Castra's MDR Service

Best-in-class SIEM Managed by Castra's 24x7 SOC

The foundation to our award-winning service starts with expert SIEM implementation headed by a Castra SIEM Implementation Engineer. Once this step is complete, your designated expert will guide you through the process of delegating high-volume security tasks to our 24x7 security operations center (SOC) staff and documenting comprehensive incident response plans.

Castra's MDR service includes a best-in-class SIEM like Exabeam or USM Anywhere managed by Castra's 24x7 SOC. Castra SOC Analysts will perform customized threat hunting as well as proactive tuning and orchestration response to security incidents on a continuous basis. We build customized behavioral models that improve alarm performance over time, augmented by recurring performance reviews. This includes training and enhancing Exabeam's machine learning-enabled behavioral analytics.

Informative monthly teleconferences give you opportunities to reduce false alarms, plan for capacity changes, and adjust security postures for new risks.

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**

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