ELITE MDR

Elite is our most in-depth and award winning service. Castra is a SOC2 Type II audited organization which is a testament to the controls we have in place governing the security of customer data.

Our 24x7 Security Operations Center (SOC) watches your network, investigates security alarms, tunes Exabeam for better visibility, and works with you when we find anomalies. You don't need to manage Exabeam or watch the console day by day - we do that for you. Let us take care of it all while you focus on your business.

This is the premier solution, and triaged alarms are reported to the client via in platform ticketing or their preferred method of notification.

CASTRA'S APPROACH

We have been successfully using Exabeam for several years, for both our clients and ourselves.

In fact, in 2018 we swapped our SIEM 1.0 platform for Exabeam for better visibility, analytics, workflow and overall risk management.

OUR FAVORITE THINGS ABOUT EXABEAM

- Data Lake, Advanced Analytics, Case Manager, Entity Analytics, Cloud Connectors are the perfect bundle
- Excellent data usage model. Starts at 50GB/day and can easily scale to 2TB/day and higher
- Machine Learning, granting the ability to model account and/or asset behavior
- UEBA is superior to any human written SIEM 1.0 correlation rule
- Ability to craft custom rules and custom models
- Easy to extract smart timelines for investigations
- Long term intuitive, active searching
- Strong dashboard, visualization and reporting capabilities

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

ELITE MDR

CASTRA
exabeam

100+ BILLION Threats Detected

6 CONTINENTS

400+ K ASSETS MANAGED

We bend platforms to work in **your** environment.

How does Elite work?

Expert Exabeam Implementation
- Expert assistance on new service deployment from Security Operations Team
- Designated Primary Security Analyst and 24x7 SOC
- Documented Incident Response Plan

24x7 Premium Alarm Monitoring and Response
- Training and enhancing Exabeam's Machine Learning
- Proactive tuning, customer notification and orchestrated response post incident detection
- Advanced alarm and orchestration response

Customized Threat Detection
- Intensive analysis of customer needs and network environment
- **Anomali Threatstream** integration - best in class threat intelligence platform (TIPS)

Notifications and Compliance Dashboards
- Custom notifications for Alarm outputs
- Compliance Based Dashboards
- Custom Reporting

Recurring Performance Reviews
- Scheduled teleconferences with Security Operations Team covering:
  - Alarm review and noise reduction
  - Capacity planning
  - Risk posture adjustments

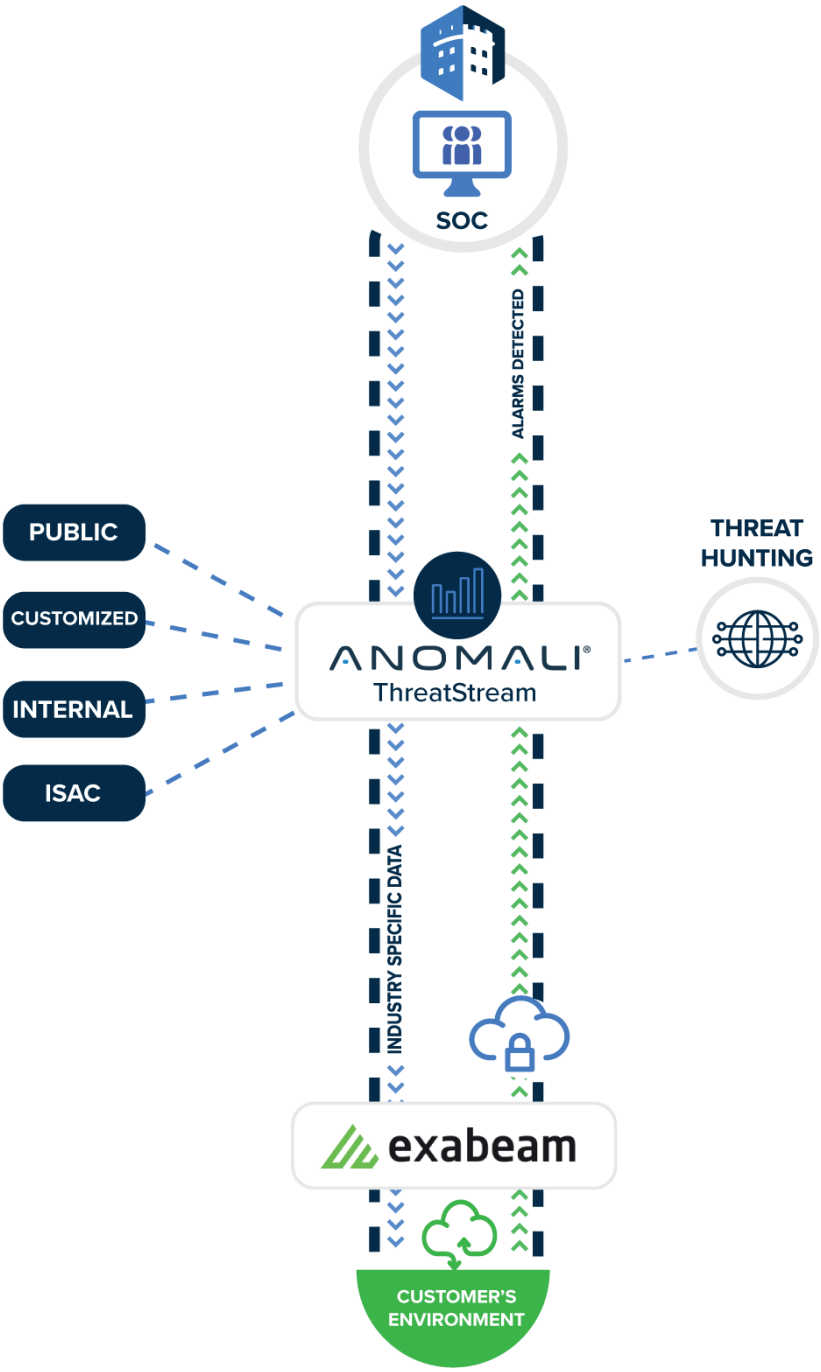
Ongoing Health Monitoring
- 24×7 health monitoring by Security Operations Team
- Cloud-based platform continuously monitors:
  - Hardware and software stats
  - Event flow rates
  - Capacity and performance information
  - Proactive tuning and customer notification upon problem detection

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

ELITE MDR

Castra utilizes **Anomali** and **Exabeam** in unison to better detect threats for our clients and strengthen their security posture with industry-specific data.



1. Post Implementation or Day2OPS, the Castra SOC monitors the Exabeam platform working through the alarm/ticket/data diving cycle.
2. The Castra SOC leverages Anomali to push targeted intel into the Exabeam platform, and it is where Threat Hunting initiates.
3. During the Threat Hunting process, the SOC receives results, concepts, and search findings that are then compared against client data from Exabeam.
4. Anomali compiles, validates, and scores all threat intel from various private, public, ISAC, and other sources (including the client's own environment).
5. By doing this, Anomali allows Castra to reduce False Positives and asses actual threat values against those presented to the analyst, resulting in better, more accurate alarming for the client and better detection for the Castra SOC.

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

About CASTRA

Tony Simone
Co-Founder

Grant Leonard
Co-Founder

Founded in 2012 by Tony Simone and Grant Leonard, Castra has successfully deployed SIEM/SOAR and various information security products and services in **over 2,000 organizations globally**.

We work with Fortune 50 organizations as well as SMB's and everything in between. We have worked with thousands of Healthcare, Financial, Retail, Technology, and Government organizations on various projects that range from tailored consulting to 24x7 Managed Services.

We have a 24x7, SOC2 Type I and Type II compliant and audited Security Operation Center located in Durham, NC, and redundant data centers throughout North America.

Our SOC is filled with well-trained, diligent analysts and some of the leading technology on the planet. We've mastered several different Information Security technologies, and **you can choose which one is best for you and your organization**.

2021 FINALIST
SCawards

exabeam
PARTNER OF THE YEAR 20
MSSP - AMERICAS
CASTRA

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