HOW TO INSTANTLY SEE PRIVILEGED ACCOUNT COMPROMISE OR ABUSE

REAL TIME VIEWS OF REAL WORLD SCENARIOS WITH PRIVILEGED BEHAVIOR ANALYTICS FOR SECRET SERVER

IT and System Admins along with security professionals know that safeguarding access to privileged accounts throughout an enterprise is critical. With up to 80% of breaches involving a compromised user or privileged account, gaining insights into privileged account access and user behavior is a top priority. Even more important, identifying a breach by an outside attacker or malicious insider involving compromised privileged accounts now averages more than 140 days---an eternity in terms of putting your critical assets at risk.

Imagine being able to identify a potential breach in minutes instead of months.

Privileged Behavior Analytics for Secret Server from Thycotic makes it possible with "at a glance" breach detection capabilities. That's becase Privileged Behavior Analytics (PBA) provides unique views into the access and activity of your privileged accounts in real time. These views give you the instant visibility you want and need to help spot suspected account compromise and potential user abuse.

Using advanced machine learning technology, Privilege Behavior Analytics starts with a learning period, where it observes, analyzes, and creates baselines for how every user in Thycotic Secret Server password protection software behaves. PBA utilizes key data points in creating individual user baselines, including User activity, Secret Access, Secret Sensitivity, Similar User Behavior, and Time of Access.

Once typical behavior baselines are established for privileged account access activity, PBA can automatically alert administrators when users are acting outside of their normal behavior patterns – an early sign of either account compromise or insider threat abuse.

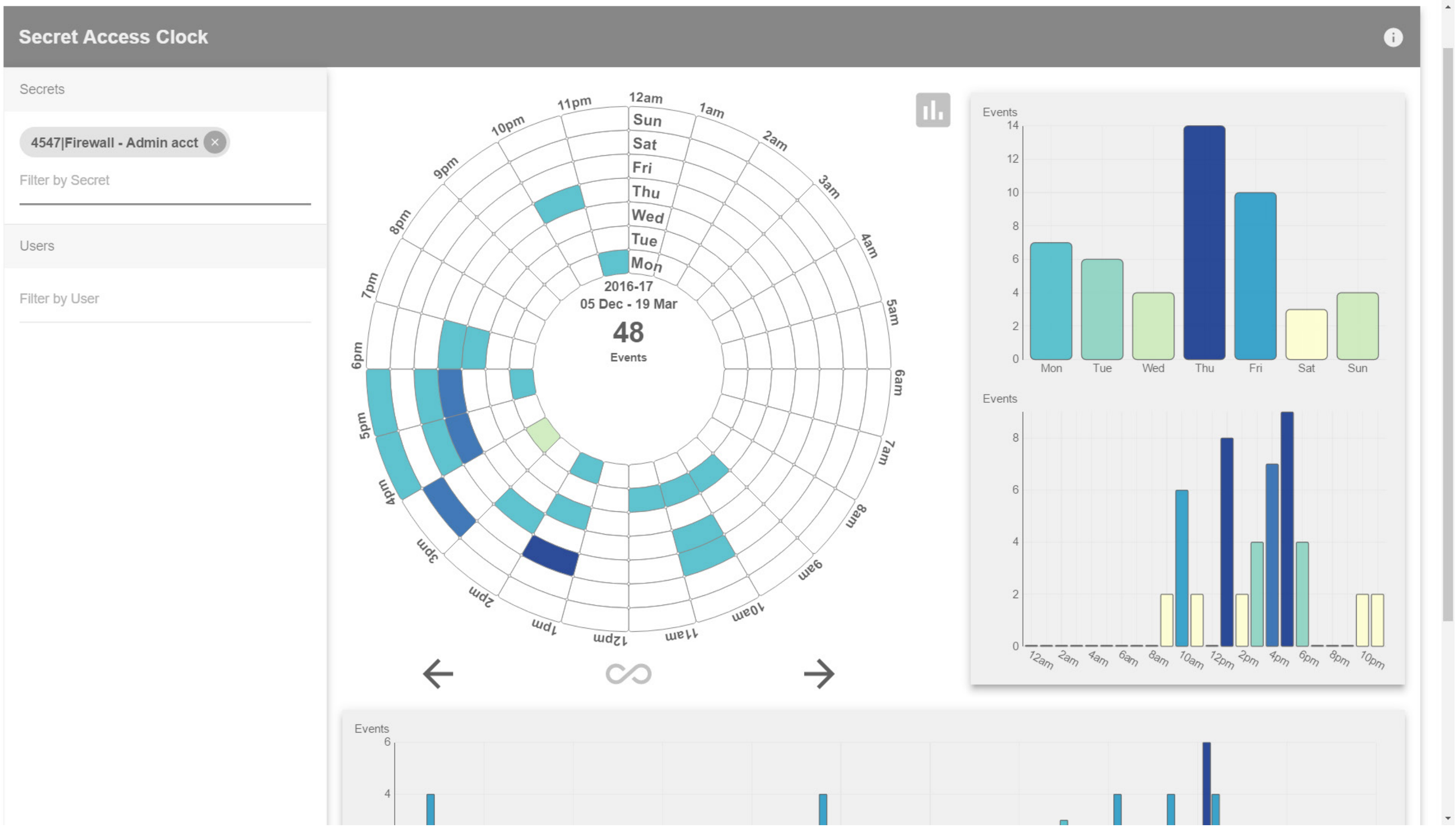
Real Time Alerts for Real World Behavioral Risks

Operating in real time, PBA delivers key views and immediate insights into potential threats or issues for privileged accounts protected by Secret Server. Administrators can readily see situational views that include: Most Active Secrets, Most Active Users, Secret Access Clock, Secret Details, and User Details. These dashboard views allow an administrator to quickly explore the details that prompted an alert, and help inform any next steps to safeguard accounts such as logging into Secret Server to revoke all privileged account access and rotating all passwords.
The following real world scenarios illustrate the power of PBA for Secret Server, enabling IT System and Security Admins to get automatic alerts for unusual behavior or access and to quickly examine details to determine if such behavior warrants further investigation.

SCENARIO 1

DO YOU KNOW IF ANYBODY IS ACCESSING PRIVILEGED ACCOUNTS AT 3AM?

With Privileged Behavior Analytics and Secret Server, you can quickly analyze the temporal behavior of your users, allowing you to quickly identify if there is unusual activity at odd-hours of the day. Privileged Behavior Analytics comes with a “Secret Access Clock” that allows security oversight teams the ability to rapidly analyze access behavior. These analysis tools can be futher filtered down to view a specific Secret or User’s behavior, in a given time period.

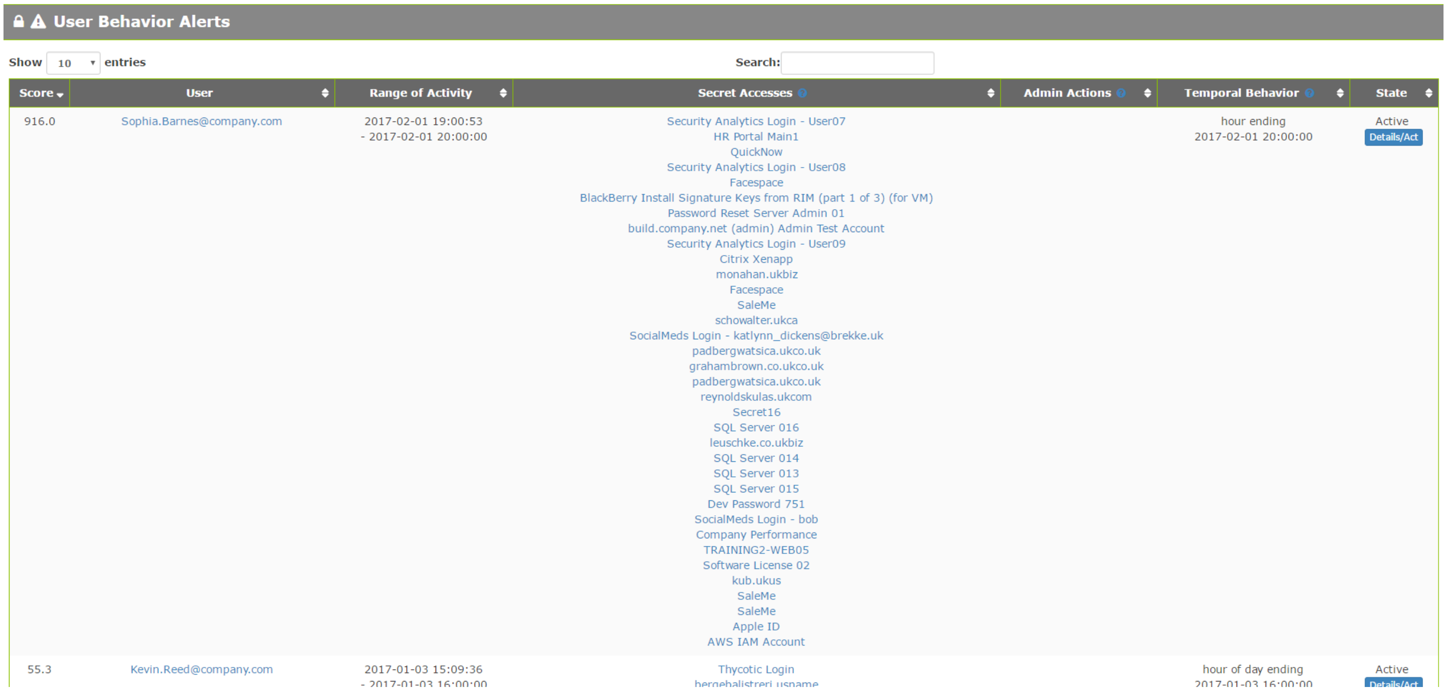


In this example, you can see that this privileged account has quite a bit of activity between the hours of 8am and 6pm. However, there are some events that have occurred on this account at 10pm and 11pm that are worth investigating and can be drilled into further by right clicking on the highlighted sections of interest.

SCENARIO 2

HOW DO YOU KNOW IF A USER IS ACCESSING A BUNCH OF ACCOUNTS THEY DON'T NORMALLY ACCESS?

An employee accessing a bunch of accounts that they don't normally access, can be a very early and critical indication of insider threat abuse, or privileged account compromise. Privileged Behavior Analytics allows your organization to be alerted, the moment a user is acting outside of normal behavior (like suddenly accessing a bunch of highly privileged accounts they don't normally use)



User Behavior Alerts

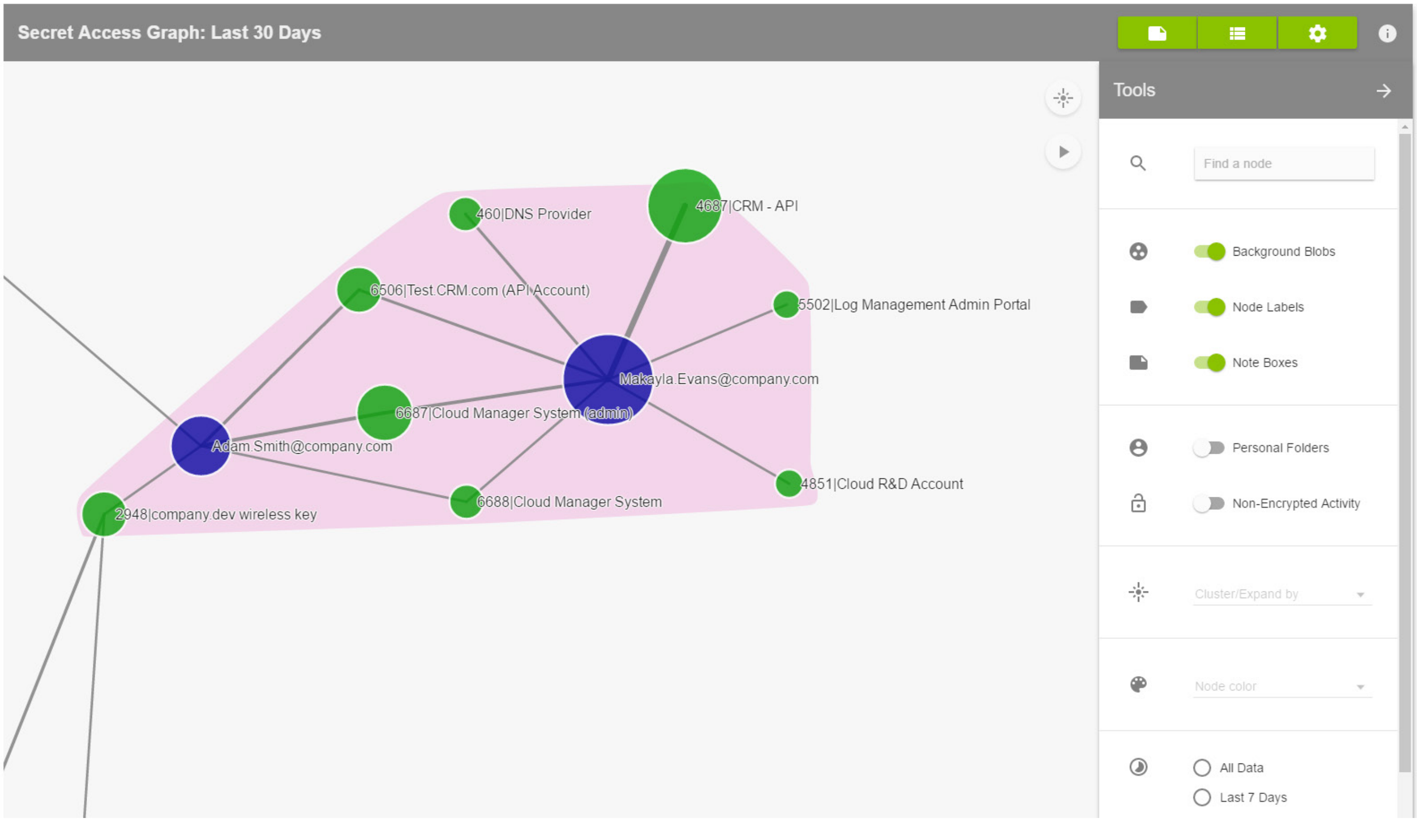
Score	User	Range of Activity	Secret Accesses	Admin Actions	Temporal Behavior	State
916.0	Sophia.Barnes@company.com	2017-02-01 19:00:53 - 2017-02-01 20:00:00	Security Analytics Login - User07 HR Portal Main1 QuickNow Security Analytics Login - User08 Facespace BlackBerry Install Signature Keys from RIM (part 1 of 3) (for VM) Password Reset Server Admin 01 build.company.net (admin) Admin Test Account Security Analytics Login - User09 Citrix Xenapp monahan.ukbiz Facespace SaleMe schowalter.ukca SocialMeds Login - katlynn_dickens@brekke.uk padbergwatsica.ukco.uk grahambrown.co.ukco.uk padbergwatsica.ukco.uk reynoldskulas.ukcom Secret16 SQL Server 016 leuschke.co.ukbiz SQL Server 014 SQL Server 013 SQL Server 015 Dev Password 751 SocialMeds Login - bob Company Performance TRAINING2-WEB05 Software License 02 kub.ukus SaleMe SaleMe Apple ID AWS IAM Account		hour ending 2017-02-01 20:00:00	Active Details/Act
55.3	Kevin.Reed@company.com	2017-01-03 15:09:36 - 2017-01-03 16:00:00	Thycotic Login bergebalistreri.usname		hour of day ending 2017-01-03 16:00:00	Active Details/Act

In this example, this is an alert showing a user accessing a bunch of accounts they don't normally access in a 1 hour time frame – including a bunch of SQL Server accounts and other Administrative Accounts.

SCENARIO 3

HOW MANY PEOPLE HAVE ACCESS TO EACH OF YOUR PRIVILEGED ACCOUNTS?

With Privileged Behavior Analytics, you can quickly see a map of your privileged accounts and all the users who have access to them. Additionally, users and Secrets are grouped together into “Communities” that serve as mini-ecosystems. You can quickly see if a Secret is contained within a group of people, or if users are accessing Secrets from other departments.

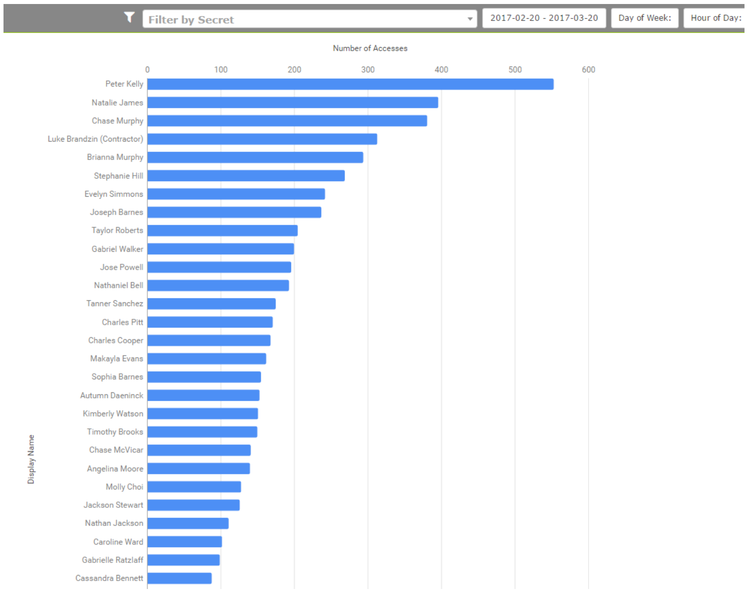


In this example, we have a two-person team. You can see the people in the blue circles, and their ecosystem of Secrets in green, with lines showing access. But there are incoming access lines from outside the two-person ecosystem. Who are these users outside of the community, and should they really have access?

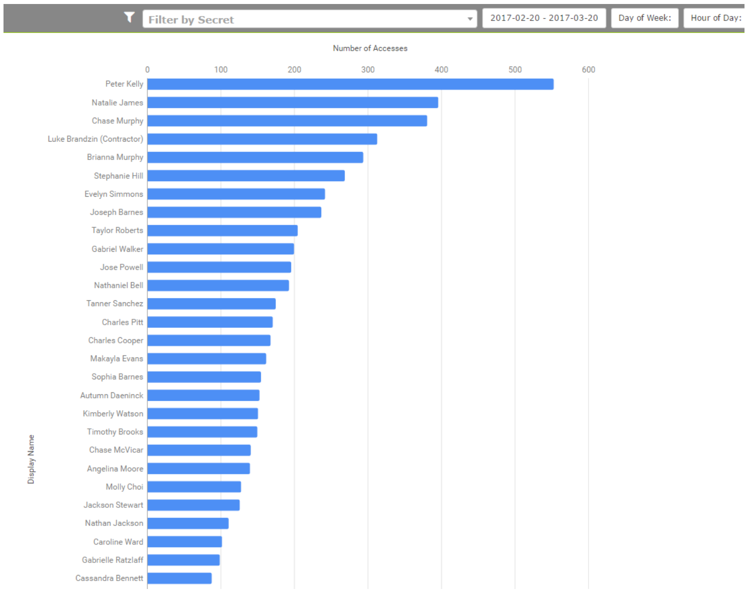
SCENARIO 4

WHO ARE YOUR MOST ACTIVE USERS? OR MOST ACCESSED ACCOUNTS?

You can quickly see two different views in Privileged Behavior Analytics that allows you to quickly see your most active users at any given time, as well as your most accessed Secrets. At a glance, you can quickly see if any one user or Secret has too much exposure.



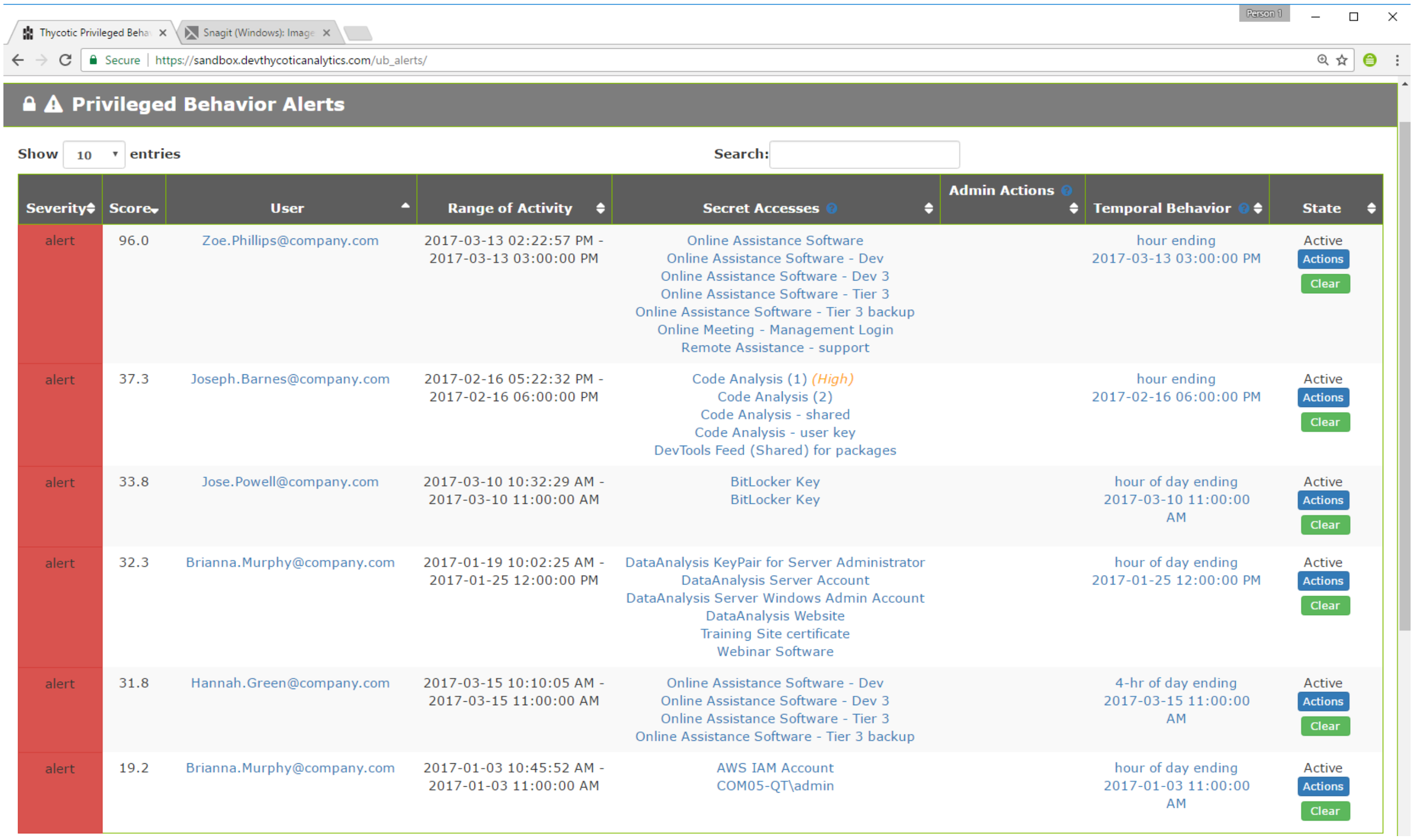
In this example, we can quickly see your most accessed accounts. You can look at a similar graph of most active users as shown below



SCENARIO 5

EVERY DAY YOU MAY ENCOUNTER ANY NUMBER OF SECURITY EVENTS AND ALERTS, HOW DO YOU KNOW WHICH ARE THE MOST IMPORTANT?

Privileged Behavior Analytics uses a behavioral baseline for user access, based on a number of machine learning algorithms that take into account temporal behavior, access behavior, credential sensitivity, and similar user behavior. Once a user deviates from this baseline, they are given a threat score. The system prioritizes these threat scores, so you can focus on the alerts with the highest potential risk to your organization first.


Thycotic Privileged Beha
Snagit (Windows): Image
Person 1
Secure | https://sandbox.devthycoticanalytics.com/ub_alerts/

Privileged Behavior Alerts

Show 10 entries Search:

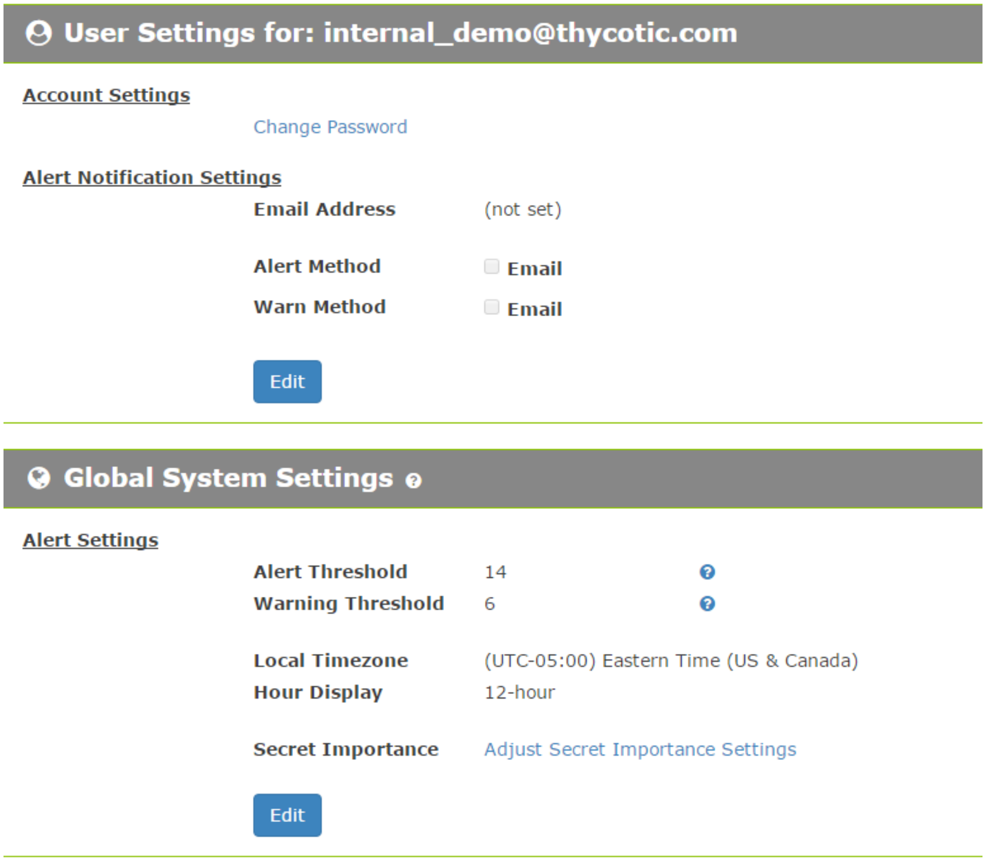
Severity	Score	User	Range of Activity	Secret Accesses	Admin Actions	Temporal Behavior	State
alert	96.0	Zoe.Phillips@company.com	2017-03-13 02:22:57 PM - 2017-03-13 03:00:00 PM	Online Assistance Software Online Assistance Software - Dev Online Assistance Software - Dev 3 Online Assistance Software - Tier 3 Online Assistance Software - Tier 3 backup Online Meeting - Management Login Remote Assistance - support		hour ending 2017-03-13 03:00:00 PM	Active Actions Clear
alert	37.3	Joseph.Barnes@company.com	2017-02-16 05:22:32 PM - 2017-02-16 06:00:00 PM	Code Analysis (1) *(High)* Code Analysis (2) Code Analysis - shared Code Analysis - user key DevTools Feed (Shared) for packages		hour ending 2017-02-16 06:00:00 PM	Active Actions Clear
alert	33.8	Jose.Powell@company.com	2017-03-10 10:32:29 AM - 2017-03-10 11:00:00 AM	BitLocker Key BitLocker Key		hour of day ending 2017-03-10 11:00:00 AM	Active Actions Clear
alert	32.3	Brianna.Murphy@company.com	2017-01-19 10:02:25 AM - 2017-01-25 12:00:00 PM	DataAnalysis KeyPair for Server Administrator DataAnalysis Server Account DataAnalysis Server Windows Admin Account DataAnalysis Website Training Site certificate Webinar Software		hour of day ending 2017-01-25 12:00:00 PM	Active Actions Clear
alert	31.8	Hannah.Green@company.com	2017-03-15 10:10:05 AM - 2017-03-15 11:00:00 AM	Online Assistance Software - Dev Online Assistance Software - Dev 3 Online Assistance Software - Tier 3 Online Assistance Software - Tier 3 backup		4-hr of day ending 2017-03-15 11:00:00 AM	Active Actions Clear
alert	19.2	Brianna.Murphy@company.com	2017-01-03 10:45:52 AM - 2017-01-03 11:00:00 AM	AWS IAM Account COM05-QT\admin		hour of day ending 2017-01-03 11:00:00 AM	Active Actions Clear

In this example, you can see a number of alerts that are sorted by their threat score which allows you to focus in on the most important events occurring in Secret Server. In the alerts, you can also see when the behavior happened and which Secrets or administrator actions were involved. If the alert happened because a user deviated from normal behavior, Temporal Behavior will contain a timestamp of when the unusual behavior happened. You can use Actions to choose how you will respond to the alert or clear the alert when it is resolved – any resolved alerts are recorded in the audit log.

SCENARIO 6

TIMING IS EVERYTHING – HOW ARE YOU NOTIFIED IF A USER IS ACTING SUSPICIOUS RIGHT NOW?

Privileged Behavior Analytics can be setup to send alerts to any number of people on your security team the moment suspicious behavior is occurring. Security teams can immediately react to these security alerts, allowing them to dive into Secret Server to view any active sessions, remediate any problems, or potentially revoke a user’s access on the spot, in order to conduct a thorough investigation.



User Settings for: internal_demo@thycotic.com

Account Settings

Change Password

Alert Notification Settings

Email Address	(not set)
Alert Method	☐ Email
Warn Method	☐ Email

Global System Settings

Alert Settings

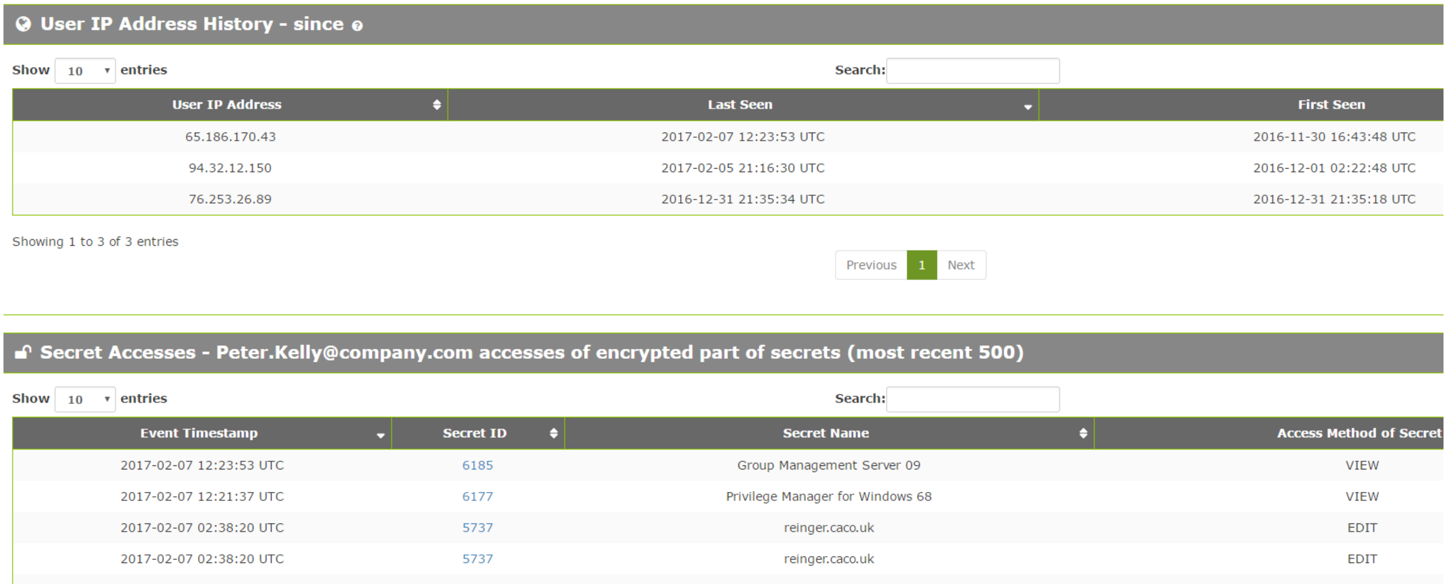
Alert Threshold	14
Warning Threshold	6
Local Timezone	(UTC-05:00) Eastern Time (US & Canada)
Hour Display	12-hour
Secret Importance	Adjust Secret Importance Settings

This screen shows the alerts settings, where you can choose how alerts are sent and who should receive them. You can configure Privileged Behavior Analytics to log alerts inside the tool, or send email notifications for certain types of alerts. If you need alerts sent to via email to be presented in your local time zone, you can set that here as well. Lastly, you can click Adjust Secret Importance Settings if you wish to tune the level of importance for any or all of your Secrets.

SCENARIO 7

DO YOU KNOW WHERE USERS ARE ACCESSING YOUR PRIVILEGED ACCOUNTS FROM? IS IT ALL ON-SITE, OR ARE USERS ACCESSING THEM REMOTELY?

With Privileged Behavior Analytics, you can view the IP Addresses of where your Secret Server users are connecting from. In the event of investigating an alert, you can quickly drill into a number of details about that user's activity history, including the IP Addresses and times they accessed it.



User IP Address History - since

Show 10 entries Search:

User IP Address	Last Seen	First Seen
65.186.170.43	2017-02-07 12:23:53 UTC	2016-11-30 16:43:48 UTC
94.32.12.150	2017-02-05 21:16:30 UTC	2016-12-01 02:22:48 UTC
76.253.26.89	2016-12-31 21:35:34 UTC	2016-12-31 21:35:18 UTC

Showing 1 to 3 of 3 entries

Secret Accesses - Peter.Kelly@company.com accesses of encrypted part of secrets (most recent 500)

Show 10 entries Search:

Event Timestamp	Secret ID	Secret Name	Access Method of Secret
2017-02-07 12:23:53 UTC	6185	Group Management Server 09	VIEW
2017-02-07 12:21:37 UTC	6177	Privilege Manager for Windows 68	VIEW
2017-02-07 02:38:20 UTC	5737	reinger.caco.uk	EDIT
2017-02-07 02:38:20 UTC	5737	reinger.caco.uk	EDIT

In this view, you can see the IP addresses that an individual user accessed Secret Server from.

LEARN MORE

See for yourself how Privileged Behavior Analytics for Secret Server can make the difference between spotting and stopping privileged account abuse and a potential cyber catastrophe. To learn more about Secret Server and its new Privileged Behavior Analytics capabilities, visit Thycotic's website at https://thycotic.com/pba