ArcSight for People Centric Attack Mitigation

ArcSight strengthens your cyber resilience by providing your SOC with prioritized context of all the riskiest and most targeted users in your organization. With a holistic SecOps solution, your team can efficiently detect and triage people-centric threats and vulnerable accounts.

ArcSight People Centric Attack Mitigation at a Glance
What sets ArcSight apart from other solutions?

Layered Analytics

ArcSight provides comprehensive, contextual user insights by combining real-time correlation, threat intelligence, behavioral analysis, anomaly detection, advanced threat hunting and MITRE ATT&CK content.

Risk Scores

ArcSight uses mathematical models to identify the riskiest users in your organization to effectively prioritize threats, accelerating your triaging efforts.

Constant Behavioral Baselining

Unsupervised ML establishes unique normal baselines of behavior for all users and continuously learns to identify the riskiest and most vulnerable people.

Elusive User Centric Threats

People centric attacks, whether negligent or malicious, can be extremely harmful and difficult to detect in any organization as every user's behavioral patterns are unique, heavily contextually based, and rarely follow traditional patterns. With these elusive threat indicators, it is critical for your security operations center (SOC) to understand the priority and extent of people centric attacks to effectively mitigate them. However, your team is likely challenged with a lack of contextual insights, large volumes of raw event data, and overwhelming false positives, distracting your team from the threats that matter most. In addition to this, a lack of visibility and control over your privileged accounts and users' access means that you will have higher vulnerability entry points for attackers. These entry point weaknesses are difficult for analysts to find and mitigate as privileged accounts are permitted in your organizational landscape. How do you appropriately safeguard your enterprise from people centric threats? You need an efficient, insightful, and accurate SecOps tool focused on behaviors.

ArcSight for People Centric Attack Mitigation

To combat people centric attacks in your organization, ArcSight enables your SOC to identify the riskiest users in your enterprise through real-time correlation and unsupervised machine learning. Distilling billions of events into a prioritized list of high-quality security leads through advanced behavioral analytics, your SOC can focus on elusive, people-centric attacks, before the damage is done. ArcSight's intuitive and unified interface

“ArcSight has added very advanced Analytics [ArcSight Intelligence] to their very strong correlation engine to provide visibility on Insider RISK & Insider Threats which is very unique to every organization.”

GARTNER PEER INSIGHT REVIEW, 2020

Contact us at **CyberRes.com**
Like what you read? Share it.

helps provide faster response time with a holistic security view through a single pane of glass. With ArcSight, your security team can focus on narrowing threats down to the right individual or group to strengthen your cyber resilience and mitigate people centric attacks.

Why ArcSight?

ArcSight is a holistic SecOps solution that enables your resilient SOC. With ArcSight, your organization can intelligently adapt your security to identify and prioritize risky or vulnerable users who are most effected or targeted by people centric attackers. By monitoring user behaviors through layered analytics, your team can effectively and accurately mitigate breaches and losses incurred by people centric attacks.

Features and Benefits

Unknown Threat Detection: People centric threats are extremely elusive and rarely follow traditional patterns. ArcSight combines supervised and unsupervised machine learning for holistic analysis of risky users to accurately and quickly uncover unknown threats.

Contextual User Insights: To detect people centric threats, your security team needs to accurately monitor actions of your users and identify which behaviors and individuals pose the greatest risk. ArcSight’s advanced behavioral analytics capability provides your team with much needed context of users’ risky behaviors to accelerate your SOC’s efforts in finding people centric attacks.

Centralized UI: When your team is using fragmented tools, they have a limited view of your security landscape, inhibiting their ability to detect elusive threats. ArcSight centralizes its user interface to enable your SOC with a single pane of glass. This holistic view gives your team the visibility to detect hard-to-find user centric threats across multiple areas in your organization.

Risk Scores: Closely monitoring individuals in your organization can overwhelm your analysts easily as there tends to be a barrage of alerts, long lists of potential leads, and many false positives. ArcSight provides your SOC team with unique risk scores for every user and entity in your enterprise to enable your analysts with the right user context while mitigating false positives.

Prioritized Threat Leads: Your analysts are likely wasting their valuable time sifting through hundreds of alerts and potential threat leads, delaying your response times. ArcSight provides your SOC with a prioritized list of threat leads based off of individual risk scores to focus analyst efforts on the people centric threats that matter most.

Security Orchestration and Automated Response: ArcSight’s native SOAR capability aids your analysts by automating repetitive tasks and initiating swift threat response. With SOAR, your team can more efficiently spend their time on critical user centric threats and automate response to stop and remediate them.

400+ Models: Unlike many behavioral analytics solutions, ArcSight leverages over 400 mathematical models to accurately identify risky behaviors hidden in your organization. With this behavioral intelligence, your team can effectively and accurately determine people centric threats.

Continuous Learning: ArcSight leverages continuous unsupervised machine learning for up-to-date behavioral insights to uncover true people centric threats, faster. With continuous learning, your analysts can prioritize true leads and focus their time on detecting critical user threats.

Unified Threat Intelligence: Your organization is likely faced with mountains of data which your analysts need to sift through to uncover threats, wasting precious time. ArcSight unifies threat intelligence to enable your SOC with a better understanding of current threats and improve coverage of risky users and accounts.

Learn more at
www.microfocus.com/en-us/cyberres/secops/arcsight-intelligence

CyberRes
A Micro Focus line of business