CyberArk Advances Threat Analytics to Identify New Types of Malicious Privileged Behavior Across Systems and Users

September 9, 2014 11:52 AM ET

Targeted Data Analytics Provides Faster Time to Attack Detection over Big Data Approach

Newton, Mass. â€“ September 9, 2014 â€“ CyberArk, the company securing the heart of the enterprise, today announced CyberArk Privileged Threat Analytics 2.0, an expert system for privileged account security intelligence. The expanded analytics includes new self-learning, behavior-based algorithms, enabling customers to detect attacks faster by pinpointing malicious privileged account activity previously hidden in the sheer volume of information collected by big data analytics solutions.

Organizations face sophisticated and determined attackers seeking to infiltrate networks. Research shows that most companies believe cyber-attackers are currently on their network, or have been in the past year.[1] Once inside the perimeter, hijacked privileged credentials enable an attacker to hide in plain sight, which is why these accounts are the most sought after target in every advanced attack.[2] CyberArk Privileged Threat Analytics 2.0 collects and analyzes privileged account activity data, including pulling feeds from security information and event management (SIEM) systems to identify the most serious of risks.

“Privileged account security needs to be at the top of the agenda for organizations to defend against the rise in advanced attacks,” said Pete Lindstrom, research director, IDC. “With the ability to understand and react to real-time activity that solutions like CyberArk Privileged Threat Analytics deliver, organizations have an opportunity to identify these high-risk incursions and address them before they lead to weeks or months of leaks and losses.”

â€œWhile big data threat analytics provide a wealth of information, knowing which data-set is important requires specialized skills most organizations donâ€™t have,â€said Roy Adar, vice president, product management, CyberArk. â€œCyberArk Privileged Threat Analytics 2.0 cuts through the clutter to quickly identify in-progress attacks and enables organizations to shut down the most dominant avenue for moving laterally within a companyâ€™s infrastructure.â€

Out-of-the-box integration of data feeds from leading SIEM solutions such as HP ArcSight ESM and Splunk Enterprise provides context to the information CyberArk Privileged Threat Analytics collects. This enables customers to pinpoint privileged-based threats amongst the wealth of data their SIEM collects. For example, if an administrator tries to access a server, firewall or other endpoint directly without going through the policy-mandated workflow, CyberArk Privileged Threat Analytics can identify and alert on this, where the SIEM would not catch this as a threat.

New forensics capabilities deliver more visibility and insight into privileged account behaviors. With the ability to view user profiles and system access, organizations can now query on anomalies, view baseline behavior models, and benchmark for risk levels across the entire privileged account ecosystem within their organization. Users can drill down into individual privileged account anomalies and behavior profiles specifically, delivering immediately actionable intelligence that allows incident response teams to immediately respond to an in-progress attack.

Key benefits include:

- Enables organizations to stop an in-progress attack, ensuring a less costly and time-consuming remediation process by identifying unusual privileged account access.
- Cuts through the clutter created through traditional big data analytics, increasing an organizationâ€™s ability to identify malicious activity related to privileged accounts.
- Detects anomalies in the behavior patterns of individual privileged users and systems in real-time, such as a user who suddenly accesses credentials at an unusual time of day or from an unusual location, demonstrates excessive usage, and other abnormal trends.

- Builds learned system and user behavior into risk assessments over time to increase efficiency and build targeted analytics.
- Speeds deployment through out-of-the-box data feed integrations with HP ArcSight ESM and Splunk Enterprise.
- Provides full behavioral analytics function as a standalone product or as part of the Privileged Account Security Solution.

For more information, please visit http://www.cyberark.com/product-detail/privileged-threat-analytics.

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

About CyberArk

CyberArk is the only security company focused 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 worldâ€™s leading companies â€“ including more than 35 percent of the Fortune 100 and 17 of the worldâ€™s top 20 banks â€“ 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.