

Career Connections: AI-Assisted Incident Response

What You Did Today Connects to Real Careers

You just coordinated incident response like a SOC Analyst!

What You Did Today

Today you responded to a realistic security incident as part of a team. You took on a specific role, whether Incident Commander, SOC Analyst, Threat Intelligence Specialist, or Communications Coordinator. You worked with AI to analyze the situation and made decisions under pressure.

This is exactly what Security Operations Center teams do when real incidents happen.

The NICE Framework Work Role: Incident Responder

What Incident Responders Do

- **Coordinate response** to cybersecurity events and breaches
- **Lead teams** with different specialties working together
- **Consult AI systems** for rapid threat analysis
- **Make time-critical decisions** about containment and recovery

Key Tasks You Practiced

What You Did	What Incident Teams Call It
Assessed the situation as a team	Incident triage
Assigned roles and responsibilities	Response coordination
Used AI to analyze threats	Automated threat detection
Decided on actions to take	Incident containment
Communicated with stakeholders	Incident communication

Related Careers

SOC Analyst: First line of defense—monitors systems 24/7 and escalates potential incidents.

Incident Commander: Leads the response team during active incidents, making critical decisions.

Threat Intelligence Specialist: Researches attackers' tactics to inform response strategies.

Security Engineer: Builds and maintains the systems that detect and respond to threats.

The Roles You Played

Your Team Roles → Real Career Paths

Activity Role	Real-World Career
Incident Commander	Security Manager, CISO
SOC Analyst	Security Analyst, Tier 1-3 Analyst
Threat Intelligence	Threat Hunter, Intelligence Analyst
Communications Coordinator	Security Communications, PR

Every role matters. Real incident response requires diverse skills working together.

How Incident Response Teams Actually Work

Industry Reality Check

In real Security Operations Centers, incident response is not a conversation with AI. Rather, it is a coordinated workflow where AI tools support human decision-making:

Your Role Activity	Real-World Equivalent
Incident Commander made final calls	IR Managers coordinate response, authorize actions, and manage communication
SOC Analyst queried AI for analysis	Analysts review automated alerts from SIEM/XDR platforms and investigate with forensic tools
Threat Intelligence researched TTPs	Intel teams use MITRE ATT&CK, threat feeds, and AI-powered analysis to identify adversary patterns
Communications notified stakeholders	Crisis communication follows pre-planned playbooks while legal teams review disclosures

The key insight is that real incidents happen fast. Teams practice with tabletop exercises like today's activity so that when real incidents occur, everyone knows their role. AI tools generate alerts and recommendations, but humans make the critical decisions about containment, communication, and recovery.

Next Steps

Interested in learning more?

- **Explore NICE Framework:** nics.cisa.gov/workforce-development/nice-framework
- **Try CyberSeek:** cyberseek.org - See the incident response career pathway
- **Practice scenarios:** NCL (National Cyber League) includes incident response challenges

 Share With Your Teacher!

“Today I learned how SOC teams coordinate during security incidents. I practiced making decisions under pressure and working with AI analysis—just like real incident responders!”