Can One Needle Penetrate Your Company’s Defenses?

As IT environments evolve to become more complex, it becomes difficult for a small security team to determine if an event was triggered by normal system behavior or part of a coordinated attack. That is unless you have a threat detection solution in place that can intelligently sort events. Micro Focus has developed a threat detection solution that takes your machine log data and applies heuristic analysis to identify patterns of normal and abnormal behavior. The result: a new level of monitoring that extends Security Information and Event Management (SIEM) so that patterns can be easily traced and monitored.

Discover Repeating Event Patterns

Micro Focus’ ArcSight ThreatDetector automatically identifies patterns of both suspicious and seemingly unsuspicious events, instantly uncovering zero-day worms, low and slow attacks, and root-kit attacks. In addition to identifying malicious event patterns, ArcSight ThreatDetector also helps you find misconfigurations of network devices, systems, and applications.
This optional package for the ArcSight SIEM solution is built on patented technology that leverages ArcSight SIEM capabilities for a comprehensive data capture, normalization, and categorization producing accurate and detailed pattern analysis.

When ArcSight ThreatDetector identifies repeating event patterns it captures event detail information that can help analysts separate benign patterns from malicious ones.

The platform automatically creates new rules in ArcSight SIEM to identify these threats in the future. By feeding this intelligence back into ArcSight SIEM, you immediately add a new layer of relevance to your security monitoring program.

ArcSight ThreatDetector automatically spots low and slow brute force attacks which may otherwise avoid detection if they fail to trigger predefined thresholds—such as consecutive failed login attempts. It also identifies repeated attacks even if the attack event behavior is out of sequence, as seen in more sophisticated scripted attacks (such as root-kits attacks).

**Heuristic Analysis and Threat Detection**

ArcSight ThreatDetector uses heuristic analysis to identify benign and malicious repeating event patterns and creates rules for future real-time detection of zero-day, and low and slow attacks.

**Key Benefits**

With ArcSight ThreatDetector, your team gets the advantage of consummate knowledge and greater responsiveness to zero-day and automated attacks.

The powerful ArcSight ThreatDetector pattern identification engine looks for event patterns across any source data in the ArcSight SIEM platform and is capable of discovering repeating patterns across various parameters such as pairs of source and destination IP addresses, event behavior, and event outcomes.

Without this analysis, the incremental behavior of derivative worms would otherwise be invisible. This is because IDSs only discover worms as defined by the signature. ArcSight ThreatDetector helps you avoid damaging consequences by identifying all events related to new worm variants, even if it has changed slightly to thwart detection.

**Key Features**

**Early Threat Detection**

There are hidden event patterns that can be found within millions of raw security events and alerts generated by devices within your IT environment. ArcSight Enterprise Security Manager (ESM) provides a broad classification of security data, thereby creating comprehensive pattern identification for these alerts. For example, ArcSight ThreatDetector can identify a new worm variant as a set of repeating, related events. Captured event detail can show events following or preceding a known worm intrusion detection system (IDS) signature. The benefit of using our sophisticated correlation technique for threat detection is that it reduces false positives so that the security team can focus on incidents that are critical.

**Sophisticated Pattern Recognition Techniques**

ArcSight ThreatDetector correlates events via our patented threat intelligence technology to find relationships that are not apparent to the human eye. By applying machine learning, it can discover subtle relationships and risks across your environment.

**Profiles Good and Abnormal Behavior**

Another unique strength is the ability to profile activity and discover patterns in large collections of events that have already occurred. Our activity-profiling engine can churn through events to find relationships that aren’t readily apparent to the human eye. This machine learning can discover subtle relationships and risks across many variables. It can profile good
and bad behavior so that if a user starts engaging in activities that are out of profile or risky, you can take action early.

**Threat Detection in User Behavior Patterns**

ArcSight ThreatDetector can be used to uncover modern cyber crime. Our system detects sophisticated threats including zero-day outbreaks and fraud by correlating the “Who”, “What”, “Where”, and “Why” an activity is happening. It includes correlating user roles and trends to determine who is violating policies and putting the business at risk.

**Takes Action**

ArcSight ThreatDetector can proactively alert and notify you when suspicious or malicious activity has occurred in your environment. Alerts and notifications can be sent via email to escalate issues to the security team so that a proper response can be deployed in a short timeframe.

**Integration with ArcSight ESM Automated Response**

Once patterns are known, and analysts determine if the pattern represents innocuous traffic on a malicious attack, ArcSight ThreatDetector seamlessly integrates with the ArcSight SIEM solution robust correlation engine, enabling one-click rule building that automatically recognizes and responds to recurring patterns. The response can range from a notification, a new case opening, or even an automated or guided response for using ArcSight Threat Response Manager. What does this mean for you? A shortened window of vulnerability and a better defense for your network.

**Expanding Library of Risks**

ArcSight ThreatDetector works by continually building a library of known suspicious event patterns that are unique to your network thereby allowing you to increasingly automate threat intelligence and security program. As a result, ArcSight ThreatDetector users can reduce time spent on analysis and instead focus on more proactive security measures.

**Learn More At**

www.microfocus.com/arcsightesm

---

**Figure 1.** ArcSight ESM Console with ThreatDetector
“Due to the sophisticated collection and correlation capabilities of ArcSight ESM, we have an intelligent system that makes sense of the thousands of events and log records we generate each day—helping us to quickly identify and respond to all of the security incidents that matter.”

Information Security Manager
NetApp