|--|--|
| <b>Technical Analysis</b> | Surface-level review      | Solid evidence correlation               | Deep technical understanding with attack chain mapping |
| <b>AI Partnership</b>     | Used AI as answer machine | Collaborated with appropriate skepticism | Strategic consultation with critical evaluation        |

| Criterion               | Developing (1-2)                  | Proficient (3)                     | Advanced (4)   |
|-------------------------|-----------------------------------|------------------------------------|--|
| <b>Decision Quality</b> | Decisions without clear rationale | Documented reasoning for decisions | Sophisticated trade-off analysis with business context |
| <b>Role Execution</b>   | Unclear responsibilities          | Fulfilled role requirements        | Leadership within role, supported teammates            |
| <b>Communication</b>    | Unclear or missing documentation  | Clear documentation produced       | Professional-quality stakeholder communications        |
| <b>NICE Alignment</b>   | No connection to work roles       | Basic awareness of career paths    | Articulated how roles connect to industry careers      |

### Assessment Connection

This table shows how activity elements connect to assessment rubric criteria:

| Rubric Criterion                  | Developed Through   | Evidence Source   |
|-----------------------------------|---|---|
| <b>AI Partnership Framing</b>     | Phase 1: SentinelAI consultation with role-specific prompts                           | Quality of AI queries and response interpretation                         |
| <b>Complementary Strengths</b>    | Phase 5 Debrief: “What did AI do well?” vs. “Where did human judgment matter?”        | Debrief discussion responses and documentation                            |
| <b>AI Limitation Awareness</b>    | SentinelAI “LIMITATION NOTICE” and human decision authority requirement               | Phase 3 decision rationale showing where AI recommendations were modified |
| <b>Synthesis Quality</b>          | Decision Matrix: integrating AI recommendation with business impact and risk analysis | Completed decision documentation with rationale                           |
| <b>Human Context Application</b>  | Evidence Package E: Business Context informing response decisions                     | How business context modified purely technical AI recommendations         |
| <b>Decision Justification</b>     | Phase 3 documentation: Decision, Rationale, AI input, Human factors                   | Quality and depth of documented decision rationale                        |
| <b>NICE Framework Application</b> | Role Cards with explicit NICE Work Role alignment, Career Connections section         | Debrief “career insights” responses and role execution quality            |

**Applicable Rubrics:** [Human-AI Collaboration Rubric](#), [Decision-Making Quality Rubric](#), [NICE Framework Application Rubric](#)



## Career Connections

### This Simulation Reflects Real SOC Work

#### What you experienced today:

- Alert triage from SIEM/SOAR platforms → Real SOC analysts do this continuously
- AI-assisted analysis → CrowdStrike, Splunk, Palo Alto all have AI capabilities
- Team coordination → SOC's have tiered analysts and specialized roles
- Executive communication → Critical skill for career advancement

### NICE Framework Career Pathways

| Work Role                   | Starting Salary | Growth Rate     | Your Simulation Role |
|-----------------------------|-----------------|-----------------|----------------------|
| SOC Analyst (Entry)         | \$55-75K        | 33% (2022-2032) | All roles            |
| Incident Responder          | \$75-100K       | 35%             | Incident Commander   |
| Threat Intelligence Analyst | \$80-110K       | 31%             | Threat Intel         |
| Security Engineer           | \$90-130K       | 35%             | Lead Analyst         |
| CISO (Executive)            | \$200-400K      | 28%             | IC → Long-term path  |

### Certifications That Prepare You

- **CompTIA Security+** → Foundation for all roles
- **CompTIA CySA+** → SOC Analyst focus
- **GIAC GCIH** → Incident Handler certification
- **CISSP** → Advanced/Management roles

### Low-Resource Adaptation

If AI access is unavailable, provide this SentinelAI analysis report as handout:

#### SentinelAI Analysis Report #7291-A

Pattern analysis indicates lateral movement consistent with credential-based attack. Service account svc\_backup shows authentication pattern anomaly: normal operation 02:00-03:00, current activity 06:58-07:12. Statistical deviation: 99.7th percentile.

Attack chain mapping: 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)

Confidence assessment: 94% probability active compromise in progress. Recommended action: Immediate containment. Risk if delayed 2 hours: Estimated 800GB additional data staging, potential OT system access.

**LIMITATION NOTICE:** This analysis does not account for: manufacturing production schedules, employee shift patterns, business-critical deadlines, stakeholder communication requirements, or reputational impact assessment. Human decision authority required.