AI Cybersecurity Careers

AI Cybersecurity: Emerging AI Roles with Real Impact

By Rob T. Lee • SANS Institute • July 2025

Two years of industry tracking reveal these emerging AI cybersecurity roles. We observed AI cybersecurity roles maturing through SANS Summit presentations, expert discussions, course development, and community insights. The focus: defending the nation's new AI technological capabilities.

SANS

AI Incident Response Orchestrator

RAPIDLY EXPANDING FIELD

What You Do

Command defensive AI agents in direct combat against adversarial agents inside your network. Your defensive swarms hunt malicious code, stop attack sequences, and repair systems faster than attacks can spread.

Problem You Solve:

AI-powered ransomware can compromise entire networks within minutes. Human response teams can't match machine-speed attacks, so you need agent-versus-agent automated warfare capabilities.

SANS TRAINING › SEC598 SEC595 FOR508

AI Offensive Orchestrator

HIGH DEMAND • RAPIDLY GROWING

What You Do

Manage AI agent swarms that run autonomous penetration testing and red teaming 24/7. Your agents continuously test every code change and network modification, adapting their attack methods based on how defenses respond.

Problem You Solve:

Iranian APT groups use AI throughout their entire attack process. Organizations need red teams that can match AI-enhanced attack methods because human-speed testing can't keep up with machine-speed threats.

SANS TRAINING › SEC598 SEC535

AI/ML Security Engineer

HIGH DEMAND • SIGNIFICANT GROWTH

What You Do

Build AI-driven security solutions that automatically map your attack surface, detect capability gaps, and respond to emerging threats. Your systems learn your environment beyond what human analysts can handle.

Problem You Solve:

BlackMamba and similar polymorphic AI malware can evade top endpoint detection systems. Organizations need defensive AI that can think like attackers and adapt faster than traditional security tools.

SANS TRAINING › SEC595 SEC545 SEC450

AI Security Specialist

STRONG DEMAND • ALL INDUSTRIES

What You Do

Guide strategic AI adoption with security intelligence. You evaluate AI projects for immediate security risks, monitor multiple AI initiatives across business units, and provide fast security impact assessments.

Problem You Solve:

Most phishing emails now contain AI-generated content, and organizations experiencing AI-related security incidents pay millions per breach. Companies need strategic guidance more than specialized technical depth.

SANS TRAINING › SEC595 SEC511 SEC450

AI Threat Intelligence Analyst

HIGH VOLUME • CONSISTENT DEMAND

What You Do

Transform threat intelligence into immediate hunting operations across hundreds of environments simultaneously. Your AI agents convert new attack patterns into executable hunting queries that deploy across partner organizations instantly.

Problem You Solve:

Dozens of nation-state actors now use AI for cyber operations. Traditional threat intelligence analysis is too slow to enable coordinated defense against AI-enhanced threats operating at machine speed.

SANS TRAINING › SEC587 FOR578 SEC497

AI SOC Orchestrator

EXCELLENT ENTRY POINT • WIDESPREAD ADOPTION

What You Do

Lead security operations centers using AI agent swarms instead of traditional alert monitoring. Your agents automatically detect, investigate, correlate, and respond to threats while you make strategic decisions.

Problem You Solve:

RansomHub and Cl0p use AI-powered "smash-and-grab" tactics that traditional SOCs can't match. You need reasoning systems that actively hunt threats instead of just responding to alerts.

SANS TRAINING › SEC598 SEC511 SEC401

AI Ethics & Compliance Officer

GROWING REGULATORY FOCUS

What You Do

Deploy real-time compliance governance agents that automatically adjust AI systems to maintain regulatory compliance. You build policy enforcement agents that block non-compliant deployments before they happen.

Problem You Solve:

Significant portions of AI prompts pose data leakage risks, and regulatory pressure is building fast. Organizations need automated compliance monitoring because static policies can't keep up with rapid AI development.

SANS TRAINING › LDR514 LDR512

AI Governance Lead

STRONG ORGANIZATIONAL NEED

What You Do

Build AI governance orchestration systems that automatically enforce policies, track compliance, and adapt to evolving AI capabilities. Your systems monitor AI utilization across all business sectors in real-time.

Problem You Solve:

North Korea infiltrated extensive U.S. technology companies using AI-generated fake identities. Organizations need governance frameworks that work before regulatory enforcement arrives, not after.

SANS TRAINING › LDR514 LDR512

Quantum-AI Security Specialist

EMERGING • EXCEPTIONAL LONG-TERM POTENTIAL

What You Do

Develop quantum-resistant security systems and quantum-powered threat detection agents. You create hybrid quantum-classical AI security architectures that provide computational advantages over traditional systems.

Problem You Solve:

Advanced threat actors will develop extensive malware repositories for training efficient AI models starting from 2027. Quantum computing will dramatically accelerate these threats against critical systems.

SANS TRAINING › SEC595 SEC598

AI Prompt Engineer (Security)

LIMITED VOLUME • PREMIUM COMPENSATION

What You Do

Build prompt orchestration systems that modify AI responses dynamically for security needs. You develop prompt libraries that work across various security AI tools and create testing agents that detect adversarial prompt vulnerabilities.

Problem You Solve:

Adversaries use "adversarial self-replicating prompts" to trick AI models into executing harmful payloads. Organizations struggle to extract meaningful value from AI security solutions without proper prompt engineering.

SANS TRAINING › SEC545 SEC495 SEC535