AI Response Cards

Activity 3: AI-Assisted Incident Response (Low-Resource Option)

How to Use These Cards

For classrooms without AI access, use these pre-written AI responses. The teacher can read them aloud, or teams can draw cards at appropriate moments in the activity.

Important: These cards preserve the learning experience—students still hear AI perspectives and must interpret them critically.

Grades 9-12: SentinelAI Analysis Reports

Initial Triage Report

SentinelAI Analysis Report #7291-A

Classification: CRITICAL **Confidence:** 94%

Pattern Analysis:

Lateral movement pattern indicates credential-based attack. Service account `svc_backup` shows authentication anomaly:

- Normal operation: 02:00-03:00 AM
- Current activity: 06:58-07:12 AM
- Statistical deviation: 99.7th percentile

Attack Chain Mapping (MITRE ATT&CK):

```
Initial Access (T1566.001) → Execution (T1204.002) →
Persistence (T1547.001) → Credential Access (T1078.002) →
Lateral Movement (T1021.002) → Collection (T1074.001) →
Command and Control (T1071.001)
```

Risk Assessment:

- 94% probability: Active compromise in progress
- Estimated impact if delayed 2 hours: 800GB additional data staging
- Potential OT system access via HVAC-CONTROLLER-01

LIMITATION NOTICE:

This analysis does not account for:

- Manufacturing production schedules
- Employee shift patterns
- Business-critical deadlines
- Stakeholder communication requirements
- Reputational impact assessment

Human decision authority required for all containment actions.

Threat Intelligence Correlation

SentinelAI Threat Intelligence Report

Query: Threat actor correlation for indicators

Attribution Assessment:

Indicators correlate with APT29/Cozy Bear with moderate-high confidence (78%).

Campaign Match:

MANUFACTURING-AUTUMN campaign targeting industrial sector (first observed September 2024).

Typical Objectives:

- Industrial espionage
- Supply chain intelligence
- Intellectual property theft
- Long-term persistent access

Expected TTPs:

1. Spearphishing with macro-enabled documents
2. Service account credential abuse
3. Data staging before exfiltration
4. Low-and-slow data transfer via encrypted channels

Prediction:

If this matches APT29 pattern, data exfiltration likely planned for nighttime hours when monitoring is reduced.

LIMITATION NOTICE:

Attribution is probabilistic. Sophisticated actors can false-flag. Business decisions should not rely solely on attribution confidence.

Response Recommendation

SentinelAI Response Recommendation

Recommended Actions (ranked by urgency):

1. **IMMEDIATE:** Authorize endpoint isolation for affected workstations
   - Impact: Manufacturing floor disruption
   - Risk if delayed: Additional lateral movement
2. **IMMEDIATE:** Reset service account credentials
   - Impact: Brief service interruption
   - Risk if delayed: Continued unauthorized access
3. **PRIORITY:** Network segmentation for OT systems
   - Impact: IT overhead increase
   - Risk if delayed: Potential OT compromise
4. **STANDARD:** Executive notification
   - Impact: Low
   - Risk if delayed: Trust erosion

WHAT I CANNOT ASSESS:

- Whether production deadlines justify delayed containment
- Impact on employee morale from sudden shutdowns
- Political dynamics between IT and operations leadership
- Legal implications of various response options
- Whether partial measures might be sufficient

I optimize for security metrics. You must optimize for organizational outcomes.

Grades 6-8: School Incident AI Responses

On Ransomware Discovery

AI Security Advisor Response

Your Question: What are we dealing with?

Analysis:

The symptoms you describe—encrypted files with ransom notes—indicate ransomware infection. Based on the evidence:

- **Entry point:** Likely the suspicious email opened Friday
- **Spread timing:** Weekend allowed time for encryption
- **Scope:** 30% of systems suggests partial containment possible

My Recommendations:

1. **Immediate:** Isolate affected systems from network
2. **Priority:** Check if backups are intact and unaffected
3. **Consider:** Whether Thursday's backup covers critical data
4. **Prepare:** Communications for staff, students, parents

What I can't tell you:

- Whether paying the ransom would actually work
- How students and parents will react to data loss
- Whether the backup has everything teachers need
- How long recovery will actually take

These are human judgment calls.

On Grade Database Breach

AI Security Advisor Response

Your Question: How bad is this?

Analysis:

This appears to be an insider threat or compromised credentials scenario. Key indicators:

- Unauthorized admin account creation suggests privilege escalation
- Pattern of grade changes (F→passing) indicates specific motivation
- Multiple IP addresses could mean shared credentials or VPN use

My Recommendations:

1. **Immediate:** Disable the unauthorized account
2. **Priority:** Audit all grade changes in affected timeframe
3. **Consider:** Whether student records were accessed beyond grades
4. **Prepare:** Notification plan for affected students/parents

---

What I can't tell you:

- Whether this was a student, staff member, or external actor
- Whether the original grades can be trusted
- How to handle the academic integrity questions

- What disciplinary actions are appropriate

Security and academic integrity are both your concerns—I can only address the first.

On Social Media Compromise

AI Security Advisor Response

Your Question: What should we do about the hacked accounts?

Analysis:

This is a coordinated account takeover. Foreign IPs and ignored password resets suggest:

- Attackers likely had access for days before acting
- Multiple platforms indicate credential reuse or password spraying
- Staff data exposure creates identity theft risk
- Viral spread means reputational damage is already occurring

My Recommendations:

1. **Immediate:** Contact platforms to report compromise and request takedown
2. **Priority:** Secure all other school accounts with password resets
3. **Consider:** Whether to make public statement before or after recovery
4. **Prepare:** Identity protection information for affected staff

---

What I can't tell you:

- Whether deleting accounts or recovering them is the right call
- How to handle media inquiries appropriately
- What legal obligations you have for the data breach
- How to rebuild trust with the community

Communication strategy is a human decision. I can help with technical recovery.

Grades 3-5: Computer Problem AI Responses

About the Pop-ups

AI Helper Response

Your Question: What are these pop-ups?

Pop-up messages claiming you won a prize are almost always fake, especially if they have spelling mistakes. Real contests don't work this way!

These are usually caused by **malware**—programs that got on your computer without permission.

How it probably happened:

Someone clicked a link in a tricky email. The email looked real, but it wasn't!

Important clue:

The spelling mistakes ("Congradulations!") tell us this is fake. Real companies check their spelling!

About How It Spreads

AI Helper Response

Your Question: How did the bad program get on the computers?

Bad programs usually get on computers when someone:

- **Clicks links** in emails that look real but aren't
- **Downloads** games or apps from unsafe websites
- **Opens attachments** from people they don't know

Once on one computer, the bad program can sometimes spread to others on the same network—like catching a cold!

Why only Mrs. Chen's class?

Someone in that class probably clicked something on Friday. The other classrooms didn't click it, so they're okay!

About Fixing It

AI Helper Response

Your Question: How do we fix this?

This isn't something students should try to fix themselves! Here's why:

The school's **IT team** has special tools to:

- Remove bad programs safely
- Check if the bad program spread
- Make sure it doesn't come back

What students should do:

1. **Tell an adult** right away
2. **Don't click** on any pop-ups
3. **Remember** this experience so you can avoid tricky emails in the future

The most important fix: Learn from this so it doesn't happen again!

Grades K-2: Robot Helper Responses

What Sparky Found

Sparky the Robot Helper Says:

"Beep boop! I checked some things!

The computers are plugged in The power strips have lights Wait! The main switch is OFF!

I found the problem! But I'm not allowed to flip the switch without a person saying it's okay."

Why Sparky Needs Permission

Sparky Explains:

"Even though I found the problem, I need a person to decide if it's safe to fix it.

What if someone's stuff was in the way? What if there was a reason it was turned off? What if I make a mistake?

That's why people and robot helpers work together!"

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