ArcSight™

Whitepaper

High-Risk User Monitoring

Using ArcSight IdentityView to Combat Insider Threats

Research 037-081910-02

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

Corporate Headquarters: 1-888-415-ARST
EMEA Headquarters: +44 (0)844 745 2068
Asia Pac Headquarters: +65 6248 4795

Overview

Security professionals once defended their networks against bots and "script kiddies," but now face determined, smart attackers capable of inflicting material financial losses through fraud, theft of intellectual property (IP), and theft of customer information. Disappearing network perimeters and spiraling insider attacks have diminished the effectiveness of traditional security controls, so facing modern cyberthreats requires a fresh look at monitoring practices. For many organizations, a move to user activity monitoring is an ideal way to mitigate the risk of cyberthreats.

While the core principles behind security monitoring, such as defense-in-depth, are still sound, it has become increasingly important to understand who is on your network, what data they are seeing, and what action they are taking. To be sure, firewall, intrusion detection and anti-virus remain a staple of an overall monitoring strategy. The network perimeter must still be monitored, and an organization must be protected against a worm infection. However, the ability to monitor users' activities provides the visibility necessary to identify much of the costly criminal activity afflicting organizations today. User activity monitoring is a crucial tool to combat insider threats, like privileged users, third parties with authorized network access, and internal accounts that have been hacked.

Particularly in large organizations, security teams must prioritize their monitoring efforts to focus on high-risk users. Classifying users into high-risk categories helps increase the effectiveness of security operations teams, which may be struggling to keep up with basic device monitoring. Further, since a substantial fraction of malicious activity occurs within specific time intervals, security groups can reduce the volume of data by focusing on those periods.

From a technology perspective, there are two keys to developing a user activity monitoring capability: the centralized collection and storage of user activity logs, and the use of a monitoring technology with the ability to track high-risk users for activity that may be malicious. Centralized log collection is critical to efficiently search and analyze user activity when needed. While most organizations don't need to actively monitor and analyze all users all the time, with the right tools a security team can monitor the riskiest users during the times that they are most likely to do harm. ArcSight IdentityView is designed to leverage the ArcSight security information and event management (SIEM) platform to enable this type of user activity monitoring.

The Insider Threat Landscape

The recent E-Crime Watch Survey reported that 49% of respondents experienced at least one malicious, deliberate insider incident in the previous year[1]. These statistics may even under-report the insider threat due to the highly sensitive nature of these types of incidents. Although insider attacks constitute a portion of the overall attacks an organization might face, the losses due to these attacks can be devastating, as insiders often have in-depth knowledge of the company's critical asset and systems.

Addressing the insider threat poses a significant challenge. First, insiders have authorized access to critical IT applications and systems. This means looking well beyond login/logoff events to find malicious behavior to what the user does within the application. Second, the insider has intimate knowledge of how internal processes work, such as the frequency of audits and the best targets to attack. Monitoring must increase in both sophistication and frequency to catch insiders. There is simply too much data generated by user activity to effectively monitor all users, so security teams must identify high-risk users.

Perhaps the best example to illustrate this point is an employee who has given notice that he will leave an organization. According to research by the US-CERT on over 150 insider threat cases[2], IP theft is typically perpetrated by an employee giving notice within the last 30 days of employment. While the employee may have been stealing IP for an extended period of time, they almost invariably will steal more on their way out the door. This presents a challenge for the security department, as well as an opportunity.

[1] http://www.cert.org/archive/pdf/ecrimesummary07.pdf
[2] http://www.cert.org/insider_threat/study.html

Identifying High-Risk Users

When a security group can categorize a user as highly risky, it can narrow the scope of monitoring to those who have the potential to cause their organization the greatest amount of harm. What makes these users high-risk in the first place is often tied to a specific event or point in time, such as an employee giving notice, the announcement of a layoff, or the granting of access to a third party vendor. These all represent significant events that allow security teams to focus their monitoring efforts on these users' activity.

Examples of suspicious actions that are easily detectable with the right monitoring technology include file transfers to external networks, emails to competitors, and sensitive application usage outside of normal business hours. Although each organization needs to evaluate its own types of user risk, the majority of high-risk users will likely fit into several general categories (see Figure 1).

Disgruntled Employees and Former Employees	Primary examples include employees who believe they will be laid off, receive poor performance evaluations, are put on performance improvement plans, did not receive an annual pay raise, or work in departments or job functions that are being eliminated or reduced.
Employees Who Have Given Notice	Employees who will steal IP from their company will typically do so within the last 30 days of their employment, making it critical to monitor employees during that period.
New Hires	Employees who are new to the organization have no established history in order to determine if their activities are normal, so additional scrutiny of their activities is advisable.
Frequent Policy Violators	Users who, knowingly or not, violate policies and proceed undeterred warrant additional monitoring.
Contractors/Vendors/ Partners	Security standards such as ISO 27002 and regulatory requirements such as PCI-DSS specifically address the risk that contractors and vendors pose to organizations and require additional IT controls.
Privileged Users	Super users and administrators pose a particularly high threat to organizations due to their access to critical systems and their elevated rights to perform sensitive functions such as creating and deleting user accounts, viewing and managing logs, and altering or manipulating data. Many regulations, such PCI and Sarbanes-Oxley, require logging and monitoring privileged user activity for just these reasons.
Shared Accounts	It is common practice for organizations to use shared accounts, particularly for IT administrators. This becomes problematic when trying to determine which of the shared account users was actually responsible for certain activity. It is often not possible to change legacy applications to eliminate the use of shared accounts, so monitoring becomes a crucial compensatory control.

Figure 1: Categories of High-Risk Users

Best Practices in User Activity Monitoring

At a minimum, technology to support user monitoring must include functionality to track large lists of risky users and develop correlation rules to detect suspicious user activity. While final root-cause analysis of malicious activity typically requires manual analysis, automated approaches are needed to collect security and activity logs and correlate that with user data, either from a directory store (like LDAP or Active Directory) or an identity management product. By tracking user activity on escalating watch lists, a security team can limit alerting to only those users whose activity has met certain criteria, which is absolutely critical to perform efficient user monitoring. As in all forms of security monitoring, information overload is a major challenge. Escalating watch lists coupled with correlation rules can automate the task of identifying malicious or highly suspicious user activity.

Escalating watch lists pare down the overall user population into smaller subsets, resulting in a small number of alerts to investigate that have the highest likelihood of being true malicious activity. A watch list of high-risk users may have thousands of entries. When suspicious activity, such as frequent file transfers or repeated policy violations, are detected for users already on the watch list, the user should be escalated to a suspicious list for further scrutiny. At this point, the overall number of suspicious users is likely to be reduced from thousands to hundreds. Users who are on the suspicious list who engage in additional suspicious behavior should be escalated to the investigate list. At this point, a SOC operator or security analyst should conduct an investigation of the user.

ArcSight IdentityView: User Activity Monitoring in Action

ArcSight IdentityView enables organizations to implement user activity monitoring best practices by leveraging data from the ArcSight SIEM platform and the organization's directory or identity management (IdM) system (see Figure 2). Each event in an activity log (such as a proxy log or server log) will be enriched with identity data. For unauthenticated logs, a user's IP address can be used to link the activity to the actual user, or actor. Typically, the directory or IdM will provide a baseline to identify most, if not all, high-risk users.

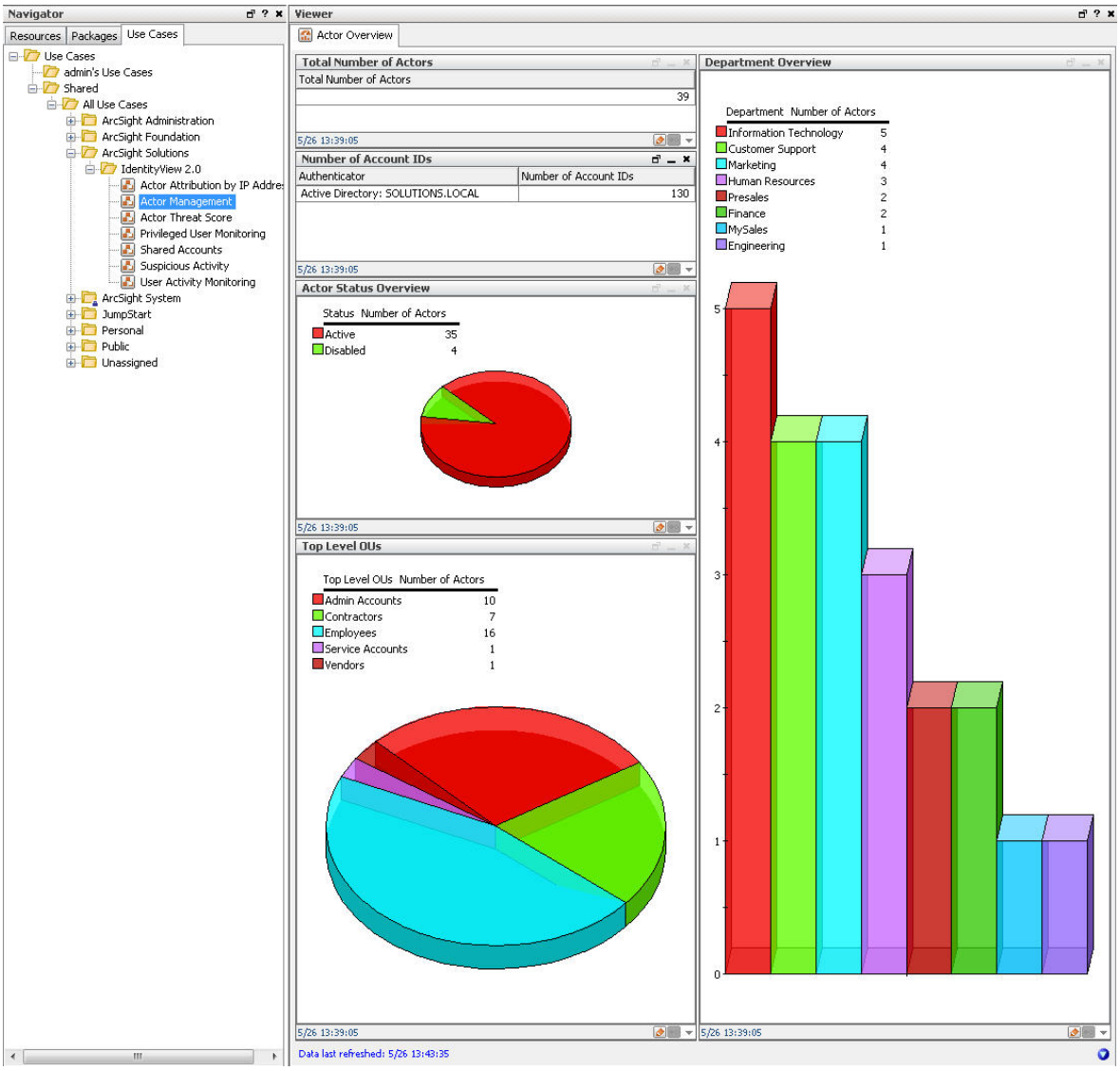

Figure 2: ArcSight IdentityView displays an organization's users by role and level of entitlement.

From this starting point, threat scores can be calculated for each actor, based on suspicious activity (see Figure 3).

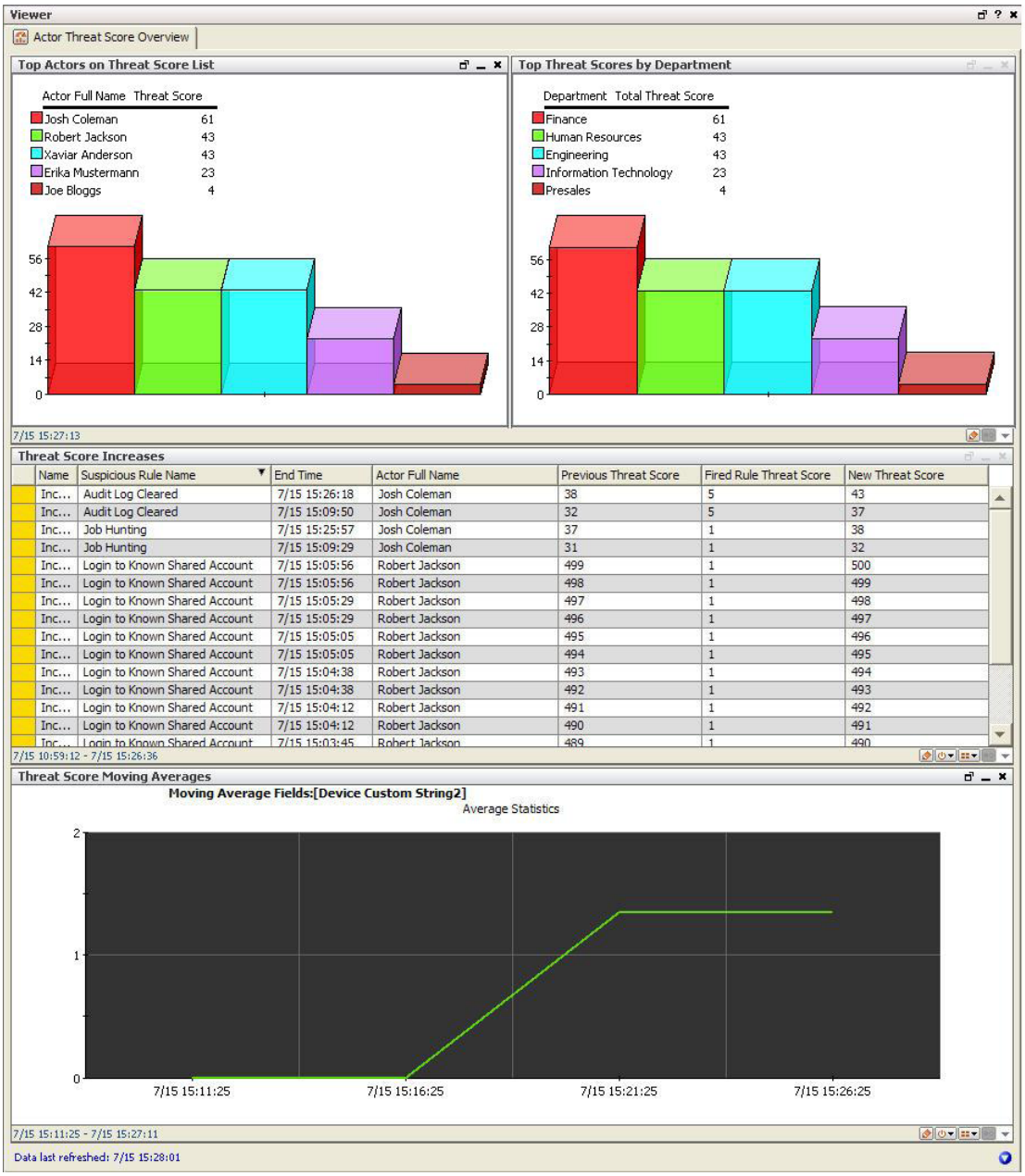

Figure 3: ArcSight IdentityView identifies two actors, Josh Coleman and Robert Jackson, who have generated high threat scores based on their actions.

When this type of malicious user activity is identified through the use of automated correlation and alerting, security analysts or incident responders will conduct investigations following an incident response process. The responder should have as much information as possible at his fingertips, like the raw events that fired the alert and the repository of user activity data. If a user engages in suspect behavior (like Josh Coleman clearing the audit log and job hunting, shown in Figure 3), time is often of the essence. Security teams need to investigate an employee before his last day with the company, and if an analyst must wait days for administrators to pull logs from disparate systems and applications across the enterprise, he will likely miss this window of opportunity. If it takes too long or the process is too arduous to obtain relevant log data, the security analyst may not even try. ArcSight IdentityView brings these logs together in user activity reports, enabling analysts to conduct their investigations in minutes.

Conclusion

As perimeter security becomes less tenable, monitoring user activity is more fundamental to what a modern information security organization does. The risks posed by insiders, third parties, contractors and other users are critical, and will continue to grow as trends like cloud computing and smarter mobile devices blur the lines between an organization's network and the rest of the world.

ArcSight helps the world's leading companies and government organizations mitigate these risks by performing user activity monitoring with ArcSight IdentityView. The solution, built on the ArcSight ESM platform, provides complete visibility of user activity by linking the user, role and group information in directory, HR, and IdM systems with the actual activity logs across the enterprise. By analyzing what each user does and comparing those actions to the user's roles, ArcSight IdentityView can detect potentially risky activity such as data theft or unauthorized access to confidential information. ArcSight IdentityView combines identity correlation, pattern discovery, and log monitoring to enable organizations to implement the high-risk user monitoring best practices discussed in this whitepaper, enhancing visibility of all user activity and processes, streamlined investigations, and above all, mitigating user risk.