ArcSight
An HP Company

Whitepaper

Addressing Insider Threats with ArcSight ESM

Research 026-053110-02

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

Executive Overview

An internal security incident is one that is perpetrated by someone with levels of trust and access greater than that of an outsider. Though the majority of publicity about security breaches today seems to focus on outsider attacks, insider threats can be just as devastating to the organization as attacks from malicious outsiders and range from information leakage to sabotage. But insider attacks are often more difficult to prevent, since these perpetrators are within the company firewall and often have permission to use the information they are either stealing or damaging.

This paper explores two disparate insider threat scenarios: passing information to a competitor and detecting and managing collaborative activities in a low-tech incident. The paper then presents the features and benefits of ArcSight ESM, demonstrating that detection, investigation, response and incident management are all critical features of a strong insider threat initiative. The paper concludes by revisiting the two insider threat examples and examines how ArcSight ESM would have managed the event to prevent the loss or damage to the enterprise's confidential information.

Introduction

Unlike an external incident perpetrated by universally despised foes – such as unethical competitors, extortionists, organized crime, identity thieves or criminal hackers for hire – the internal incident is often perpetrated by someone trusted. The insider may be an employee, consultant, partner, temporary worker or company visitor. These individuals already have more privileges than an external attacker. They are behind some or all of an organization's preventative safeguards. And because they are trusted and supposed to be there, they aren't monitored as closely.

Insider activity can also be much more difficult to pinpoint than conventional external activity, such as scans, DDoS attacks, worm outbreaks or CGI exploits. And there is no doubt that insiders sometimes employ sophisticated measures to perpetrate their crimes. According to a 2005 U.S Secret Service and CERT Coordination Center/SEI Insider Threat Study, 39 percent of attacks utilize a "sophisticated" method. It is important to watch for these types of actions, as well as for less extravagant, low-tech actions, which can be committed more easily by a larger subset of society – but can still produce similar devastating results.

Since it is common for internal policies to be loosely adhered to and often sidestepped, this opens the door even wider for the insider. The consequences can be loss of confidential data or intellectual property, having personal information exposed, damaged assets, severed communications or delayed business processes. This can result in significant financial losses, loss of shareholder faith, severed business relationships or tarnished business reputations.

If stolen information is regulated by the government as in Sarbanes-Oxley, or industry-specific sponsored standards such as Payment Card Industry (PCI) Data Security Standards, enterprises may also be in breach of compliance regulations. In addition to all of the other detrimental effects listed above, the company may need to alert all of its customers to the security breach, pay legal fees, regulatory fines and spend greater resources on public relations.

All Organizations are Vulnerable

An emergency medical technician (EMT) at the University of Illinois Medical Center is accused of using his legitimate access to sensitive data of at least eight patients for his own use. The EMT has been fired from the hospital for improperly accessing patient records. He faces several charges, including identity theft.

The hospital has sent out letters to over 240 patients saying their records may have been similarly breached and they should take steps to avoid becoming victims of identity theft. Administrators were able to look at the electronic medical records system and actually track what records this employee had access to and it actually helped in the investigation.

Insiders Can Become Malicious Over Time

Yonggang (Gary) Min plead guilty to stealing $400 million in trade secrets from DuPont in 2006 after ten years as a research chemist. Over a five month period he downloaded 22,000 abstracts & over 16,000 documents (15 times more than anyone else) from DuPont's Electronic Data Library (EDL) server, which was located at a company facility in Wilmington. The EDL server hosts DuPont's primary databases for storing confidential information. A large portion of the downloaded material had nothing to do with his primary areas of research; instead, it covered most of DuPont's major technology and product lines, including some emerging technologies

Real-Life Scenarios of Insider Threats

Let's start by looking at two sample scenarios of how insiders can pose a threat to the enterprise.

Example One: Passing Information to a Competitor

A system administrator wants to give his company's source code to a competitor that he plans on joining in a few weeks. He performs the following actions:

1. He plugs in his laptop to receive a DHCP lease. Windows DHCP Server Logs are generated.
2. He opens an SSH session with the dev server. UNIX & Internal Firewall Accept Logs are created.
3. The access to the source code was denied under his account so he performs an SU to root. Access is then granted. UNIX Logs are recorded.
4. He downloads the files through SCP. UNIX & Internal Firewall Accept Logs are generated.
5. He then FTPs the files to the competitor's site. IDS Alerts & External Firewall Drop Logs are created.

Since this employee's company did not have an enterprise security platform that was able to detect this kind of insider threat or provide an early warning system by monitoring and correlating log entries, the system administrator was able to transfer the code to the competitor. His former organization was never even aware of the theft.

Example Two: Detecting and Managing Collaborative Activities in a Low-Tech Incident

A hybrid of the insider threat is the collaborative threat that is a function of an outsider working with an insider. Often the outsider will elicit the help of an insider. This is commonly the case when the outsider has criminal contacts willing to buy information such as social security numbers for cash, while the insider has access to the confidential information. Frequently the outsider is just a middleman or a broker, passing the information from the insider to the outside buyers. Because this can be highly lucrative, it attracts various criminals and organized crime groups. These groups will employ techniques used in other criminal activities to solicit cooperation from the insider.

Discovering patterns and being able to interact with the data are critical pieces to identifying this type of incident. Sometimes the low-tech incident is more difficult to detect, yet it can produce similar devastating results. Usually there are no IDS events or dropped firewall packets alerting you or even suspicious looking logs – at least at first glance.

In this example, a malicious private investigator was collaborating with an operator in a call center to extract customer information in exchange for money so the information could be given to his clients.

1. Instead of calling into the call center pool, the private investigator called the operator directly.
2. The operator accessed multiple customer files per his requests and read the output to the caller. (In a normal instance, the operator would only access one file per call.)
3. The transaction ended. Since this company did not have a robust security management solution that could detect unusual insider activity, no red flags or warnings were issued. The private investigator was able to successfully obtain the information and deliver it to his clients.

that were still in the research-and-development stage. When FBI/Commerce agents raided his home they discovered several computers with confidential documents, a software erasure program actively scrubbing disks, garbage bags filled with shredded paper and burned documents. Min pleaded guilty to stealing trade secrets and faces up to 10 years in prison and a fine of up to $250,000.

To further complicate matters, when an insider is identified, the company must gather copious, clear and indisputable evidence. Well-defined corporate policies and procedures must be followed to enable cross-departmental coordination with groups such as information technology, legal, human resources, public relations and senior management. With the risks high and the company reputation on the line, protecting the enterprise against insider threat is of paramount importance. In many cases employees working alongside a threatening insider are reluctant to blow the whistle when they uncover evidence of wrong-doing. Overcoming this requires awareness, training and enforcement of policies and procedures coupled with robust and extensible monitoring tools.

Addressing Insider Threats with ArcSight ESM

ArcSight ESM is a comprehensive enterprise security platform that uses technology to help augment human intuition. By centrally collecting and analyzing security data from heterogeneous devices, ArcSight ESM helps customers worldwide to manage information risk, achieve compliance and protect critical assets – from both external and internal attackers.

The ArcSight ESM console provides security organizations with comprehensive, real time, expert security information analysis and remediation capabilities. ArcSight ESM helps organizations by enabling them to collect massive amounts of mission-critical, internal data from various sources and leverages powerful capabilities around correlation, anomaly detection and pattern discovery. Figure 1 depicts an internal, brute force password attack relying on nothing but system logs. The ArcSight ESM correlation engine and visualization techniques helped uncover the insider's actions by making the detailed computer-based analysis actionable insider's actions by making the detailed computer-based analysis actionable through human interpretation.

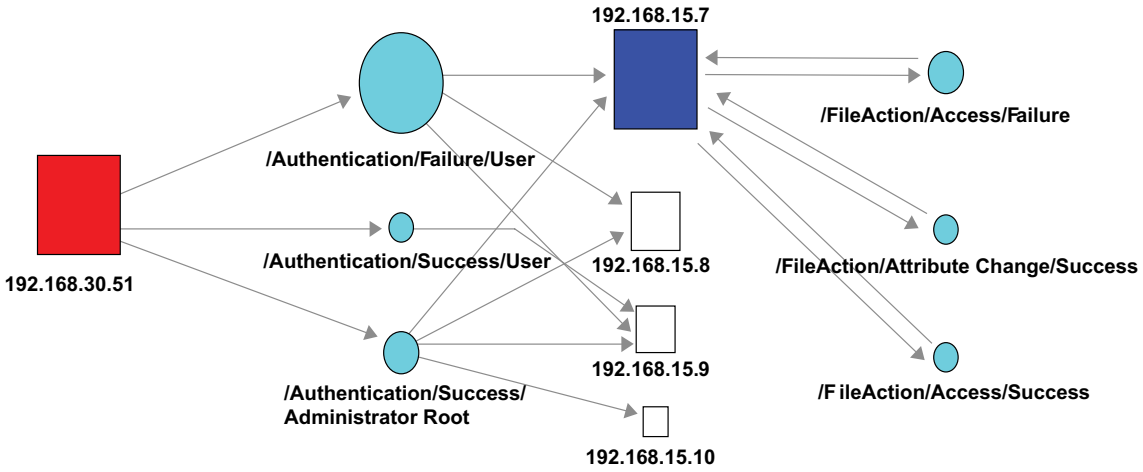

Figure 1. ArcSight Event Graph: This visualization illustrates a successful brute force login attempt. The boxes represent source and target IPs, and the circles represent actions. The size of each element is based on count; color is based on severity, where red is an attacker and blue is a compromised device.

Chain of custody best practices for litigation-quality data This and similar types of correlation scenarios wouldn't be possible without a robust solution around event capture, like that offered by ArcSight ESM. ArcSight ESM starts with the basics – secure, reliable, 100 percent data capture from all mission-critical assets following best practices outlined in NIST 800-92 in terms of filtering, normalization, aggregation and so forth. Leveraging distributed computing capabilities, ArcSight SmartConnectors normalize, categorize, encrypt, compress and timestamp every event so that it can be accurately correlated in its entirety – all without placing any software on the event-generating devices.

The multi-dimensional correlation in ArcSight ESM takes into consideration several facets of an incident, such as the real-time events, vulnerability information, business context, regulatory requirements, data sensitivity, geography, network architecture and asset information such as ports, patches and users.

Not All Insider Attacks are Technical

Three Coca-Cola employees were charged with stealing confidential information and samples of a new drink in hopes of selling them to competitor PepsiCo Inc. Pepsi reported the incident and worked with Coca-Cola and authorities to investigate it. Coke's chief executive, Neville Isdell said that the breach "… underscores the responsibility we each have to be vigilant in protecting our trade secrets. Information is the lifeblood of the company."

ArcSight ESM for Insider Threats

- Ability to correlate disparate events types to a central point
- Industry-leading performance across global enterprise and government/ military grade deployments
- Executive oversight and situational awareness
- Real-time analysis and alerting and forensic investigation
- Automatic remediation
- Detailed reporting
- Integrated case management and incident tracking
- Integration with policy and regulatory compliance (local laws)

Additionally, ArcSight can consider operational time – the ability to use a time baseline of network and system usage. For example, the finance team rarely accesses the financial database before 5am or after 8pm, or perhaps outbound email activity is relatively slow during non-business hours. All of these parameters can lead to a powerful correlation capability that renders prioritized events. Based on these prioritized events, automated actions can be taken in the form of generating alerts, firewall rule changes, router ACL changes, creating a case or launching software.

ArcSight SmartConnectors

ArcSight SmartConnectors can gather all of the mission-critical information, data and logs from the systems that are important to insider threat including operating systems, databases, applications, access control systems and mainframes. Additionally, logs and alerts from traditional network and security devices such as firewalls, IDS, VPNs and routers are also collected.

The ArcSight ESM breadth of coverage goes far beyond traditional scope of perimeter devices to deliver a complete system security. Its data collection engines can utilize a variety of logging mechanisms (Syslog, SNMP, O/JDBC, OPSEC, binary, flat files) while working from a central ArcSight ESM platform – and can be fully distributed where beneficial or necessary.

ArcSight has a number of customers pursuing the convergence of physical and logical security for addressing insider threats by monitoring physical access control cards, biometric authentication mechanisms, RFID, environmental parameters (e.g., power, HVAC) and alarm systems as well as integrating with video surveillance systems and vertical-specific solutions such as SCADA and fraud detection.

Real-Time and Historical Analyses

Suspicious insider activity warrants real-time and historical analysis. ArcSight ESM can even act as an early warning system for suspicious activity by leveraging active lists that will track suspicious users, and escalate them to malicious users if they meet specific criteria. This is particularly important because once an insider is discovered the organization needs to determine what the next steps should be, how far back the actions went, who else may have been involved and what else may have been compromised. ArcSight ESM provides powerful reporting and visualization tools that make investigating historical events fast, easy and inclusive of all relevant data points.

Some insider incidences can go on for years without notice since most investigators only look for things they've been trained to see. Thus there must be a capability to look beyond the commonplace to discover patterns and outliers that when viewed holistically can identify an incident. ArcSight Pattern Discovery is an optional product that helps analysts identify truly malicious patterns from within seemingly insignificant data.

ArcSight Pattern Discovery is an advanced pattern identification engine that automatically examines massive amounts of security events collected and processed by ArcSight ESM to discover repeating event sequences characteristic of threats such as emerging worms, new worms variants, rootkit and low-and-slow attacks. It then automatically creates rules that fingerprint these threats for future identification and response.

In addition to ArcSight Pattern Discovery product, ArcSight ESM has native anomaly detection that provides the reciprocal of pattern discovery. It will detect statistical anomalies, one-offs and events that don't appear to be part of normal traffic patterns. A simple example is a worm outbreak. While anomaly detection will help detect the unusual events related to worm activity, pattern discovery will assist in creating a footprint of the worm's actions.

Insider Attack on a Financial Organization

A 63-year-old, former system administrator that was employed by UBS PaineWebber, a financial services firm, was found guilty of infecting his company's network with malicious code. The malicious code he used is said to have cost his company $3 million in recovery expenses and thousands of lost man hours. He was apparently irate about a poor salary bonus he received. In retaliation, he wrote a program that would delete files and cause disruptions on the UBS network. After installing the malicious code, he quit his job. Following, he bought "puts" against UBS. If the stock price for UBS went down, because of the malicious code for example, he would profit from that purchase. His malicious code was executed through a logic bomb. The attack impaired trading while impacting over 1,000 servers and 17,000 individual work station.

Alerts: Responding To and Managing Incidents

Responding and managing an insider incident can be the most difficult phase of the insider threat response cycle. ArcSight ESM can alert analysts via pager, email, SMS, flashing lights, buzzers and escalate those alerts. It can stop the progression of the activity in real time with or without human intervention.

For example, by leveraging ArcSight TRM, malicious activity from outside an organization or within its perimeter can be addressed. Remediation can take place without or without human intervention in the form of quarantining or blocking an IP address, disabling a MAC address port on a layer-2 switch and terminating a user's account. This limits their ability to login to the network or even physically access the building if the organization has combined their physical and logical security solutions. The remediation capabilities follow industry best practices, organizational procedures, leverage change management parameters and provide full documentation of each change, change rollback and auditing capabilities.

If automated remediation action is enacted, it should only be done for the most severe issues related to the most mission-critical assets. With ArcSight solutions, you decide what is responded to automatically and what requires analyst intervention. When addressing insider threat scenarios that may have limited response windows, a growing number of organizations are now taking advantage of automatic remediation. This is a fundamental shift in how organizations have typically addressed remediation in the past, but a required change because the risks are now so great that there is often little to no time for a human response.

ArcSight ESM can generate and append cases within its own ticketing system or work with third-party applications, such as HP OpenView and Remedy. It can add suspicious data points to an active list, launch applications or simply build tabular and graphical representations of the events.

Active lists are extremely valuable for larger organizations because they help track suspicious network activity, such as somebody attacking or scanning the network, devices that have been compromised, users that appear to be malicious, target ports prone to attack or any other parameter of a packet.

Active lists can be built to represent any group the organization finds significant. For example, if a network is experiencing a horizontal port scan, it is likely that it will not be a high priority event. In fact, many organizations regularly experience such high volumes of scanning activity so that when the port scans stop, it is cause for alarm because perhaps the network is experiencing difficulty.

If an IP address is part of the organization's malicious active list because that address launched a buffer overflow attack against the organization's Web server in the past, it will be treated differently. Now when the organization receives a fairly innocuous port scan from this IP, the casual actions will automatically increase the priority, irrespective of where in the organization the attack was targeting.

In addition, active lists can help determine if an attack is targeted or opportunistic. Opportunistic attacks may appear less focused. Monitoring in an organizational-wide deployment that leverages active lists helps to identify targeted attacks even when they are across various geographies. For example, you could determine if there is one isolated insider trying to steal sensitive information or if it is a pandemic across the entire business.

Industrial Espionage

A Chinese national programmer at Ellery Systems, a Boulder, Colorado software firm working on advanced distributive computing software transferred via the Internet the firm's entire proprietary source code to another Chinese national working in the Denver area. The software was then transferred to a Chinese company, Beijing Machinery. Subsequently, foreign competition directly attributed to loss of the source code drove Ellery Systems into bankruptcy.

Data Retention

Event data is retained following chain of custody best practices where all access is audited and logged. Information in transport between the ArcSight system of Connectors and Managers and Consoles and Managers is encrypted and database partitions use hashing when backed up data is restored. Access Control Lists govern who has access to which pieces of data and their privileges. Analysts and non-analysts alike can view and share various portions of information, annotate data, update cases and render reports based on their privilege levels.

Having this level of incident management control is particularly valuable when organizational policies need to be integrated into the response procedures. ArcSight solutions allow for the alignment of an organization's response capability, ensuring that workflow function of organizational policy is within the appropriate levels of supervisory oversight. Of course this also becomes relevant when working within the legal system to justify litigation-quality data under state and federal laws, such as: the Wiretap Act, Pen Register Track and Trace statute and ECPA.

Regulatory Compliance

Regulatory compliance is prevalent in the media due to its wide-spread impact – valuable consumer data and personal information reside in networks with limited control. Because of this, the issue of compliance has become very personal. All organizations need to take steps to identify systems that contain data governed by compliance regulations. This can be difficult and appeasing auditors can be equally challenging when demonstrating best practices and documenting due diligence.

Historically, many of the systems related to insider activities contain data that would fall under regulatory compliance, such as financial data, healthcare records and personal information. ArcSight compliance solutions address the issues tied to regulations such as HIPAA, Sarbanes-Oxley and PCI through:

- Automatically gaining information for risk assessments
- Supporting existing policies and procedures
- Instituting an effective monitoring and incident response program
- Generating due diligence documentation
- Responding to multiple incidences quickly
- Detecting changes on the network
- Tracking security improvements
- Automatically performing much of the systems activity review process
- Demonstrating improvement and process

ArcSight builds its compliance solution atop a framework that is also designed to address IT governance. From the bottom up, this includes:

- Vendor-neutral data feeds from primary controls (applications, databases, operating systems) and secondary controls (firewalls, IPS and network devices)
- Event collection from data feeds are inline with NIST 800-92 (Guide to Computer Security Log Management)
- Technical checks based on NIST 800-53 (recommended security controls)
- Business relevance added through ISO 17799:2005 providing business process, policy monitoring and risk management
- COBIT frameworks applied for specific IT governance needs as can COSO for internal business controls
- ITIL applied at each level to incorporate best practices

The framework to this point is often called ISO over NIST and is often used to create an IT governance program. Specific compliance regulations can be layered atop this framework. The output can be realized through specific content such as visuals, correlation, active lists and reports. Ultimately, this methodology is equally valuable for security and insider threats as well as both single and multi-regulated environments.

Detecting and Managing Suspicious Insider Activity

Suspicious insider activity is one of the most common issues related to insider threats – and one of the broadest. Depending on the organization and its policies, many things can be considered suspicious, including unsuccessful user logins, attaching removal media devices to servers, cross-departmental access to sensitive data, use of prohibited applications such as encryption programs, and P2P or instant messaging. ArcSight ESM can automatically move users conducting suspicious activity to a malicious group based on threat priorities. Further, the classification of the data and the empirical evidence of the data content (email and IM content, word documents and images) itself as gleaned from content management solutions and supply empirical, supporting evidence to justify an insider as malicious.

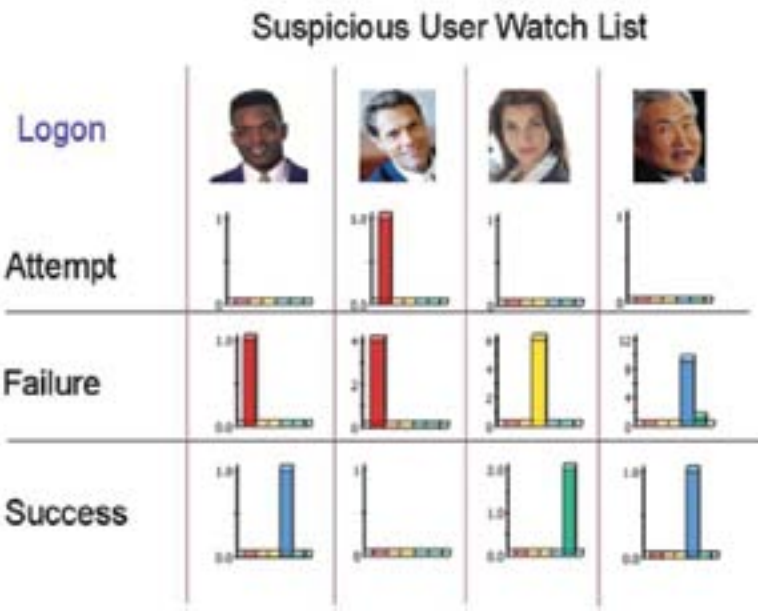

Figure 2. This ArcSight ESM dashboard represents internal users that are deemed suspicious against logon actions. Dashboards can be nested to form multiple graphical drilldowns and ultimately display the underlying event data.

Correlation and Prioritization of Events

Suspicious activity cannot always be identified by looking at just a single set of logs and rarely by only monitoring perimeter devices. That is why correlation among multiple vendors and formats is critical. In addition to correlation, the ArcSight Manager will assign prioritization. If there are several events happening at once, an analyst needs to be able to respond to the most critical one first. For example, consider an attack at an automobile manufacturer. If an insider is attacking a print server in the marketing department, and a CAD server containing confidential schematics of a new car, the threat priority for the CAD server should be higher based on the system's content, even though both servers are running the same operating systems and patches and are vulnerable to the same attacks.

Another correlation example may be an attack that is seen through an accept packet on the firewall, a network IDS alerting to the fact that the packet represents an attack, the target system's application logs producing anomalistic output and asset and vulnerability data stating that this is a mission-critical server and that it is in fact vulnerable to the attack detected by the IDS alert. Correlating the various products, vendors and log formats and calculating vulnerability and asset information into the threat prioritization algorithm helps ArcSight ESM to effectively increase and decrease priorities, minimize false positives and ensure that the most critical events are quickly made known to the relevant audience based on pre-determined alerting, escalation, case management and response procedures.

Identity and Role-Based Correlation

ArcSight ESM offers a unique capability for addressing insider threats called identity- and role-based correlation. This form of correlation helps bridge the gap that has existed between IT/physical events and actual people and/or roles.

This correlation provides the ability to model the typical behavior of groups of machines or individuals. This provides a framework that allows an analyst to follow a malicious insider's footsteps and build baselines against which anomalies can be derived. Some general examples may be a QA engineer accessing financial systems, or a temporary employee downloading sensitive development information such as source code. More specific examples may be connecting the dots between a user's IP and MAC address, various network accounts, badge readers, and so on. With this capability, insiders can be more effectively identified and subtle events can be looked at holistically against an individual's entire event trail to determine if suspicious behavior is in fact malicious. Best of all, this capability works in dynamic environments where DHCP, VPNs, wireless access, physical security devices, and multiple user IDs associated with a single individual may be in place. Because ArcSight ESM can track a user's sessions, the underlying physical and IT feeds are abstracted to a particular user, thus providing clarity amongst seemingly unrelated data points.

Out-of-the-Box Content

ArcSight has a dedicated team focused on building solutions for specific customer needs such as compliance and insider threat. The ArcSight Insider Threat Package is a combination of rules, reports and dashboards. This purpose-built solution alleviates organizations from spending time and money on creating their own insider threat solution from scratch.

ArcSight solution packages are built on industry best practices – as well as direct input from consultants, government organizations and Fortune 1000 companies. This Insider Threat package has been field tested by ArcSight customers and effectively enables robust insider threat detection as well as provides special provisions for managing the risk associated with insiders. Overall, the out-of-the-box content for insider threat detection and management helps reduce risk, increase operational efficiencies and mitigate custom development costs around insider threat detection.

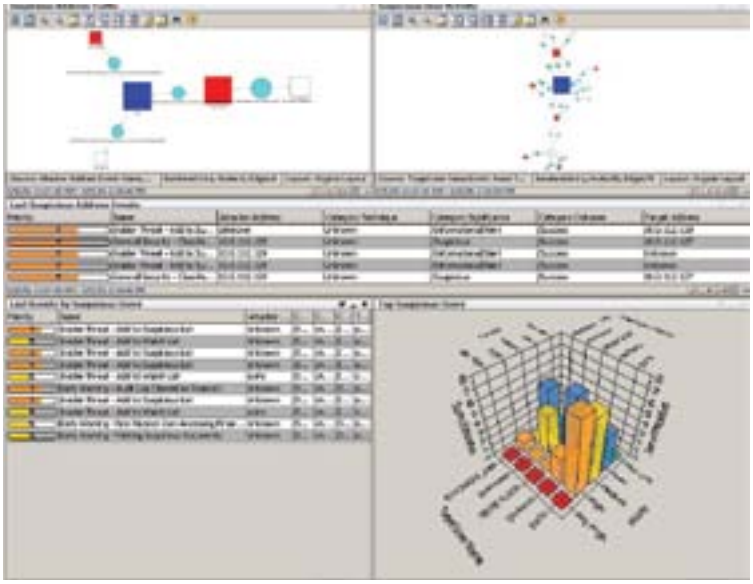

Figure 3. ArcSight Insider Threat Package containing rules, reports and dashboards allows you to easily identify insider threats.

Biggest Bank Heist in History

In 2005 at the London branch of Sumitomo Mitsui Bank was attacked with the help of an insider. Had the attack been successful, it would have been the largest bank heist in history with funds upwards of $440 million being transferred to accounts in other countries. Disguised as a cleaning crew, and with the assistance of an insider – a bank security guard – the criminals installed hardware-based keyloggers. The thieves captured the credentials of individuals responsible for wire transfers over the SWIFT (Society for Worldwide Interbank Financial Telecommunication) network. Using this information they were able to transfer roughly $440 million. They were caught, and the money was recovered.

Managing Insider Threats with ArcSight ESM

Revisiting two threat scenarios aforementioned:

Example One: Passing Information to a Competitor

In this scenario, the system administrator wanted to give his company's source code to a competitor. He went through a series of steps to download and FTP the files to the competitor.

1. He plugged in his laptop and received a DHCP lease. Windows DHCP server logs were generated.
2. He opened an SSH session with dev server. UNIX & internal firewall accept logs were created.
3. The access to the source code was denied under his account so he performs an SU to root. Access is then granted. UNIX logs are recorded.
4. He downloaded the files through SCP. UNIX & internal firewall accept logs were generated.
5. He then FTP'd the files to competitor's site. IDS alerts & external firewall drop logs were created.

The ArcSight Session Reconciliation Data Monitor allows ArcSight ESM to associate a DHCP address directly back to the insider's computer. ArcSight ESM can then associate this information with the UNIX system logs such as login, SU and file download even though the connection itself was encrypted. A complete chronology was built in real time, detailing the actions of the insider and generating correlated events that interpreted the seemingly unrelated events.

When ArcSight ESM detected from the IDS that files considered sensitive were trying to be uploaded to an external site, ArcSight automatically generated a remediation action changing the rules on all perimeter firewalls to block all outbound traffic from the insider's source IP to the Internet.

The enterprise's security analysts received this information, investigated it further, generated reports, followed the organization's incident management procedures (which entailed presenting the normalized data along with graphical representations) and reported the incident to management. Content management tools were used in conjunction with ArcSight solutions to provide empirical evidence that this information was sensitive. Not only was the file transfer to the competitor blocked, charges were filed against this employee for attempted theft of valuable corporate information. Further, the analysts were able to investigate forensic information to discover how long this activity had been going on, who else may have been involved and what other malicious acts were associated with the suspicious users.

Example Two: Detecting and Managing Collaborative Activity in a Low-Tech Incident

In this case, a malicious private investigator was collaborating with an operator in a call center to extract customer information in exchange for money so the information could be given to his clients. The process the private investigator used was:

1. Instead of calling into the call center pool, the private investigator calls the operator directly. This was slightly unusual and raised a yellow flag within ArcSight ESM.
2. The operator accessed multiple customer files per the private investigator's requests and read the output to the collaborator. Since in a normal instance the operator would only access one file per call, this also raised a red flag.
3. The transaction ended.

ArcSight ESM uses advanced data visualization and correlation techniques for discovering patterns. It enables security analysts to interact with the data though various graphical models even further by identifying outliers within ArcSight Interactive Discovery. Analysis can be based on long or short time periods, as well as large or small data sets. This technical data can be represented in easy-to-share and understand formats utilizing charts and graphs.

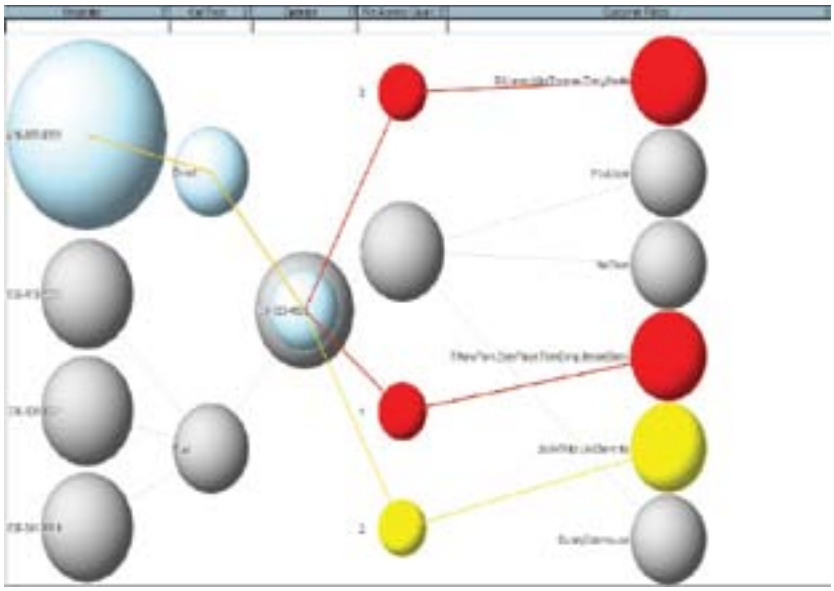

Figure 4. This visual illustrates ArcSight Interactive Discovery. Sphere size is based on event count, color is based on priority and the links between spheres represent relationships. The large sphere on the upper left is the private investigator. It is clear that he only made direct calls to the operator and during each of those calls multiple files were accessed. Two files may be a medium issue thus the color yellow, but three very suspicious, thus red. Finally, the actual customer files accessed are displayed on the far right.

In this low-tech incident example, interesting data patterns were identified within a propriety call center application that tracked telephony and file access through various logs generated by its operators. Every time a direct call was made, it was by the private investigator, further, several files were accessed during each of those calls while random, pooled calls were associated with the typical 1:1 ratio for call to file access.

System logs can often be difficult to understand in their native format and organizations may create hundreds of gigabytes of data with millions of entries that need to be processed daily. ArcSight ESM can analyze this massive data set in real time or forensically by looking for patterns and trends. It can then render visuals that can be investigated, annotated and shared. These patterns can identify the anomalies and outliers embedded within the data set.

Using ArcSight ESM, reports and charts were rendered, annotated and shared with management teams, legal and HR departments. This output greatly reduced the time the team needed to interpret the findings. In this example, the security team was alerted by numerous “red flags” and the operator and private investigator were apprehended.

Summary

This paper has explored two disparate insider threat scenarios to demonstrate that detection, investigation, response and incident management are all critical features of a strong insider threat initiative. ArcSight ESM in conjunction with the ArcSight Insider Threat Package is the best choice for an insider threat solution because it is built to be a mission-critical, enterprise-class solution developed on best practices and with content and features contributed from government organizations and Fortune 1000 organizations around the globe.

The ArcSight Insider Threat Package alleviates organizations from spending time and money on creating their own insider threat solution from scratch. The out-of-the-box content for insider threat detection and management helps reduce risk, increase operational efficiencies and mitigate custom development costs around insider threat detection.

The ArcSight solution is designed to be extensible to capture any data types and scalable to ensure it can process all of the mission-critical data. With unparalleled vendor-neutral, cross-correlation capabilities, pattern discovery and interactive discovery features, ArcSight ESM produces the best prioritized, summarized and human-understandable results. ArcSight ESM has the richest feature set focused on insider threats and allows organizations to render virtually limitless tabular and graphical views, investigation scenarios and reports.

ArcSight ESM threat prioritization leverages active lists and the automated escalation of users from suspicious to malicious. ArcSight ESM can detect preludes to an attack based on said suspicious behavior. Using asset management, vulnerability management and content management solutions, ArcSight ESM can paint a complete picture of the organization's security posture in real time.

The ArcSight ESM data aggregation strategy is a complete, 100 percent mission-critical capture of the status, alarms and alerts from the various firewalls, intrusion detection systems, mainframes, databases and other relevant sources that are being monitored, nor matter what topology of distributed connectors and centralized connectors is used. This means that every field from every event is available for real-time correlations, display, investigation and reporting. ArcSight ESM goes far beyond just standard perimeter security to complete system security. The same features that make ArcSight ESM analysis so powerful in real time can be used in exactly the same way for forensic analysis.

In terms of incident management and workflow, ArcSight ESM provides alerting, escalation, case management, annotation and auditing as native features and has full integration with third-party products. ArcSight ESM also provides remediation capabilities that can be carried out automatically or with human intervention through a number of policy-defined response mechanisms (quarantine, disable at layer-2, layer-3 and terminate user accounts). ArcSight ESM uses best practices from NIST and ISO for its IT governance and compliance solutions which also benefits traditional security and insider threat strategies. All of these aspects are taken as a whole yield – not just a technically superior solution – and has been rigorously tested in real-world environments.