opentext™ | Cybersecurity

Flyer

Incubate an Insider Threat Program Leveraging the ArcSight Intelligence Fast Start Program

ArcSight Intelligence empowers security teams to detect and investigate behavior-based anomalies to uncover insider threats. The Fast Start Program helps deliver powerful insider threat detection quickly through fixed log sources, while offering the flexibility to scale for richer results.

Today's Market Reality

Many organizations have important assets to protect, whether it's customer information, intellectual property, critical infrastructure, or all of the above. Attempts to protect these assets frequently fall short due to fragmented security ecosystems and new attack vectors. Security teams also have to contend with rigid rules-based correlation and a never-ending barrage of alerts—most of which end up being false alarms. Meanwhile, these teams are expected to flawlessly protect against critical threats like insider threats and advanced attacks which may not have a precedence. Most businesses today are interested in initiating an Insider Threat Detection Program on-premise or in the cloud to anticipate and address threats originating from risky behavior before damage is done.

Succeed with ArcSight Intelligence

Enterprises with valuable data to protect, significant surface area to monitor, and limited security controls or financial resources can benefit from ArcSight Intelligence by OpenText™'s unique ability to find the threats that matter. ArcSight Intelligence behavioral analytics bypasses rules and thresholds, and instead assesses the potential risk of a user or entity in an enterprise using unsupervised machine learning models. These advanced mathematical algorithms constantly incorporate billions of data points from logs to discern information on available entities (users, machines, IP addresses, servers, printers, etc.) in order to create and analyze their 'unique normal behavior'. Understanding this 'unique normal behavior' enables ArcSight Intelligence to reveal hard-to-find threats like insider threats, data breaches, advanced persistent threats (APT), IP theft, fraud, and more. This approach, combined with ArcSight Intelligence's native big data architecture, allows security teams to detect threats with speed and at scale.

Prioritized use cases within the Fast Start Program

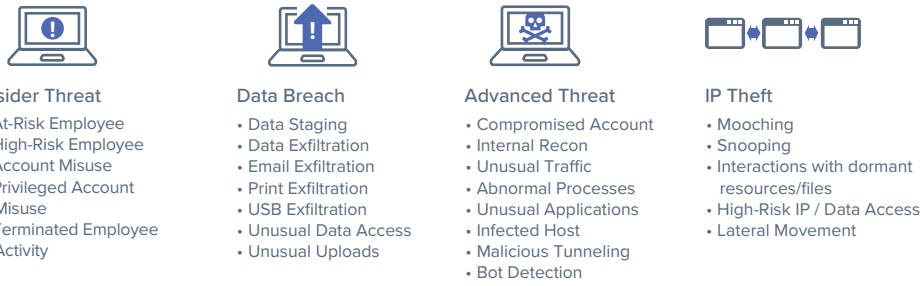

Figure 1. Existing use cases which are leveraged in the ArcSight Intelligence Fast Start Program

Adopt ArcSight Intelligence Quickly and Simply

The ArcSight Intelligence Fast Start Program takes away the complexity of a long drawn UEBA Threat Detection Program by focusing on fixed data sources, defining the resource requirements, and anticipating potential use cases for quicker and effective behavioral analytics results. In many cases, it's hard for companies to identify specific threat conditions at the early stages of an evaluation because it can be too complex and time consuming. Using historical logs from the Domain Controller and Web Proxy, companies can quickly and effectively evaluate ArcSight Intelligence's capabilities and functionalities within four to six weeks. Given a high probability of identifying anomalies, enterprises can now detect hard-to-find threats such as stolen credentials, data exfiltration, lateral movement or account compromise.

Insights with ArcSight

Security Intelligence is at the heart of any next-generation Security Operations Center as it empowers organizations to truly stay ahead of everchanging threats. The combination of ArcSight's powerful correlation with ArcSight Intelligence's

Connect with Us
www.opentext.com

unsupervised machine learning models allows SOCs to detect threats like insider threats and advanced attacks for a more effective layered-security approach. This supercharged combo also helps reduce false positives, deliver more accurate threat detection, and improve SOC efficiency. Enterprises are then enabled to have more effective threat hunting, while implementing resolution and remediation actions through partnering SOAR technologies with ease.

Request a Demo of ArcSight Intelligence Today

www.microfocus.com/products/arcsight-intelligence

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

761-000045-003 | O | 10/23 | © 2023 Open Text