ArcSight for Preemptive Threat Detection

Your security team is challenged with detecting and responding to elusive threats before the damage is done. With ArcSight's automated, proactive, and holistic SecOps solution, you can swiftly uncover known and unknown threats for effective preemptive threat detection.

Preemptive Threat Detection at a Glance
What sets ArcSight apart from other solutions?

Layered Analytics

ArcSight combines intelligence from real-time correlation, behavioral analysis, anomaly detection, threat hunting and MITRE ATT&CK to focus on the right threats before damage is done.

Combined Machine Learning

By bringing together multiple ML methods, ArcSight automates unique behavioral monitoring and response with risk scores, minimizing alert fatigue and false positives.

Unified Intelligence

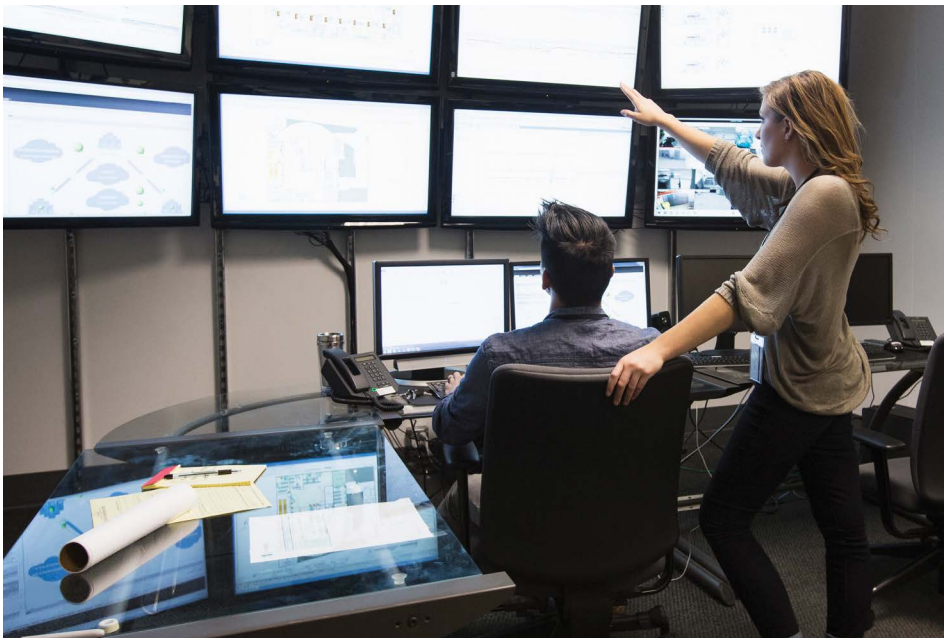
ArcSight unifies threat intelligence on a shared interface and storage platform for scalable and comprehensive coverage of known and unknown threats.

The Timing Challenge

Today, too many security teams are faced with overwhelming alerts, and many of which end up being false positives. These time-consuming, false leads make it difficult for your analysts to effectively detect, triage, and respond to real threats within your enterprise in time. When your analysts are overwhelmed and unable to spend their valuable time on real threats, you'll likely be left with a longer window of vulnerability for attacks and high-cost data breaches. On top of this, many current tools employed by SOCs are ineffective at detecting and responding to both known and unknown threats in a growing threat landscape. You need to focus your SOC on collecting and deriving valuable insights from mass amounts of threat intelligence to find threats like insiders and zero-days before it's too late.

Preemptive Threat Detection

ArcSight's automated, proactive and holistic security operations solution enables your SOC with layered analytics and contextual threat insights. With this, you can accelerate and focus the efforts of your overburdened analysts on the threats that matter within your entire threat landscape. This unified SecOps solution empowers your team to accurately prioritize threats and swiftly act before damage is done.



“Very Sophisticated Correlation Engine, which enables us for advanced threat readiness.

GARTNER PEER INSIGHT REVIEW, 2020

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

Why ArcSight?

ArcSight’s unique layered analytics approach helps SOCs efficiently detect and respond to known and unknown threats before damage is done by seamlessly combining contextual threat intelligence derived from real-time correlation, behavioral analytics, and advanced threat hunting. Its intelligent combination of machine learning helps to minimize alert fatigue and false positives by identifying and prioritizing suspiciously anomalous users and entities that may indicate an insider threat or advanced attack. These analytical methods with native SOAR capabilities work together to proactively protect critical data by accelerating the efforts of your analysts. With a greater ability to focus valuable time on the threats that matter, you can ensure comprehensive coverage of your growing threat landscape while streamlining processes to speed up actions.

Features and Benefits

Combined Machine Learning: Your SOC is likely overwhelmed with alerts and false positives, wasting your analysts’ valuable time and delaying response. ArcSight combines supervised machine learning from ArcSight Recon and unsupervised machine learning from ArcSight Intelligence to optimize your SOC’s leads to focus analysts’ efforts on the threats that matter most.

Security Orchestration and Automated Response: Acting quickly when faced with a potential threat is critical for SOCs to safeguard the enterprise. ArcSight’s native SOAR capability enables your analysts to act with speed by automating repetitive tasks and initiating threat response.

Centralized User Interface: With fragmented security tools running independently, your analysts are unable to gain a holistic view of your entire threat landscape, hindering swift threat detection and response. ArcSight’s centralized user interface reduces “swivel-chair syndrome” and wasted time so your analysts’ can accurately find and react to threats with speed.

Unique Behavioral Baselines: Unknown threats are extremely difficult to combat and even harder to preemptively detect. ArcSight identifies unique baselines for all users and entities within your enterprise to uncover unusual and suspicious behaviors. With accurate behavioral monitoring, you can detect hard-to-find, unknown threats such as insider, zero-days, and APTs with additional threat context to reduce false positives and speed up detection time.

Custom Risk Scores: Your analysts are likely wasting much of their time chasing down false leads based on lack of context. ArcSight’s behavioral analytics capability creates custom risk scores on your organization’s users’ and entities’ activities. With these contextual risk scores that identify suspicious users and entities, your analysts will have a prioritized list of threat leads to accelerate SOC efforts and minimize alert fatigue

Continuous Unsupervised ML: ArcSight leverages continuous unsupervised machine learning to contextualize the threats in your enterprise to reduce false positives. With unsupervised ML, your analysts can prioritize leads and focus their time on detecting critical threats before the damage is done.

Unified Platform: The security tools employed in your SOC need to be able to effectively detect both known and unknown threats to stop bad actors in their tracks. ArcSight provides end-to-end security operations coverage delivered on a single platform to quickly and accurately find documented and elusive threats before it’s too late.

Holistic 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 amalgamates threat intelligence with unified data storage and analysis through ArcSight Recon to provide faster threat insights, boosting your SOC’s detection and response times.

Identification of Known and Unknown Threats: Accurately detecting both known and unknown threats is key to stopping attacks before they take place. ArcSight helps you protect your organization from community-known threats with real-time correlation and the unknowns with advanced behavioral analytics.

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

CyberRes
A Micro Focus line of business