CyberArk Integrates Privileged Threat Analytics with McAfee's Next Generation SIEM

October 29, 2014 2:00 PM ET

Identification of Malicious Privileged Behavior Data to Speed Time to Attack Detection and Remediation

LAS VEGAS--(BUSINESS WIRE)--Oct. 29, 2014-- CyberArk (NASDAQ: CYBR), the company that protects organizations from cyber attacks that have made their way inside the network perimeter, today announced the integration of CyberArk Privileged Threat Analytics with McAfee Enterprise Security Manager (ESM). The integrated solution empowers customers to pinpoint and immediately act against privileged-based threats in their security information and event management (SIEM) data. The integration is being demonstrated at McAfee FOCUS 2014 in Las Vegas, where CyberArk, a gold sponsor, is located at booth #104.

Privileged accounts, which consist of IT administrative credentials, default and hardcoded passwords, application backdoors and more, are targeted in nearly every significant cyber attack. External attackers and malicious insiders exploit unprotected privileged accounts to move laterally and anonymously across the network, to access critical systems and exfiltrate data.

CyberArk Privileged Threat Analytics 2.0 collects and analyzes privileged account activity data to provide organizations with visibility into potentially malicious behavior. McAfee Enterprise Security Manager collects, correlates, and analyzes intelligence and event data in real time and orchestrates adaptive protection to disrupt the attack chain and prevent data loss. Leveraging the McAfee data exchange layer (DXL), CyberArk's full integration with McAfee Enterprise Security Manager will provide customers with more context to the information CyberArk Privileged Threat Analytics collects, while increasing the real-time visibility and the precision of actions that can be driven by the McAfee SIEM.

"Securing privileged accounts plays a critical role in protecting against advanced threats. Attackers exploit these powerful accounts to conduct network reconnaissance against security infrastructure and execute their attacks, often without detection," said Roy Adar, vice president, product management, CyberArk. "The integration of CyberArk Privileged Threat Analytics with McAfee Enterprise Security Manager will help incident responders cut through the clutter of big data security analytics to pinpoint and enable action on previously undetected malicious privileged behavior and disrupt in-progress attacks."

CyberArk Privileged Threat Analytics reports on malicious privileged behavior in real time over the McAfee DXL messaging bus, making it available to all McAfee products. McAfee Enterprise Security Manager reads the CyberArk Privileged Threat Analytics event data, and issues alerts, response and remediation activity in real time to threat response teams, and enables watch lists that can monitor and mine event data to detect related future and historical events.

Prompt action is part of how organizations shift from data historians to real-time incident management. For example, once a privileged user account is determined by CyberArk Privileged Threat Analytics to be associated with suspicious activity, McAfee Enterprise Security Manager can help disable, restrict, suspend, or reset the privileges of that user and the host. McAfee Enterprise Security Manager will also push security event information from critical systems to CyberArk Privileged Threat Analytics. This data will be analyzed and correlated with privileged account information to detect anomalous privileged behavior and user activities. The solutions will alert each other in real time about security events.

"Abuse of privileged credentials is a common thread between recent headline grabbing security breaches," said Ed Barry, vice president, Global Technology Alliances at McAfee, part of Intel Security. "Timing is everything when dealing with advanced threats and having visibility into behavior across the entire range of privileged account use greatly improves detection and remediation efforts. The integration with CyberArk's product offering will enable our customers' threat response teams to focus on privileged activity, detect suspicious events earlier in an attack chain, and have peace of mind that all endpoints and users are secure. We are excited to have CyberArk be one of the first Security Innovation Alliance

partners to participate in the DXL ecosystem."

The integration uses an innovative real-time messaging bus called the McAfee data exchange layer (DXL). Unlike point-to-point integrations that are expensive to implement and fragile, this new model provides more access to more information more quickly and reduces integration maintenance effort and dependencies. This data sharing and resilience enhances an organization's overall visibility and ability to adapt as threats change. By becoming "DXL-ready," CyberArk Privileged Threat Analytics will also be able to selectively publish its data to and subscribe to updates from other products from McAfee and Security Innovation Alliance partners, without the cost and overhead of direct integrations. Organizations gain flexibility and simplicity as part of a more resilient security infrastructure.

Key benefits of the CyberArk/McAfee integration include:

- Enables organizations to stop an in-progress attack before serious damage is done by focusing on privileged accounts, enabling a less costly and time-consuming remediation process.
- Detects a range of anomalies in the behavior patterns of individual privileged users in real time, such as a user who suddenly accesses credentials at an unusual time of day.
- Extends effectiveness of McAfee Enterprise Security Manager by enabling incident response teams to identify anomalous privileged account user behavior and prioritize incidents that involve privileged accounts.
- Builds learned user behavior into risk assessments over time to increase efficacy and build targeted analytics.

For more information, please visit http://www.cyberark.com/products/privileged-account-security-solution/privileged-threat-analytics.

To view a video introduction to CyberArk Privileged Threat Analytics, please visit: http://youtu.be/SCZYHMrLw6U.

About CyberArk

CyberArk (NASDAQ: CYBR) focuses on eliminating the most advanced cyber threats; those that use insider privileges to attack the heart of the enterprise. Dedicated to stopping attacks before they stop business, CyberArk proactively secures against cyber threats before attacks can escalate and do irreparable damage. The company is trusted by the world's leading companies – including more than 35 percent of the Fortune 100 and 17 of the world's top 20 banks – to protect their highest value information assets, infrastructure and applications. A global company, CyberArk is headquartered in Petach Tikvah, Israel, with U.S. headquarters located in Newton, MA. The company also has offices throughout EMEA and Asia-Pacific. To learn more about CyberArk, visit www.cyberark.com, read the company blog, http://www.cyberark.com/blog follow on Twitter @CyberArk or Facebook at https://www.facebook.com/CyberArk.

Forward-Looking Statements

This release may contain forward-looking statements, which express the current beliefs and expectations of our management. Such statements involve a number of known and unknown risks and uncertainties that could cause our future results, performance or achievements to differ significantly from the results, performance or achievements expressed or implied by such forward-looking statements. Important factors that could cause or contribute to such differences include risks relating to: changes in the new and rapidly evolving cyber threat landscape; our failure to effectively manage our growth; fluctuations in our quarterly results of operations; real or perceived shortcomings, defects or vulnerabilities in our solution or the failure of our solution to meet customers' needs; our inability to acquire new customers or sell additional products and services to existing customers; competition from IT security vendors and other factors discussed under the heading "Risk Factors" in the final prospectus for our initial public offering filed with the Securities and Exchange Commission on September 24, 2014. Forward-looking statements in this release are made pursuant to the safe harbor provisions contained in the Private Securities Litigation Reform Act of 1995. These forward-looking statements are made only as of the date hereof, and we undertake no obligation to update or revise the forward-looking statements, whether as a result of new information, future events or otherwise.

Source: CyberArk

Media Relations Contacts:
fama PR
Brian Merrill, +1 617-986-5005
cyberark@famapr.com
or
CyberArk
Christy Lynch, +1 617-796-3210
press@cyberark.com
or
Investor Relations Contact:
ICR
Staci Mortenson, +1 617-558-2132
IR@cyberark.com