

COGNNA Nexus

# Agentic AI SOC Platform

Revolutionize cybersecurity operations with an AI-powered, autonomous SOC platform that predicts, prevents, and responds to threats in real-time, freeing human analysts to focus on strategic initiatives.



## Legacy detection and response is broken. It's time to reimagine your SOC.

**COGNNA Nexus** is an AI-powered, autonomous SOC platform leveraging cognitive analytics and intelligent AI agents to proactively predict, validate, analyze, prevent, and autonomously respond to threats in real time across diverse environments, allowing analysts to focus on strategy and reducing reliance on human experts. Unlike fragmented solutions, COGNNA unifies deep telemetry, real-time detection, advanced threat hunting, autonomous investigation, advanced threat intelligence, and guided response into a flexible, scalable, intelligence-first platform enhanced by context-aware AI, CVE/CPE mapping, and automated correlation. This provides complete context, reduces noise, and offers actionable clarity with built-in compliance and explainable automation, shifting the SOC to a proactive, analyst-friendly operation that improves MTTR and reduces fatigue, acting as a collaborative AI force multiplier.

### PLATFORM ADVANTAGES

**Autonomous Threat Management:** AI-powered platform predicts, prevents, and responds to threats.

**Reduced Reliance on Human Experts:** Automation and intelligent agents minimize the need for extensive manual analysis.

**Enhanced Efficiency:** Streamlines threat detection, investigation, and response processes.

**Improved Accuracy:** Cognitive analytics validates and analyzes threats, reducing false positives.

**Comprehensive Visibility:** Provides real-time asset tracking and vulnerability scanning.

**Simplified Operations:** Eliminates SIEM complexity and the need for multiple external tools.

**Faster Response Times:** Enables swift action and streamlined incident resolution.

**Continuous Learning:** Adaptive and always learning AI agents improve security posture over time.

## PLATFORM MODULES

### DISCOVER

#### Autonomous Asset & Vulnerability Visibility

Provides real-time, risk-prioritized asset tracking and comprehensive vulnerability scanning, eliminating the need for manual effort and external tools.

### DETECT

#### Streamlined Threat ID & Prioritization

Enables immediate threat correlation, automated alert triage, and enriched threat intelligence, simplifying detection and eliminating SIEM complexity.

### INVESTIGATE

#### Accelerated Threat Analysis & Root Cause ID

Facilitates real-time threat validation and comprehensive post-incident forensics, enabling rapid analysis and root cause determination.

### RESPOND

#### Decisive & Unified Incident Resolution

Offers remote device isolation and centralized case management, ensuring swift action and streamlined incident response.

## USE CASES

### Automated Security Operations Center (SOC)

Fully automate threat detection, investigation, and response workflows.

### Real-time Threat Prevention

Proactively identify and block malicious activities before they impact the organization.

### Vulnerability Management

Continuously monitor and prioritize vulnerabilities for remediation.

### Incident Response Automation

Automate incident response procedures, minimizing downtime and impact.

### Security Posture Assessment

Gain a real-time understanding of the organization's security risk and receive actionable recommendations.

### Enhanced Alert Triage

Automatically filter and prioritize security alerts, reducing alert fatigue for security teams.

### Post-Incident Forensics

Rapidly analyze security incidents to determine the root cause and prevent future occurrences.



Proactive Security. Redefined.

COGNNA transcends conventional cybersecurity. Our Agentic AI for SOC platform, Nexus, cuts through the noise, delivering only actionable threat insights. We offer industry-leading capabilities like YARA and Sigma scanning on live endpoints, alongside IOC Scans for domains, IP addresses, and more.

Empower your team to act swiftly. Respond immediately to regulatory threat advisories and proactively hunt down active national threats. COGNNA isn't just about staying safe – it's about taking control.

Experience the confidence of proactive defense. With COGNNA, every move is calculated, every threat met with precision. Redefine your security strategy. Act now and embrace innovation that transforms your digital shield into a weapon of proactive defense.

Learn more and take a product tour at [cognna.com](https://cognna.com), or connect with our team at [info@cognna.com](mailto:info@cognna.com).

