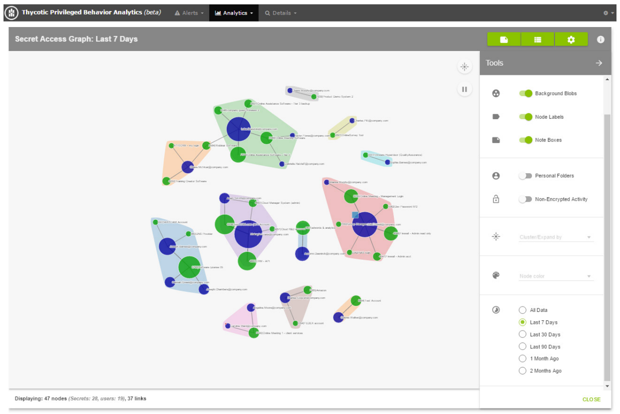
Privileged Behavior Analytics

Overview

PRIVILEGED BEHAVIOR ANALYTICS

DETECTING BREACHES AND DATA THEFT BEFORE THEY HAPPEN - POWERED BY THE CLOUD


Thycotic Privileged Behavior Analytics (beta)
Alerts
Analytics
Details
Secret Access Graph: Last 7 Days
Tools
CLOSE

Background Blobs (on)
Node Labels (on)
Note Boxes (on)
Personal Folders (off)
Non-Encrypted Activity (off)
Cluster/Expand by
Node color
○ All Data
● Last 7 Days
○ Last 30 Days
○ Last 90 Days
○ 1 Month Ago
○ 2 Months Ago

Displaying: 47 nodes *(Secrets: 28, users: 19)*, 37 links

IMPROVE SECURITY AND REDUCE RISKS

Reducing the security risks to your organization by improving security will help save your department time, money, and resources while maximizing your current investment in Secret Server.

Privileged Behavior Analytics can help IT and Security administrators quickly detect breaches before they happen, analyze distribution of privileged accounts and access across your organization, and add a layer of security to your Secret Server deployment.Free up your time to focus on discovering, managing, and protecting your privileged account credentials.

DETECT EARLY SIGNS OF BREACHES

Is a powerful privileged account, accessed at 3am appropriate behavior in your organzation?

Suddenly unusual behavior by a user can potentially be an early sign of data breach or insider threat. Privileged Behavior Analytics can quickly detect this anomalous behavior and instantly alert your security team to a cyberattack or insider threat before the data breach happens.

PRIORITIZE THE ALERTS THAT MATTER THE MOST

How do you know which security alert or activity is important to focus on first?

Machine learning and behavior pattern recognition helps to prioritize activities in your system, alerting you to what matters most. Know the instant that suspicious activity is happening, so you can swiftly take actions.

Sort your alerts by threat score, so you can focus on the critical alerts first.

REQUIREMENTS

Privileged Behavior Analytics requires any paid edition of Secret Server on-premise.

Deployed on the Amazon AWS platform. No hardware to setup or software to install!

PRICING STRUCTURE

Privileged Behavior Analytics is billed on an annual subscription, and priced based on the number of Secret Server user licenses you currently have.

Privileged Behavior Analytics

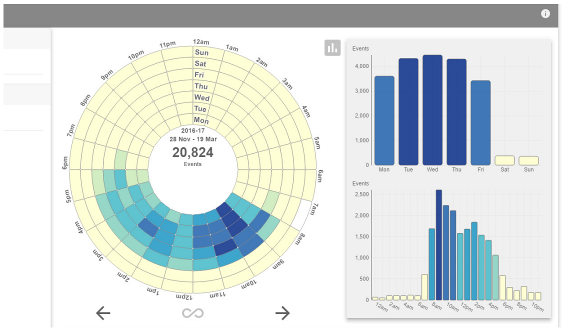
Use Cases

DETECTING BREACHES BEFORE THEY HAPPEN

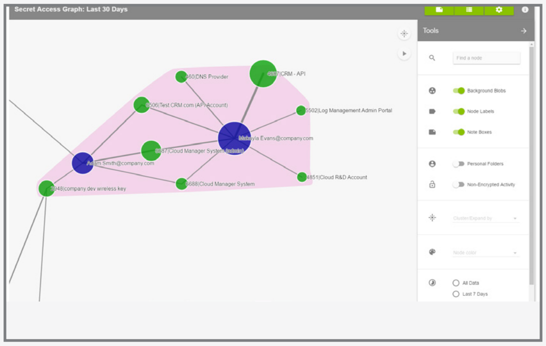
According to Forrester, it is estimated that 80% of breaches involve Privileged Accounts. Some of these breaches are due to privileged accounts that have been compromised or owned by insider threats. In addition to protecting all of your privileged accounts, it is important to track and analyze who has access to which privileged accounts, as well as when and how they are using them. Thycotic's Privileged Behavior Analytics helps you detect a potential breach before it happens. Our cloud based solution uses machine learning technology to analyze Privileged Behavior within Secret Server, our Privileged Account Management Solution, in order to quickly alert your security team to anomalous behavior, an early indication of compromise or abuse.

PEOPLE 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 Users behavior, in a given time period.



Screenshot: Access Lock



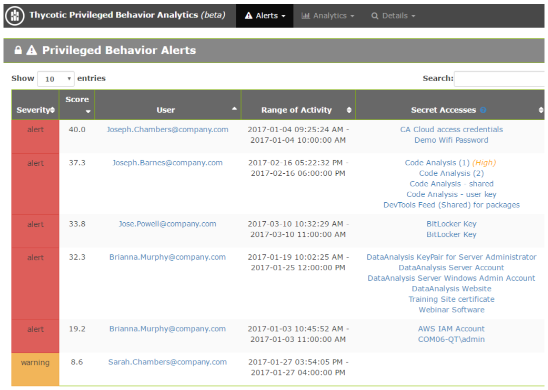
Screenshot: Access Graph

WHO HAS ACCESS TO WHICH ACCOUNTS?

With Privileged Behavior Analytics, you can quickly see a map of your privileged accounts and all of the users that 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 that are in other departments.

WHICH ALERTS 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, depending on the algorithms, 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.



Privileged Behavior Alerts

Show 10 entries

Search:

Severity	Score	User	Range of Activity	Secret Accesses
alert	40.0	Joseph.Chambers@company.com	2017-01-04 09:25:24 AM - 2017-01-04 10:00:00 AM	CA Cloud access credentials Demo Wifi Password
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
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
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
alert	19.2	Brianna.Murphy@company.com	2017-01-03 10:45:52 AM - 2017-01-03 11:00:00 AM	AWS IAM Account COM06-QT\admin
warning	8.6	Sarah.Chambers@company.com	2017-01-27 03:54:05 PM - 2017-01-27 04:00:00 PM	

Screenshot: Threat Scoring

thycotic

DC | LONDON | SYDNEY

e: sales@thycotic.com
t: @thycotic
www.thycotic.com