HPE ArcSight Integration with Exabeam
Technology Partner Solution Brief

Exabeam’s user behavior analytics solution leverages HPE ArcSight’s log data to quickly detect advanced attacks leveraging stolen credentials and accelerate incident response.

Solution overview
What Exabeam does
- Exabeam extracts additional value from log data already stored in ArcSight and combines it with data from Active Directory for identity context.
- Exabeam uses behavior analytics to learn normal credential behaviors and provide a risk score for those that are anomalous.
- Exabeam’s Stateful User Tracking automatically creates a credential activity timeline that includes any account switching and attribution of security alerts to credentials.
- With easy plug-and-play set up, Exabeam offers very fast time-to-value. Without the need for connectors, agents, network taps, or tuning, customers are reviewing high-scoring user credential sessions within a few hours after deployment.

Exabeam provides a new layer of detection shifting focus away from ever changing malware to the account credential that enables it.

The Exabeam solution pulls credential access logs from HPE ArcSight via API and enriches this data with identity information collected from Active Directory (LDAP). This provides an identity context for credential use. Using behavior modeling and analytics, Exabeam learns normal IT user credential activities and access characteristics and automatically asks questions of the data to expose anomalous behaviors. Finally, Exabeam uses Stateful User Tracking to place all user credential activities and characteristics on a timeline with scores assigned to anomalous access behavior. Traditional security alerts are also scored, attributed to identities, and placed on the activity timeline. All systems touched by the compromised credential are identified to reveal the attacker’s path through the IT environment. Exabeam uses additive risk scoring to highlight the riskiest user sessions, thereby reducing noise and helping security analysts focus on the most critical incidents. Automated analysis and real-time event timeline creation enable quicker, efficient, and more accurate response by security operations team with zero false positives.

High scoring credential sessions can be set to trigger an alert and fed back into ArcSight ESM workflows for further automation, correlation, and centralized incident management.
Exabeam and **HPE ArcSight Integration**

- Exabeam capitalizes on ArcSight’s advanced data collection capabilities, extracting additional value from data you already have.
- Exabeam automates the discovery of compromised accounts that enable advanced attacks with no overhead to your existing ArcSight deployment.
- Once Exabeam identifies account takeover and creates an attack timeline, it sends a syslog or CEF formatted message to ArcSight for processing into existing workflows.

**More info**
For additional Exabeam information visit: [exabeam.com/product](exabeam.com/product)