FireEye Threat Analytics Platform (TAP)and CyberArk Privileged Threat Analytics™ (PTA)

Deliver Targeted Threat Analytics on Privileged Account Activity

SOLUTION BRIEF

INTEGRATED SOLUTION 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 the Security Operation 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 Threat Analytics Platform (TAP) to deliver targeted threat analytics on privileged account activity. By combining CyberArk Privileged Threat Analytics with FireEye Threat Analytics Platform (TAP), 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 account security, has integrated their solution with FireEye Threat Analytics Platform (TAP) 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.

FIREEYE PRODUCT AND VERSION

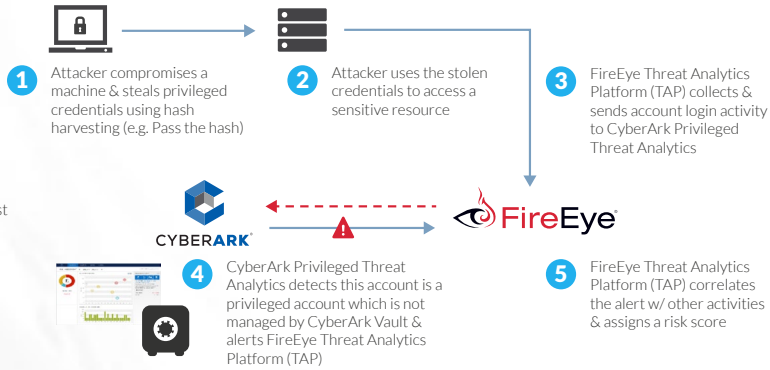
FireEye Threat Analytics Platform (TAP)

CYBERARK PRODUCT AND VERSION

CyberArk Privileged Threat Analytics™ (PTA)

CyberArk Alert

- Event type & name
- IP Address/Source host
- User name
- Target machine
- Time stamp
- Severity
- Link to CyberArk Privileged Threat Analytics for further investigation



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 Threat Analytics Platform (TAP) dashboard for single-pane-of-view analysis of all unusual activity across the organization.

HOW THE JOINT SOLUTION WORKS TOGETHER

FireEye Threat Analytics Platform (TAP) 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 account activities, such as a privileged user accessing a server during irregular hours, the solution generates an alert in real-time. FireEye Threat Analytics Platform (TAP) 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 Threat Analytics Platform (TAP) dashboard, security teams can receive, triage, and respond to alerts from a single-pane-of-view.

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 protects the most valuable assets in the world from today's cyber attackers. Our combination of technology, intelligence, and expertise — reinforced with an aggressive incident response team — helps eliminate the impact of breaches. FireEye has over 4,000 customers across 67 countries, including more than 650 of the Forbes Global 2000.

ABOUT CYBERARK

CyberArk is the only security company that proactively stops the most advanced cyber threats — those that exploit insider privileges to attack the heart of the enterprise. The company has pioneered a new category of targeted security solutions to protect against cyber threats before attacks can escalate and do irreparable business damage.

For more information contact CSC@fireeye.com.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**

FireEye