

## Product Brief: ArcSight Pattern Discovery

### Powerful Pattern Identification

ArcSight Pattern Discovery automatically identifies benign and malicious repeating event patterns and creates rules for future real-time detection of zero day and low and slow attacks.

#### Highlights

- Quickly identify emerging worms and worm variants before signature detection is available
- Review new patterns daily to automatically uncover active yet unknown threats
- Accelerate your security program with intelligent, automated rule creation

***“Within five minutes of deploying ArcSight Pattern Discovery, we found a new worm variant, attacks in progress on our Web servers and resolved suspicious activity that had been under research for 40 analyst hours”***

— Fortune 50 Manufacturing Company

#### Discover Repeating Event Patterns

ArcSight™ Pattern Discovery automatically identifies patterns of both suspicious and seemingly unsuspecting events, instantly uncovering zero-day worms, low and slow attacks and root kit attacks. In addition to malicious event patterns, Pattern Discovery can help you find misconfigurations of network devices, systems and applications. This optional module for ArcSight™ ESM is built on a patent-pending pattern identification engine that leverages ArcSight ESM’s 100% data capture, normalization and categorization ensuring the most accurate and detailed analysis.

When Pattern Discovery identifies repeating event patterns it captures event detail information to help analysts separate benign from malicious patterns, and automatically creates new rules in ArcSight ESM to identify these threats in the future. By feeding this intelligence back into ArcSight ESM, you immediately add a new layer of relevance to your security monitoring program. Pattern Discovery automatically identifies low and slow brute force attacks which may otherwise avoid detection if they do not trigger

pre-defined thresholds, such as consecutive failed login attempts. Pattern Discovery also identifies repeated attacks even if the attack event behavior sequence is out of order as seen in more sophisticated scripted attacks such as rootkits attacks.

#### Powerful Pattern Identification Engine

ArcSight Pattern Discovery pattern identification engine looks for event patterns across any source data available in ArcSight ESM. It can discover repeating patterns across pairs of source and destination IP addresses, ports, event behavior, event outcomes or any other event classification category. The pattern identification is comprehensive, since ArcSight ESM provides the broadest available classification of security data—uncovering event patterns hidden within the millions of raw security events and alerts generated each day by firewalls, intrusion detection systems and system logs.

For example, Pattern Discovery 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 IDS signature. Without Pattern Discovery, the incremental behavior of the derivative worm would otherwise be invisible because the IDS only discovered the portion of the worm that is defined by the signature. Pattern Discovery helps you avoid damaging consequences by identifying all events related to new worm variants.

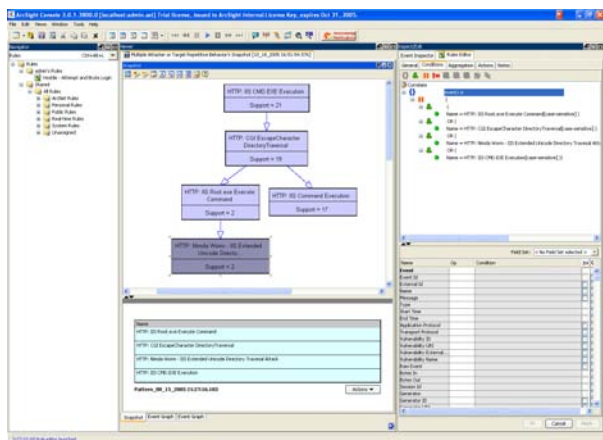


## Integration with ArcSight ESM Automates Response

Once patterns are known, and analysts determine if the pattern represents innocuous traffic or a malicious attack, Pattern Discovery can seamlessly integrate with ArcSight ESM's robust correlation engine. This integration provides one-click rule building to automatically recognize and take action against recurring patterns. The resulting action can range from notification or opening a new case, all the way to an automated response. The result is a shortened window of vulnerability and a better defense for your network.

## Expanding Library of Risks

ArcSight Pattern Discovery continually builds a library of known suspicious event patterns unique to your network, allowing you to increasingly automate your security program. This key advantage enables Pattern Discovery users to experience an exponential decline in time spent on analysis, leaving them more time to focus on proactive security measures.



**ArcSight Pattern Discovery identifies patterns for your review, and automatically authors rules to automate your response.**

## Gain Greater Value

With ArcSight Pattern Discovery, your team will have unsurpassed knowledge and responsiveness to zero-day and automated attacks, allowing it to focus efforts on improving your organization's security posture.

## ArcSight Pattern Discovery Capabilities include:

- Flexible, automated pattern discovery
- Comprehensive data capture for malicious pattern identification
- One-click rule building for fingerprinting unique patterns
- Automated notification and response
- Periodic or on-demand scheduling
- Seamless integration with ArcSight ESM

## About ArcSight

ArcSight, the recognized leader in Enterprise Security Management (ESM), provides real-time threat management and compliance reporting yielding actionable insights into your security data. By comprehensively collecting, analyzing and managing security data, ArcSight ESM enables enterprises, government organizations and managed security service providers to centrally manage information risk more efficiently. ArcSight's customer base includes leading worldwide companies across all verticals—and more than 20 of the top 30 U.S. federal agencies.

### ArcSight, Inc.

5 Results Way, Cupertino, CA 95014, USA

[www.arcsight.com](http://www.arcsight.com)

Email: [info@arcsight.com](mailto:info@arcsight.com)

Corporate Headquarters: 408 864 2600

EMEA Headquarters: +44 870 351 6510

Asia Pac Headquarters: 852 2166 8302

© 2005 ArcSight, Inc. All rights reserved. ArcSight, ArcSight ESM and ArcSight Pattern Discovery are trademarks of ArcSight, Inc. All other product and company names may be trademarks or registered trademarks of their respective owners. 10/05