Flyer
Security

Speeding Up Discovery Time of Hidden Threats

Multi-vector, insider, evasive, and sophisticated unknown threats work hard to keep hidden from security controls and detection.

On average it takes an organization 191 days to identify a data breach and another 66 days to contain that breach.[1] Breaches from insider threats can take years to detect.[2] And with their elusiveness, sometimes the actual cost and damage they cause never gets fully determined.[3]

But it's not just the sophistication of these threats and their evasive ability that slows down detection. A big challenge with advanced threat detection is the massive amount of data that needs to be analyzed and its incoming speed. To keep up and find your way through all that data noise, you need automated analytics operating at machine speeds to help you identify suspicious events and find possible indicators of compromise.

Another problem that delays detection of adversaries within your environment is over reliance on rule-based tools that only send alerts when specific actions occur or thresholds are reached. While these help with efficiency and rapid responses, they only spotlight narrow areas of concern rather than illuminating anomalous behaviors occurring outside of normal baselined system activity. To get a holistic view of activity within your environment you need to be able to make connections between individual activities that on their own seem normal, but when examined collectively expose suspicious behavior. You can overcome these challenges and significantly speed up discovery and remediation of hidden threats by combining the complementary capabilities of user behavior analytics tools with those of hunt investigative analytic tools.

User Behavior Analytics

User behavior analytics uses big data and machine learning algorithms to create baselines on how users, devices, systems, and networks normally behave and then it detects anomalies in their behaviors to help security teams become aware of suspicious activity for further investigation. One of the key differentiators that Micro Focus® User Behavior Analytics (UBA) delivers over other solutions in this category is that you don't have to be a data scientist to take advantage of its full power.

Micro Focus UBA helps you detect hidden threats without having to build your own algorithms, risk profiles, and other detection capabilities. It automates all that for you to deliver immediate insight into security risks and enhanced visibility into suspicious activities and behavior associated with attacks. It builds comprehensive risk profiles of your users based on their activity, access levels, responsibilities, tech smarts, and other behavior-related characteristics. It compares those user risk profiles against peers, as well as known threat indicators, to present you with interactive risk scores that can help you identify true risk areas.

UBA also employs real-time data mining, automated data correlation and enrichment, identity correlation, insider threat investigation, and advanced analytics to help you see connections between individual user actions that on their own appear harmless, but collectively infer real threats.

Hunt and Investigation Analytics

In addition to the advanced detection provided by UBA, it's important to also have hunt/investigative tools as part of your security design. Search and analytic capabilities in these tools allow security analysts to proactively sift through large amounts of data to detect unknown threats. But with millions of potential incidents and threats to explore, many hunt tools simply don't scale. Micro Focus Investigate delivers the high speed and big data scalability needed to find hidden threats easier and faster. Investigate takes advantage of Vertica, the high-performance big data analytics platform that delivers unprecedented analytical power. It enables you to execute searches for suspicious activity10 times faster than other investigation tools and processes large volumes of data almost instantly from all your different sources, including SIEMs, user behavior analytics, business intelligence, and other hunt tools.

The intuitive search interface in Investigate simplifies creation of complex search queries, empowering security analysts of all levels to perform more sophisticated and effective searches. That reduces the need for training and frees up more time to hunt bad actors. Its ability to investigate at scale gives security analysts greater flexibility and reach to explore

1 *Ponemon Institute, "2017 Cost of Data Breach Study." June 2017.*
2 *Verizon, "2017 Data Breach Investigations Report."*
3 *SANS Institute, "Defending Against the Wrong Enemy: 2017 SANS Insider Threat Survey." August 2017.*

Contact us at:
www.microfocus.com

data without limiting time spans or size of search results. Investigate's visual analysis of potential threat indicators makes it easy to detect threats that elude machine correlation and other analytical tools. Its analytics-driven, guided investigation enables analysts to do more with less, accelerating both threat detection and incident investigation.

Elevate Your Threat Discovery Aptitude

Combine the automated intelligence of user behavior analytics with the flexibility and reach of investigative analytics to increase analyst productivity, gain better threat visibility, improve situational awareness, make better, more accurate decisions, and minimize breach costs and damage by considerably speeding up the discovery of hidden and unknown threats in your environment.

To learn more about how Micro Focus User Behavior Analytics and Micro Focus Investigate can elevate your threat discovery efforts, register for an ArcSight workshop today.

Learn More At
microfocus.com/arcsight