Activity 1: Security Detective Teams

Threat Investigation with AI Partnership (Grades 9-12)

Dr. Ryan Straight

2025-12-07

> **!** Instructor Overview
>
> Students investigate a realistic security incident at a fictional company, partnering with AI to analyze evidence. This activity mirrors authentic Security Operations Center (SOC) workflows where analysts coordinate with AI-powered security tools daily. Students experience the NICE Framework's Cyber Defense Analysis work role firsthand.
> **Duration**: 50-60 minutes **Grade Levels**: 9-12 **Group Size**: Pairs or small groups (2-4) **Technology**: One device per group minimum; individual access preferred

Learning Objectives

By the end of this activity, students will:

- Conduct systematic security investigation using AI as an analytical partner
- Distinguish between AI pattern-recognition capabilities and human contextual analysis
- Apply investigation methodology aligned with industry SOC practices
- Connect activity experience to cybersecurity career pathways

CYBER.org Standards Alignment (9-12)

- **9-12.SEC.THR**: Advanced threat analysis
- **9-12.SEC.INC**: Incident investigation procedures
- **9-12.SEC.MON**: Security monitoring concepts
- **9-12.SEC.FOR**: Digital forensics fundamentals

NICE Framework Alignment

Primary Work Role: Cyber Defense Analyst (PR-CDA-001)

- Analyze collected information to identify vulnerabilities and potential for exploitation
- Identify security implications and apply methodologies for incident analysis
- Determine tactics, techniques, and procedures (TTPs) of threat actors

The Incident

Incident Brief: Apex Financial Services

Company: Apex Financial Services (500 employees, regional financial advisory firm) **Date**: Thursday, 2:47 PM **Alert Source**: Security Information and Event Management (SIEM) system

Initial Alert: Unusual authentication patterns detected for multiple user accounts in the Finance department. After-hours access attempts, unusual geographic locations, and failed MFA challenges logged.

Your Assignment: As SOC analysts, your team must investigate this incident, determine the attack vector, assess the scope of compromise, and provide initial recommendations.

Stakeholder Expectations: CFO wants preliminary findings within the hour. IT Security Manager needs technical details for remediation planning.

Evidence Package

Evidence A: Authentication Logs

```
TIMESTAMP            USER           ACTION          LOCATION        STATUS
2024-11-14 02:34:12  jmorris@apex   LOGIN_ATTEMPT   IP: 185.42.x.x  MFA_FAILED
2024-11-14 02:34:45  jmorris@apex   LOGIN_ATTEMPT   IP: 185.42.x.x  MFA_FAILED
2024-11-14 02:35:22  jmorris@apex   LOGIN_ATTEMPT   IP: 185.42.x.x  SUCCESS (MFA bypassed*)
2024-11-14 02:36:01  jmorris@apex   FILE_ACCESS     SharePoint/Finance/Q3Reports
2024-11-14 02:41:18  kpatel@apex    LOGIN_ATTEMPT   IP: 185.42.x.x  MFA_FAILED
2024-11-14 02:42:03  kpatel@apex    LOGIN_ATTEMPT   IP: 185.42.x.x  MFA_FAILED
2024-11-14 03:15:44  mchen@apex     LOGIN_ATTEMPT   IP: 192.168.1.x SUCCESS (office IP)
2024-11-14 08:22:31  jmorris@apex   LOGIN           IP: 10.0.45.x   SUCCESS (normal)

*Note: MFA bypass via legacy authentication protocol
```

Evidence B: Email Security Gateway Logs

```
DATE       RECIPIENT       SUBJECT                                VERDICT    ACTION
11/12      jmorris@apex    "Urgent: Update your credentials"      SUSPICIOUS DELIVERED*
11/12      kpatel@apex     "Urgent: Update your credentials"      SUSPICIOUS DELIVERED*
11/12      tkim@apex       "Urgent: Update your credentials"      SUSPICIOUS QUARANTINED
11/13      jmorris@apex    "Re: Q3 Financial Review"              CLEAN      DELIVERED
11/13      kpatel@apex     "FW: Updated payroll schedule"         CLEAN      DELIVERED

*Note: Delivered due to user override of warning
```

Evidence C: User Profile Information

User	Role	Recent Activity	Notes
jmorris@apex	Sr. Financial Analyst	High access to financial data	Works remotely 2 days/week
kpatel@apex	Accounting Manager	Payroll system access	Recently promoted

User	Role	Recent Activity	Notes
mchen@apex	IT Administrator	Full admin rights	On-call this week
tkim@apex	Junior Analyst	Limited access	Started 3 months ago

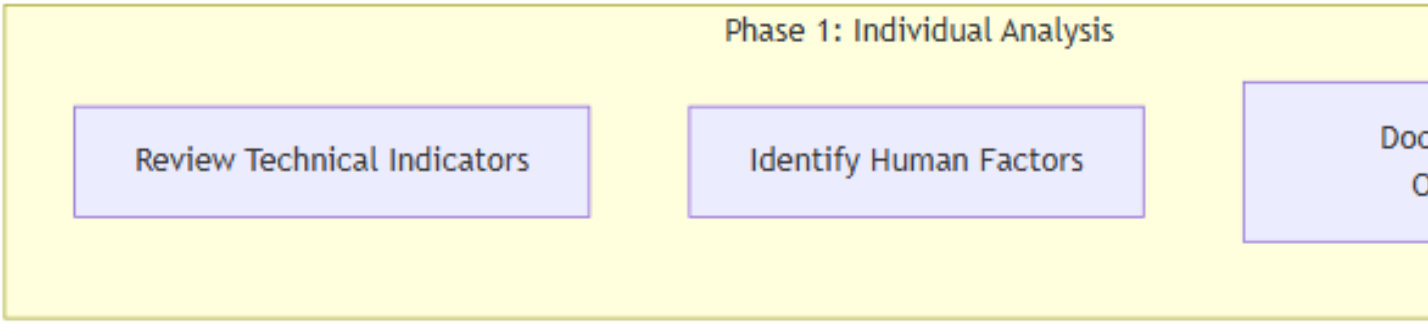
Evidence D: Threat Intelligence Feed

```
INDICATOR                   TYPE        CONFIDENCE    CONTEXT
185.42.x.x                  IP          HIGH          Known credential stuffing infrastructure
apex-login[.]com            Domain      HIGH          Typosquatting domain registered 11/10
"Urgent: Update your..."    Pattern     MEDIUM        Common phishing subject line
Legacy auth exploitation    TTP         HIGH          Trending attack vector Q4 2024
```

Evidence E: HR Information (Confidential)

- **jmorris**: Recently had public disagreement with management over bonus structure. LinkedIn shows active job searching.
- **kpatel**: New to role, undergoing additional training on security awareness.
- **tkim**: Newest team member, completed security training with high scores.

Investigation Framework



Security Investigation Workflow

Phase 1: Individual Evidence Analysis (10 minutes)

Before consulting your AI partner, analyze each evidence piece:

Technical Indicators: - What IP addresses are suspicious and why? - What authentication anomalies do you observe? - What does the email timeline suggest?

Human/Contextual Factors: - What do the HR notes suggest about potential insider risk? - Why might users have overridden email warnings? - What organizational factors might be relevant?

Phase 2: AI Partnership Investigation (15 minutes)

Engage your AI partner as a fellow analyst. Frame the conversation professionally:

Recommended Opening: > "I'm a SOC analyst investigating a potential credential compromise at a financial services firm. I need your help analyzing the evidence and identifying attack patterns. I'll share the logs and indicators—help me build a timeline and identify TTPs. I'll add contextual factors you might not be able to assess."

Investigation Prompts:

1. "Analyze these authentication logs. What attack pattern do you recognize?"
2. "Cross-reference the email gateway logs with the authentication timeline. What's the likely initial access vector?"
3. "Based on the threat intelligence data, what threat actor profile or campaign might this align with?"
4. "What evidence would you want to collect next to confirm your hypothesis?"
5. "What's your confidence level, and what are you uncertain about?"

Document AI Insights: | Question | AI Analysis | My Assessment | |———-|———-|———-| | Attack pattern | | | | Initial access vector | | | | Scope of compromise | | | | AI's stated limitations | | |

Phase 3: Integrated Analysis (10 minutes)

Synthesize human and AI analysis:

1. **What AI identified well**:
   - Technical patterns (timing, IP correlation, TTP matching)
   - Threat intelligence correlation
   - Attack timeline reconstruction
2. **What required human analysis**:
   - Insider risk assessment (HR context)
   - Why users overrode security warnings (organizational culture)
   - Business impact assessment
   - Appropriate response considering employee relations
3. **Combined conclusion**:
   - Initial access vector: _____
   - Compromised accounts: _____
   - Scope of data access: _____
   - Recommended immediate actions: _____

Phase 4: Incident Report (10 minutes)

Draft Executive Summary (for CFO):

Incident Type: _____ Affected Users: _____
Data at Risk: _____ Recommended Actions: _____
Confidence Level: _____

Technical Findings (for IT Security Manager):

Attack Vector: _____ IOCs Identified: _____
Systems Affected: _____ Remediation Steps: _____

Assessment Rubric

Criterion	Developing (1-2)	Proficient (3)	Advanced (4)
AI Partnership Quality	Used AI for simple lookups	Engaged AI in analytical dialogue	Strategic AI consultation with critical evaluation
Technical Analysis	Identified some indicators	Correlated multiple evidence sources	Comprehensive TTP identification and timeline
Contextual Integration	Limited human context added	Integrated organizational factors	Sophisticated synthesis of technical + human factors
Investigation Methodology	Disorganized approach	Systematic investigation	Industry-aligned SOC methodology
Communication	Unclear findings	Clear technical communication	Executive + technical audience differentiation

Assessment Connection

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

Rubric Criterion	Developed Through	Evidence Source
AI Partnership Framing	Phase 2: Professional analyst-to-analyst framing	Worksheet: Recommended opening prompt usage
Complementary Strengths	Phase 3: "What AI identified well" vs. "What required human analysis"	Integrated analysis documentation
AI Limitation Awareness	AI response to "What are you uncertain about?"	Documented AI limitations in analysis table
Synthesis Quality	Phase 3: Combined conclusion	Written synthesis of AI + human analysis
AI Input Integration	Phase 2: Investigation prompts	Documentation of how AI insights shaped conclusions
Critical Evaluation	Phase 3: Assessment of AI analysis	"My Assessment" column in documentation
Human Context Application	Evidence E: HR Information analysis	Integration of insider risk, organizational factors
Decision Justification	Phase 4: Incident Report	Executive summary rationale and recommendations
NICE Framework Application	Career Connections discussion	Verbal/written career pathway analysis

Applicable Rubrics: Human-AI Collaboration Rubric, Decision-Making Quality Rubric, NICE Framework Application Rubric

Career Connections

This Activity Mirrors Real SOC Work

In actual Security Operations Centers: - Analysts review alerts from SIEM systems (just like our scenario) - AI/ML tools flag anomalies for human review - Analysts add contextual knowledge AI lacks - Teams coordinate technical findings with business stakeholders

Related NICE Framework Work Roles

Work Role	How This Activity Connects
Cyber Defense Analyst	Core investigation methodology
Incident Responder	Escalation and remediation planning
Threat Intelligence Analyst	IOC correlation and threat profiling
Security Operations Center Analyst	Alert triage and initial analysis

Career Pathway Discussion

- What surprised you about working with AI on security analysis?
- How would you describe the human analyst's value-add to someone considering this career?
- What skills would you want to develop to be effective in this role?

Extension Challenges

Advanced Technical Analysis

- Research the specific TTP "Legacy Authentication Exploitation" (MITRE ATT&CK T1078.001)
- Create detection rules that would have caught this attack earlier

Incident Response Planning

- Draft a full incident response plan for this scenario
- Include communication templates for affected users

Threat Hunting

- What proactive queries would you run to find similar compromises?
- Design a threat hunting hypothesis based on this incident

Policy Recommendations

- What security policy changes would prevent this attack?
- How would you balance security with user experience?

Instructor Notes

Preparation

- ☐ Ensure AI access for all groups (or prepare detailed pre-generated responses)
- ☐ Print evidence packets or prepare digital distribution
- ☐ Review MITRE ATT&CK framework basics for context
- ☐ Prepare discussion of local career opportunities in cybersecurity

Key Discussion Points

- **AI limitations**: AI doesn't know about the HR context, organizational politics, or why users made the decisions they did
- **Human judgment**: Deciding whether jmorris is a compromised victim or potential insider threat requires human assessment
- **Real-world complexity**: Actual incidents involve more ambiguity and incomplete information

Common Student Questions

- "Would AI actually be used this way?" → Yes, SOAR platforms and AI copilots are standard in enterprise SOCs
- "How accurate is AI analysis?" → Varies; AI excels at pattern matching but struggles with context and novel attacks
- "What certifications relate to this work?" → CompTIA Security+, CySA+, GIAC GCIH

Low-Resource Adaptation

If AI access is limited, use this pre-generated analysis:

> **AI Analysis Summary**:
>
> Based on the evidence provided, I identify a credential phishing campaign with the following characteristics:
>
> **Timeline Reconstruction**: - Nov 10: Typosquatting domain registered (preparation phase) - Nov 12: Phishing emails sent to Finance department - Nov 14 02:34 AM: Credential use from known malicious IP
>
> **Attack Pattern**: This matches a Business Email Compromise (BEC) precursor campaign. The attacker harvested credentials via phishing, then accessed financial data during off-hours to avoid detection.
>
> **Technical Indicators**: - IP 185.42.x.x: HIGH confidence malicious - Legacy auth bypass: Known exploitation technique - MFA bypass method: Indicates sophisticated attacker
>
> **What I Cannot Assess**: - Whether jmorris is victim only or potentially complicit - Why users overrode email security warnings - Organizational factors that enabled the attack - Appropriate HR/legal response considerations - Business impact relative to company priorities

Recommended Next Steps: Preserve evidence, reset affected credentials, audit legacy authentication, interview affected users.