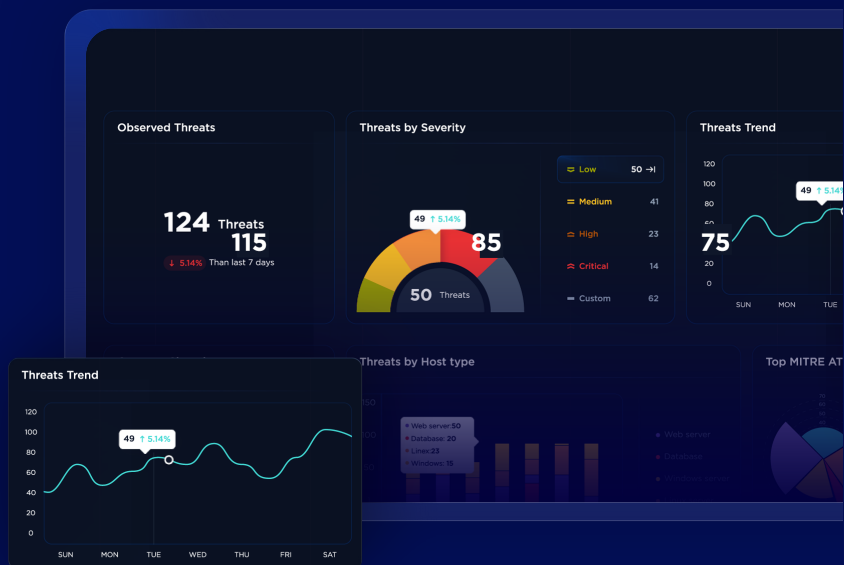# COGNNA

COMPROMISE ASSESSMENT SERVICE

COGNNA Nexus Elevating Cybersecurity

COGNNA stands as a global leader in cybersecurity, empowering customers to thrive by **safeguarding against cyber threats with effectiveness, speed, and simplicity.** The Misson of COGNNA Nexus is to defeat today's threats to protect tomorrow's future of humanity.

The **COGNNA Nexus platform** is an AI-driven threat management solution tailored to safeguard infrastructure and proactively mitigate evolving cyber threats. By integrating human intuition with advanced machine intelligence, **COGNNA Nexus** enables real-time threat detection, analysis,

COMPROMISE ASSESSMENT

COGNNA's Guardians Team utilizes the Nexus platform to offer **Compromise Assessment** services to provide comprehensive detection against sophisticated cyber attacks. These thorough assessments uncover advanced persistent threats (APTs) faster, reducing dwell time and mitigating potential damage. Identifying signs of compromise, such as malware or unauthorized access, allows organizations to remediate issues promptly and prevent future attacks. The results from these assessments inform risk management, resource allocation, budgeting decisions, and enhance overall cybersecurity posture.

Benefits of Compromise Assessments:
• Reduces dwell time to prevent APTs.

• Identifies threat actors and breaches, decreasing the likelihood of data theft.

• Proactively detects security practice flaws, improving overallsecurity posture.

• Offers evidence for audits and provides recommendations for future upgrades.

PLATFORM OVERVIEW
From asset identification to threat detection and rapid response to c ompliance assurance, COGNNA provides comprehensive detection against sophisticated cyber-attacks through an AI-driven threat management platform. Our innovative technology integrates human intuition and experience with advanced machine intelligence to detect, analyze and respond to threats in real-time.
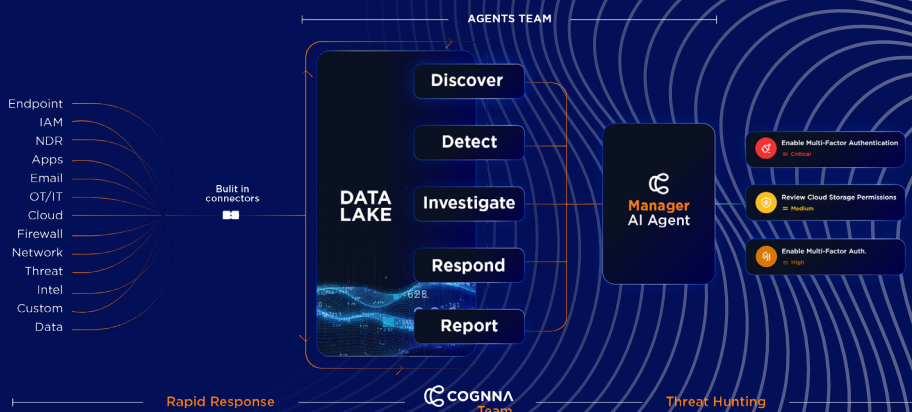
Pinpoint suspicious signals and take appropriate action.

Utilise custom detection rules to uncover advanced adversaries.

Provides a complete understanding of the scope of threats with deep data exploration capabilities.

Generates comprehensive threat reports revealing the tools and steps of attacks for quick action.

Offers assistance from experts answering questions and providing guidance on threat reports and their impact.

COGNNA's Approach

1. Information Gathering:
A meeting is scheduled to define the scope of the compromise assessment, critical assets involved, and the authorized point of contact. An initial engagement plan is prepared during this meeting.

2. Deployment of COGNNA Nexus Sensors:
COGNNA Nexus sensors are deployed across all systems within the defined scope. These sensors investigate systems from a security perspective, covering both servers and workstations.

3. Assessment of Environment:
Leveraging COGNNA's threat intelligence data, the assessment involves hunting for signs or potential evidence of compromises throughout the entire infrastructure. Comprehensive threat intelligence and user behavior analytics are applied to evaluate system artifacts and uncover any indications of compromise in the environment.

4. Reporting and Recommendations:
A detailed and comprehensive technical report is generated by COGNNA's expert team, summarizing all findings and providing recommendations. The report includes actionable intelligence, outlines next steps for remediation, and suggests actions to contain any malicious actors identified during the astsessment. Initiatives for preventive action are initiated based on the assessment results.

Features & Benefits

COGNNA Nexus sensors automate the collection of both point-in-time and historic forensic triage data, facilitating effective and efficient **compromise assessments.**

The single solution for analyzing large quantities of data in real-time and historically eliminates the need for multiple tools or data ingestion methods, simplifying analyst workflows.

The **compromise assessment** not only identifies compromise but also helps in recognizing ineffective security practices, providing a path for correction to improve overall security posture.Results from the assessment can inform future decisions related to risk management plans, resource allocation, budgeting, and contribute to building better strategic decisions for cyber resiliency.

Information Gathering

Threat Discovery and Assessment

Reporting and Delivery

Agent Depoloyment

Analyze Evidence and Validate

THE GUARDIANS

The Guardians Team conducts continuous examination and analysis of an organization's systems, networks, and data to determine whether any compromises or unauthorized access have occurred. This assessment helps to detect potential security breaches and enables organizations to take prompt action to mitigate any threats or vulnerabilities.

Empower your organization with COGNNA's Compromise Assessment Services, where cutting-edge technology meets human expertise to secure your digital future.

COGNNA

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

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.