

ArcSight for Exposure Time Reduction

The ArcSight product line elevates your organization's cyber resilience by reducing total exposure time with faster and more effective threat detection and response, backed by machine learning, automation, and multi-layered security analytics from a unified platform.

The ArcSight Product Line

Exposure Time Reduction at a Glance

What sets ArcSight products apart from other solutions?

Multiple Security Analytics Tools

The ArcSight product line's end-to-end platform delivers real-time correlation, threat intelligence, behavioral analysis, and advanced threat hunting to quickly detect both known and unknown threats.

Layered Analytics

ArcSight products combine contextual insights from each layer of analysis onto a single UI, to help you better understand the overall risk of events and increase alert accuracy.

Automation

Establish an efficient human-machine team. Machine-driven analysis and automation will identify and begin responding to possible threats, reducing exposure time by speeding up response.

Exposure and Risk

One of the most critical roles of your security operations team is its responsibility to limit business risk by reducing your organization's exposure to breaches and other security threats. For many security teams, this can be a trying task. SOCs like yours are going up against a wide variety of cyber threats, including more common threats following established attack patterns, as well as newer threats that continue to evolve.

Insider threats, APTs, and other elusive threats consistently challenge the detection capabilities of SOCs globally, and the longer a threat goes undetected, the more damage it can do to your business' critical assets.

Siloed security analysis tools do their best to catch these threats but end up overwhelming your analysts with a flood of alerts, false positives, and disjointed interfaces. This slows investigation and response, giving threat actors even more time to harm your organization. In the end, SecOps teams are left with a dire need to reduce their exposure through faster, more accurate threat detection and response.

Reducing Exposure Time with ArcSight Products

The ArcSight product line by OpenText's end-to-end security operations platform helps you get your risk of exposure under control



by enabling your security team to detect and respond to threats with both speed and accuracy. The ArcSight product line employs a layered analytics approach that allows you to collect and normalize all the security event data in your organization as it occurs, then analyze it with multiple threat analytics tools. Detect threats following established attack patterns (known threats) in real time with the ArcSight product line's first-class correlation engine. Keep your analysts alerted to unusual behavior, potential insider threats, and APTs, with behavioral analytics driven by unsupervised machine learning. Proactively hunt for more elusive threats with an innovative Big Data analytics solution that is optimized for security operations and backed by powerful visualizations and anomaly detection. Together, these tools provide comprehensive threat detection of both known and unknown threats. And even more so when paired with powerful threat intelligence platforms like MISP and Anomali.

But why stop there? ArcSight products then centralize the insights from each of its analytics components through a layered analytics interface, providing your security team with a single pane of glass to contextually visualize, identify, and analyze the most severe threats facing your organization. This greater context increases your alert accuracy and drastically reduces the alert fatigue facing your analysts. The ArcSight product line's native ArcSight SOAR by OpenText capabilities then further reduce your exposure time by facilitating rapid, automated threat response.

Reduce your exposure time with fast, accurate threat detection and response from a unified SecOps platform. Empower your SOC with the ArcSight product line's enterprise-wide security event visibility, comprehensive threat detection, layered analytics, and automated response.

Why ArcSight Products?

The ArcSight product line is a holistic SecOps solution that enables greater cyber resilience by helping you intelligently adapt

your resources to reduce your overall threat exposure. With the ArcSight product line's advanced technologies you can reduce both your detection and response times, even in the face of overwhelming incident volume, strangling bottlenecks, and taxing incident fatigue. The ArcSight unified product line enables you to sharpen your resource focus on what truly matters with faster, more accurate threat detection of both known and unknown threats through layered analytics, and with accelerated response through native ArcSight SOAR capabilities.

Features and Benefits

Real-time Threat Detection: The ArcSight product line's industry leading correlation engine ingests and correlates events in real time, enabling you with almost immediate detection and escalation of known threats.

Behavioral Analytics: Unknown threats can be extremely difficult to detect and combat. ArcSight products identify unique baselines for all users and entities within your enterprise to uncover unusual and suspicious behaviors. With accurate behavioral monitoring, you can detect elusive threats such as insider threats and APTs, with additional threat context to speed up detection time.

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

Big Data Threat Hunting: ArcSight products incorporate Big Data analytics optimized for security operations and simplified for everyday use. Backed by powerful visualizations, it enables analysts to investigate and proactively hunt for threats within mountains of data, without requiring a database administrator to operate.

Integration with Threat Intelligence:

Integration with threat intelligence feeds, such as those provided by MISP and Anomali, help keep the ArcSight product line up-to-date so that it can detect the latest attacks in today's evolving threat landscape (including zero-day attacks).

Centralized User Interface: The ArcSight product line's various components share a centralized interface to enable your SOC with a single pane of glass that reduces "swivel-chair syndrome" and saves your analysts' time.

Contextual Threat Insights: By merging the insights from multiple analysis tools onto a single UI, the ArcSight product line's layered analytics can collectively analyze results and provide your team with greater context behind each threat alert and risky user. This increases the accuracy of your SOC in separating true threats from false positives, allowing your team to quickly prioritize and address the riskiest threats.

Security Orchestration and Automated Response: The ArcSight product line's native ArcSight SOAR capabilities aid your analysts by automating repetitive tasks and initiating swift threat response. With ArcSight SOAR, you'll reduce the workload of your analysts, saving them time and enabling them to focus on more critical exposure reduction activities.

Unified Platform: Siloed security solutions waste time and add complexity to your SOC, requiring your analysts to manage multiple data stores, and to move between various tools and interfaces. ArcSight products simplify SecOps by uniting an end-to-end solution on a single platform, complete with a unified data platform, common storage, layered analytics, and a shared intuitive interface.

Prioritized Threat Leads: Your analysts waste a lot of time sifting through hundreds of alerts and potential threat leads, which delays your response time. ArcSight products provide

“With [the ArcSight product line], we don’t just detect real attacks quickly, but we also automate orchestrated responses in near-real time. The flexibility of [ArcSight products] helps us intelligently adapt for the future.”

Dmitriy Ryzhkov
Senior Information Security Analyst
NPC Ukrenergo

Connect with Us
www.opentext.com



your SOC with a prioritized list of threat leads based off of individual risk scores and

contextual insights, to accelerate SOC efforts and focus analysts on the riskiest threats.

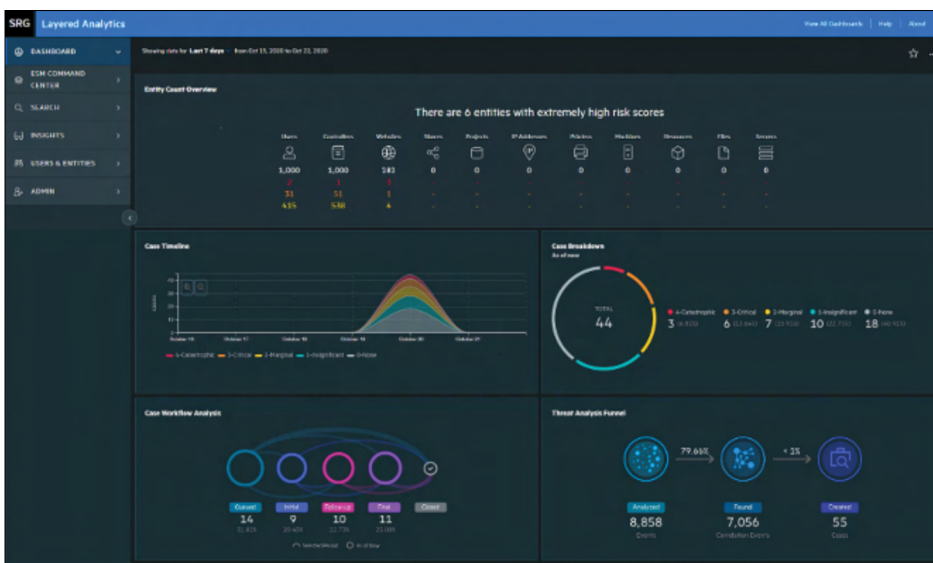


Figure 1. The ArcSight product line centralizes the insights from each of its analytics components through a layered analytics interface, providing your security team with a single pane of glass to contextually visualize, identify, and analyze the most severe threats facing your organization.

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.