Career Connections: Security Detective Teams

What You Did Today Connects to Real Careers

You just analyzed security data like a Cyber Defense Analyst!

What You Did Today

Today you investigated a security incident by examining login patterns, password weaknesses, and suspicious activity. You worked with an AI partner to spot patterns—and discovered that humans and AI together find things neither would catch alone.

This is exactly what cybersecurity professionals do every day.

The NICE Framework Work Role: Cyber Defense Analyst

What Cyber Defense Analysts Do

- **Analyze log data** to identify potential security threats
- **Correlate information** from multiple sources to build a complete picture
- **Partner with AI tools** that flag suspicious activity
- **Make recommendations** about what's really happening

Key Tasks You Practiced

What You Did	What Analysts Call It
Looked at login timestamps	Log analysis
Found patterns in password choices	Indicator correlation
Combined AI insights with your own	Human-AI collaboration
Decided what the evidence meant	Threat assessment

Related Careers

SOC Analyst: Works in a Security Operations Center monitoring alerts and investigating incidents in real-time.

Digital Forensics Analyst: Examines digital evidence after incidents to understand exactly what happened.

Vulnerability Analyst: Identifies weaknesses in systems before attackers can exploit them.

Threat Intelligence Analyst: Researches attack patterns and threat actors to predict future risks.

Next Steps

Interested in learning more?

- **Explore NICE Framework**: niccs.cisa.gov/workforce-development/nice-framework
- **Try CyberSeek**: cyberseek.org - See cybersecurity career pathways and job demand
- **Find competitions**: CyberPatriot, National Cyber League, picoCTF

> 💡 **Share With Your Teacher!**
>
> "Today I learned that Cyber Defense Analysts work with AI systems to protect organizations. I practiced analyzing security data just like they do!"