A background image of a man in a suit talking on a mobile phone, with a purple gradient overlay at the bottom.

Solution Brief: Addressing Insider Threats

Detecting and Responding to Malicious Insiders

Insider threats are the easiest to perpetrate, most difficult to prevent, and can be the most challenging of all threats to detect and manage.

Impact Highlights

- Why insiders can pose a significant risk for virtually any organization
- Identifying malicious insiders with user context and early warning
- Responding to insider threats efficiently and effectively with end-to-end management

Inside the Insider

Insiders have two things that external attackers don't: privileged access and trust. This allows them to bypass preventative measures, access mission-critical assets, and conduct malicious acts all while flying under the radar unless a strong incident detection solution is in place. Some employees become malicious over time; others may be spies planted to conduct industrial espionage; while still others simply make unwitting mistakes that put the organization at risk.

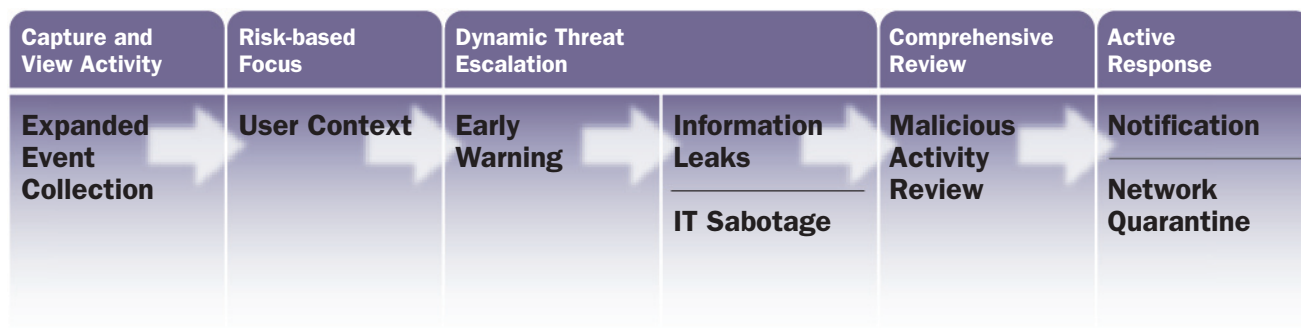
A number of variables motivate insiders, but the end result is that they can more easily perpetrate their crimes than an outsider who has limited access. It doesn't take a skilled hacker to print out sensitive data, copy files to an MP3 player or send confidential information to a competitor. Because of this, anybody can become a malicious insider—from the disgruntled system administrator hoping to sabotage access to business critical systems to the human resources intern that is selling employee salary information to recruiters. Insiders can directly damage your business resulting in lost revenue, lost customers, reduced shareholder faith, a tarnished reputation, regulatory fines and legal fees. With such an expansive threat, organizations need an automated solution to help detect and analyze malicious insider activity.

“With ArcSight, we easily detected and prevented an employee from stealing confidential customer records from our financial systems.” Global Bank

Detecting and Analyzing Insider Threats

Detecting insider activity starts with an expanded log and event collection. Firewalls, routers and intrusion detection systems are important, but they are not enough. Organizations need to look deeper to include mission-critical applications such as email applications, databases, operating systems, mainframes, access control solutions, physical security systems as well as identity and content management products. Many organizations addressing insider threats start by identifying critical applications, information and devices. Once this has been determined and events are being collected from these sources, the events must be processed with automated insider detection techniques. These techniques include:

- Correlation: identifying known types of suspicious and malicious behavior
- Anomaly detection: recognizing deviations from norms and baselines
- Pattern discovery: uncovering seemingly unrelated events that show a pattern of suspicious activity



ArcSight Insider Threat solution transforms the ArcSight ESM system into an early warning and response system for insider threats.

Once a user is determined to be a suspicious insider, analysis tools can be leveraged. These tools working either with real-time or forensic data will interpret the output from the insider detection phase. Working from prioritized events, visual analytics, situational dashboards, investigation channels and other integrated tools will enhance your ability to identify the insider.

Traditional security prioritization schemes tied to external attacks do not translate well to the insider threat. Instead, organizations need to deploy a flexible threat escalation system, whereby individual acts of a suspicious nature—such as off-hours physical access to data centers or encrypted file uploads—elevate the person’s threat level. Should the suspicious activity persist, the user threat level will continue to escalate until it triggers a response. In fact, industry research shows that 40% of known insider threat attacks could have been detected based on early indicators of suspicious behavior.

If user malice is derived from the investigation, or an analyst observes an outright malicious act—such as emailing customer or financial records to a competitor—ArcSight leverages a range of response strategies.

Responding and Managing Insider Threats

All security events need end-to-end management, but this is particularly relevant for insiders. Managing an insider can be a sensitive topic that is politically-charged and it requires that policies and procedures be directly integrated into the solution. From case management, event annotation and escalation to reporting, auditing and access to insider-relevant information, the technical solution must be in line with the organization’s procedures. This will ensure that insiders are addressed consistently, efficiently and effectively regardless of who they are. This process requires executive sponsorship

and the involvement of major stakeholders such as human resources, legal, IT and management. Security teams can identify the insider, but the company needs to carry out the disciplinary actions. In fact, one of the key requirements in managing insider threats is the right of privacy, whereby the observed activity is analyzed with an indirect reference to the individual performing it. Only authorized system users, such as IT security management or human resources actually know the identity of the suspicious individual.

Depending on the nature of the insider threat, rapid response may be appropriate. Based on your company’s policies, the response may be automated or may require human intervention. Regardless of the events triggering the response, a number of techniques can be used including: moving the malicious user to a quarantined network, disallowing them access to sensitive assets, completely blocking their computer from getting network connectivity, disabling user accounts and even preventing them from physically entering access controlled areas.

“With insiders, our perception of risk has changed. ArcSight allows us to address insider threats by enhancing our detection and response—ensuring that attacks from inside the organization are consistently managed.” Regional Utility Company

The ArcSight Solution

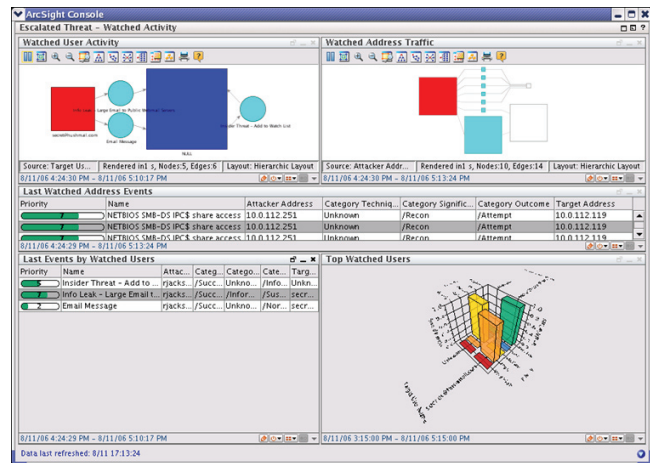
ArcSight has a wide spectrum of products to address the internal threat. We have a dedicated team of researchers focused on developing content for insider threat use cases. A cornerstone of our strategy is the ArcSight™ Insider Threat Package, an add-on module to ArcSight™ ESM.



With the ArcSight Insider Threat Package, you can extend ArcSight ESM to match your company's specific needs. A few examples of the pre-defined insider threat content available in this solution pack include the ability to:

- Identify suspicious user activity patterns and identify anomalies
- Visually track and create business-level reports on user's activity
- Automatically escalate the threat levels of suspicious and malicious individuals
- Respond according to your specific and unique corporate governing guidelines
- Early detection of insider activity based on early warning indicators of suspicious behavior, such as:
 - Stale or terminated accounts
 - Excessive file printing, unusual printing times and keywords printed
 - Traffic to suspicious destinations
 - Unauthorized peripheral device access
 - Bypassing security controls
 - Attempts to alter or delete system logs
 - Installation of malicious software

The ArcSight Insider Threat package offers integrated case management that includes case-specific features for collaboration, incident annotation, real-time dashboards and reports. This allows you to effectively and efficiently limit the information users can access. Also included is an integrated knowledge base that can house contact information, policies, procedures and other pertinent information that is necessary when investigating insiders. The entire process from detection through response, and the general management of the incident is audited. This audit information can be made available in a report to outline the chronology of the investigation.



ArcSight Insider Threat Package containing rules, reports and dashboards allow you to easily identify insider threats.

About ArcSight

ArcSight, a leader in Enterprise Security Management, provides solutions that serve as the mission control center for real-time threat management, compliance reporting and automated network response. By comprehensively collecting, analyzing and managing security data, ArcSight solutions centrally manage and mitigate information risk for security, insider threat and compliance. ArcSight's customer base includes leading global enterprises, government agencies and MSSPs.



ArcSight, Inc.
5 Results Way, Cupertino, CA 95014, USA
www.arcsight.com
email: info@arcsight.com

Corporate Headquarters: 408 864 2600
EMEA Headquarters: +44 870 351 6510
Asia Pac Headquarters: 852 2166 8302

© 2006 ArcSight, Inc. All rights reserved. ArcSight and ArcSight ESM and ArcSight Insider Threat are trademarks of ArcSight, Inc. All other product and company names may be trademarks or registered trademarks of their respective owners. 8/06