Cyber Security
Pro-Agentics Platform

Aug 2025

Cyber Security Challenges

Multiple Security Tools

Avr. Cyber Tools (Enterprises): ~76

Overflow Of Threats & Vulnerabilities

Avr. Daily Alerts: ~10k-15k/day

Avr. Critical Vulnerabilities: 476

Talent Shortage

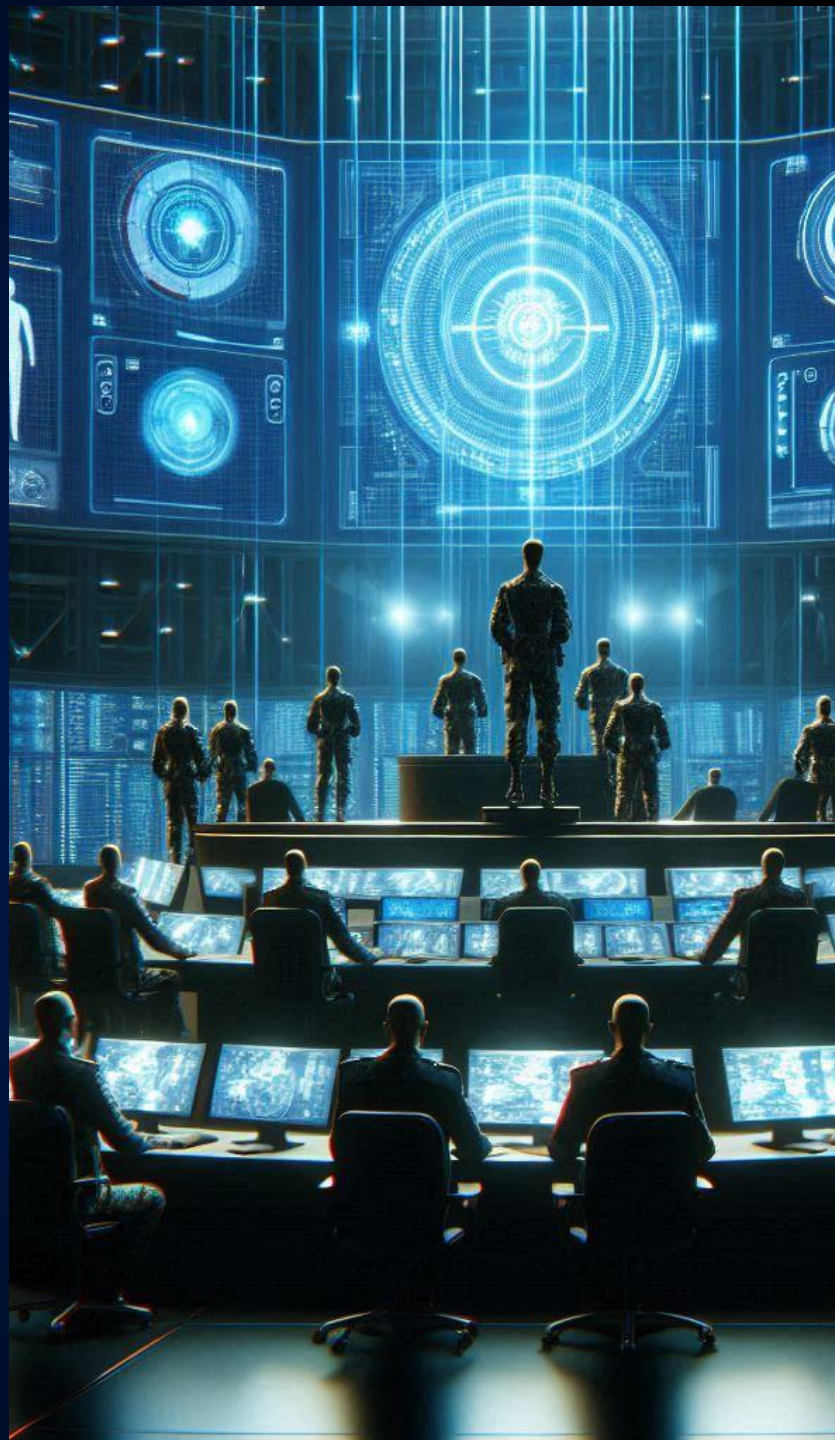
Current Shortage gap of 3.4 million cybersecurity experts

2025 All Right reserved to Neo CISO, Inc.

Assuming Control

A Pro-Agentics Centralized Platform

- Context-Aware Analysis
- Clear Holistic Organizational Picture
- Professional Grade Decisions



2025 All Right reserved to Neo CISO, Inc.

Across Multiple Security Domains

Holistic Cyber View

- Threats
- Identity
- Posture

IT / OT / Cloud

2025 All Right reserved to Neo CISO, Inc.

NeoCISO Acts As A Security Professional

Builds the picture

The Agent pulls and validates all the relevant data points

Synthesizes context

What happened / why it matters / impact - narrative

Determinations

Severity, Priorities, Trade-offs Laid Out

Owns The Workflow

Orders The Next Steps & Identified Stakeholders

Records Rationale

Every Choice And Its Evidence Were Logged

2025 All Right reserved to Neo CISO, Inc.

Cyber Professionals' Essentials

Governed

Credible

Managed

NeoCISO's
Pro-Agentics

Practical Knowledge

Proven Strategies

Battle Tested Techniques

2025 All Right reserved to Neo CISO, Inc.

Augmented Power Multiplier

Utilizing Current Security Tools & Operational Data i.e:

2025 All Right reserved to Neo CISO, Inc.

Cyber Professional Agentics

Interpreting Your Cyber Security Data
Into A Clear Picture

By Implementing The Best Of Industry
Practical Knowledge
Battle-Tested Techniques
Proven Strategies

2025 All Right reserved to Neo CISO, Inc.

Uncovering The Story Through Time

An XDR detects suspicious activity in one of the servers.

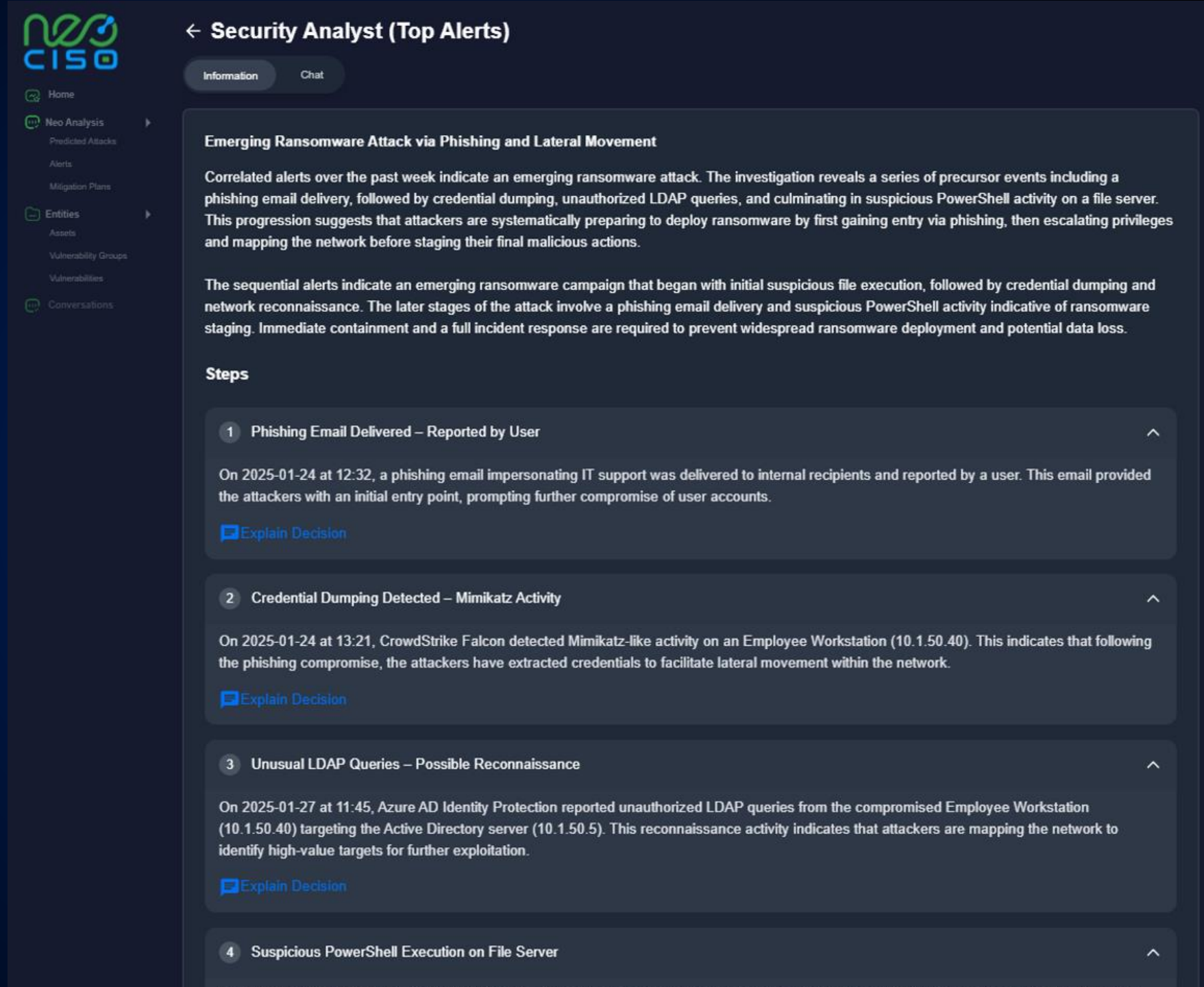
NeoCISO connects the dots to past events to uncover the story of an emerging attack.

2025 All Right reserved to Neo CISO, Inc.

Uncovering The Story Through Time

An XDR detects suspicious activity in one of the servers.

NeoCISO connects the dots to past events to uncover the story of an emerging attack.



2025 All Right reserved to Neo CISO, Inc.

Automating Audit Reports

Automated cybersecurity reports that comply with ISO 27001, NIST, SOC2, GDPR

2025 All Right reserved to Neo CISO, Inc.

Executive Summary

This report provides an analysis of potential cyber attack vectors targeting Acme Corporation, based on vulnerabilities detected during our April 2024 security assessment. It highlights changes from the March 2024 report and identifies emerging threats.

Total Vulnerabilities Detected

237

(↑12% from last month)

Critical Vulnerabilities with Viable Attack Paths

17

(↑3 from last month)

Key Findings and Trends:

1. Windows Privilege Escalation: The number of workstations vulnerable to CVE-2021-28310 has increased by 15% since last month. This persistent issue now affects **127** systems, up from **110**, indicating that patch management processes are falling behind.
2. Web Application Risks: While **60%** of the Apache Struts 2 vulnerabilities (CVE-2020-17530) identified last month have been addressed, we've detected new instances on recently deployed servers. This suggests a gap in security protocols for new system deployments.
3. VPN Vulnerabilities: Unpatched Cisco AnyConnect systems remain a significant concern. The number of affected systems has decreased by only **10%**, leaving **85%** of these critical access points still vulnerable.
4. Phishing Susceptibility: Our latest simulated phishing campaign shows a 5% increase in click-through rates compared to last month, with the Finance department showing the most significant decline in resilience.
5. Legacy System Exposures: While efforts to isolate vulnerable legacy systems in the manufacturing division have begun, 90% of the issues identified last month remain unaddressed. Two new critical vulnerabilities were also discovered this month in these systems.
6. Emerging Threat - Cloud Misconfigurations: As Acme accelerates its cloud migration, we've identified **23** instances of misconfigured cloud storage buckets, a new category of vulnerability not present in last month's report. These misconfigurations could lead to unauthorized data access or leakage.

The persistence and growth of several key vulnerabilities month-over-month is particularly concerning. The increase in total vulnerabilities, despite some issues being resolved, indicates that new weaknesses are being introduced at a faster rate than existing ones are being addressed. This trend is especially evident in the rising number of critical vulnerabilities with viable attack paths.

The report provides detailed attack methodologies for each vulnerability category, including potential impact and specific exploitation techniques. We've also included a new section this month analyzing the patterns in vulnerability introduction and remediation, aiming to identify systemic issues in Acme's security processes.

Given the increasing exploit success probability and potential financial impact, immediate attention to these vulnerabilities is crucial. The persistent nature of many issues from last month's report suggests a need for a comprehensive review of Acme's vulnerability management and patching processes, particularly focusing on the gaps in addressing known issues and preventing the introduction of new vulnerabilities in system

Getting The Job Done

- Triage–Sec. Incidents
- Builds Mitigation Plans
- Vulnerability Analysis & Prioritization
- SIEM/SOC Augmentation
- Mapping Incidents Across Kill-Chain
- Unified Threats Visibility
- Simulated Risk Impact Scenario

Competitive Landscape

	AI Traditional Approach	Pro-Agentics Platform
Contextual Awareness	✗ **Static Playbooks**	✓ Live Organizational Context Drives Every Analysis & Decision
Decision Auditability	✗ **Black-Box AI, Opaque Algorithms With No Audit Trail**	✓ Step-By-Step Professional Reasoning & Auditability
Governed Decisions	✗ **Hard-Coded Rules, Limited Oversight**	✓ Governed Organizational Principles & Processes
Mitigation Plans	✗ **Reactive, Inconsistent Responses**	✓ Holistic, Methodology-Backed Mitigation Within Organizational World View & Limitations

2025 All Right reserved to Neo CISO, Inc.

Market Opportunity

AI in Cybersecurity is projected to reach $93.75 billion by 2030 CAGR of 24.3% (2023-2030)

MSSPs Market is projected to reach $141.18 billion by 2030 CAGR of 15.6% (2023-2030)

The Cybersecurity Workforce Gap Market is projected to reach $306 billion by 2030– a CAGR of 4% (2023-2030)

*(ISC)²'s Cybersecurity Workforce Study (2023)

2025 All Right reserved to Neo CISO, Inc.

Pro-Active Cyber Security Professional Agentic Platform

Get in Touch:

+972. 54.678.6042

Info@neociso.com

https://www.neociso.com

*NeoCISO Logo, Brand & Tool are a proprietary & copyright of NeoCISO, INC.

2025 All Right reserved to Neo CISO, Inc.