CNXN HELIX
CENTER FOR APPLIED A.I. AND ROBOTICS

Turning Security Alerts into Actionable Outcomes

A practical approach to reducing alert fatigue, improving SOC efficiency, and helping security teams focus on real threats.

Security operations teams are under increasing pressure to improve outcomes without increasing overhead. Alert volumes continue to rise, security environments grow more complex, and experienced cybersecurity talent remains difficult to find and retain. As a result, many organizations struggle to investigate every alert, maintain consistent coverage, and keep pace with evolving threats. Security leaders are looking for ways to improve visibility, accelerate investigations, and extend the capacity of their teams without continuously adding headcount.

AI security operations center (AI SOC) helps address these challenges by automating investigation, enrichment, and triage activities—enabling security teams to investigate more alerts, improve efficiency, and maintain control over critical security decisions.

The Challenge

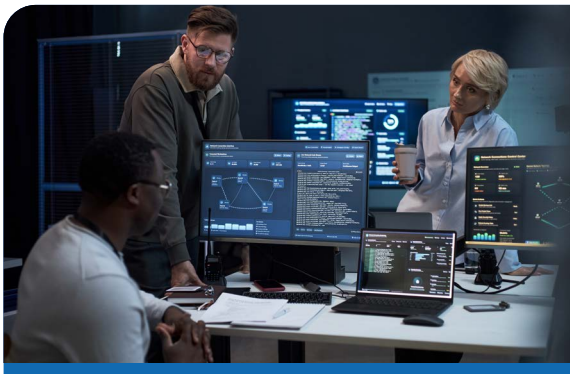
Most organizations have invested heavily in cybersecurity technologies. Yet despite stronger tools and more data, security teams continue to face significant operational challenges.

Common barriers include:

- Thousands of alerts generated across security platforms every day
- High false-positive rates that consume valuable analyst time
- Limited ability to provide consistent 24/7 coverage
- Low- and medium-severity alerts that often receive little or no investigation
- Growing pressure to improve security outcomes without increasing headcount
- Analyst burnout caused by repetitive manual triage and investigation tasks

The Result

Security teams spend too much time managing alerts and not enough time responding to real threats.



AI SOC is not about replacing security teams—it's about helping them operate at a greater scale.

A New Operating Model for Security Operations

Leading organizations are adopting AI-assisted security operations to improve efficiency, expand coverage, and investigate more alerts without proportionally increasing staffing requirements.

Investigate More Alerts

Apply AI-driven triage and investigation across security telemetry from endpoints, cloud environments, identities, email systems, networks, and SIEM platforms.

Reduce Alert Fatigue

Automatically classify, enrich, and prioritize alerts so analysts can focus their attention where it matters most.

Accelerate Investigations

Provide security teams with actionable context and evidence faster, reducing time spent gathering information across multiple systems.

What Makes This Work

Improving SOC performance requires more than adding another security tool. It requires the right combination of automation, intelligence, integration, and human oversight. CNXN Helix helps organizations build that foundation through:

AI-driven Investigation and Triage

Automate repetitive investigation tasks while ensuring alerts receive the attention they deserve.

Security Context and Enrichment

Correlate information across security platforms to provide analysts with deeper insight into potential threats.

Integration with Existing Security Investments

Enhance the value of existing SIEM, EDR, XDR, cloud security, identity, and security operations platforms.

Continuous Improvement

Investigation outcomes can be used to improve detection quality, reduce noise, and strengthen security operations over time.

Human-guided Decision Making

AI helps perform investigation and analysis while security teams remain in control of response and remediation decisions.

Organizations are not starting over—they are building upon the investments they have already made.

- **Business Outcomes:** Organizations adopting AI-assisted security operations can achieve meaningful improvements across their SOC.
- **Improve SOC Efficiency:** Reduce repetitive investigation work and enable analysts to focus on higher-value security activities.
- **Expand Security Coverage:** Increase visibility across alerts, systems, and environments without relying solely on additional personnel.
- **Improve Analyst Retention:** Minimize repetitive triage activities that contribute to burnout and turnover.
- **Accelerate Response:** Reduce investigation times by providing analysts with enriched context and actionable insights.
- **Increase Operational Capacity:** Support growing alert volumes and security demands without proportionally increasing staffing requirements.
- **Strengthen Security Posture:** Help security teams identify, investigate, and respond to meaningful threats more effectively.

The CNXN Helix Approach

Successful AI initiatives begin with business outcomes, not technology alone. CNXN Helix™ Center for Applied AI and Robotics helps organizations evaluate where AI can improve security operations, align those opportunities with existing security investments, and build a practical path from initial deployment to operational scale.

Our team works with customers to:

- Assess current SOC operations, workflows, and challenges
- Identify opportunities for AI-driven automation and efficiency
- Align security objectives with business priorities
- Integrate AI capabilities alongside existing security investments
- Develop a practical roadmap for adoption and scale

The Path Forward

Security teams do not need more alerts. They need a better way to investigate them. Organizations that successfully adopt AI SOC start with a clear understanding of their operational challenges, security priorities, and desired outcomes.

Whether your goal is improving SOC efficiency, expanding security coverage, reducing analyst fatigue, or accelerating investigations, AI SOC provides a practical path forward.

To learn how Connection and CNXN Helix can help modernize your security operations with AI, contact your Account Team today.

Business Solutions
1.800.800.0014

Enterprise Solutions
1.800.369.1047

Public Sector Solutions
1.800.800.0019

www.cnxnhelix.com

© 2026 PC Connection, Inc. All rights reserved. Connection®, CNXN Helix™ and we solve IT® are trademarks of PC Connection, Inc. All other copyrights and trademarks remain the property of their respective owners. 3799671-0626