Guardicore

SOLUTION BRIEF

Cyber Security Analyst Service

Prevent breaches, continuously hunt for threats, and accelerate response times by partnering with elite security experts

The Guardicore Cyber Security Analyst (CSA) Service, built on Guardicore Centra, offers the expertise of a team of elite security experts from Guardicore Labs to perform around-the-clock threat hunting in your infrastructure and take proactive breach prevention actions. The CSA team zeros in on the most critical threats, giving you the details, context, and recommendations you need to respond quickly. Access to specialized expertise when you need it saves your security team time and accelerates incident response and remediation. The most advanced security techniques available will be applied to your infrastructure on an going basis for a fraction of the cost of deploying new security tools or hiring and training specialized security operations staff.

The CSA Service helps you unlock additional value from your investment in Guardicore Centra by providing:

- Ongoing threat hunting and security incident monitoring.
- Email notifications about new threats detected in your network with a detailed analysis of the threat and actionable response recommendations for remediation.
- Ongoing access to specialized security experts to assist with incident investigation and remediation.
- Monthly management-level reports, attack surface reduction recommendations, Guardicore Centra configuration suggestions, and overall status updates.

About Guardicore Labs

The Guardicore CSA Service is staffed by security experts from Guardicore Labs with extensive training and real-world experience in both the private sector and military intelligence organizations, including the Israel Defense Force's 8200 unit. Combining deep experience in security with a daily exposure to threats in a variety of complex networks gives them unique insight into the latest hacking techniques and groups, including state-sponsored attack efforts. In addition to its customerfacing work, Guardicore Labs regularly publishes cyber security research and provide analysis, insights, and response methodologies for emerging cyber threats. The team also maintains several free tools, among them the Infection Monkey, a popular open-source network resiliency test tool and their own cyber threat intelligence portal.

More information is available at www.guardicore.com/labs

Maximize your investment in Guardicore Centra by using it to its full potential.

- Hunt for threats continuously across all of your environments.
- Eliminate false positive and avoid false negative alerts.
- Partner with world-class security experts to respond to new threats faster.
- Prevent security breaches.

Service Components

The Guardicore CSA Service includes two tiers, giving you the flexibility to choose the level of CSA engagement that best meets your organization's needs.

	CSA Essentials	CSA Enterprise
Managed Threat Hunting	✓	✓
High-Severity Incident Email Alerts	✓	✓
Guardicore Community Insights		✓
Alert Policy Optimization		✓
Investigation & Remediation Support		✓
Protection from Emerging Threats		✓
Attack Surface Reduction		✓
On-Demand Expert Access		✓
Monthly Management Reports		✓
Early Preview Feature Access		✓

Guardicore

Service Components

The CSA Service includes the following distinct service elements:

Managed Threat Hunting
The CSA team seamlessly taps into the vast information reported by Guardicore Centra from across your on-premises and cloud environments and analyzes it on an ongoing basis to zero in on possible threats. Alerts are investigated by an experienced team of researchers, and you are provided with concise, actionable insights about real threats to your infrastructure.

High-Severity Incident Email Alerts
Information-rich email notifications are provided when high-severity security incidents are detected, giving your team the context and guidance needed to respond quickly and effectively.

Guardicore Community Insights
Using its unique visibility across all Guardicore deployments, the CSA team will proactively detect and instantly mitigate new threats in your environment based on attacks detected in other Guardicore instances. The CSA team analyzes these attacks, extracts Indicators of Compromise (IOC), proactively follows their trail in your environment, and stops them.

Alert Policy Optimization
The CSA team continuously optimizes monitoring rules to eliminate false positive and avoid false negative alerts.

Investigation and Remediation Support
When critical security incidents are detected, the CSA team will collaborate with your security team to plan and execute an effective response. Experienced investigators will analyze the attack techniques and impact and provide detailed containment and remediation recommendations.

Protection from Emerging Threats
The CSA team assesses the external threat landscape on an ongoing basis. As new major industry threats and major security vulnerabilities are discovered, the CSA team proactively assesses the potential impact to your infrastructure and provides risk mitigation guidance.

Attack Surface Reduction
Your security team will have access to specialized policy templates created by the CSA team, which will help you protect core IT infrastructure services, reduce your network attack surface, and implement security best practices.

On-Demand Expert Access
Your security team will have direct access to experienced security experts whenever needed to assist with security challenges and provide advice and guidance as new needs arise.

Monthly Management Reports
The CSA team will provide monthly management-level reports that summarize the threat hunting activity executed in the past month with its findings. The report will also provide an overview of the proactive prevention actions that were taken, attack surface reduction policies, configuration fine-tuning, and other optimizations tailor-made to your environment.

Early Preview Feature Access
CSA Service customers will receive early previews of new Guardicore Centra features, and the CSA team will work collaboratively with your team to assess how new product enhancements can further protect your infrastructure from breaches.