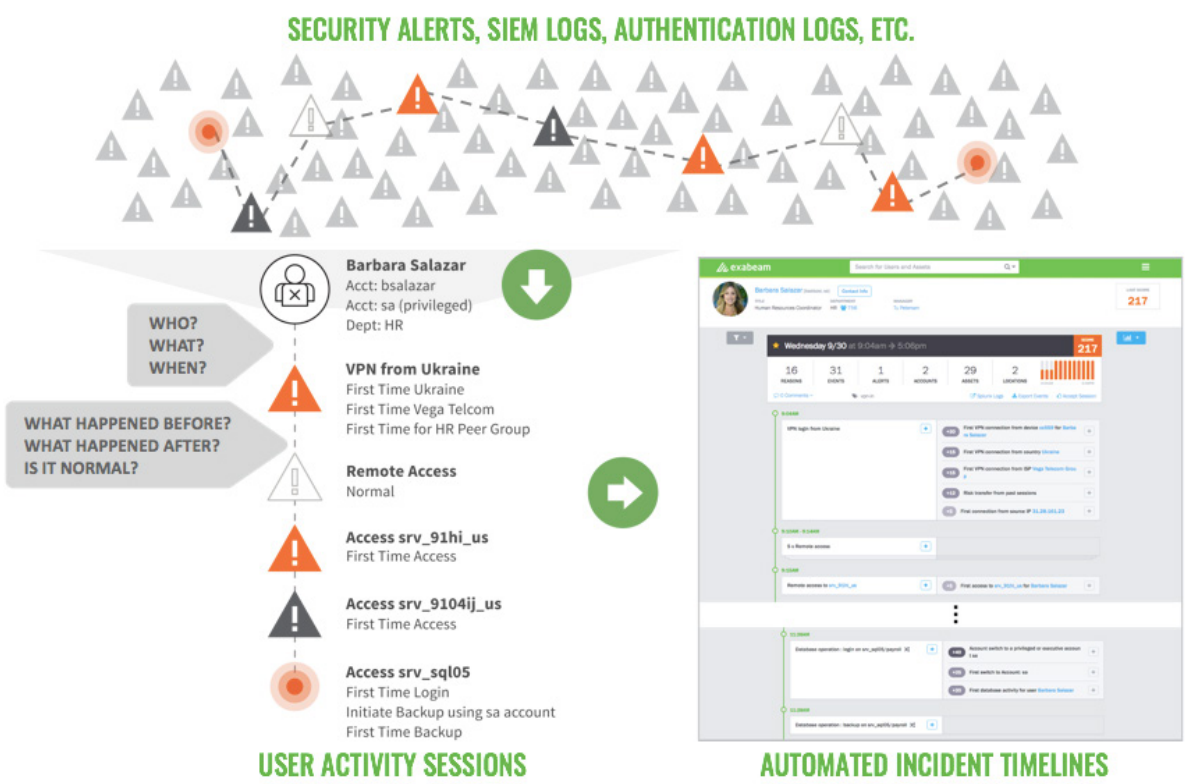
Name of vendor 1	Exabeam
Name of vendor 2	Palo Alto Networks
Title	Exabeam & Palo Alto Networks Joint Solution
The Challenge	Whether it's a malicious insider or compromised insider, credential-based threats are tricky to identify; after all the attacker is abusing legitimate access privileges. Once inside, attackers frequently move laterally by changing devices or leveraging privileged accounts to gain access to valuable resources. Pieces of this story are available in various logs such as Windows event logs, application logs, file access logs, database logs, etc. and also from vendor specific logs such as the VPN logs from Palo Alto Networks firewalls and security alerts from Palo Alto Networks Wildfire, however without additional context these insidious threats would be impossible to detect.
The Solution	Detect Insider Threats, Prioritise Security Alert Investigation and Accelerate Incident Response
The Integrated Solution Features / Benefits	**The Palo Alto Networks and Exabeam integration provides:** • Increased detection of credential-based attacks, insider threats, and lateral movement via data science and behavioral modeling • Prioritised security alert investigation to help analysts identify and focus on high-risk alerts • Accelerated Incident investigation and SOC automation using Exabeam's user session timelines to triage security anomalies By ingesting Palo Alto Networks VPN, Wildfire and Endpoint logs, and combining them with other existing data sources such as those found in a SIEM, Exabeam is able to profile and analyse the activity and behaviour of all users and assets within an organisation. Exabeam's stateful user tracking methodology stitches together user activities into session timelines and then employs behavioural modeling to determine what is normal for those users. Anomalous behaviour such as abnormal VPN connections, excessive distance since the last log-in, a rare Wildfire malware alert, etc. may be a sign of compromise; and are automatically detected and assigned a risk score for prioritisation. For example, Exabeam could tie a Wildfire security alert back to a specific user, and then produce a timeline of all the activities surrounding that alert. These user session timelines provide deep context around risky events, which aid security analysts in quickly prioritising and investigating alerts and accelerating incident response. **How it works:** 1. Palo Alto Networks VPN logs, Palo Alto Networks Wildfire security events, Palo Alto Networks Traps, and other logs are fetched from a SIEM or ingested directly to Exabeam via Syslog 2. Exabeam parses, normalises, and enriches the data with context from the environment. 3. The Exabeam Session Engine creates user sessions based daily user activity 4. A behavioural engine identifies anomalous risky behaviour and assigns a risk score 5. Incidents are displayed with complete timelines of user behaviour for quick investigation by security analysts

Diagram



About Exabeam

Exabeam provides security intelligence and management solutions to help organizations of any size protect their most valuable information. The Exabeam Security Intelligence Platform uniquely combines a data lake for unlimited data collection at a predictable price, machine learning for advanced analytics, and automated incident response into an integrated set of products.

About Palo Alto Networks

Palo Alto Networks is the next-generation security company, leading a new era in cybersecurity by safely enabling applications and preventing cyber breaches for tens of thousands of organisations worldwide. Built with an innovative approach and highly differentiated cyberthreat prevention capabilities, Palo Alto Networks game-changing security platform delivers security far superior to legacy or point products, safely enables daily business.

Contact

Exclusive Networks
Svärdvägen 19
182 33 Danderyd

Tel: +46 (0)8 400 255 00
Mail: info_se@exclusive-networks.com