Member-only story

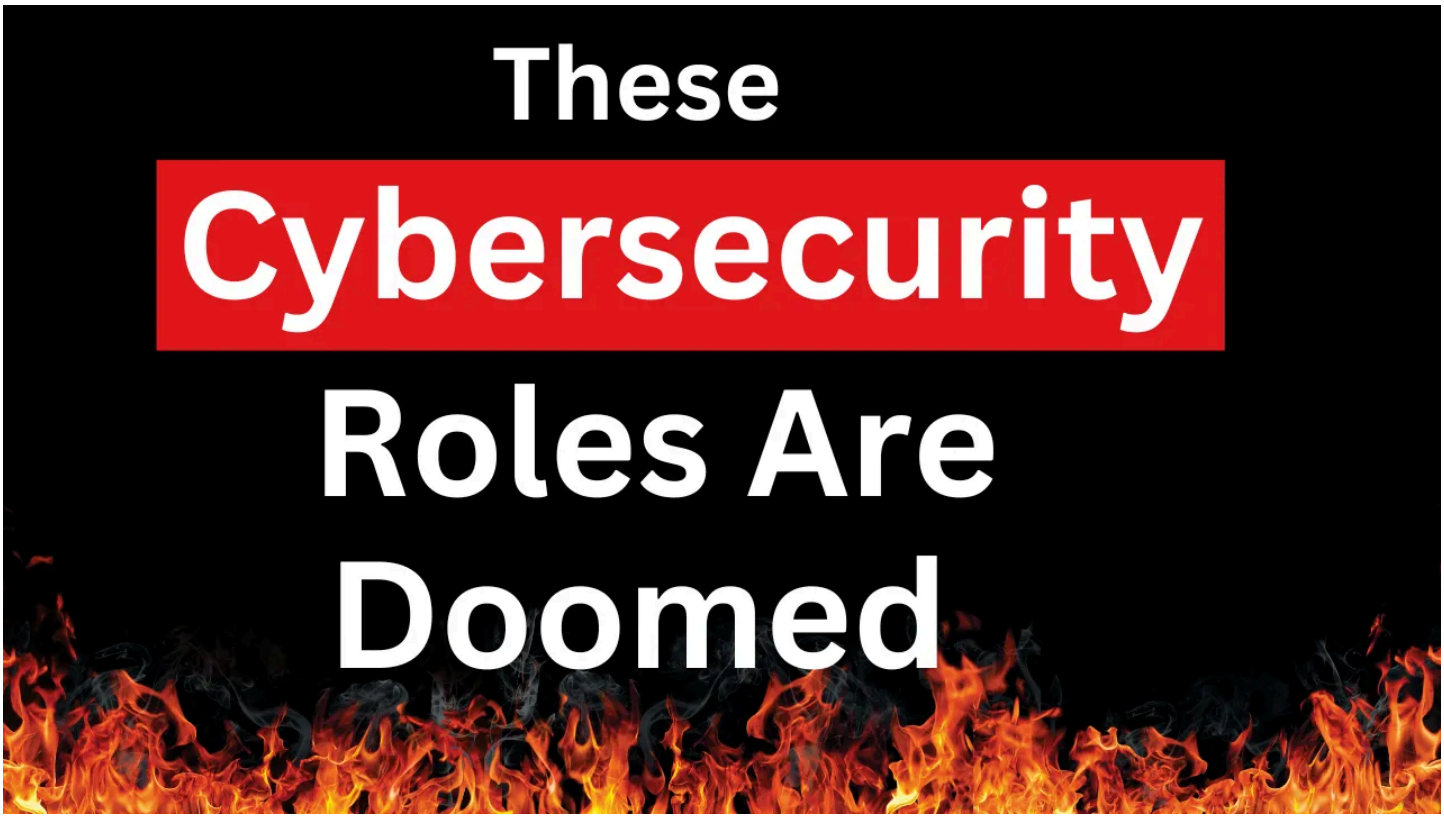
The 5 Cybersecurity Roles That Will Disappear First

Think your job is safe from AI? Think again. These are the first cybersecurity roles AI will eat.”

5 min read · 1 day ago

Taimur Ijlal Follow

Listen Share More



Last week, I had a coffee chat with a cybersecurity analyst — let’s call him Adeel.

He looked relaxed. Confident, even.

He told me:

> “AI won’t affect my role. I monitor security alerts and escalate anything weird. We’ll always need humans for that, right?”

I asked him .. “Adeel, what if I told you there are already AI agents triaging alerts, contextualizing threats, and auto-escalating critical incidents faster than you can say ‘SIEM’?”

Thankfully Adeel did listen to me and agreed to assess where he stood but he is not alone.

Cybersecurity is evolving fast.

And while demand for expertise is growing, the kind of work that’s valued is changing even faster.

The types of roles that will thrive — and those that will quietly fade — are changing fast.

If you’re in cybersecurity today or planning to enter the field, knowing which roles are at risk is no longer optional. It’s essential to surviving the shift.

So here’s your wake-up call: these are the 5 cybersecurity roles most at risk of disappearing — and what you can do to avoid becoming obsolete.

1. Tier 1 SOC Analyst

Why it will disappear:
This role often involves manually reviewing logs, triaging alerts, and following predefined workflows in SIEM systems. It’s repetitive, rules-based, and slow.

How AI is replacing it:
Modern security platforms are already integrating AI-driven alert prioritization, auto-triage, and decision trees. Combine that with LLMs capable of contextualizing

alerts, and suddenly, what once required human eyes can now be done by an intelligent agent in seconds.

What's at risk:
If your job is mostly "reading alerts, matching patterns, escalating when unsure," you're on borrowed time.

What to do instead:
Upskill toward Tier 2/3 incident response. Learn scripting, automation or cloud incident triage. Become the person who builds and tunes the systems — not just someone who reads them.

2. The Security Compliance Checklist Auditor

Why it will disappear:
Many entry-level GRC roles involve collecting evidence for audits, checking off control implementation, and ensuring adherence to frameworks like ISO 27001 or NIST 800–53. It's tedious and highly structured.

How AI is replacing it:
AI systems can now ingest policies, controls, logs, and configuration snapshots, then automatically map them to compliance standards. Tools are already automating large parts of this process. With the rise of GenAI, we'll see AI-powered policy interpreters and evidence collectors do this work even faster.

What's at risk:
The "compliance analyst" who moves spreadsheets and screenshots between folders will be replaced by bots that integrate directly with cloud platforms.

What to do instead:
Pivot into AI governance strategy (understanding regulatory impact) or compliance automation engineering (writing logic to pull audit data). Learn how to apply compliance frameworks to novel environments like AI systems, which still need human interpretation.

3. Basic Vulnerability Assessor

Why it will disappear:
This role typically involves running scanners (e.g., Nessus, Qualys), generating reports, and flagging common misconfigurations. It's mostly mechanical.

How AI is replacing it:
Modern cloud-native scanners already auto-prioritize findings.

AI agents can contextualize vulnerabilities, assess exploitability based on environment, and even propose remediation.

Soon, companies won't need someone to run a scan — they'll need someone to understand the risk *in context*.

What's at risk:
If your value is tied to "running scans and sending reports," you'll be undercut by tools that do it faster, better, and cheaper.

What to do instead:
Focus on vulnerability management, not just assessment. Learn how to prioritize based on threat intel, asset criticality, and business risk. Or specialize in emerging areas like AI model vulnerability scanning or SBOM analysis for supply chain risk.

4. Firewall Rule Manager

Why it will disappear:
This role revolves around managing rule changes, updating signatures in IDS/IPS, and maintaining allow/block lists. It's reactive and driven by known threats.

How AI is replacing it:
AI models trained on years of traffic and threat data can now auto-generate and refine firewall policies and IDS signatures. Agentic AI systems are capable of identifying anomalous flows and adjusting controls in real time — without waiting for human approval.

What's at risk:
If your work consists of "reacting to tickets to modify ports and protocols," your role

is likely to be phased out in the next few years.

What to do instead:
Move toward network security architecture or zero trust design. Focus on strategic segmentation, microservices traffic modeling, or IAM-based access controls — areas where critical thinking still trumps automation.

5. Access Review Coordinator

Why it will disappear:
These roles often involve checking identity access reports, enforcing password resets, or managing periodic access certifications. Again, highly rules-based.

How AI is replacing it:
With identity governance platforms integrating AI-driven access reviews, much of this is being automated. AI can now analyze behavioral anomalies, enforce just-in-time access, and auto-remove stale accounts.

What's at risk:
If your job is "sending reminder emails and collecting approvals," AI bots will do it better — and won't forget.

What to do instead:
Lean into identity engineering — how systems authenticate, federate, and issue tokens securely. Or specialize in AI-augmented access governance, where you build logic and rules for continuous authentication, behavioral scoring, and decentralized access models.

Final Thoughts: It's Not All Doom and Gloom

This isn't a doomsday article. It's a wake-up call.

Cybersecurity isn't going away.

In fact, it's expanding. But boring, repetitive cybersecurity is being automated. If your role is easy to document, it's easy to replace.

Here's what won't be automated anytime soon:

- Threat modeling complex AI/ML systems
- Designing secure architectures for multi-cloud environments
- Managing the ethics and risks of agentic AI
- Advising the board on data governance or cyber liability
- Communicating security posture to non-technical stakeholders

In other words: **thinking, creating, deciding, and leading** still matter. And they'll matter more than ever.

What You Should Do Next

1. **Audit your role**: Is most of your day repetitive or judgment-based? If it's the former, your clock is ticking.
2. **Level up**: Learn about AI risks, secure software architecture, GenAI governance, or cloud-native security. Don't get left behind.
3. **Build a brand**: Start teaching what you learn — on LinkedIn, YouTube, blogs. The people who teach will lead in the AI era.
4. **Explore independence**: The rise of solopreneur cybersecurity professionals (powered by AI agents) is real. Start planting seeds now.

Good luck in the exciting future ahead !