exabeam

SOLUTION BRIEF

EXABEAM INGESTER FOR CROWDSTRIKE

Detect and investigate advanced attacks and insider threats with UEBA

EXTENDING VISIBILITY: ENDPOINT DATA AND BEYOND

With threats constantly targeting end users, entities and devices, endpoint detection and response (EDR) solutions are valuable tools for proactive threat detection, investigation and protection. And, while endpoint data provides essential information about your security posture, it does not offer a complete picture for teams tasked with assessing risk and detecting advanced threats. To understand the scope of an attack, security teams also must collect and contextually analyze information from a broad array of inputs, including servers, badge readers and cloud-based services, to collect, detect, investigate and respond to suspicious activity.

Exabeam's user and entity behavior analytics (UEBA) solution uses behavioral modelling to automatically baseline normal activity and detect anomalous behaviors indicative of a threat – across all your security solutions of choice. The powerful combination of Exabeam and CrowdStrike uses behavior to bridge the gap between endpoint activity and other security and IT infrastructure tools, as part of a modern security management strategy.

CROWDSTRIKE

"CrowdStrike and Exabeam are uniquely positioned to jointly deliver an integrated, fully SaaS offering. This provides customers with the flexibility to solve complex security management problems while also adhering to cloud-first and cloud-only procurement mandates."

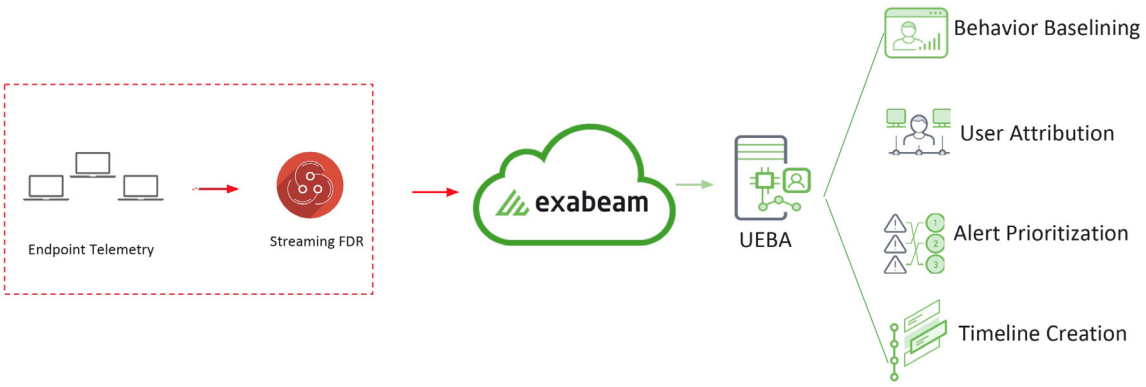
CHRIS STEWART, SR. DIRECTOR OF BUSINESS DEVELOPMENT, EXABEAM

ACCELERATE INCIDENT ANALYSIS AND RESPONSE

Exabeam utilizes CrowdStrike EDR data from Falcon Data Replicator (FDR) to attribute endpoint activity to a user and establish a behavioral baseline for normal activity. With user and entity behavior analytics (UEBA), Exabeam identifies anomalies to enable security teams to more efficiently detect, prioritize and investigate endpoint threats. Analysts can then use machine-built Smart Timelines to investigate user activity before, during, and after an alert, drastically reducing mean time to respond (MTTR).

Key Integration Benefits:

- Secure the enterprise against modern attacks by accurately detecting advanced attacks and insider threats using user and entity behavior analytics (UEBA)
- Run a more effective and efficient SOC by automatically prioritizing alerts based on risk, to guide analyst investigations
- Enhance analyst productivity by automating investigations using machine-built timelines



CROWDSTRIKE FDR DATA IS INGESTED INTO EXABEAM FOR UEBA-BASED THREAT DETECTION, PRIORITIZATION, AND RAPID INVESTIGATION.

HOW IT WORKS

- CrowdStrike monitors endpoint activity using its EDR solution and endpoint agents.
- Data is sent to Crowdstrike Falcon Data Replicator (FDR) in real-time.
- Exabeam ingests data from FDR via the Exabeam Ingestor for Crowdstrike connector.
- Exabeam baselines normal user and endpoint activity using UEBA and then automatically detects deviations from those behavioral baselines.
- Risk is added to the relevant user or entity for each anomalous activity detected
- Threats are automatically prioritized by risk score to focus analyst efforts on high risk anoamalies
- Concurrently, Exabeam stitches together CrowdStrike data with third party security solutions' data to create machine-built incident timelines, for rapid threat investigation

TOP USE CASES

USE CASE / CHALLENGES	SOLUTION DESCRIPTION	BENEFITS
Advanced Threat Detection - Endpoint telemetry is unable to provide visibility into user behavior across all systems, making it difficult to detect advanced and insider threats.	UEBA uses machine learning to distinguish normal and abnormal behavior for a user, helping to identify risky activity—like that associated with credential compromise, insider threats, and privilege abuse— even if it has never been seen before.	Improve security posture and detect modern threats by augmenting EDR with UEBA.
Lateral Movement Detection - Threats using lateral movement become difficult to detect due to changes in IP address, device, or credentials.	Patented host-to-IP mapping allows Exabeam to automatically follow attacks and attribute endpoint activity back to the related user, regardless of how an attacker moves through the network.	Ensure sophisticated attacks involving lateral movement don't go undetected.
Alert Prioritization - Analysts deal with an overwhelming volume of alerts from the numerous attacks on endpoints.	Exabeam UEBA aggregates alerts and activity by user, prioritizes them by risk score, and focuses analysts in the highest risk threats.	Increase SOC efficiency and effectiveness by quantifying focusing analyst efforts on the highest risk threats.
Incident Investigation - Analysts must spend too much time investigating an attack to ensure effective post-incident remediation.	Exabeam Smart Timelines enable analysts to dramatically reduce time spent on incident investigations by automatically stitching together events before and after an alert to give the full picture of an attack.	Enhance analyst productivity by automating tedious investigations with machine-built timelines.

exabeam

ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over two trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform. Learn more: www.crowdstrike.com.

ABOUT EXABEAM

Exabeam is the Smarter SIEM™ company. We help security operations and insider threat teams work smarter, allowing them to detect, investigate and respond to cyberattacks in 51 percent less time. Security organizations no longer have to live with excessive logging fees, missed distributed attacks and unknown threats, or manual investigations and remediation. With the modular Exabeam Security Management Platform, 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, sequences of user and device behavior created using machine learning, 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. For more information, visit www.exabeam.com.

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