

## Activity 3: AI-Assisted Incident Response

### Team-Based Security Crisis Management

#### Overview

Students assume team roles during realistic security incidents, experiencing firsthand how cybersecurity professionals coordinate with AI systems when time pressure demands rapid, coordinated action.

**Core Learning:** Incident response requires diverse roles working in concert, each contributing specialized expertise that complements AI-driven analysis. Effective response emerges from coordination, not individual heroics.

#### Incident Response Workflow



#### Grade-Band Versions

##### K-2: Fix It Team!

**Duration:** 20-25 minutes

Young students assume simple roles (Finder, Helper, Fixer, Talker) to solve a classroom technology problem, learning that teams with different jobs work together to address challenges.

[View K-2 Version](#)

##### Grades 3-5: Computer Problem Solvers

**Duration:** 35-40 minutes

Students form investigation teams with defined roles to respond to a school computer problem. They discover that different team members contribute different skills, with their AI partner serving as one member of the team.

[View Grades 3-5 Version](#)

### **Grades 6-8: AI-Assisted Incident Response**

**Duration:** 50-60 minutes

Teams respond to realistic security incidents using NICE Framework-aligned roles. Multiple scenario options allow flexibility in complexity and focus areas.

[View Grades 6-8 Version](#)

### **Grades 9-12: SOC Analyst Simulation**

**Duration:** 55-60 minutes

An enterprise-level breach scenario with technical depth. Students experience the pressure and coordination demands characteristic of Security Operations Center work during an active incident.

[View Grades 9-12 Version](#)

### **NICE Framework Alignment**

**Primary Work Roles:** Incident Response, Defensive Cybersecurity, and Threat Analysis (Protection and Defense category)

**Skills students practice:** Incident triage, response coordination, automated threat detection integration, incident containment, and stakeholder communication

#### **i Learn More: How Real SOCs Work**

Security Operations Centers coordinate human analysts with AI-powered detection systems under intense time pressure—exactly what students experience in this activity. The NICE Framework defines these work roles precisely, and research on team-based cybersecurity learning shows that role-playing incident response builds lasting understanding of coordination dynamics.

[Explore the research →](#)

### **Supporting Materials**

- [Career Connections](#)
- [Assessment Rubrics](#)