exabeam

SOLUTION BRIEF

SPLUNK + EXABEAM ADVANCED ANALYTICS SOLUTION BRIEF

Deploying Exabeam Advanced Analytics (AA) alongside Splunk enables customers to use their existing Splunk log data to perform truly comprehensive, analytics-led threat detection. Joint customers enjoy quick time-to-value by analyzing historical logs to rapidly achieve behavioral baselines. Customers also benefit from increased visibility as new log sources, such as proxy logs or endpoint logs, which were previously cost-prohibitive to store within Splunk can be directly ingested into Advanced Analytics via syslog for analysis.

EXABEAM AND SPLUNK INTEGRATION

Exabeam Advanced Analytics deploys quickly in any environment via a physical or virtual appliance, which is then configured to fetch the requisite logs via Splunk's API, or to receive them via Syslog forwarding. Unlike competitive UEBA solutions, Exabeam Advanced Analytics can be setup within hours, often without the need for professional services.   Exabeam also ingests data from contextual sources like Active Directory, HR systems, and CMDB systems.

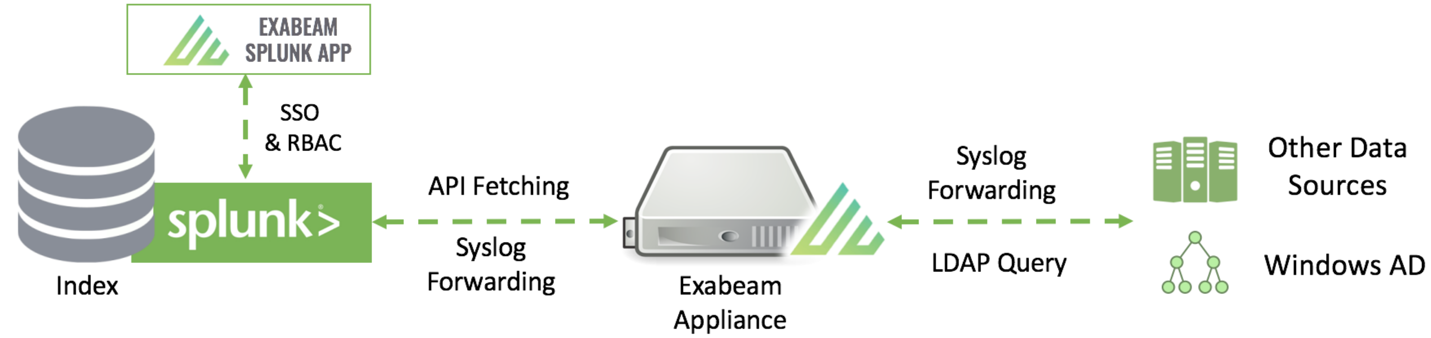
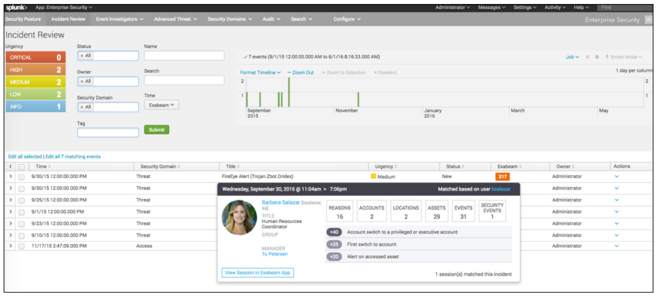


Figure 1. - Deploying Exabeam Advanced Analytics alongside Spunk: Data flow and architectural components.

EFFICIENT INTERFACING VIA EXABEAM SPLUNK APP

In many Security Operation Centers,there are well established workflows and procedures which are utilized to triage, investigate, and respond to security alerts and incidents. Advanced Analytics provides analysts with seamless access to advanced threat detection without changing these workflows by leveraging a Splunk App. App users enjoy easy access via SSO, while admins benefit from rich RBAC that helps quickly provision users, assign them to roles, and grant the appropriate access privileges.



Incident Review

Urgency

CRITICAL	0
HIGH	2
MEDIUM	2
LOW	2
INFO	1

Status: × All

Name:

Owner: × All

Search:

Security Domain: × All

Time: Exabeam

Tag:

✓ 7 events (9/1/15 12:00:00.000 AM to 6/1/16 8:16:33.000 AM)

Edit all selected | Edit all 7 matching events

i	□	Time	Security Domain	Title	Urgency	Status	Exabeam	Owner	Actions
>	□	9/30/15 12:00:00.000 PM	Threat	FireEye Alert (Trojan.Zbot.Dridex)	Medium	New	217	Administrator	⌄
>	□	9/30/15 12:00:00.000 PM	Threat					Administrator	⌄
>	□	9/25/15 12:00:00.000 PM	Threat					Administrator	⌄
>	□	9/1/15 12:00:00.000 PM	Threat					Administrator	⌄
>	□	9/23/15 12:00:00.000 PM	Threat					Administrator	⌄
>	□	9/10/15 12:00:00.000 PM	Threat					Administrator	⌄
>	□	11/17/15 2:47:09.000 PM	Access					Administrator	⌄

Wednesday, September 30, 2015 @ 11:04am > 7:06pm   Matched based on user bsalazar

Barbara Salazar [bsalazar, sa]

TITLE
Human Resources Coordinator

GROUP

MANAGER
Tu Petersen

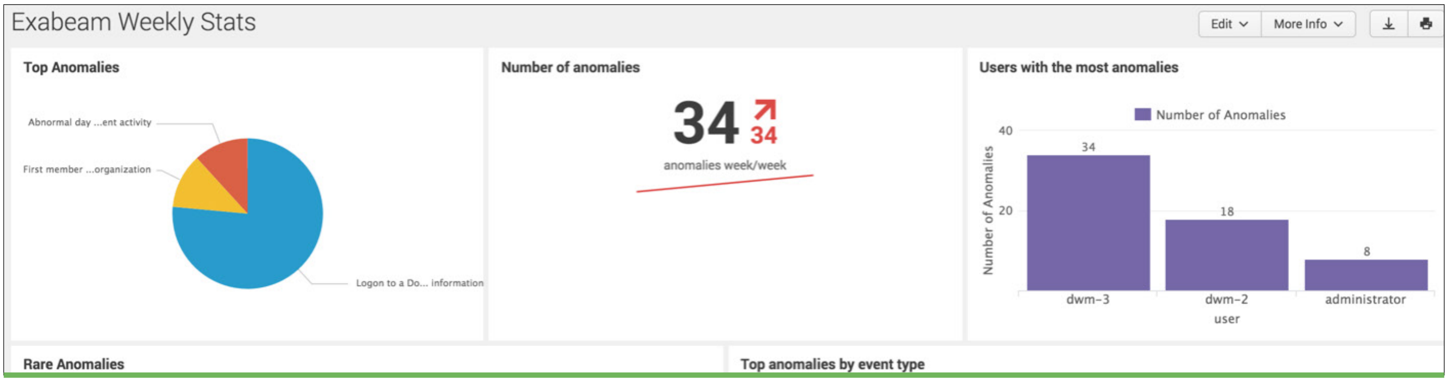
REASONS	ACCOUNTS	LOCATIONS	ASSETS	EVENTS	SECURITY EVENTS
16	2	2	29	31	1

+40	Account switch to a privileged or executive account
+25	First switch to account
+20	Alert on accessed asset

1 session(s) matched this incident

Figure 2. - The Exabeam Advanced Analytics Splunk app

The Advanced Analytics Splunk app amplifies analyst productivity by providing risk scores, investigation timelines, and enriched user context, embedded within the Splunk user interface; thus minimizing changes to existing workflows and processes. Advanced Analytics enables users to perform rapid incident investigations via the app. An Investigation that would take days or weeks to accomplish by pivoting and querying through raw logs in Splunk, can be accomplished in minutes via Exabeam's Splunk app.



KEY FEATURES AND BENEFITS

Quick Time-to-Value

Exabeam Advanced Analytics deploys in hours using a physical or virtual appliance. It then rapidly builds user and entity baselines from existing historical log data in Splunk. The system then begins to automatically identify risky, anomalous activity - often an indicator of threats or malicious action - and populates the results in a pre-built Splunk App for easy access by analyst

The World's Most-Deployed UEBA Solution

Exabeam detects complex insider threats using the Exabeam Advanced Analytics solution, the most-deployed User and Entity Behavior Analytics (UEBA) product in the world. SIP not only identifies risky user anomalies, it recreates entire attack chains including both normal and anomalous activities for related users.

Leverage Existing Workflows

A full-featured Splunk App enables Advanced Analytics users to obtain Exabeam risk scores, review notable users, and perform rapid incident investigations using Exabeam's pre-built incident timelines, all from within the Splunk User interface.

Enhanced Lateral Movement Detection

Exabeam's patented session data model automatically tracks changes in user state including changes of credentials, IP addresses, or devices. This unique stateful user tracking ability enables Advanced Analytics to easily detect lateral movement and to provide an incident timeline documenting the event.

Rapid Incident Investigation

Advanced Analytics automatically stitches all user and entity activity together into chronological timelines which are available for analyst use in the Splunk app. These pre-built incident timelines greatly reduce investigation time and effort by automating the tedious process of gather raw event logs and assembling them into a timeline for review.

Utilize Exabeam Data in Splunk Reports & Dashboards

The Exabeam / Splunk integration provides seamless access to Exabeam data and detection results, which can be incorporated into compliance reporting, visualizations, and SOC dashboards.

For more information, please contact Exabeam at info@exabeam.com