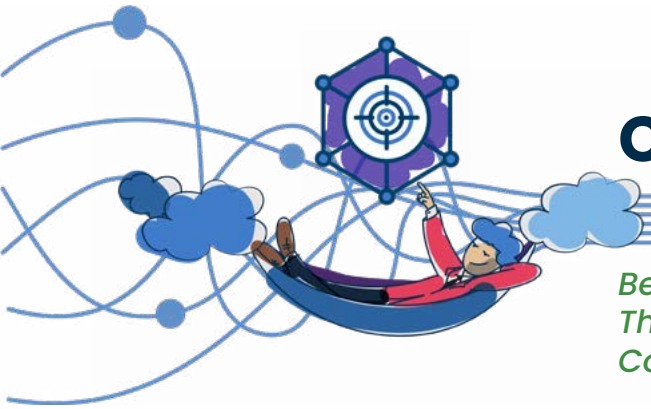

Castra's MXDR Pro Service

Best-in-class SOC-as-a-Service fueled by Anomali ThreatStream intelligence data, and Palo Alto Network's Cortex platform

Castra's top-tier managed detection and response solution includes best-in-class SOC-as-a-Service functionality fueled by Anomali ThreatStream intelligence data, and adds a license for Palo Alto Network's Cortex platform. Cortex is an extended detection and response (XDR) solution that expands detection capabilities to endpoints while enabling fast, comprehensive investigation and the ability to take action on the endpoint.

With Castra using Exabeam or USM Anywhere as the SIEM/SOAR component, Anomali for Threat Intelligence, and Cortex XDR to secure your IT environment, Castra will be able to quickly identify and isolate compromised endpoints, instantly terminate unauthorized processes, and block additional executions. This is the ideal way to leverage best-in-class security technology towards preventing advanced and persistent threats in sensitive industries.

With its focus on proactive detection and risk mitigation, Castra MXDR Pro is ideally suited for organizations that face significant and constant security threats. Financial institutions, critical infrastructure providers, and tech-enabled enterprises can use MXDR Pro services to gain control over their security posture while adhering to strict compliance guidelines.

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
- Customized Threat Detection
- 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

Scheduled Teleconference with the SOC Covering:

- Alarm review and noise reduction
- Capacity planning
- Risk posture adjustments
- 24x7 health monitoring

Cloud-based platform continuously monitors:

- Hardware and software stats
- Event flow rates
- Capacity and performance information
- Proactive tuning and customer notification upon problem detection
- **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!

- **Palo Alto Cortex Licenses**
- 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