SOLUTION BRIEF

Threat Analytics Focused on Privileged Access Activity

CyberArk Privileged Threat Analytics™ and FireEye Helix

HIGHLIGHTS

Together, the integrated FireEye and CyberArk solution provides the capability to:

- Conduct targeted threat analytics on the most critical privileged attack vectors to detect quickly and respond rapidly to cyber attacks.
- Avoid a lengthy deployment process by leveraging existing infrastructure and data within the enterprise.
- Enable a security operations center (SOC) to prioritize alerts that involve privileged accounts and respond quickly to the most damaging threats.

Overview

The new battleground for information security is inside the network. Perimeter security, such as firewalls and anti-malware, remain a necessary and significant component of every security strategy. However, the perpetrators of advanced, targeted threats are aggressively breaking through the perimeter. Patient, cunning and armed with the resources to succeed, these threats eventually find their way inside your organization.

In an enterprise IT organization, countless security events occur daily. These include innumerable false positives, causing organizations to struggle to know how to respond appropriately to the real threat. The spotlight should be on privileged accounts where there is the highest risk for extensive damage and the greatest opportunity to stop in-progress attacks.

The challenge

Privileged accounts are typically shared accounts and are not tied to an individual user. These accounts prohibit traditional analytics solutions from attributing activity to a single user. According to analysis by FireEye Mandiant, advanced persistent threat attackers prefer to leverage privileged accounts where possible. Their specific targets are domain administrators, service accounts with domain privilege, local administrator accounts, and privileged user accounts. The challenge for IT security staffs is to use threat analytics to identify the source of the threats made to the various types of shared accounts.

The integrated solution

CyberArk has partnered with FireEye Helix to deliver targeted threat analytics on privileged account activity. By combining CyberArk Privileged Threat Analytics (which is a part of CyberArk Core Privileged Access Security) with FireEye Helix organizations can analyze a rich set of data to detect, alert and rapidly respond to cyber attacks.

Cyber attackers target privileged accounts to reach the heart of the enterprise and gain access to sensitive, valuable data. CyberArk, the trusted experts in privileged access security, has integrated their solution with FireEye Helix to help organizations detect and quickly respond to anomalous privileged account activities. CyberArk Privileged Threat Analytics conducts targeted analytics on the most critical data, enabling organizations to recognize indicators of an attack in real-time, prioritize alerts that require immediate attention, and quickly respond to stop an in-progress attack.

A bi-directional data integration enables the joint solution to correlate more data and provide critical threat intelligence with each detected incident. The integration also allows organizations to receive real-time threat alerts in the FireEye Helix dashboard for single-pane-of-view analysis of all unusual activity across the organization.

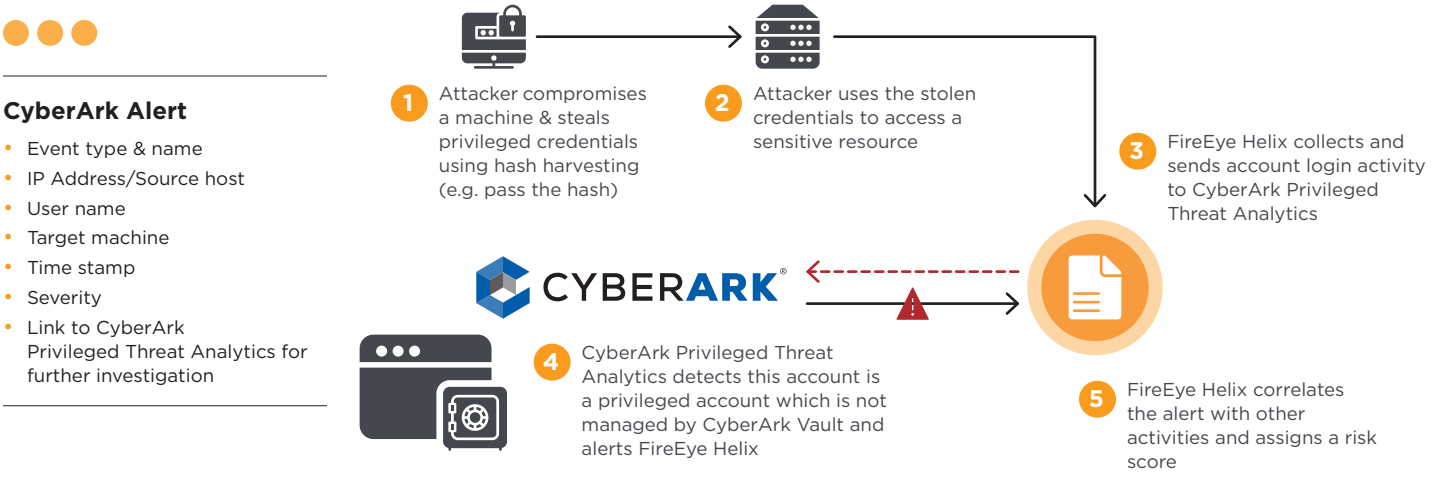

Figure 1. How CyberArk Privileged Threat Analytics™ and FireEye Helix work together.

How the joint solution works together

FireEye Helix collects data from across the enterprise, including privileged account login activity on endpoints. It forwards the collected information to CyberArk Privileged Threat Analytics. This data feed provides a rich set of data for analytics and new insights when correlated with CyberArk Digital Vault data. Privileged Threat Analytics conducts User Behavior Analysis (UBA) with custom, built-in algorithms.

When CyberArk Privileged Threat Analytics detects anomalous privileged access activities, such as a privileged user accessing a server during irregular hours, the solution generates an alert in real-time. FireEye Helix receives threat alerts as Syslog messages in Common Event Format (CEF). Alerts include detailed, critical intelligence that helps incident response (IR) teams provide context to detected incidents and enables quick prioritization of critical alerts. By sending alerts to the FireEye Helix dashboard, security teams can receive, triage and respond to alerts from a single dashboard.

The value of this partnership

Threat analytics is a critical component of a comprehensive security strategy. Since attackers are targeting privileged accounts, organizations need to detect, alert and quickly respond to anomalous privileged account activity. This joint solution enables organizations to leverage existing data and infrastructure to quickly and seamlessly add threat analytics to their overall security solution. These two solutions combined deliver industry-leading threat analytics on the most critical attack vectors — those involving privileged accounts.

About FireEye

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

About Cyberark

CyberArk (NASDAQ: CYBR) is the global leader in privileged access security, a critical layer of IT security to protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline. CyberArk delivers the industry's most complete solution to reduce risk created by privileged credentials and secrets. The company is trusted by the world's leading organizations, including more than 50 percent of the Fortune 100, to protect against external attackers and malicious insiders. A global company, CyberArk is headquartered in Petach Tikva, Israel, with U.S. headquarters located in Newton, Mass. The company also has offices throughout the Americas, EMEA, Asia Pacific and Japan. To learn more about CyberArk, visit www.cyberark.com, read the CyberArk blogs or follow on Twitter via @CyberArk, LinkedIn or Facebook.

For more information contact **CyberArkPartner@FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

© 2018 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. CB-EXT-SB-US-EN-000079-01

CYBERARK

FireEye