Castra's MXDR+ for Exabeam

24x7 Security Operations for Growing Organizations

MXDR+ for exabeam includes:

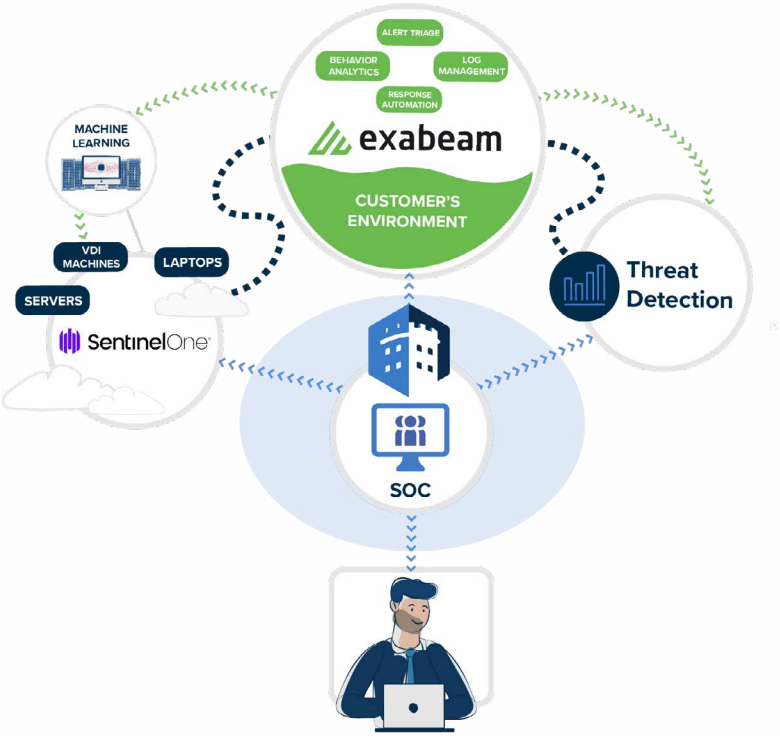
Machine Learning | **UEBA** | **XDR** | **Threat Detection**

Put Exabeam's sophisticated user entity and behavioral analytics (UEBA) technology to work securing your organization. Castra's MXDR+ for Exabeam package lets small businesses leverage the visibility and insight of machine learning-enhanced activity data.

Managing complex detection and response workflows and customizing security technologies to fit real-world needs has never been more accessible.

Exabeam + Castra: Unlimited and 24x7 Security Guaranteed

Exabeam uses machine learning to establish a baseline risk score for every user account, hardware device, and software asset in your organization. It observes these assets continuously and triggers alerts when their activities deviate from that norm. The SIEM calculates a risk score for every IT asset and updates it as those assets interact.



Your primary security analyst will walk you through the process of deploying Exabeam and configuring it to ingest log data from every corner of your organization. Castra's 24x7 security operations team can then calibrate the system to meet your unique security needs and respond to malicious activity when it occurs.

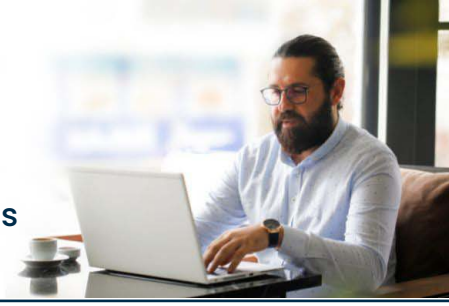
Enhancing your security posture with our 24x7 security operations team makes enterprise-level performance available to organizations of any size. Our team monitors alarms, investigates security events, and orchestrates incident response on your behalf. We document our activities according to a comprehensive incident report plan that details every step taken to secure your IT infrastructure and assets.

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

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

Castra's MXDR+ for Exabeam

24x7 Security Operations for Growing Organizations



MXDR+ for exabeam includes:

Machine Learning **UEBA** **XDR** **Threat Detection**

will help improve your security posture and identify new opportunities to calibrate your detection and response service moving forward.

Threat Detection Tailored to Your Risk Profile

No two organizations are alike. We begin every partnership with a thorough examination of our customer's IT environment and propose customized technology deployments to match.

Castra's MXDR+ package includes a complete analysis of your organization's security posture. This helps us categorize and triage malicious activity so we can reinforce your most vulnerable defenses first. Our analysts work continually to improve these models and add value to the detection and response process.

Extended Endpoint Protection with SentinelOne Singularity XDR

MXDR+ users gain additional endpoint protection with SentinelOne's unified XDR solution. Integrating XDR into Exabeam allows analysts to collect and analyze endpoint data when conducting investigations. Once suspicious activity pushes an endpoint's risk score beyond a pre-established threshold, Exabeam can use SentinelOne to automatically isolate the endpoint, terminate malicious processes, and block additional executions.

With Exabeam and SentinelOne working together, analysts can standardize their detection and response processes according to pre-programmed playbooks and launch them automatically. Castra's combination of XDR technology, UEBA insights, and robust product expertise makes enterprise security excellence available to organizations of any size.

Customize Your Security Tech Stack with Castra

The customization process does not stop at SIEM deployment. Castra continuously gathers performance feedback and uses that data to improve its policies, fine-tune its behavioral models, and adjust security rules to reduce false positives.

This feedback is what motivates our regularly scheduled teleconferences with customers. Beyond custom reports and dashboards, we look for opportunities to optimize capacity resources, adjust to new and emerging risks, and help customers achieve their security goals moving forward.

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