exabeam

SOLUTION BRIEF

EXABEAM AND RECORDED FUTURE

Turbocharge detection with Threat Intelligence and Behavior Analysis

TRADITIONAL SECURITY INFORMATION AND EVENT MANAGEMENT SOLUTIONS (SIEMS) offer situational awareness by collecting log entries and security alerts from a multitude of enterprise security solutions. However, they often don't provide an elegant workflow for leveraging feeds from Threat Intelligence platforms in an efficient way. The integration of Recorded Future and Exabeam solves this problem by ensuring that accurate threat intelligence data is always available when and where analysts need it most.

Exabeam uses behavioral modelling of users, peer groups, and devices to automatically baseline normal behavior, assign a risk score to suspicious activity, and intelligently prioritize threats – across all your security solutions of choice. The combination of Exabeam and threat intelligence provider, Recorded Future, uses behavior to bridge the gap between threat intelligence and the data generated by other security services to allow joint customers to more effectively detect, investigate, and respond to potential threats and threat actors. By making threat intelligence directly available in its detection results and timelines, Exabeam creates significant efficiencies for threat intelligence users who otherwise must pivot between their SIEM, point security products and threat intelligence platform to act upon the information discovered.

Recorded Future

IDENTIFY RELEVANT CYBER THREATS FASTER

The Exabeam-Recorded Future integration helps security professionals more effectively assess risks related to indicators of compromise (IoCs) such as suspect files or URLs that may indicate a malware attack. It also enhances detection and investigation processes by importing threat intelligence feeds including malicious file hashes, IP addresses and domains, directly into Exabeam for use in threat detection. Exabeam makes this data actionable for security teams by weaving it into existing SIEM detection and investigation workflows, thus enhancing analyst productivity. Analysts can further speed

investigation and response using machine-built incident timelines and run playbooks that coordinate actions in 3rd party IT and security solutions to perform further investigation, containment, or mitigation of discovered threats.

INTEGRATION BENEFITS

COLLECT

A pre-built connector ingests and regularly updates Recorded Future data in Exabeam thereby reducing security maintenance efforts. This ensures IoCs are up to date without consuming analyst resources.

DETECT

Enhance threat detection by leveraging real time threat intelligence data in Exabeam including correlation rules and behavioral analytics. Exabeam uses Recorded Future threat intelligence data to improve threat detection and reduce false-negatives by increasing the risk score when IoCs from Recorded Future are found in an environment. Exabeam also applies user and entity behavior analytics (UEBA) to solve the concern that out of date IoCs might result in a false positive that causes unnecessary investigation cycles—by using behavioral analysis to focus on IoCs in sessions with high risk scores due to large volumes of anomalous activity.

INVESTIGATE

Dramatically reduce the time analysts spend investigating incidents using Exabeam Smart Timelines to automate the manual assembly of evidence from multiple, disparate systems into machine-built timelines. By making threat intelligence directly available in its machine-built timelines, Exabeam drives significant efficiencies for users who would otherwise need to toggle back and forth between their SIEM, point security products and threat intelligence platform to action upon discovered IoCs.

> "Combining real time threat intelligence with behavioral analytics empowers security teams to identify and detect the latest, most risky threats, even those never seen before. "

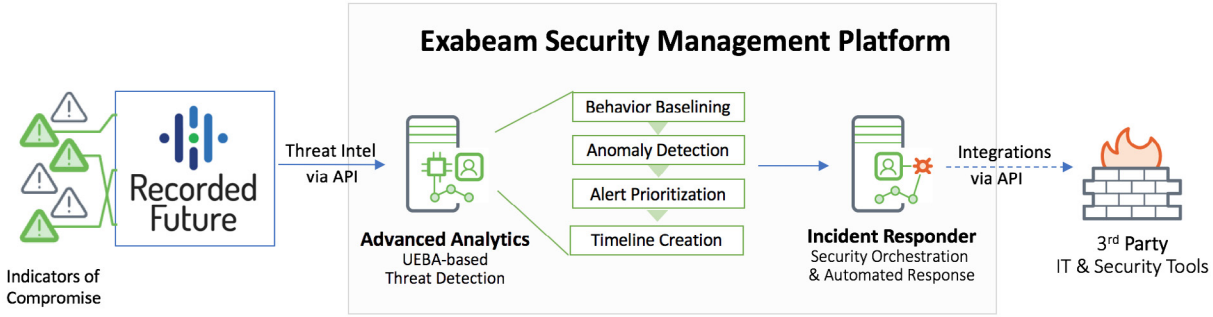
CHRIS STEWART, SR. DIRECTOR OF BUSINESS DEVELOPMENT, EXABEAM

RESPOND

Reduce human error and response times with pre-built, out-of-the-box playbooks that automate and standardize incident response actions including containment, investigation and mitigation for any detected threats.

TOP USE CASES

- Improved malware detection
- Enrich investigations with context for IoCs
- Threat hunting with real-time intelligence and IoCs



EXABEAM AND RECORDED FUTURE ENHANCE SECURITY PROFESSIONALS' DETECTION, INVESTIGATION AND RESPONSE TO SUSPICIOUS EVENTS.

HOW IT WORKS

- API-based integration brings the Recorded Future threat intelligence feed into Exabeam on a regular basis, providing Exabeam with a stream of current threat intelligence for use in behavioral analysis.
- Threat detection is improved—by lowering false-negatives and increasing user and asset risk scores— whenever malicious IoCs are found in an environment.
- False positives are reduced by applying behavior analytics to IoCs obtained from threat intelligence. Exabeam UEBA functionality helps ensure that only IoCs associated with users or entities with increased risk scores are discovered and escalated to an analyst.
- All detected threats are naturally prioritized by risk scores, thus naturally sorting the highest risk threats to the top
- And, in the event that a suspect file hash, IP address, or domain is identified in a user's system (and thereby the overall organization), Exabeam creates a machine-built incident Smart Timeline for that particular threat, providing all of the surrounding context for rapid investigation.
- Exabeam can also use playbooks take corrective action in other third party security tools for automated incident investigation, containment, or response.

exabeam

ABOUT RECORDED FUTURE

Recorded Future delivers the only complete threat intelligence solution powered by patented machine learning to lower risk. Recorded Future empowers organizations to reveal unknown threats before they impact business, and enable teams to respond to alerts 10 times faster. To support the efforts of security teams, Recorded Future technology automatically collects and analyzes intelligence from technical, open web, and dark web sources and aggregates customer-proprietary data. Recorded Future delivers more context than threat feeds, updates in real time so intelligence stays relevant, and centralizes information ready for human analysis, collaboration, and integration with security technologies.

ABOUT EXABEAM

Exabeam empowers enterprises to detect, investigate and respond to cyberattacks more efficiently so their security operations and insider threat teams can work smarter. With Exabeam, analysts can collect unlimited log data, use behavioral analytics to detect attacks and automate incident response, both on-premises or in the cloud. Exabeam Smart Timelines further reduce the time and specialization required to detect attacker tactics, techniques and procedures.

Exabeam is continuously adding new integrations with best of breed security vendors to its offering. These integrations are included as part of the solution at no additional cost, supporting organizations as they expand their security ecosystem, and providing peace of mind that Exabeam integrations will support your unique environment as it evolves over time.

TO LEARN MORE ABOUT HOW EXABEAM CAN HELP YOU, VISIT EXABEAM.COM TODAY.