exabeam

SOLUTION BRIEF

EXABEAM AND CROWDSTRIKE

Combining Behavior Analytics, SOAR, and EDR for Enhanced Detection and Automated Response for Endpoint Security

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 all attack vectors. 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 endpoint visibility and behavioral analytics to bridge the gap between endpoint activity and other security and IT infrastructure tools, as part of a modern security management strategy.

CROWDSTRIKE

ACCELERATE INCIDENT ANALYSIS AND RESPONSE

Using data from the CrowdStrike Falcon platform, Exabeam enables rapid detection of endpoint threats by monitoring and assigning risk scores to anomalous endpoint and network activity, such as a file entering the network from a user's laptop. Machine-built incident timelines automatically bring together normal and abnormal behaviors for users and devices, allowing SOC analysts to quickly and efficiently analyze and respond to threats using incident response playbooks that ensure timely and consistent action.

INTEGRATION BENEFITS

COLLECT

Collect data from the CrowdStrike Falcon platform for threat detection and eliminate unpredictable volume-based expenses with Exabeam's flat pricing model. Quickly collect and search all your data sources without making compromises due to lack of scalability or budget.

DETECT

Generate behavioral baselines unique to your organization and automatically identify anomalous, risky behavior that may be indicative of security incidents or threats. Eliminate manual assembly of data from multiple, disparate systems.

INVESTIGATE

Dramatically reduce analyst time spent investigating incidents with intelligent risk scoring and Exabeam Smart Timelines - even for attacks not seen before. Accurately pinpoint anomalous events and improve productivity while significantly reducing response time.

RESPOND

Reduce human error and boost response productivity with pre-built playbooks that automate and standardize actions including containment, mitigation, and response using ten security orchestration, automation, and response (SOAR) actions specific to the Exabeam-CrowdStrike integration.

"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."

TREVOR DAUGHNEY, VP OF PRODUCT MARKETING, EXABEAM

TOP USE CASES

THREAT DETECTION

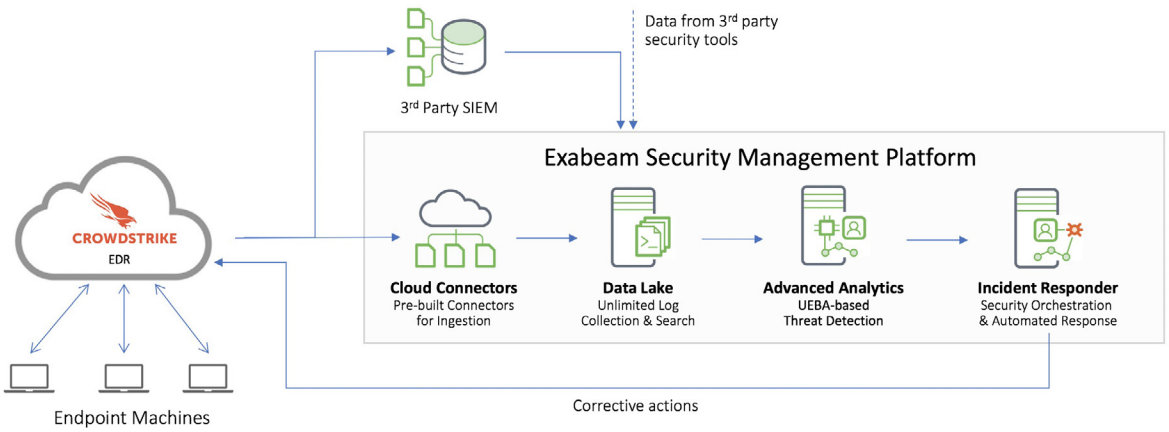
Insider threat detection
File-based malware
IoT threat detection

SOC OPERATIONS

Incident investigation
Ticket tracking and resolution
Automated Incident Response

Analysts can run ten actions in CrowdStrike directly from Exabeam including:

- Get Device Info
- Get Domain Reputation
- Get File Reputation
- Get IP Reputation
- Get Process Info
- Hunt File
- Hunt URL Domain
- List Process on Host
- Search Device(s)
- Upload IOC



CROWDSTRIKE FALCON PLATFORM DATA IS INGESTED INTO EXABEAM FOR LOGGING, UEBA-BASED THREAT DETECTION AND AUTOMATED INCIDENT RESPONSE

HOW IT WORKS

- CrowdStrike® Falcon Insight™ monitors and records all activities of interest on the endpoints with deployed lightweight Falcon sensor.
- Exabeam ingests this endpoint telemetry via CrowdStrike's Falcon API. Exabeam parses, normalizes and enriches the data with context from your environment.
- Logs are sent to Exabeam Data Lake for unlimited log collection and search, and ingested into Advanced Analytics for analysis and threat detection.
- 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.
- Concurrently, Exabeam stitches together CrowdStrike Falcon Platform data with third party security solutions' data to create machine-built incident timelines, for rapid threat investigation.
- When user risk scores surpass a pre-defined risk threshold, an incident is opened in Exabeam's case management system.
- Response playbooks in Exabeam Incident Responder, a SOAR solution with ten pre-built integration points with the CrowdStrike platform, automate containment, investigation and response using CrowdStrike and other security and infrastructure tools.

exabeam

ABOUT CROWDSTRIKE

CrowdStrike® Inc., 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.

There's only one thing to remember about CrowdStrike: We stop breaches.

Learn more: www.crowdstrike.com

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.