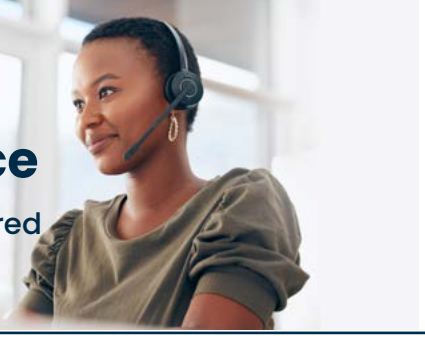

Castra's MXDR Enterprise Service

Scalable threat detection and mitigation services powered by Exabeam, Anomali ThreatStream, and EDR/XDR.

Castra's MXDR Enterprise solution combines the industry's most trusted technologies with the irreplaceable value of professional product expertise and customization. In one step, enterprise-level organizations can leverage some of the most advanced information security technology available on the market as a scalable, on-demand service.

Castra provides 24x7 cloud-based security and health monitoring using Exabeam as its security information and event management platform. Event data is enriched with a curated threat intelligence feed from Anomali ThreatStream, providing much-needed context to correlate log data with emerging threats. Castra's deep product expertise ensures a customized deployment that corresponds to the enterprise's real-world risk profile on an individual basis – not a composite of generic global threats.

SentinelOne Singular XDR gives Castra analysts the ability to quickly identify compromised endpoints, instantly block unauthorized activities, and protect sensitive data from exfiltration.

With Exabeam as the core SIEM/SOAR component, this process is automated to match the organization's strategic growth goals, ensuring a no-compromise approach to enterprise information security.

Castra's focus on scalability, customization, and unlimited visibility gives enterprise cybersecurity leaders a way to meet and exceed security requirements while addressing tech stack challenges head-on. By combining automated workflows with in-depth customization at scale, Castra empowers enterprise leaders to transform security from a necessary cost to a value-generating asset.

Castra's SOC team provides 24x7 cloud-based security and health monitoring that includes:

- **Expert SIEM Implementation**
- Primary Security Analyst
- SOC2 Type II Audited and Accredited
- **24x7 Security Operation Center**
- 24x7 Premium Alarm Monitoring and Response
- Documented Incident Response
- Proactive tuning, customer notification and orchestrated response post incident detection
- Advanced alarm and orchestration response (SOAR)
- Intensive analysis of customer needs and network environment
- Custom behavioral modeling and detection rules for improved alarming
- Custom Reporting and Dashboards
- Compliance-Based Dashboards
- Reoccuring Performance Reviews

Cloud-based platform continuously monitors:

- Hardware and software stats
- Event flow rates
- Capacity and performance information
- **Threat Hunting Pro**
- **Anomali ThreatStream Subscription**
- Push Known IoC's into SIEM, Firewalls, etc.
- Compiles, Validates, Scores all threat intel from private, public, ISAC, your environment, and more!

SentinelOne Singular XDR License

- Isolate Endpoints
- Terminate Processes
- Block additional Executions

CASTRA

e: info@castra.io | p: 919.595.8560 (EST) | p: 408.476.8488 (PST)
a: 3308 Durham-Chapel Hill Blvd Suite #201 Durham, NC 27707