Castra's MDR Pro Service

Gain threat intelligence and cyber resilience directly through your SIEM dashboard

Castra's MDR Pro service includes SIEM implementation and SOC-as-a-service capabilities enhanced with sophisticated technologies and valuable threat intelligence analysis. MDR Pro customers gain best in class Threat Intelligence.

As an MDR Pro customer, your security team will benefit from valuable insights from Anomali ThreatStream, providing up-to-date threat intelligence and cyber resilience directly through your SIEM dashboard. Additionally, Castra takes on the responsibility of pushing known indicators of compromise (IoCs) into your SIEM system.

MDR Pro compiles, validates and scores all threat intel from various private, public, ISAC and other sources, including the client themselves! This is the ideal solution for organizations that want to take a proactive approach to finding the latest threat.

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!

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