



# Cyber Security Pro-Agents 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*





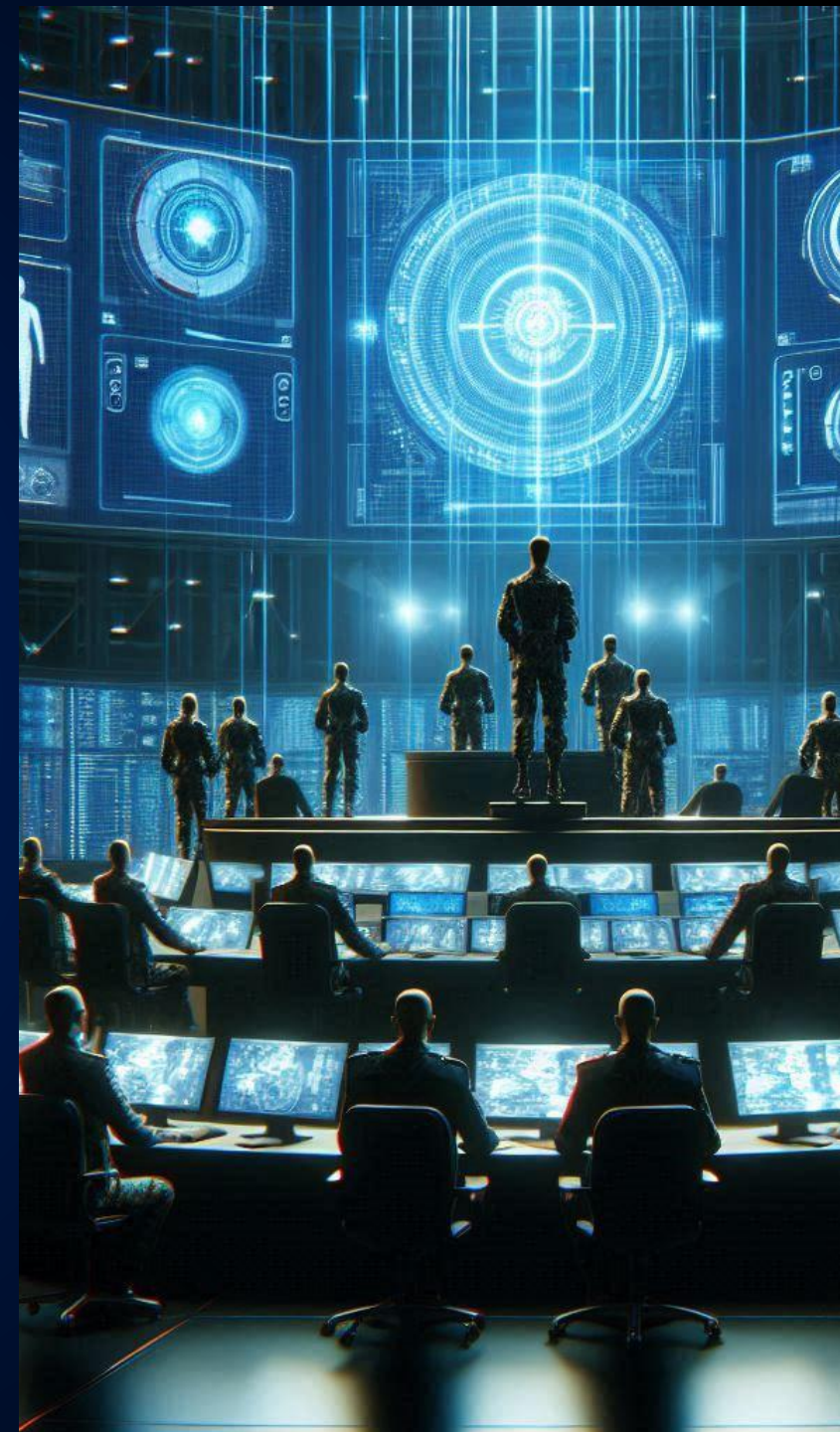
# Assuming Control

## A Pro-Agentics Centralized Platform

Context-Aware  
Analysis

Clear Holistic  
Organizational  
Picture

Professional  
Grade Decisions





# Across Multiple Security Domains

## Holistic Cyber View

Threats

Identity

Posture

IT / OT / Cloud





# 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



# Cyber Professionals' Essentials



# Augmented Power Multiplier

Utilizing Current Security Tools & Operational Data i.e:





# 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





# 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.





# 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.



- Home
- Neo Analysis
  - Predicted Attacks
  - Alerts
  - Mitigation Plans
- Entities
  - Assets
  - Vulnerability Groups
  - Vulnerabilities
- Conversations

## ← Security Analyst (Top Alerts)

Information

Chat

### Emerging Ransomware Attack via Phishing and Lateral Movement

Correlated alerts over the past week indicate an emerging ransomware attack. The investigation reveals a series of precursor events including a phishing email delivery, followed by credential dumping, unauthorized LDAP queries, and culminating in suspicious PowerShell activity on a file server. This progression suggests that attackers are systematically preparing to deploy ransomware by first gaining entry via phishing, then escalating privileges and mapping the network before staging their final malicious actions.

The sequential alerts indicate an emerging ransomware campaign that began with initial suspicious file execution, followed by credential dumping and network reconnaissance. The later stages of the attack involve a phishing email delivery and suspicious PowerShell activity indicative of ransomware staging. Immediate containment and a full incident response are required to prevent widespread ransomware deployment and potential data loss.

#### Steps

##### 1 Phishing Email Delivered – Reported by User

On 2025-01-24 at 12:32, a phishing email impersonating IT support was delivered to internal recipients and reported by a user. This email provided the attackers with an initial entry point, prompting further compromise of user accounts.

[Explain Decision](#)

##### 2 Credential Dumping Detected – Mimikatz Activity

On 2025-01-24 at 13:21, CrowdStrike Falcon detected Mimikatz-like activity on an Employee Workstation (10.1.50.40). This indicates that following the phishing compromise, the attackers have extracted credentials to facilitate lateral movement within the network.

[Explain Decision](#)

##### 3 Unusual LDAP Queries – Possible Reconnaissance

On 2025-01-27 at 11:45, Azure AD Identity Protection reported unauthorized LDAP queries from the compromised Employee Workstation (10.1.50.40) targeting the Active Directory server (10.1.50.5). This reconnaissance activity indicates that attackers are mapping the network to identify high-value targets for further exploitation.

[Explain Decision](#)

##### 4 Suspicious PowerShell Execution on File Server



# Automating Audit Reports

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



## 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)

### Key Findings and Trends:

- 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.
- 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.
- 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.
- 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.
- 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.
- 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.

Critical Vulnerabilities with Viable Attack Paths

**17**

(3 from last month)

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





# Competitive Landscape

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



# 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)<sup>2</sup>'s Cybersecurity Workforce Study (2023)



Pro-Active Cyber Security  
Professional Agentic  
Platform

## Get in Touch:

 +972. 54.678.6042

 [Info@neociso.com](mailto:Info@neociso.com)

 <https://www.neociso.com>

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