



# Castra's MDR Pro for Exabeam

UEBA-enhanced Security with Curated Threat Intelligence



MDR Pro for  exabeam includes:

-  Machine Learning
-  UEBA
-  SIEM/SOAR
-  Threat Intelligence

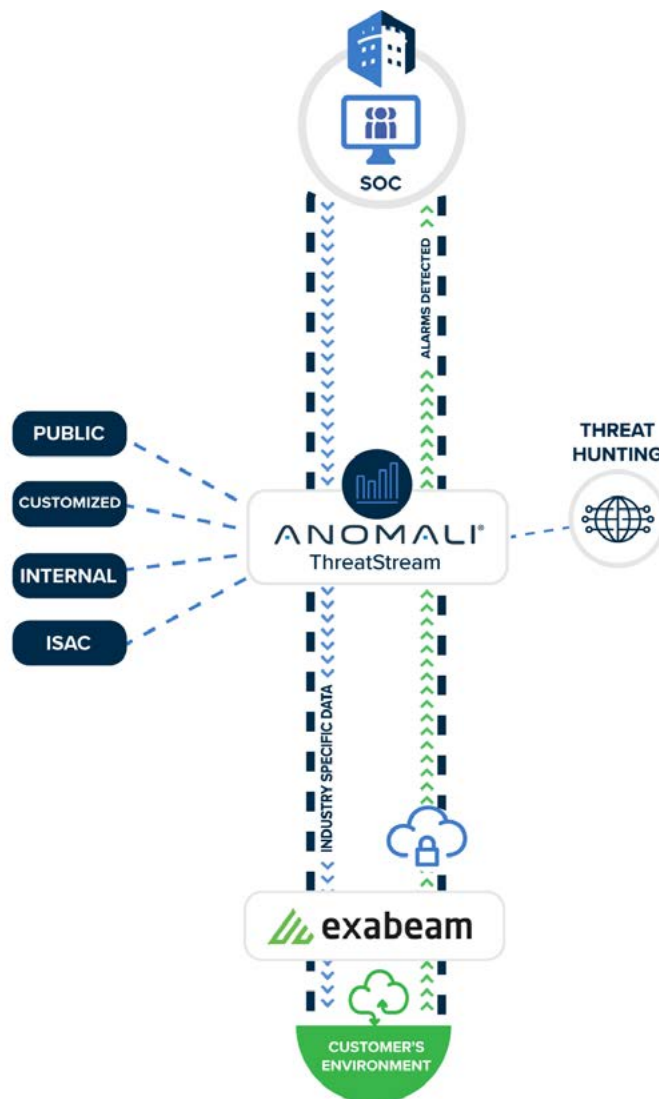
Improve your security capabilities with user entity and behavioral analytics (UEBA) technology informed by proactive threat hunting. Castra's MDR for [Exabeam](#) package makes some of the industry's most valuable enterprise technologies more accessible than ever before.

Castra's unparalleled product expertise and scalable service enables growing organizations to achieve operational security excellence without building and deploying in-house solutions. Every MDR Pro customer has a single point of contact for all security concerns – your primary security analyst. Your SIEM implementation and all related integration efforts will be spearheaded by this dedicated expert.

## Exabeam + Castra: Detailed Analytics and 24x7 Threat Response

Exabeam's SIEM platform gathers log data collected throughout your organization and analyzes it to identify suspicious behaviors. It leverages machine learning to establish a risk threshold baseline for every individual user, server, and application on your network. When user activity deviates from this baseline by a certain amount, it triggers an alarm, prompting a security analyst to investigate.

Castra security analysts conduct thorough investigations to determine if suspicious activity is malicious in nature. We challenge ourselves to continuously improve our methods, conducting intensive analyses of customer needs and fine-tuning our approach to reduce false positives, lower response times, and guarantee the integrity of our customers' IT assets.





# Castra's MDR Pro for Exabeam

UEBA-enhanced Security with Curated Threat Intelligence



MDR Pro for  exabeam includes:

 Machine Learning  UEBA  SIEM/SOAR  Threat Intelligence

Your primary security analyst will guide you through the process of implementing Exabeam and optimizing it for your organization's unique risk profile. Regular teleconferences will help improve your security posture and identify new opportunities to calibrate your detection and response service moving forward.

## In-Depth Threat Hunting with Anomali Threat Intelligence

Threat intelligence is critical to achieving operational security excellence. You can't protect against emerging threats and zero-day vulnerabilities without being aware of them.

Your Exabeam implementation includes a generic threat intelligence feed that showcases these threats. However, the volume of daily feed data is extremely high, and your organization isn't vulnerable to every threat.

Castra's MDR Pro package includes its premium Threat Hunting Pro service. We use [Anomali ThreatStream](#) to curate threat intelligence data and categorize threats based on their severity to your organization. This allows us to focus threat hunting resources on the most critical threats and vulnerabilities first – and avoid spending that valuable time on relatively low-impact issues.

## Gain Visibility into Security Operations with Castra

Castra's MDR Pro service is designed for transparency. Our team tailors alarm notifications, creates compliance dashboards, and customizes reports to meet your needs specifically. We schedule regular teleconferences with our customers, providing an open forum for reviewing tickets, reducing noise, and planning for the future.

All our customers benefit from cloud-based platform monitoring solutions showing event flow rates, capacity, and performance data. Castra's culture of open communication and extraordinary product expertise makes enterprise-level cybersecurity accessible to organizations of any size. Scale your security performance to meet growing needs by relying on managed detection and response partners you can trust.