exabeam

SOLUTION BRIEF

EXABEAM AND F5 NETWORKS

DETECT INSIDER THREATS AND ACCELERATE INCIDENT RESPONSE

Integrated solutions

F5® BIG-IP® Access Policy Manager®

Benefits at a glance

- Increased detection of Insider threats and lateral movement
- Improved SOC efficiency and reduced investigation response time

In today's threat landscape, credential based attacks involving compromised or malicious insiders are more common than ever. These sophisticated attacks are difficult to detect because hackers are impersonating legitimate users, abusing their access rights, and moving laterally through an organization to obtain valuable business data.

F5 Networks® offers users a host of solutions that optimize the delivery of network-based applications, and the security, performance, and availability of servers, data storage devices, and other network resources. The logs from these products provide valuable insight and context around potential incidents.

Exabeam is a security intelligence platform that leverages existing data to quickly detect modern cyber-attacks and accelerate effective response. By ingesting data from F5 BIG-IP Access Policy Manager (APM®) and combining it with existing logs, endpoint, and other types of data, Exabeam is able to detect risky behavior and fast-track incident investigation.

The F5 BIG-IP APM and Exabeam integration provides

- Increased detection of credential-based attacks, insider threats, and lateral movement via data science and behavioral modeling
- Accelerated Incident investigation and SOC automation using Exabeam's user session timelines to triage security anomalies

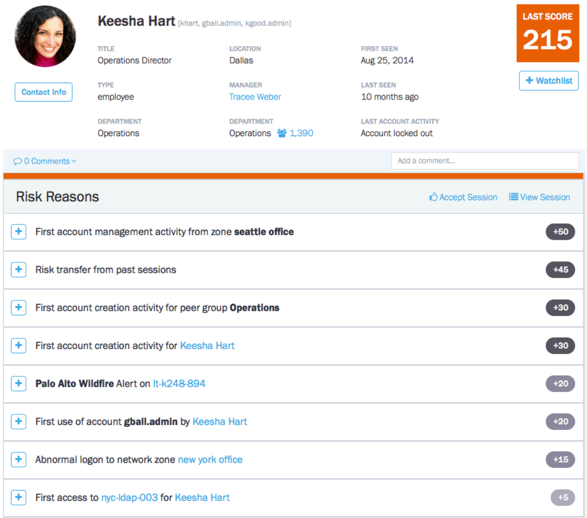
Increased Detection of Insider Threats

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 APM logs from F5 BIG-IP, however without additional context these insidious threats would be impossible to detect.

Solution

By ingesting F5 BIG-IP APM logs and combining them with other existing data sources such as those found in a SIEM, Exabeam is able to profile and analyze the activity and behavior of all users and assets within an organization. Exabeam's stateful user tracking methodology stitches together user activities into session timelines and then employs behavioral modeling to determine what is normal for those users. Anomalous behavior such as abnormal VPN connections, excessive distance since the last log-in, etc., may be a sign of compromise; and is automatically detected and assigned a risk score for prioritization.



Keesha Hart [khart, gball.admin, kgood.admin]

TITLE
Operations Director

LOCATION
Dallas

FIRST SEEN
Aug 25, 2014

TYPE
employee

MANAGER
Tracee Weber

LAST SEEN
10 months ago

DEPARTMENT
Operations

DEPARTMENT
Operations 1,390

LAST ACCOUNT ACTIVITY
Account locked out

LAST SCORE
215

0 Comments

Add a comment...

Risk Reasons

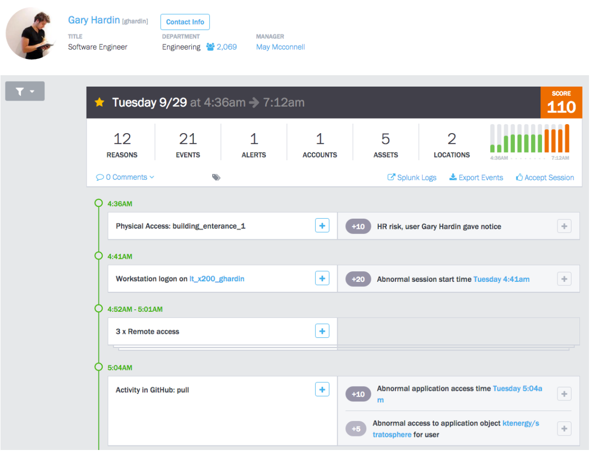
First account management activity from zone **seattle office**	+50
Risk transfer from past sessions	+45
First account creation activity for peer group **Operations**	+30
First account creation activity for Keesha Hart	+30
Palo Alto Wildfire Alert on lt-k248-894	+20
First use of account **gball.admin** by Keesha Hart	+20
Abnormal logon to network zone new york office	+15
First access to nyc-ldap-003 for Keesha Hart	+5

Risky users and their anomalous behavior are automatically identified and presented to analysts for quick identification.

ACCELERATED INCIDENT INVESTIGATION

Challenge

Once identified, security incidents warrant an investigation to determine their scope and impact. These investigations provide analysts with the information needed to take corrective action. During an investigation, security analysts must manually sift through event logs to gather raw data and reconstruct a timeline of the event. This process takes time. Sometimes investigations can take days, and many organizations simply cannot hire enough security talent to expedite them.



Gary Hardin [ghardin] Contact Info
TITLE Software Engineer
DEPARTMENT Engineering 2,069
MANAGER May Mcconnell

Tuesday 9/29 at 4:36am → 7:12am SCORE 110

12	21	1	1	5	2
REASONS	EVENTS	ALERTS	ACCOUNTS	ASSETS	LOCATIONS

0 Comments · Splunk Logs · Export Events · Accept Session

4:36AM
Physical Access: building_enterance_1 | +10 HR risk, user Gary Hardin gave notice

4:41AM
Workstation logon on lt_x200_ghardin | +20 Abnormal session start time Tuesday 4:41am

4:52AM - 5:01AM
3 x Remote access

5:04AM
Activity in GitHub: pull | +10 Abnormal application access time Tuesday 5:04am | +5 Abnormal access to application object ktenergy/stratosphere for user

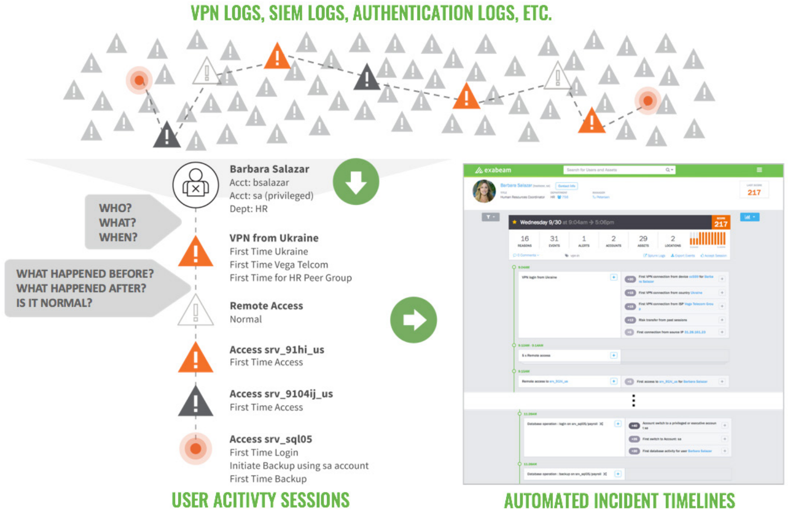
Incident timelines are automatically constructed in order to faciliate quick investigations.

Solution

Exabeam's unique session data model automatically creates a complete timeline of every event and anomaly tied to an attack, even if attackers change devices, IP addresses, or credentials. These stateful These stateful user session timelines provide the context around the user and asset behavior associated with an event that is needed to properly validate the alert. Exabeam automates many tasks of the incident response investigation to greatly reduce the time and effort of these investigations; what used to take days, can be accomplished with Exabeam in minutes.

HOW IT WORKS

1. F5 BIG-IP APM logs and other existing data logs are fetched from a SIEM or ingested directly to Exabeam via Syslog
2. Exabeam parses, normalizes, and enriches the data with context from the environment.
3. The Exabeam Session Engine creates user sessions based daily user activity
4. A behavioral engine identifies anomalous risky behavior and assigns a risk score
5. Incidents are displayed with complete timelines of user behavior for quick investigation by security analysts



ABOUT EXABEAM

Exabeam's user and entity behavior analytics solution leverages existing log data to quickly detect advanced attacks, prioritize incidents and guide effective response. The company's Stateful User Tracking™ automates the work of security analysts by resolving individual security events and behavioral anomalies into a complete attack chain. This dramatically reduces response times and uncovers attack impacts that would otherwise go unseen. Built by seasoned security experts and enterprise IT veterans from Imperva, ArcSight and Sumo Logic, Exabeam is headquartered in San Mateo, California and is privately funded by Aspect Ventures, Icon Ventures, Investor Shlomo Kramer and Norwest Venture Partners.

ABOUT F5 NETWORKS

F5 provides solutions for an application world. F5 helps organizations seamlessly scale cloud, data center, telecommunications, and software defined networking (SDN) deployments to successfully deliver applications and services to anyone, anywhere, at any time. F5 solutions broaden the reach of IT through an open, extensible framework and a rich partner ecosystem of leading technology and orchestration vendors. This approach lets customers pursue the infrastructure model that best fits their needs over time. The world's largest businesses, service providers, government entities, and consumer brands rely on F5 to stay ahead of cloud, security, and mobility trends.