Activity 1: Security Detective Teams

Investigating Security Incidents with AI Partners

Overview

Students investigate security incidents alongside an AI partner, discovering through hands-on experience that AI demonstrates strength in pattern recognition while humans bring irreplaceable contextual understanding. Together, they solve mysteries that neither could unravel independently.

Core Learning: AI excels at pattern recognition across large datasets; humans excel at understanding context and making judgment calls. Together, they achieve insights neither could reach alone.

> **Learn More: Pattern Recognition vs. Contextual Understanding**
>
> This distinction—AI for patterns, humans for context—reflects how Security Operations Centers actually function. Research shows that effective threat detection requires both computational pattern matching and human judgment about organizational context. The detective metaphor helps students internalize this complementary relationship.
> Explore the research →

Grade-Band Versions

K-2: Mystery Helpers

Duration: 20-25 minutes

In this simplified version, young students work with a "helper friend" to solve a classroom mystery using picture-based clues. The teacher voices the AI partner, introducing the foundational concept of teamwork with technology helpers.

View K-2 Version

Grades 3-5: Locked Library Computers

Duration: 30-35 minutes

Students investigate why library computers keep getting locked. Working with an AI partner through guided prompts, they discover how AI spots patterns while humans understand the reasons behind events.

View Grades 3-5 Version

Grades 6-8: Security Detective Teams

Duration: 45-50 minutes

The complete investigation experience. Student teams examine evidence packets, consult AI partners authentically, and synthesize their findings to determine what happened in a school security incident.

View Grades 6-8 Version

Grades 9-12: Threat Investigation

Duration: 50-60 minutes

A Security Operations Center-style simulation with technical depth. Students analyze authentication logs, network data, and social engineering indicators while working with AI to conduct a comprehensive threat investigation.

View Grades 9-12 Version

NICE Framework Alignment

Primary Work Roles: Cyber Defense Analyst (PR-CDA-001) and Vulnerability Assessment Analyst (PR-VAM-001)

Skills students practice: Log analysis, indicator correlation, human-AI collaboration, and threat assessment

Supporting Materials

- Career Connections
- Quick-Start Guide
- Student Worksheet
- Evidence Packet
- AI Response Cards (for low-resource implementation)