Exabeam vs. CrowdStrike

Five Ways to Compare and Evaluate

No single cybersecurity tool can block all threats, but some are better than others at detecting and mitigating attacks. This is where Exabeam comes in, offering a comprehensive suite of tools designed to make sense of a multitude of alerts and protect against a broad range of cyberthreats.

When comparing Exabeam to other SIEM options like CrowdStrike®, it's important to consider these five factors that show why Exabeam is the better choice:

1. User and Entity Behavior Analytics (UEBA)

A modern security operations center (SOC) must prioritize high-fidelity detection and identify normal versus abnormal behavior. This is where user and entity behavior analytics (UEBA) provides value. UEBA can detect threats that traditional tools miss because it does not rely on fixed rules or known attack patterns and covers multiple systems and data sources.

While CrowdStrike's SIEM solution does have UEBA capabilities, UEBA is an integral piece of the Exabeam Security Operations Platform, offering over 790 pre-built behavior models with over 1,100 anomaly and more than 680 fact-based rules. Exabeam automates routine processes and uses advanced detection methods, allowing security teams to focus on what matters most: neutralizing threats before they impact operations.

2. AI Innovation

To keep pace with cybercriminals' changing tactics, SOCs must adopt advanced AI technologies. These technologies should be capable of learning normal behavior patterns, identifying potential threats quickly, and improving the efficiency of analyst workflows.

Exabeam delivers AI-driven persona-based workflows that automate threat detection by providing automated threat timelines, impact analyses, and intuitive search capabilities in natural language. This accelerates decision making and response. While CrowdStrike has Charlotte AI, an integration with ChatGPT that provides insights into particular events, it's important to note that this feature is not presently available in Falcon LogScale.

Exabeam is an AI leader, integrating advanced machine learning and other AI technologies into cybersecurity with features like Threat Center. Threat Center simplifies security analyst workflows by centralizing threat management, investigation tools, and automation to efficiently investigate and respond to threats. Additionally, Exabeam Copilot enhances the Exabeam Security Operations Platform with generative AI, boosting productivity and providing deep insights. It incorporates natural language processing (NLP) to simplify the creation of complex queries in almost any language, bypassing the need for advanced query language or regex knowledge. This generative AI functionality also accelerates analyst training and risk communication by providing detailed threat explanations, which are powered by a cybersecurity-specific large language model (LLM), ensuring current and accurate responses to security-related prompts.

3. Ease of Use

CrowdStrike Falcon LogScale was developed for log management on a smaller scale, focusing less on enterprise-level security. This results in challenges related to adding and parsing new third-party logs for improving monitoring capabilities. Such limitations complicate the process for SOCs to fully adopt an effective TDIR strategy.

On the other hand, Exabeam is designed with security professionals in mind. The Exabeam Security Operations Platform offers user-friendly point-and-click options that simplify searches. Unique to Exabeam, NLP search within Threat Center further streamlines the search process, which can be time consuming on other platforms. The Exabeam commitment to simplicity covers TDIR processes from triage to response. With Outcomes Navigator, Exabeam guides analysts through the steps needed to expand visibility, all aimed at making the user experience more straightforward.

4. Flexible and Customizable Rules

CrowdStrike has around 30 pre-built rules, mainly for basic detection. Users might need to create additional, complex queries or rule chaining on their own. This limitation could lead to increased workload for analysts and reduced visibility into their environment.

The Exabeam Security Operations Platform features more than 1,800 detection rules, including for cloud threats, with over 790 behavioral models. These are integrated into Threat Timelines for easier investigation, with a threat explainer that can tell an analyst what happened, determine the scope of the event, and make recommendations for mitigation and response. This allows analysts to customize detections to effectively address complex attacks.

5. Superior Integrations

CrowdStrike faces additional challenges when it comes to log ingestion and the number of integrations it supports. Adding third-party logs to Falcon LogScale can be difficult. As a workaround, the team recommends using CrowdStream, powered by open observability company Cribl, to ingest logs like O365 and Entra ID, but this comes at an extra cost, which usually isn't mentioned until after purchase.

In contrast, Exabeam integrates with more than 350 vendors and 680 products and has over 9,500 pre-built parsers. It features scalable and flexible log retention; rapid data ingestion; AI-assisted, lightning-fast query performance; and advanced behavioral analytics. These capabilities help identify threats that might be missed by other tools. For customers already using Cribl, Exabeam has a pre-built Cribl collector available for no additional charge.

	Exabeam	Crowdstrike
Detection Content		
Behavior-based Models to Detect Abnormalities	790+ Behavioral Models	✗
Detection Rules to Detect Known Threats	1800+	30+
Integrated Commercial-grade Threat Intelligence	✓	✓
Detection Content Mapped to Use Cases	✓	✗
Investigative Automation		
Automatically Generated Threat Timelines	✓	✓
ML-based Alert Prioritization	✓	✗
Pre-built Watchlists for Risky Users and Entities	✓	✗
Granular Risk-based Scoring	✓	✗
Log Management		
Self-service Data Collection Interface	✓	✓
Search Query Builder Assistant	✓	✗
Up to 10 Years of Searchable Data Without Rehydration	✓	Unknown
Deploy Architecture		
Fully Cloud Native	✓	✓
Integrated SIEM + UEBA + SOAR	✓	No native UEBA – disjointed platform

Conclusion

Regardless of an organization's size or sector, security teams face challenges in managing security operations. They often struggle to detect critical threats due to a massive influx of data and the use of disparate tools. While CrowdStrike excels in many areas, Exabeam distinguishes itself as a pioneering security company. As a trailblazer in the UEBA market and holder of several machine learning patents, Exabeam provides a dedicated solution purpose-built to meet the growing demands of cybersecurity.

The AI-Driven Exabeam Security Operations Platform

The Exabeam Security Operations Platform applies AI and automation to security operations workflows for a holistic approach to combating cyberthreats, delivering the most effective threat detection, investigation, and response (TDIR). AI-driven detections pinpoint high-risk threats by learning normal behavior of users and entities, and prioritizing threats with context-aware risk scoring. Automated investigations simplify security operations, correlating disparate data to create threat timelines. Playbooks document workflows and standardize activity to speed investigation and response. Visualizations map coverage against the most strategic outcomes and frameworks to close data and detection gaps. Exabeam empowers security operations teams to achieve faster, more accurate, and consistent TDIR.

About Exabeam

Exabeam is a global cybersecurity leader that delivers AI-driven security operations. The company was the first to put AI and machine learning in its products to deliver behavioral analytics on top of security information and event management (SIEM). Today, the Exabeam Security Operations Platform includes cloud-scale security log management and SIEM, powerful behavioral analytics, and automated threat detection, investigation, and response (TDIR). Its cloud-native product portfolio helps organizations detect threats, defend against cyberattacks, and defeat adversaries. Exabeam learns normal behavior and automatically detects risky or suspicious activity so security teams can take action for faster, more complete response and repeatable security outcomes.