DEMISTO AND EXABEAM PARTNERSHIP

Detect Threats, Automate Incident Response and Accelerate Investigations

Benefits

Demisto and Exabeam for Faster Incident Resolution and Response

- Detect insider threats and lateral movement using machine learning and data science.
- Automatically enrich the investigation data with user risk score and complete session details.
- Mark relevant security information as evidence to track origin and change of custody for breaches.
- Add risky users to watchlist based on investigation artifacts beyond logs.

All sophisticated attacks involve compromise of user credentials in one form or another. Hackers can impersonate employees to compromise business data. Insiders can "hide" behind their enterprise credentials to steal data or attack systems.

Exabeam provides user behavior analytics, leveraging existing log data to detect modern attacks, prioritize incidents efficiently, and help valuable SOC staff respond effectively.

Demisto helps Security Operations Centers scale their human resources, improve incident response times, and capture evidence while working to solve problems collaboratively.

The Exabeam and Demisto Integration Provides:

- Detection of compromised credentials, lateral movement, rogue insiders using data science and machine learning
- Automatic data enrichment and analysis with Demisto's playbooks and Exabeam
- Marking certain users as high risk via Demisto's playbooks and automation scripts to add them to watchlist in Exabeam
- On demand querying of Exabeam rich contextual information about users and assets form virtual war-rooms to enable faster resolution of incidents

USE CASE #1

Integrated detection and incident response

Challenge:

If a high risk alert goes unnoticed and the investigation process is delayed, it results in higher impact on organization.

Solution:

Exabeam's session model leveraging data science can find lateral movement, privilege escalation and other signs of modern attacks quickly. Demisto integrates with Exabeam to ingest the high severity alerts and trigger automatic playbooks and workflows across different security products. This reduces the time between detection and response.

USE CASE #2

Enrich investigation data with user context and timeline of activities

Challenge:

When an organization is under attack time is of the essence. Every minute that passes until response is made may mean bigger damage. In most organizations this is a manual process where an analyst may ask the IT helpdesk or end user to get more details about user sessions and other details. The process may take unnecessary time and is error prone. Also the information about the user is prioritized and processed for security risk

Solution:

When an incident is investigated in Demisto, rich contextual information and activity timeline can be collected from Exabeam automatically as part of playbooks. This information can help save time for analyst and resolve incident faster.

Additional Benefit:

All actions are recorded in the virtual war-room so that the information can be used as forensics evidence in case the incident turns into a public breach. incident turns into a public breach.

USE CASE #3

Enhance Exabeam data with information from investigations

Challenge:

Currently Exabeam does an amazing job of analyzing the logs information from multiple sources. But the human analyst decision data and rich security data from endpoints like memory analysis can make the analysis way better.

Solution:

Demisto Enterprise can create watchlist on users based on the investigation data solved or marked by human analyst. These watchlisted users can further be analyzed by Exabeam.

About Demisto

Demisto helps Security Operations Centers scale their human resources, improve incident response times, and capture evidence while working to solve problems collaboratively. Demisto Enterprise is the first comprehensive, Bot-powered Security ChatOps Platform to combine intelligent automation with collaboration. Demisto's intelligent automation is powered by DBot which works with teams to automate playbooks, correlate artifacts, enable information sharing and auto document the entire incident lifecycle. Demisto is backed by Accel and has offices in Silicon Valley and Tel Aviv. For more information visit www.demisto.com or email info@demisto.com.

About Exabeam

Exabeam is a user behavior analytics solution that leverages existing log data to quickly detect advanced attacks, to help analyst prioritize incidents, and to enable more effective response. Exabeam's Stateful User Tracking™ automates the work of security analysts by resolving individual security events and behavior anomalies into a complete attack chain. This dramatically reduces time to respond and uncovers attack impacts that would otherwise go unseen. Built by seasoned security and enterprise IT veterans from Imperva and Sumo Logic, Exabeam is headquartered in San Mateo, California and is privately funded by Norwest Venture Partners, Aspect Ventures and Investor Shlomo Kramer. Visit us on Facebook or Twitter and follow us on LinkedIn.

DEMISTO

10056 Orange Avenue
Cupertino, CA 95014, USA

54 Achad Ha'am St.
Tel Aviv, Israel

Website: www.demisto.com
Email: info@demisto.com
Twitter: @demistoinc