exabeam

DATASHEET

THREAT HUNTER
FOR FEDERAL AGENCIES

One of the biggest challenges for any federal agency is finding ways to identify and minimize the impact of *insider threats* -- that someone with access to the organization's networks (an employee, former employee, or contractor) will use that access maliciously. Compounding the problem, if someone external to the agency gains network access, they can look like an insider. While SIEM is a *collection of dots,* Exabeam enables richer context from connecting these dots.

The Federal Government continues to reduce paths that outsiders could use to penetrate government networks. From patching critical vulnerabilities to strengthened policies and procedures for privileged users to requiring multi-factor identification for network access, the goal is to make outside intrusion both more difficult and easier to detect when it happens.

User Behavior Analytics (UBA) relies on machine learning to transform millions of events into the handful of users that are performing risky behavior right now. In essence, UBA is about the machine telling the security analyst where to focus. Threat hunting is a complementary technique that enables analysts to query the event data to find users that match a specific set of criteria. Threat Hunting is about the analyst telling the machine to find the users that fit X, Y, and Z parameters. Exabeam is the only security intelligence vendor to provide both powerful UBA capabilities and market-leading threat hunting functionality, now available through **Exabeam Threat Hunter**.

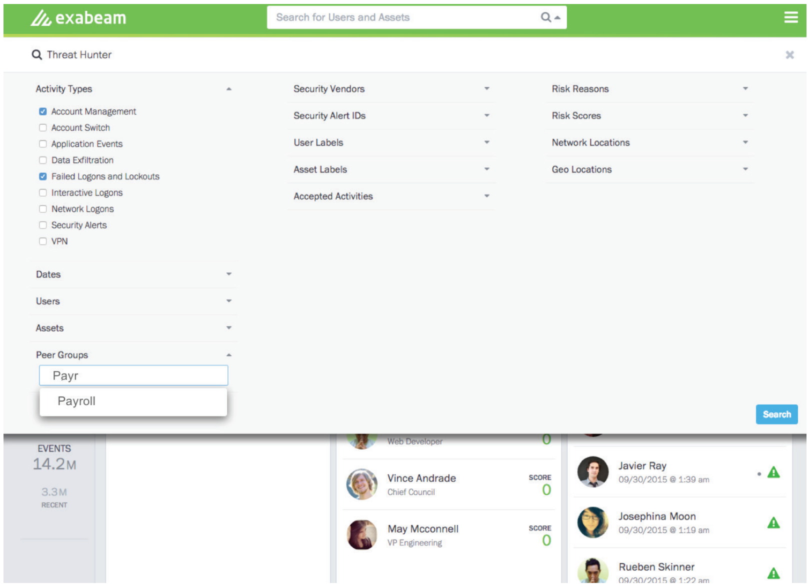
Query, Pivot, and Drill Down on Session Data

The Exabeam platform uses Stateful User Tracking™ to connect individual user activities into a session data model. Threat Hunter allows security professionals to query the platform to find all users whose sessions contain specific activities or attributes, or any combination of activities or attributes. For example, an analyst might first ask for all user sessions where the user logged into the VPN from a foreign country for the first time. The analyst can then trim the results by asking for users who then accessed a server for the first time, and then later the anti-malware software flagged a problem on that server. While each of these activities is independent of the others, the ability to combine them in a simple, point-and-click search provides significant power to even a junior analyst.

Proactive Security Intelligence

In the example shown here, an analyst uses Threat Hunter to clean up after a malware outbreak in the Payroll Department that allowed hackers to penetrate the network.

The analyst begins by hunting for all sessions where any user in Payroll performed account management (i.e. new account creation or privilege escalation) and also had a failed logon. The analyst doesn't need to understand the structure of the applicable logs, nor the search language of the underlying log management system. She simply clicks a few fields and hits "Search."



Activity Types

- ☑ Account Management
- □ Account Switch
- □ Application Events
- □ Data Exfiltration
- ☑ Failed Logons and Lockouts
- □ Interactive Logons
- □ Network Logons
- □ Security Alerts
- □ VPN

Peer Groups: Payr

Payroll

Threat Hunter: *Easily Enter Hunt Parameters*

Filter and Drill Down

The analyst filters the result set further by adding a parameter where the event type equals "Account password was changed." Threat Hunter responds with a list of all users, within the default time period, who are in the marketing department and had credentials that were used to perform account management, had a failed logon, and then changed the account password.

Near the top of the list we see one user, Angella French, who has been flagged by Exabeam UBA as having unusual account lockout activity.

The analyst clicks on Angella, a Payroll Support agency employee, and Exabeam displays detailed information about her identity and the events associated with this lockout.

We see a very high number of failed logons across thirteen different systems. As account lockouts can be a strong signal of a compromised account and a hacker impersonating a valid internal user, this is worth further investigation.

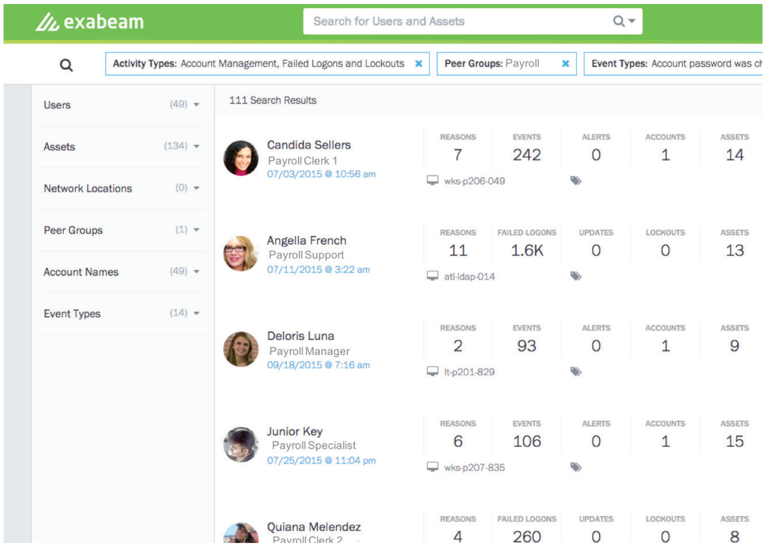
The analyst now has an additional candidate for malware infection and account takeover within the Payroll department, and can respond accordingly.

Works With Any Log or SIEM System

Exabeam UBA and Threat Hunter include prebuilt integrations with all leading log management products, including:

- IBM QRadar
- Splunk
- HP ArcSight
- McAfee ESM
- RSA Security Analytics

In addition, Threat Hunter and UBA can integrate with any log system via syslog forwarding. Additional feeds from products such as Data Loss Prevention, endpoint security, cloud security, and others can be easily integrated and used in threat hunting.



Activity Types: Account Management, Failed Logons and Lockouts ✖ | Peer Groups: Payroll ✖ | Event Types: Account password was ch

Users (49)
Assets (134)
Network Locations (0)
Peer Groups (1)
Account Names (49)
Event Types (14)

111 Search Results

Candida Sellers
Payroll Clerk 1
07/03/2015 @ 10:56 am
REASONS 7 | EVENTS 242 | ALERTS 0 | ACCOUNTS 1 | ASSETS 14
wks-p206-049

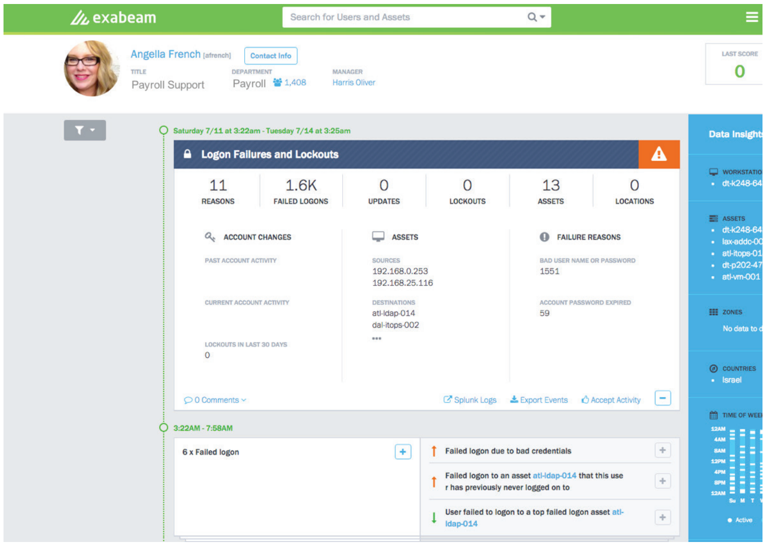
Angella French
Payroll Support
07/11/2015 @ 3:22 am
REASONS 11 | FAILED LOGONS 1.6K | UPDATES 0 | LOCKOUTS 0 | ASSETS 13
atl-ldap-014

Deloris Luna
Payroll Manager
09/18/2015 @ 7:16 am
REASONS 2 | EVENTS 93 | ALERTS 0 | ACCOUNTS 1 | ASSETS 9
lt-p201-829

Junior Key
Payroll Specialist
07/25/2015 @ 11:04 pm
REASONS 6 | EVENTS 106 | ALERTS 0 | ACCOUNTS 1 | ASSETS 15
wks-p207-835

Quiana Melendez
Payroll Clerk 2
REASONS 4 | FAILED LOGONS 260 | UPDATES 0 | LOCKOUTS 0 | ASSETS 8

Threat Hunter: *Session Results List*



Angella French [afrench]
TITLE Payroll Support
DEPARTMENT Payroll 1,408
MANAGER Harris Oliver
LAST SCORE 0

Saturday 7/11 at 3:22am - Tuesday 7/14 at 3:25am

Logon Failures and Lockouts

11 REASONS | 1.6K FAILED LOGONS | 0 UPDATES | 0 LOCKOUTS | 13 ASSETS | 0 LOCATIONS

ACCOUNT CHANGES
PAST ACCOUNT ACTIVITY
CURRENT ACCOUNT ACTIVITY
LOCKOUTS IN LAST 30 DAYS
0

ASSETS
SOURCES
192.168.0.253
192.168.25.116
DESTINATIONS
atl-ldap-014
dal-itops-002
•••

FAILURE REASONS
BAD USER NAME OR PASSWORD
1551
ACCOUNT PASSWORD EXPIRED
59

3:22AM - 7:58AM

6 x Failed logon

Failed logon due to bad credentials

Failed logon to an asset atl-ldap-014 that this use
r has previously never logged on to

User failed to logon to a top failed logon asset atl-ldap-014

Data Insight
WORKSTATIO
- dt-k248-64

ASSETS
- dt-k248-64
- lax-addc-00
- atl-itops-01
- dt-p202-47
- atl-vm-001

ZONES
No data to d

COUNTRIES
- Israel

Threat Hunter: *Drill Down Into a Specific User Session*

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