CASTRA
ALIENVAULT®
USM
APPLIANCE™

ELITE MDR

Castra has been partners with AT&T AlienVault since 2012 and we have deployed USM in over 2,200+ organizations all over the world. 2,200+ successful USM Implementations are a testament to our mastery of SIEM and USM Appliance expertise.

USM's rise in adoption amongst Small to Medium Businesses and Small to Medium Enterprises, played a key role in Castra's growth since our inception. Deploying 2,200 platforms is one thing, deploying 2,200 successfully with a large percentage of customers returning for more services is another.

CASTRA'S APPROACH

Castra was using USM Appliance when it was an open source tool called OSSIM (Open Source Security Information Management) and we still work closely with AT&T AlienVault's development team to continue to support and enhance the product. We have deep knowledge of this platform.

OUR FAVORITE THINGS ABOUT USM APPLIANCE

- Asset Discovery - active and passive network discovery
- Vulnerability Assessment – active network scanning, continuous vulnerability monitoring
- Intrusion Detection - network and host IDS, file integrity monitoring
- Behavioral Monitoring - netflow analysis, service availability monitoring
- SIEM - log management, event correlation, analysis, and reporting

55+ BILLION
Threats Detected

6
CONTINENTS

400+ K
ASSETS MANAGED

We bend platforms to work in *your* environment.

CASTRA
ALIENVAULT®
USM
APPLIANCE™

CASTRA'S ELK LOGGER & USM APPLIANCE

> ElasticSearch is fast! Based on our testing on lab and production systems, we're seeing 50x-100x speed improvements.

Castra has developed a powerful log management tool meant to become, expand or replace your existing USM Appliance Logger. It is a fully-integrated, drop-in replacement that is built using the ultra-fast ElasticSearch engine (a standard ELK stack), but incorporates several custom components that allow it to connect transparently to your USM Appliance as if it were a "real" Logger. Treat it like any other long term Logger. It brings fully indexed, rapid search capability to your log data, plus all of the benefits of the Kibana UI for advanced reporting and visualizations.

From your USM Appliance UI, it appears like a standard Logger, and you can search Raw Logs normally. Reports configured to run against the Logger also work as-is. And outside of the full USM Appliance integration, you also get the full Kibana interface with its visualization and reporting capabilities that have helped make the ELK stack so popular.

SPEED

Based on our testing on lab and production systems, we're seeing searches return in seconds and large reports running in a minute or two. This makes your analysts more productive while making the overall USM Appliance platform more valuable for your security monitoring.

ElasticSearch Speed Comparison
The ELK Logger is more than just Raw Logs searches, the Castra Elastic solution is *fully* integrated, bringing its power to USM and appears to the system just like a normal Logger.

EXPANDABILITY

Since it uses the ElasticSearch engine, this also opens up other possibilities including machine learning and anomaly detection using your log data. There are many other behavioral anomaly products out there, that can also sit on top of a Elastic data pool and provide new security insights for your environment.

CASTRA'S ELK LOGGER & USM APPLIANCE

SCALABILITY

With Castra's ElasticSearch you're not limited by the amount of data you need to store. Need 4TB, 8TB, more? No problem, increase the storage size or add more nodes! Need redundancy? Also no problem, add more nodes! Elasticsearch was built to run as a cluster, so it can scale to dozens or even hundreds of TB of data.

VIRTUAL REQUIREMENTS

Total Cores: 8

RAM (GB): 32

Storage Capacity (TB) Compressed / Uncompressed: 10TB / 4TB

Virtual Interfaces: 2 x 1GbE

Virtualization Support: VMware ESXi 4.0+ Hyper-V v3.0+ (Windows Server 2008 SP2 and later)

TYING IT ALL TOGETHER

Castra and other high profile SOC teams shoot for the rule of thirds, where 1/3 of the analyst time is spent on alert response, 1/3 analyst of the time is spent on hunting and 1/3 analyst of the time is spent on alert improvement.

This is moving away from the stacked team goal of numerous Tier1 individuals managing tickets and triage, moving things to Tier2 individuals for analysis and review, finally landing on a Tier3 desk for improvement and tuning.

While we will always grow teams from within, Alienvault reduces the need for "numerous Tier1 individuals" helping our SOC be focused and productive while improving analyst retention due to reducing "alarm fatigue."

CASTRA
ALIENVAULT®
USM
APPLIANCE™

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 USM Appliance for better visibility, and works with you when we find anomalies.

You don’t need to manage USM Appliance 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.

How does Elite work?

Expert USM Appliance 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 USM Appliance’s correlation engine
- 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)
- Custom behavioral modeling and detection rules for improved alarming

Notifications and Compliance Dashboards

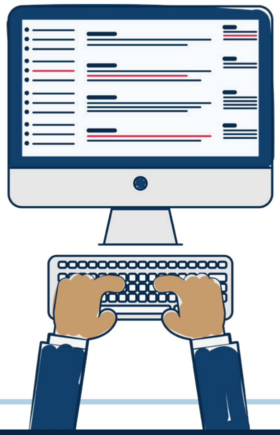
- Custom notifications for Alarm outputs
- Compliance Based Dashboards
- Custom Reporting

Recurring Performance Reviews

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

Ongoing Health Monitoring

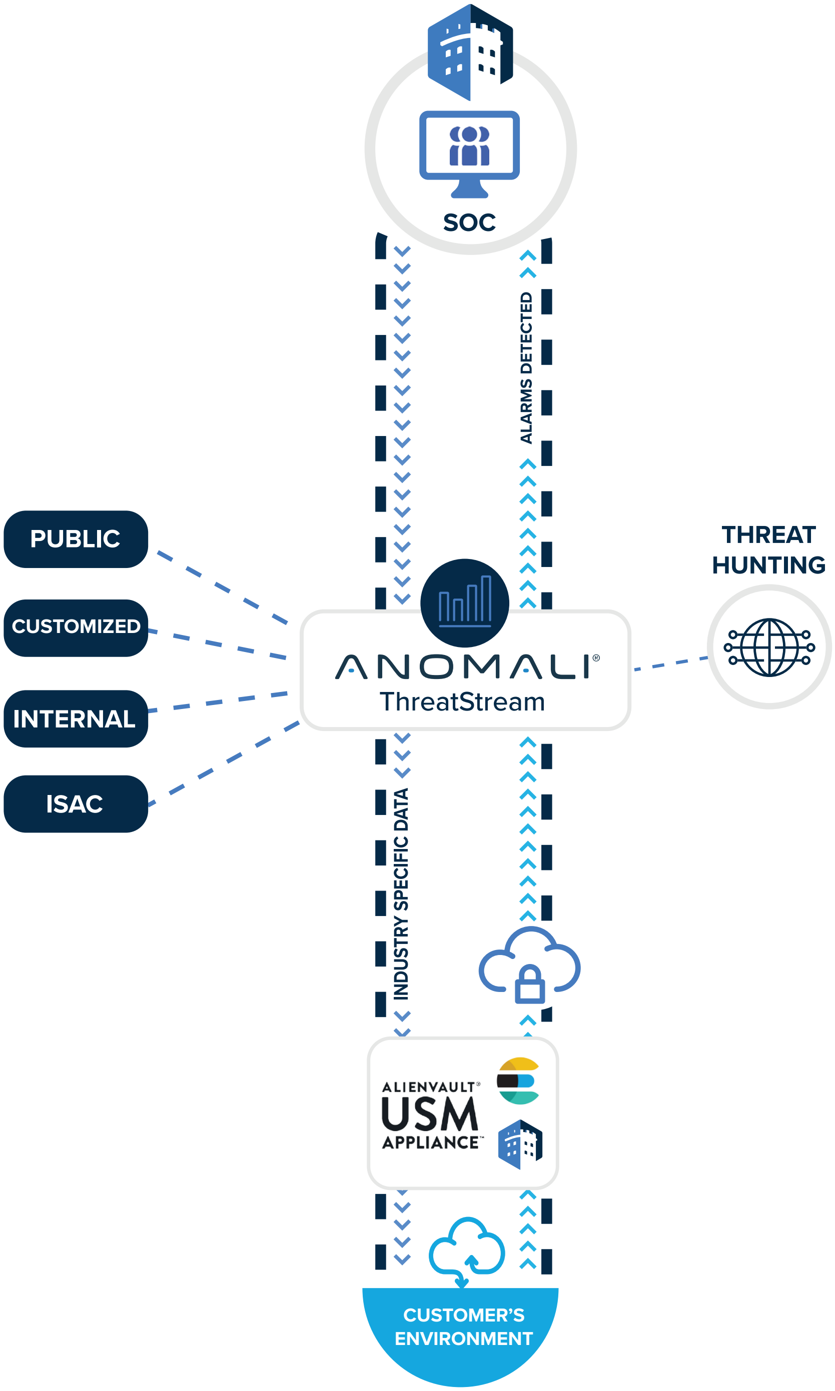
- 24×7 health monitoring by Security Operations Team
- Cloud-based platform continuously monitors:
    - Hardware and software stats
    - Event flow rates
    - Capacity and performance information
    - Proactive tuning and customer notification upon problem detection



ELITE MDR

CASTRA
ALIENVAULT® USM APPLIANCE™

Castra utilizes **Anomali** and **USM Appliance** 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 USM Appliance platform working through the alarm/ticket/data diving cycle.

2. The Castra SOC leverages Anomali to push targeted intel into the USM Appliance 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 USM Appliance.

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.

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**.

SCawards 2021 FINALIST

exabeam
PARTNER OF THE YEAR 20
MSSP - AMERICAS
CASTRA