Incident Briefings

Activity 3: AI-Assisted Incident Response

How to Use These Briefings

Print one briefing per team. Teams read the briefing together at the start of the activity to understand their incident scenario.

Grades 9-12: Enterprise SOC Simulation

Scenario: APT Attack on Manufacturing

INCIDENT BRIEFING - CLASSIFICATION: URGENT

Organization: TechCorp Industries **Date/Time:** Monday, 07:12 AM **Alert Source:** SentinelAI SOAR Platform **Priority:** CRITICAL

Situation Overview

Multiple high-confidence alerts have been detected across the manufacturing floor network segment. SentinelAI has identified indicators consistent with advanced persistent threat (APT) activity.

Organization Context

- **Size:** 2,500 employees
- **Industry:** Manufacturing
- **Infrastructure:** Hybrid cloud (Azure + on-premises)
- **Security Stack:** CrowdStrike EDR, Splunk SIEM, Microsoft Defender
- **AI Platform:** SentinelAI SOAR with automated detection

Initial Indicators

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

Affected Systems

- 47 manufacturing workstations (MFG-WORKSTATION-042 through -089)
- File server MFG-FS-01 (2.3TB sensitive data)
- HVAC-CONTROLLER-01 (OT/IT bridge system)

Automated Actions Already Taken

- Alert generation
- Network traffic logging enabled
- Endpoint isolation AWAITING HUMAN AUTHORIZATION

Your Mission

Analyze the evidence, coordinate your team response, and make critical decisions about containment, escalation, and communication.

Remember: SentinelAI can recommend, but only humans can authorize containment actions that impact business operations.

Grades 6-8: School Incident Response

Scenario A: Ransomware Discovery (Beginner)

INCIDENT ALERT - PRIORITY: HIGH

Location: Riverside Middle School **Date/Time:** Monday, 7:45 AM **Reported By:** Multiple teachers

---

What's Happening

Several teachers arrived this morning and couldn't access their lesson plans. Their files show a weird ".locked" extension and there's a message demanding payment in cryptocurrency.

What We Know

- **Friday afternoon:** Everything was working fine
- **Weekend:** Unknown activity occurred
- **Monday morning:** 30% of school computers affected
- **Ransom note:** Demanding Bitcoin payment

Evidence Available

- Email logs showing suspicious attachment opened Friday
- Network traffic spike over the weekend
- Backup status: Last successful backup was Thursday night

Your Team's Mission

1. Assess the situation
2. Decide on immediate containment actions
3. Determine who needs to be notified
4. Plan recovery steps

Key Decisions You'll Face

- Isolate affected systems or shut down entire network?
- Contact law enforcement now or assess first?
- Inform parents immediately or after initial response?
- Attempt backup recovery or consider other options?

Scenario B: Grade Database Breach (Intermediate)

INCIDENT ALERT - PRIORITY: HIGH

Location: Riverside Middle School **Date/Time:** Wednesday, 2:30 PM **Reported By:** Anonymous tip

---

What's Happening

Someone reported that student grades have been changed in the system. When administrators checked, they found several suspicious modifications—all failing grades changed to passing.

What We Know

- **Two weeks ago:** An unauthorized admin account was created
- **Grade changes:** All follow the same pattern (F → C or better)
- **Access logs:** IP addresses from multiple locations
- **Data concern:** Student information may have been accessed

Evidence Available

- Unauthorized account creation timestamp
- List of modified grades
- IP address logs
- System access history

Your Team's Mission

1. Determine scope of the breach
2. Decide how to secure the system
3. Plan stakeholder communication
4. Consider academic integrity implications

Key Decisions You'll Face

- Lock down grade system or keep investigating first?
- Notify affected students individually or mass communication?
- Invalidate current grades or try to restore originals?
- Is this a security issue, a discipline issue, or both?

Scenario C: Social Media Compromise (Advanced)

INCIDENT ALERT - PRIORITY: CRITICAL

Location: Riverside Middle School **Date/Time:** Thursday, 11:00 AM **Reported By:** Parents, students, media

---

What's Happening

All school social media accounts have been hacked. Someone is posting inappropriate content and threats. The posts are going viral and local news media are calling.

What We Know

- **Last week:** Password reset emails were sent (staff ignored them)
- **Account access:** Coming from foreign IP addresses
- **Attack scope:** Multiple platforms (Instagram, Twitter, Facebook)
- **Data leak:** Staff personal information being posted

Evidence Available

- Timeline of suspicious activity
- Screenshots of malicious posts
- IP address traces
- List of compromised accounts

Your Team's Mission

1. Assess the damage
2. Decide on immediate actions
3. Develop communication strategy
4. Consider legal implications

Key Decisions You'll Face

- Delete accounts entirely or attempt recovery?
- Issue public statement or stay quiet until resolved?
- Lock down all school digital assets or targeted response?
- Involve law enforcement? School lawyers?

Grades 3-5: Mystery at Maple Elementary

COMPUTER PROBLEM ALERT

School: Maple Elementary **Classroom:** Mrs. Chen's 4th Grade **Date:** Monday morning

---

What's Wrong

The computers in Mrs. Chen's classroom are acting strange!

Symptoms:

- Pop-up messages keep appearing
- Messages say "CONGRATULATIONS! You WON!"
- Learning websites won't load
- Computers are running very slowly

Timeline

- **Friday:** Everything was working perfectly
- **Weekend:** No one was in the classroom
- **Monday:** Problems discovered when class started

Clues

- The pop-ups have spelling mistakes: "Congradulations!"
- Mrs. Chen remembers a student clicked on an email last Friday
- Other classrooms do NOT have this problem
- The pop-ups say "Click here for your prize!"

Your Mission

As the Computer Problem Solvers team:

1. Gather clues about what happened
2. Ask your AI helper for information
3. Figure out what went wrong
4. Recommend how to fix it

Remember: This kind of detective work is what real cybersecurity professionals do!

Grades K-2: Fix It Team Story

OH NO! THE COMPUTERS WON'T TURN ON!

(Teacher reads this aloud)

It's computer time at school! Everyone is excited to use the computers.

But when the teacher tries to turn on the classroom computers…

Nothing happens!

The screens stay dark. No lights. No sounds.

Mrs. Garcia tries another computer. Dark. She tries another one. Dark too!

"We need our Fix It Team!" says Mrs. Garcia. "Can you help figure out what's wrong?"

What We Know

- The computers worked yesterday
- The computers are plugged in
- The power strip lights are on
- But the computers won't start

Your Mission

Work together to find out what's wrong and fix it!

From "True Teamwork: Building Human-AI Partnerships" — NICE K12 2025 Dr. Ryan Straight, University of Arizona • ryanstraight@arizona.edu