Activity 2: AI-Assisted Incident Response

Experiencing NICE Work Roles Through Human-AI Collaboration (Grades 6-8)

Dr. Ryan Straight

2025-12-07

AI-Assisted Incident Response

Authentic Work Role Experience Through Team-Based Response

> ❗ Instructor Overview
>
> Students experience authentic NICE Framework Work Roles by responding to realistic security incidents. Each team member assumes a specific role while collaborating with AI as their technical analyst. This activity demonstrates how different cybersecurity professionals work together during actual incidents.
>
> **Duration**: 50-60 minutes **Grade Levels**: 6-8 (with role complexity variations) **Group Size**: Teams of 3-4 students **Technology Requirements**: One device per team minimum, ideally one per student

Learning Objectives

Primary Objective

Students will experience authentic cybersecurity Work Roles through collaborative incident response, understanding how human decision-making and AI analysis combine in crisis situations.

NICE Framework Alignment

- **Incident Response**: Lead role in response coordination
- **Cyber Defense Analysis**: Technical analysis and monitoring
- **Vulnerability Assessment**: System weakness identification
- **Cybersecurity Management**: Decision-making and resource allocation

CYBER.org Standards (Supplemental)

- **6-8.SEC.NICE**: Understanding NICE Framework roles
- **6-8.SEC.INFO**: Information security principles
- **6-8.DC.RESP**: Incident response procedures
- **6-8.SEC.RCVR**: Recovery and resilience

Career Exploration

Students actively experience roles: Incident Commander, SOC Analyst, Threat Intelligence Specialist, Communications Coordinator

Pre-Activity Setup

Role Assignment System

Role Card Templates

Incident Commander (IC) - Makes final decisions - Coordinates team response - Manages resource allocation - Consults AI for impact assessment

SOC Analyst - Monitors system alerts - Analyzes technical indicators - Partners with AI for pattern recognition - Reports findings to IC

Threat Intelligence Specialist - Researches attack methods - Identifies threat actors - Uses AI to analyze TTPs (Tactics, Techniques, Procedures) - Provides context to team

Communications Coordinator - Drafts stakeholder messages - Manages information flow - Works with AI to craft clear explanations - Documents response timeline

Incident Scenarios

Scenario 1: The Ransomware Discovery (Beginner)

Initial Alert: Monday, 7:45 AM Several teachers report they cannot access their lesson plans. Files show a ".locked" extension with a ransom note demanding cryptocurrency.

Evidence Available: - Email logs showing suspicious attachment opened Friday afternoon - Network traffic spike over the weekend - 30% of school computers affected - Backup system status: Last successful backup Thursday night

Critical Decisions Required: 1. Isolate affected systems or shut down entire network? 2. Contact law enforcement immediately or assess damage first? 3. Inform parents/community now or after initial response? 4. Attempt recovery from backups or negotiate with attackers?

Scenario 2: The Grade Database Breach (Intermediate)

Initial Alert: Wednesday, 2:30 PM Anonymous tip claims student grades have been changed in the system. Initial check confirms several suspicious modifications.

Evidence Available: - Unauthorized admin account created two weeks ago - Grade changes pattern: All failing grades changed to passing - IP logs show access from multiple locations - Student information potentially exposed

Critical Decisions Required: 1. Lock down grade system or maintain access for investigation? 2. Notify affected students/parents individually or mass communication? 3. Invalidate current grades or attempt to restore originals? 4. Involve student discipline process or focus on system security?

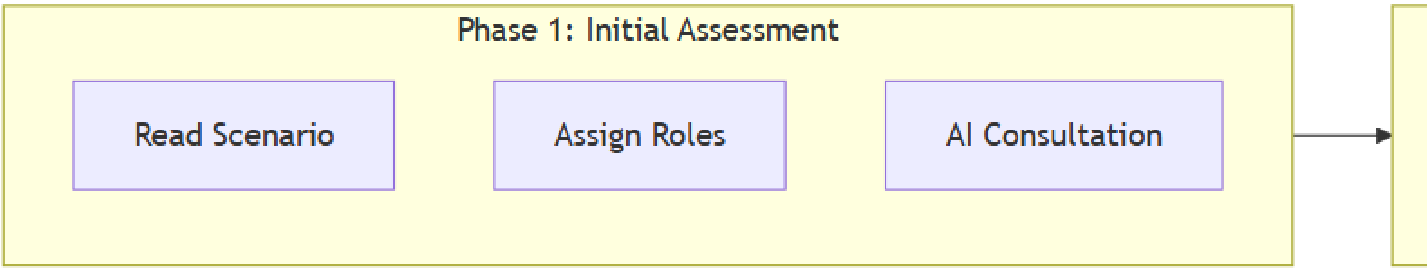
Scenario 3: The Social Media Threat (Advanced)

Initial Alert: Thursday, 11:00 AM School social media accounts compromised, posting inappropriate content and threats. Posts going viral with media attention growing.

Evidence Available: - Password reset emails ignored by staff - Account access from foreign IP addresses - Coordinated attack across multiple platforms - Personal information of staff being posted

Critical Decisions Required: 1. Delete accounts or attempt recovery? 2. Issue public statement or stay silent until resolved? 3. Lock down all school digital assets or targeted response? 4. Legal action priorities: Criminal investigation or civil remedies?

Response Framework



Incident Response Workflow

Phase 1: Initial Assessment (10 minutes)

Team Actions

1. **Read scenario briefing** as a team
2. **Assign roles** based on strengths/interests
3. **Individual role preparation** (3 minutes):
   - IC: List immediate priorities
   - SOC: Identify technical indicators
   - Threat Intel: Note attack patterns
   - Comms: Draft initial stakeholder groups

AI Consultation Prompts

For IC: "As my incident response advisor, what are the top 3 immediate actions we should prioritize for [scenario type]?"

For SOC: "Help me analyze these technical indicators: [list evidence]. What attack patterns do you recognize?"

For Threat Intel: "Based on these characteristics [list], what type of threat actor might be responsible?"

For Comms: "What key information should we include in our initial incident notification?"

Phase 2: Response Planning (15 minutes)

Collaborative Planning Process

1. **SOC Analyst** presents technical findings
2. **Threat Intel** provides attacker context
3. **Team discusses** response options with AI input
4. **IC makes** preliminary decisions
5. **Comms prepares** messaging strategy

Decision Log Template

Time	Decision Point	Options Considered	AI Input	Final Decision	Rationale
T+5min	Network isolation	Full/Partial/None	[AI recommendation]	[Team choice]	[Reasoning]
T+10min	Stakeholder notification	Immediate/Delayed	[AI suggestion]	[Team choice]	[Reasoning]

Phase 3: Response Execution (15 minutes)

Action Implementation

Teams execute their response plan while managing emerging complications:

Complication Injections (Instructor introduces at 5-minute intervals): 1. “Media has picked up the story - reporters calling” 2. “New systems showing signs of compromise” 3. “Parent group demanding immediate meeting”

Real-Time Adaptation

- Teams must adjust plans based on complications
- AI consultation for handling unexpected developments
- Document changes to original response plan
- Maintain role responsibilities while adapting

Phase 4: After-Action Review (10 minutes)

Team Debrief Structure

1. **What went well?** Role execution and teamwork
2. **What challenged us?** Unexpected complications
3. **How did AI help?** Specific contributions
4. **What would we change?** Lessons learned
5. **Career insights?** Interest in specific roles

Assessment Framework

Performance Rubric

Criteria	Emerging (1)	Developing (2)	Proficient (3)	Advanced (4)
Role Execution	Unclear on role duties	Basic role understanding	Clear role performance	Leadership within role
Team Collaboration	Works independently	Some coordination	Good teamwork	Exceptional synergy
AI Partnership	AI as answer source	AI as advisor	True partnership	Strategic AI use
Decision Quality	Random choices	Some reasoning	Logical decisions	Strategic thinking
Communication	Unclear messages	Basic clarity	Clear and appropriate	Professional quality
NICE Alignment	No connection	Some awareness	Clear connections	Deep understanding

Extension Activities

Advanced Challenges

Multi-Vector Attack

Combine two scenarios simultaneously (e.g., ransomware during grade breach investigation)

Historical Recreation

Research and respond to famous real incidents (WannaCry, SolarWinds, Colonial Pipeline)

Red Team Exercise

One team plays attackers while another defends, AI assists both sides

Policy Development

After incident, create new security policies to prevent recurrence