Privileged Threat Analytics™

Detect, alert, and respond to the most critical cyber attacks that could significantly impact the business.

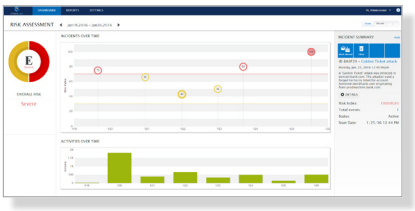

Figure 1. CyberArk Dashboard: This visual representation of detected incidents over time shows a detected Golden Ticket attack. Critical information such as the malicious user and machine are provided on the dashboard; security analysts can drill-down to get more detailed information on all security incidents.

Why CyberArk?

CyberArk is the trusted expert in helping organizations stop the most critical cyber-attacks **before** they stop the business.

The Challenge

Cyber attackers constantly advance their techniques in order to operate within a network while not setting off any alarms. Once they've breached the perimeter, attackers navigate the network as inconspicuously as possible, escalating privileges along the way until they gain access to the target. As they follow this path, attackers use legitimate privileged credentials in order to impersonate authorized users which enables them to stay under the radar. Due to attackers' strategy of impersonating legitimate users, organizations face a number of challenges monitoring user activity in order to detect and respond when and if an attacker is on the network.

Ambiguity on what data to analyze.

There are many tools that intend to help organizations detect cyber attacks, but most solutions analyze all data and activity. Because they have such a wide scope, security analysts end up frequently missing damaging attacks that are more difficult to detect, such as compromised privileged accounts and Kerberos attacks. And even worse, without expertise in a particular area, all-encompassing analysis tools end up producing many false alarms that result in security teams spinning their wheels.

Uncertainty on how to respond to incidents.

Even when security teams are able to detect and prioritize alerts, the alerts often lack the critical information required to respond to the incident. Alerts related to privileged accounts can be particularly challenging because the accounts are typically shared among multiple users – leading to challenges when pinpointing the source of an alert. So, even if anomalous privileged activity is detected, traditional monitoring solutions lack the critical information that is necessary to quickly respond to an incident, such as which individual user performed the anomalous activity.

Difficulty maintaining accurate monitoring.

The sheer volume of network and user activity presents challenges for security teams to continuously monitor them. And, traditional monitoring and detection tools often require a lot of maintenance. First, security teams need to understand and define what "normal" activities are, then they need to know how to define and detect "abnormal" activities. This includes a time-consuming process of tweaking reports, writing new rules, updating policies, etc. As a result, many solutions require a lot of time to constantly manage and update the solution over time.

The Solution

CyberArk Privileged Threat Analytics is a security intelligence solution that allows organizations to detect, alert, and respond to anomalous privileged activity indicating an in-progress attack. By focusing analytics only on privileged activity instead of analyzing everything on the IT network, CyberArk Privileged Threat Analytics is able to deliver targeted, prioritized alerts on the most critical malicious activity - where attackers are targeting.

The Solution collects a targeted set of data from multiple sources, including the CyberArk Digital Vault, SIEM, and network taps/switches. Then, the analytics engine applies a complex combination of statistical and deterministic algorithms, enabling organizations to detect indications of compromise early in the attack lifecycle by identifying malicious privileged account activity. This provides an opportunity for security teams to be able to stop an attack before it stops business. After identifying a potential attack, CyberArk Privileged Threat Analytics can automatically respond to contain the attack by invalidating a stolen credential to block an attacker from continuing.

CyberArk Privileged Threat Analytics:

Detects and alerts on critical attacks.

Focused on privileged account activity, CyberArk Privileged Threat Analytics employs built-in algorithms, written by experts in privileged account security, to analyze only the most critical activity in the IT network. The solution is designed to enable detection and alerts on indications of an attack such as lateral movement, privilege escalation, and credential theft.

- **Detects attacks abusing privileged accounts.** Malicious insiders and external attackers use privileged accounts to move laterally and escalate privileges, thus, not following normal behavior patterns for account usage. CyberArk Privileged Threat Analytics conducts Privileged User and Entity Behavior Analytics (UEBA) in order to build behavioral profiles of all privileged users, accounts and systems. The analytics engine then looks for deviations from the baseline to help detect and alert on anomalous activity such as login activity during an abnormal time of the day.
- **Detects attacks exploiting Kerberos authentication.** Attackers leverage vulnerabilities in the Kerberos authentication protocol to impersonate legitimate users and freely navigate the IT network. CyberArk Privileged Threat Analytics conducts Network Behavior Analytics to help detect in-progress Kerberos attacks such as Kerberos Golden Ticket, as well as lateral movement and privilege escalation activities that exploit Kerberos vulnerabilities. By detecting Kerberos attacks promptly, organizations can quickly respond to stop attackers' progress before irreparable damage occurs.

Delivers actionable intelligence in every alert.

CyberArk Privileged Threat Analytics alerts only on the most critical incidents – those that involve privileged accounts – enabling security teams to prioritize critical alerts. Each alert contains detailed, user-level intelligence including the malicious user, compromised machine, IP address, date and time of the event(s), etc., that enables security teams to quickly respond to threats.

Automatically responds to security incidents.

Detecting an incident is just the first step in the incident response lifecycle. Security teams must analyze alerts, contain threats, and then remediate and recover from the incident. CyberArk solutions deliver a built-in automatic response capability that can promptly contain detected threats by immediately invalidating a suspected stolen privileged credential. This enables organizations to quickly contain threats without requiring human intervention.

Benefits

CyberArk Privileged Threat Analytics enables organizations to:

- **Identify previously undetectable attacks.** Attackers often operate under the radar for months or even years before being detected. CyberArk Privileged Threat Analytics analyzes the right data in order to help detect and alert on the most critical attacks, such as compromised privileged credentials and Kerberos attacks.
- **Limit an attacker's window of opportunity.** By focusing on privileged account activity and critical attack vectors, CyberArk Privileged Threat Analytics is able to assist in the detection of cyber attacks earlier in the attack lifecycle than traditional detection tools. This enables security teams to respond immediately, even automatically, to stop an attacker from continuing the attack.
- **Improve the efficiency of security teams.** By focusing analytics on privileged accounts, CyberArk Privileged Threat Analytics helps incident response teams prioritize alerts that involve privileged credentials. Each alert contains detailed, actionable information enabling security teams to quickly respond by immediately invalidating the credential. And, alerts can be sent directly to a SIEM dashboard for single pane-of-view analysis.
- **Receive quick time to value.** For data collection, organizations can leverage existing network tap aggregators and end point connectors from SIEM solutions for essentially seamless integration with CyberArk Privileged Threat Analytics. The solution can quickly generate critical privileged account intelligence because algorithms are built-in to the analytic engine, meaning security teams do not have to spend excessive time configuring, tuning, or writing rules and parsers.

A Comprehensive Solution

CyberArk Privileged Threat Analytics is a component of the CyberArk Privileged Account Security Solution, a complete solution designed to proactively secure and manage privileged credentials, isolate and monitor privileged sessions, and detect and respond to anomalous privileged account activity. Products in the solution can be managed independently or combined for a complete Privileged Account Security Solution.

Specifications

Supported Browsers

Privileged Threat Analytics currently supports the following browsers:

- Chrome 26 and above
- Firefox 20 and above
- Internet Explorer 9.0

CyberArk Vault Integration

Privileged Threat Analytics integrates with the CyberArk Vault v7.1.6 and above

PTA Server

Supported Platforms

The solution is delivered as a virtual appliance that runs on the following platforms:

- VMware Player 4.0 and above
- VMware Workstation 8.0 and above
- VMware ESX/i 4.0 and above
- Microsoft Hyper-V v6.3

Minimum VM requirements

- 4-Core CPU
- 16GB RAM Memory
- 500GB hard disk storage

PTA Network Sensor

The PTA Network Sensor is a component that connects to the network, captures network traffic and runs deep packet inspection. A single PTA Server can be configured to receive data from multiple PTA Network Sensors.

Supported Platforms

The PTA Network Sensor runs on CentOS 7.x and can be installed on a physical or virtual machine.

Minimum Server / VM requirements

- 8-Core CPU
- 8GB RAM memory
- 200GB hard disk storage
- Management NIC
- Tapping NIC