Role Cards

Activity 3: AI-Assisted Incident Response

How to Use These Cards

Print and cut these cards for team assignments. Each team member receives one role card that defines their responsibilities during the incident response simulation.

Grades 9-12: SOC Analyst Simulation

Incident Commander (IC)

NICE Framework: Cyber Defense Incident Responder (PR-CIR-001)

Your Mission: You are the leader. You coordinate the team, make final decisions, and manage communication with leadership.

Your Responsibilities:

- Make final containment and escalation decisions
- Coordinate team activities and information flow
- Balance technical response with business impact
- Communicate with simulated executives

AI Partnership Focus:

Ask SentinelAI for:

- Impact assessment of different response options
- Prioritization recommendations based on risk
- Timeline estimates for response actions

Key Question to Keep Asking:

> "What's the business impact of each option?"

Remember: The team looks to you for decisions. Gather input, but don't delay—in incidents, delayed decisions have costs too.

Lead Analyst

NICE Framework: Cyber Defense Analyst (PR-CDA-001)

Your Mission: You are the technical expert. You analyze evidence, build the attack timeline, and identify the scope of compromise.

Your Responsibilities:

- Perform deep technical analysis of indicators
- Correlate data across network, endpoint, and authentication logs
- Build the attack timeline
- Determine attack vector and scope

AI Partnership Focus:

Ask SentinelAI for:

- Pattern analysis of network traffic
- MITRE ATT&CK technique mapping
- Correlation of indicators across evidence sources
- Known malware family identification

Key Question to Keep Asking:

> "What does the technical evidence tell us?"

Remember: You translate technical data into actionable intelligence for the team.

Threat Intelligence Analyst

NICE Framework: Threat/Warning Analyst (AN-TWA-001)

Your Mission: You are the context expert. You research who might be attacking, why, and what they typically do next.

Your Responsibilities:

- Research threat actor TTPs (Tactics, Techniques, Procedures)
- Identify attack campaign characteristics
- Predict likely next steps in the attack chain
- Provide attribution context

AI Partnership Focus:

Ask SentinelAI for:

- Threat actor profile matching
- Campaign correlation with known attacks
- TTP analysis and prediction
- Indicator enrichment from threat feeds

Key Question to Keep Asking:

> "Who is doing this and what do they typically want?"

Remember: Understanding the attacker helps predict their next move and prioritize defenses.

Communications Specialist

NICE Framework: Related to Cybersecurity Management

Your Mission: You are the voice of the team. You draft communications, document decisions, and ensure stakeholders are informed appropriately.

Your Responsibilities:

- Draft executive flash reports
- Prepare stakeholder notifications
- Maintain incident timeline documentation
- Coordinate messaging across audiences

AI Partnership Focus:

Ask SentinelAI for:

- Help translating technical findings into business language
- Suggested communication frameworks
- Key points for different audiences
- Timeline organization

Key Question to Keep Asking:

> "Who needs to know what, and when?"

Remember: Clear communication during incidents prevents panic and builds trust.

Evidence Coordinator (Optional 5th Role)

NICE Framework: Cyber Defense Forensics Analyst

Your Mission: You protect the evidence. You ensure proper documentation and chain of custody for potential legal proceedings.

Your Responsibilities:

- Ensure evidence preservation
- Maintain chain of custody documentation
- Coordinate forensic data collection
- Interface with potential law enforcement needs

AI Partnership Focus:

Ask SentinelAI for:

- Evidence prioritization recommendations
- Forensic artifact identification
- Timeline correlation assistance
- Documentation completeness checks

Key Question to Keep Asking:

> "Will this evidence hold up if we need it later?"

Remember: Evidence handled improperly becomes useless in investigations or legal proceedings.

Grades 6-8: Incident Response Teams

Incident Commander

Your Job: Team Leader

What You Do:

- Make final decisions when the team disagrees
- Keep the team focused on solving the problem
- Decide what to do first, second, third
- Report to the "principal" (teacher)

Ask AI About:

- "What should we prioritize?"
- "What are the risks of waiting?"

Remember: Good leaders listen to everyone, then decide.

SOC Analyst

Your Job: Technical Detective

What You Do:

- Look at the technical evidence (logs, alerts)
- Figure out what's happening on the systems
- Spot patterns the team might miss
- Explain technical stuff to teammates

Ask AI About:

- "What do these patterns mean?"
- "What attack is this similar to?"

Remember: You translate computer language for the team.

Threat Intelligence Specialist

Your Job: Attacker Expert

What You Do:

- Research what kind of attacker this might be
- Figure out what the attacker wants
- Predict what they might do next
- Help the team understand the threat

Ask AI About:

- "What type of attacker does this?"
- "What do they usually want?"

Remember: Understanding the enemy helps you beat them.

Communications Coordinator

Your Job: Message Crafter

What You Do:

- Write messages to tell others what's happening
- Keep track of what the team decides
- Make sure information is clear for non-technical people
- Document the timeline

Ask AI About:

- "How do I explain this simply?"
- "What should we tell parents/teachers?"

Remember: Clear communication prevents panic.

Grades 3-5: Problem Solver Teams

Detective

Your Job: Find the Clues!

What You Do:

- Look carefully at the evidence card
- Notice things that seem wrong or unusual
- Ask "What do I see?"
- Tell your team what you found

Remember: Good detectives notice small details!

AI Partner

Your Job: Talk to the AI Helper!

What You Do:

- Ask the AI helper good questions
- Listen to what the AI says
- Share the AI's answers with your team
- Remember: AI helps, but doesn't decide!

Remember: Good questions get good answers!

Recorder

Your Job: Write It Down!

What You Do:

- Write what the team discovers
- Keep track of decisions
- Make notes about the solution
- Fill out the team worksheet

Remember: If it's not written down, we might forget!

Reporter

Your Job: Tell the Class!

What You Do:

- Share your team's findings with the class
- Explain what happened and how you fixed it
- Answer questions from other teams
- Make sure everyone understands

Remember: Practice what you'll say before you present!

Grades K-2: Fix It Team (Whole Class)

Detective Badge

I am a Detective!

My job is to look for clues.

- What do I see?
- What's different?
- What's wrong?

Thinker Badge

I am a Thinker!

My job is to come up with ideas.

- What might have caused this?
- What could we try?
- What's another idea?

Helper Badge

I am a Helper!

My job is to do what the team decides.

- I'll try that!
- Let me help!
- What should I do next?

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