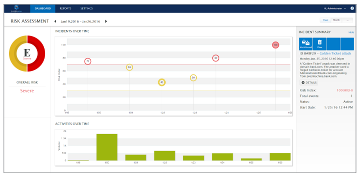
CYBERARK®

Privileged Threat Analytics™

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



ID 8A9F29 – Golden Ticket attack

Monday, Jan. 25, 2016 12:46:00pm

A "Golden Ticket" attack was detected in domain bank.com. The attacker used a forged Kerberos ticket for account Administrator@bank.com originating from prodmachine.bank.com.

Risk Index:	100(HIGH)
Total events:	1
Status:	Active
Start Date:	1/25/16 12:44 PM

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.

The Challenge

Cyber attackers constantly advance their techniques to operate within a network undetected. Once inside, attackers navigate the network as inconspicuously as possible, escalating privileges until they gain access to the target. Attackers use privileged credentials to impersonate authorized users and stay under the radar. As a result, organizations face a number of challenges monitoring user activity in order to detect and respond when and if an attacker is on the network.

Too much data to analyze

With big data, there's a lot to analyze. Whether relying solely on a SIEM solution or employing a broad analytics tool, organizations often try to analyze everything with just one solution. But, by casting such a wide scope, security analysts are overwhelmed with data, resulting in missed indicators of compromise. Without targeted data collection to identify the most critical attack methods, organizations struggle with a combination of too many alerts and false alarms.

Uncertainty on how to respond to incidents

Alerts related to privileged accounts can be particularly challenging because the accounts are typically shared among multiple users – making it difficult to pinpoint the source of an alert. Even if anomalous privileged activity is detected, traditional monitoring solutions lack the critical information necessary to quickly respond to an incident.

Difficulty maintaining accurate monitoring

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.

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.

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 and user activity. This provides an opportunity for security teams to stop an attack before it stops business.

After identifying a potential attack, CyberArk Privileged Threat Analytics can work with integrated CyberArk solutions to accelerate threat response. CyberArk Enterprise Password Vault can automatically receive alerts on potentially compromised accounts and immediately invalidate credentials to contain the attack. When an alert is generated on high-risk privileged user activity, security teams can watch the suspicious session in real-time via CyberArk Privileged Session Manager and optionally disconnect the session to block the attacker from continuing.

CyberArk Privileged Threat Analytics:

- Detects and alerts on critical attacks. Built-in algorithms, written by experts in privileged account security, 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, credential theft and suspicious command-line activity.
- Delivers actionable intelligence in every alert. 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 be able to quickly respond to threats.
- Automatically responds to security incidents. Detecting an incident is just the first step. Security teams must analyze alerts, contain threats, and then remediate and recover from incidents. CyberArk solutions deliver

an automatic response capability that invalidates suspected stolen credentials to immediately contain detected 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, malicious privileged user activity and Kerberos attacks.
- Limit an attacker's window of opportunity. By focusing on privileged account activity, privileged user activity, and critical attack vectors, CyberArk Privileged Threat Analytics is able to help organizations detect cyber attacks earlier in the attack lifecycle than traditional detection tools. This enables security teams to respond immediately, even automatically, to disrupt 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 accounts and credentials. Each alert contains detailed, actionable information enabling security teams to respond quickly. 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 SIEM endpoint connectors 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

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

Supported Browsers

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

PTA Server

Supported Platforms

- VMware Player 4.0 and above
- VMware Workstation 8.0 and above
- VMware ESX/ESXi 4.0 and above
- Hyper-V for Microsoft Windows Server 2012 R2

Minimum VM requirements

- 8-Core CPU
- 16GB RAM Memory
- 2TB 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
- 200 GB hard disk storage
- Management NIC, Tapping NIC

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice.