ArcSight
An HP Company

Whitepaper

Combating Fraud & Data Theft in the Financial Services Industry

Research 016-081509-05

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 Summary

Growing Incidence and Cost of Data Breaches

- Widespread digitization of bank assets has increased efficiency but has also enabled new cyber-threats such as online, ATM, and call center fraud schemes and large-scale hacking activity
- The financial sector alone accounts for over 90% of all records breached
- Over 80% of records breached in the financial sector are the result of malicious and intentional acts
- Trusted insiders already account for a quarter of all breached records and are a growing concern
- Over 50% of insider breaches are perpetrated by privileged users such as IT administrators
- The cost of breaches is growing and already stands at $6.6M/breach and $200/record

Unique Challenges for the Banking Sector

- Banks are a prime target for cyber-criminals because they are the richest source of identities and provide direct access to monetary assets
- The multi-channel and distributed nature of banking creates more opportunities for cyber-attacks
- Widespread M&A activity has increased the risk of disgruntled employees and the risk from heterogeneous and legacy applications
- The effort to address security threats is compounded by significant regulatory oversight in banking
- Point security technology investments (DLP, DAM, etc.) have helped, but do not provide the much needed visibility into how users interact with data and applications

Importance of Automated Monitoring

- Continuous collection and analysis of log data is the most efficient approach to monitoring and enables the visibility into user activity that is needed to detect breaches, security threats, and to streamline compliance efforts
- Commercial SIEM (Security Information and Event Management) solutions are much more cost effective than home-grown log monitoring, but not all solutions have the capabilities needed to address the challenges specific to the banking sector

Requirements for Effective Monitoring

- To detect the various forms of internal and external cyber-threats, banks should consider commercial SIEM solutions that can effectively and comprehensively monitor:
  - All bank locations and infrastructure including data centers, branch offices, ATMs, online infrastructure, call centers, etc.
  - All access to confidential data, systems, and applications
  - All activity by users across their identities and based on their role (customer, traders, privileged users, terminated users, etc.)

The ArcSight SIEM Platform for Banking

- The ArcSight SIEM platform enables complete monitoring of all data, process, application, user, and system activity across locations and channels (online, branch offices, ATM, call centers, etc.)
- ArcSight leads the market in monitoring scalability, flexibility, and built-in knowledge (pre-packaged content for bank fraud, perimeter threat, insider threat, cross regulatory compliance, etc.)
- ArcSight is used by leading banks throughout the globe to reduce the risk of cyber-security threats and to efficiently demonstrate compliance across regulations

Introduction

Over the last few decades banks throughout the globe have undergone a significant transformation. From paper checks to credit cards and from physical branches to direct deposits and online portals—the global banking industry has largely digitized its customer interactions as well as its backend infrastructure and supporting operations. This widespread digitization of financial data, transactions, and processes has certainly enabled greater efficiency for banks and consumers alike. However it has also been accompanied by significant new cyber-threats ranging from elaborate online, ATM, and call center fraud schemes to targeted large-scale hacking activity.

In fact, the financial industry now accounts for a significant majority of all breached records. The risk to banks and other financial institutions started with external sources, but insiders now account for a significant and growing share of breaches. The cost of even a single breach is significant in terms of penalties, lawsuits, customer attrition, negative publicity, and brand impact. To that end, this whitepaper will begin with a summary of the incidence, sources, and cost of breaches in the banking and finance industry.

Banks also have numerous physical branches and ATM locations, maintain online portals, operate legacy infrastructure and applications, outsource backend operations, and merge with or acquire other banks. These factors only compound the risk of breaches and open

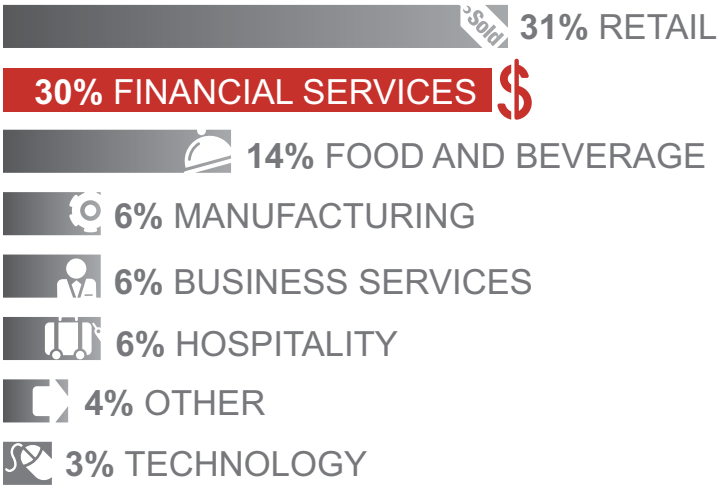
the door to more threat vectors. These challenges are elaborated upon in the next section.

To combat such breaches along with their numerous regulatory requirements, banks have invested in technologies ranging from firewalls and intrusion detection systems, to identity management and data leak prevention. Yet, despite these investments, most banks still lack visibility into how their employees, contractors, partners, and customers interact with their systems, applications, and data. To effectively weather the ongoing financial crisis, address requirements across regulations, and combat cyber-crime, banks must have continuous visibility into all user activity on their networks. This is the realm of monitoring solutions which the next section will detail while also describing the advantages of automated and continuous log-based monitoring.

The paper will conclude with a review of requirements for a comprehensive monitoring solution followed by an overview of the ArcSight SIEM platform and use cases from leading banks across the globe that have successfully used ArcSight to combat cyber-security risk and make technology a source of competitive advantage.

Incidence, Source, and Cost of Breaches

The *Verizon 2009 Data Breach Investigations Report* reveals that the Financial Sector leads all industries in percentage of breach incidents as well as percentage of breached records. In fact, the financial sector alone accounts for an overwhelming majority (over 90%) of all records breached. This suggests that the scale of an individual breach (or the yield of accounts per breach) in the financial sector is much larger than in other industries.



Industries Represented by Percent of Breaches

Industries Represented by Percent of Records

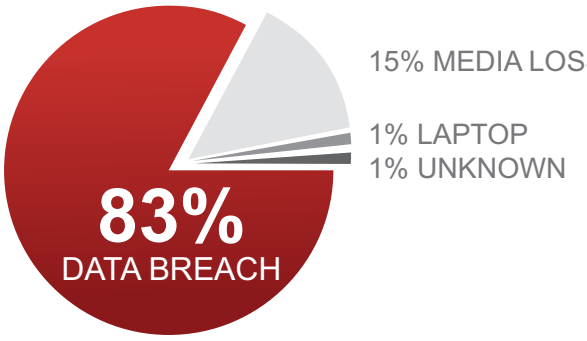
While breach incidents in North America contributing to those statistics have received widespread press coverage, similar incidents of breach or fraud have certainly impacted banks in other parts of the world as well. A few recent examples include:

COUNTRY	BREACH DESCRIPTION
UK May 2009	UK's financial regulator, FSA, fined Morgan Stanley $2.1M for systems and controls failings which led the bank to make a negative adjustment in mid 2008. Trader Mathew Piper deliberately mis-marked the positions he traded on behalf of Morgan Stanley and sought to hide losses by manipulating processes to monitor trading activity.
Germany Dec. 2008	Microfilm containing extensive stolen data, including account numbers, credit card PIN numbers, and details of payments, was sent to the Frankfurter Rundschau newspaper anonymously in the post. Although the data was from the Landesbank Berlin which is the country's biggest issuer of credit cards, customers from all sorts of institutions up and down the country were affected.
France Oct. 2008	In a cyber-attack that was likely aimed more at publicity than financial gain, thieves broke into French President Nicholas Sarkozy's bank account and withdrew several small amounts.
UAE Sept. 2008	Accounts of numerous UAE bank customers, including HSBC, Citibank, Lloyds TSB, National Bank of Abu Dhabi, and Emirates NBD, were breached. Reports suggest this was the result of payment processing servers being infiltrated and/or ATM skimming. Breached accounts were then used to make fraudulent purchases in other countries.

The impact of just a single breach can be significant in terms of customer attrition or lost revenue, class action lawsuits, regulatory penalties, and negative press. According to the 2008 Ponemon data breach report, the average cost of a data security breach is $6.6 million and more than $200 per compromised record. The bulk of this cost stems from customer loss following a breach. Beyond lost revenue, there is the broader impact on a bank's brand image as well as a loss of shareholder and partner confidence.

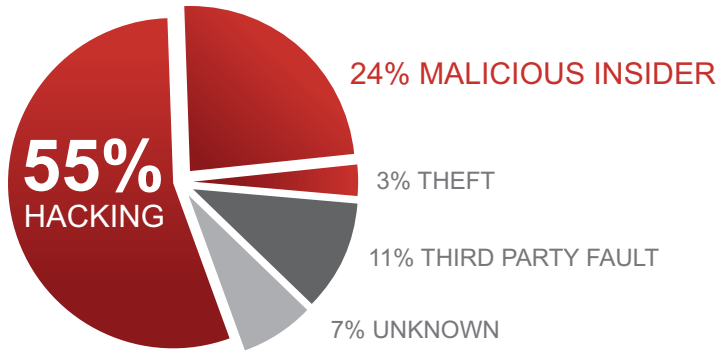
While the cost of breaches in surveys has largely been focused on customer data, many banks offer trading, investment, and advisory (M&A, etc.) services and therefore also need to protect intellectual property related to those business services and investment trading strategies.

Perimeter eSecurity's 2008 Study of Financial Data Security shows that malicious data breaches account for over 80% of breached records in financial institutions. So in contrast to inadvertent incidents that stem from poor security awareness and training, the bigger threat to banks comes from malicious insiders and hackers.



Records Compromised By Breach Category

The same report also reveals that within malicious breaches, external hacking accounts for 55% of breaches, while malicious insiders represent another 24% (and growing) source of the breaches.



Breach Source for Malicious Breaches

Additionally, 50% of insider breaches are perpetrated by privileged users such as IT administrators. This highlights the need for more visibility into network activity from super-users in any banking environment.

The threat to banks from insiders comes from other groups as well. Disgruntled traders have quite literally caused banks to collapse in recent years. In many cases, effective monitoring could have triggered early signs of fraudulent activity. Call centers for customer support are often outsourced and staffed by younger, lower wage contract employees who may be more susceptible to organized crime pressure and bribery.

The collapse of the global banking industry in 2008 has led to more mergers and acquisitions across consumer and investment banking firms. Such mergers are accompanied by the need to connect IT networks and carefully manage access across applications—a challenging task when applications are homegrown and lack robust, inbuilt security or access controls. This creates a bigger opportunity for malicious insiders to carry out breaches unnoticed.

The recent downturn and mergers have also resulted in significant layoffs. In the process, some employees will invariably turn disgruntled and potentially engage in fraudulent activities. Terminated employees and contractors are a major source of risk, especially because it is difficult to ensure that physical and network access is in fact terminated across the board.

Unique Challenges for the Banking Sector

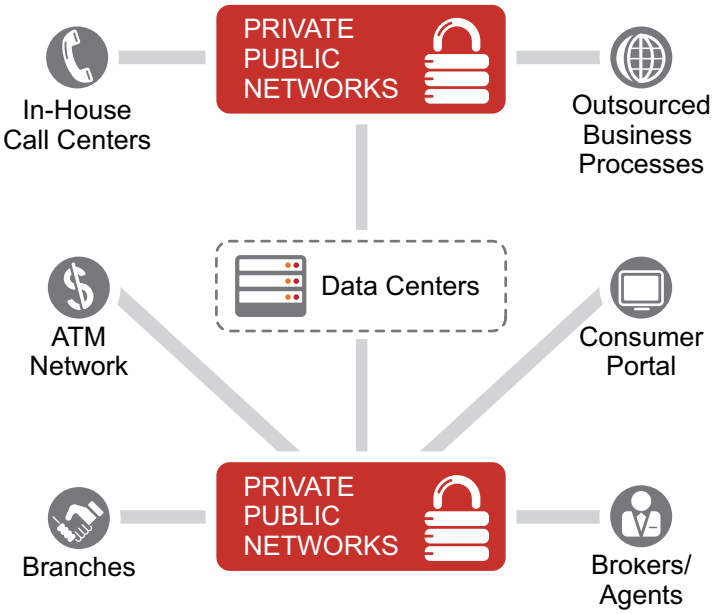
Banking Challenge #1: More Dollars at Risk

Incidents of fraud and breaches are very widespread in the banking industry, even though banks are highly regulated and are generally early adopters of security technology. This is because banks are and will remain the richest source of personal consumer data and more importantly monetary assets. This makes the industry a prime and highly lucrative target for cyber-crime, ranging from identify theft to fraud.

Banking Challenge #2: Multi-Channel and Distributed Networks

Although sensitive data within banks may be protected within a data center, it is accessed and processed by a wide range of internal users, partners, and customers through numerous channels and applications.

Consumers interact with their banks through online portals, ATMs, and directly at branch offices. Even credit card purchases at a retailer need to be processed by the issuing banks or their outsourced business partners.



For example, online banking portals are a growing target for execution of numerous fraud schemes such as phishing and smishing (SMS-based phishing). Similarly, skimming devices on ATMs which are increasingly outsourced represent another common fraud target. Individual branch offices may also store a lot of sensitive information about daily transactions and associated account data. Unfortunately, infrastructure at branch locations is rarely as secure as the centralized data centers and is more susceptible to hacking attempts. Finally, the incidence of multi-channel cyber attacks and fraud schemes is on the rise which makes effective monitoring and tracking of user activity across all these touch points paramount.

Banking Challenge #3: Several Levels of Trust

Any bank will have employees in various roles—each with access to certain types of sensitive data. As the background section of this document revealed, insiders account for a growing number of data breaches at banks, highlighting the importance of user monitoring for early signs of breaches and policy violations. For example, traders should be monitored for anomalous activity such as excessively large trades; contractors can be monitored for after-hours access to sensitive data; call center representatives should be monitored for access to accounts that do not have any unresolved calls or open tickets; and privileged IT users, such as DBAs, should be monitored for direct access to sensitive data which they are responsible for managing but do not need to actually view. These are simply examples. To effectively detect breaches and policy violations, any bank must have the broader ability to monitor and correlate any and all activity, such as excessive printing, emailing sensitive data, after-hours access to confidential data, badge swipes, transactions, database queries, and all application activity.

Banking Challenge #4: Decades of Constant Mergers and Acquisitions (M&A)

The frequent occurrence of M&A activity in the banking industry makes monitoring especially challenging. For one, the transition process itself is complex and often creates security holes such as terminated users with continued network access. At the same time, banks have heterogeneous infrastructure and legacy applications which only increases with M&A activity. Heterogeneous infrastructure also implies that any user could have numerous identities. Tracking and unifying an actual user's activities across those identities is a significant challenge that impairs visibility into threats and breaches. A related problem in banking is the widespread reliance on several legacy applications (accrued across mergers and acquisitions) with limited access controls and privileged shared accounts. This makes it very difficult to uniquely track and associate actions back to a specific user.

Banking Challenge #5: Widespread Regulatory Oversight

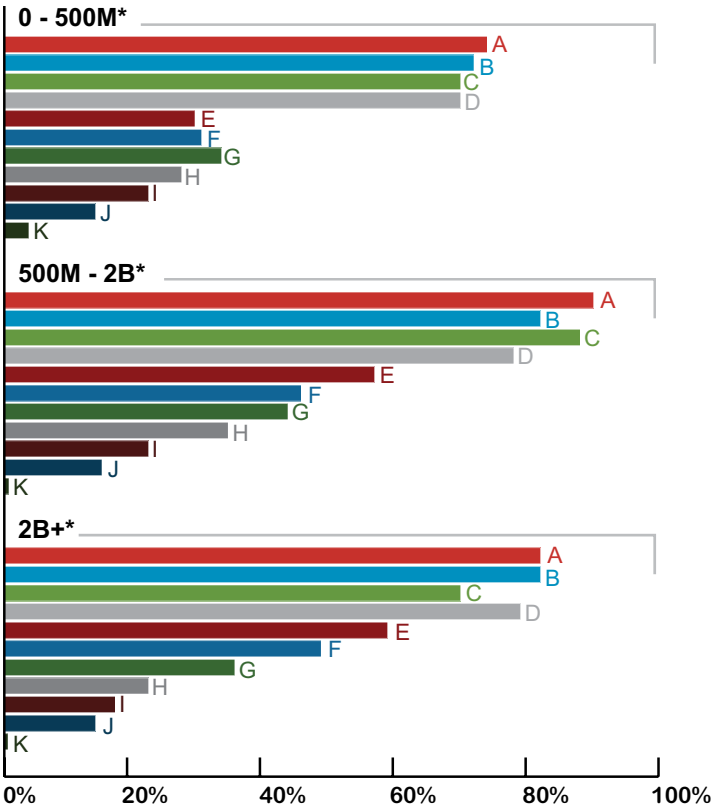
The banking sector has also been subject to more regulatory oversight than most other industries and this is only likely to increase in the face of the recent global financial crisis. For example, large public consumer banks generally have a global presence, and as a result, are subject to numerous regulations including BASEL II, Sarbanes-Oxley, Bill 198 (Canada), JSOX (Japan), the German Corporate Governance Code, etc. They are also subject to privacy acts, such as GLBA, PCI, and increasingly to the many national data privacy acts that are enforced on a country-by-country basis.

The Need for Enterprise-Wide Automated Monitoring

To combat the growing incidence of cyber-threats, banks have made numerous technology investments. For example, most banks are now well past the point of implementing basic protection measures like firewalls and IDS devices. In fact, the *State of Banking Information*

Security Survey 2008 by BankInfoSecurity.com indicates banks are aggressively investing in the next generation of point security technologies, such as application layer firewalls, purpose-built fraud detection tools, and identity management systems.

QUESTION: What strategies have you adopted to prevent identity theft?



LEGEND

A: Network-based intrusion detection/prevention systems
B: Employee background checks
C: Application firewalls
D: Network access control technologies
E: Fraud detection technologies
F: Log analysis technologies
G: Documented ID theft prevention program
H: Identity management technologies
I: Behavioral-based anomaly detection technologies
J: Automated data-leakage technologies
K: Other

*Company Revenue Size in Dollars

Each of these investments certainly provides some additional protection and visibility into potential sources of risk. However, even collectively, these investments do not enable the much needed visibility across the entire enterprise. For example, even with identity management systems in place, banks do not have clear visibility into all activity by a trader across his/her physical and logical identities. Similarly, specialized banking fraud detection tools are generally application specific and may be able to detect application specific fraud incidents—but lack visibility into a user's actions in other parts of the network. Without that visibility, even the basic questions below will remain unanswered and as a result many breaches and compliance violations will remain undetected.

- When a user is terminated, what level of visibility do we have into activity from any remaining active accounts?
- Can we associate activity back to a unique user, even when widely prevalent shared accounts in legacy applications are used?
- Are we able to contextualize a user's actions based on the user's role and level of risk (contractors vs. privileged users vs. traders etc.)?
- Do we have the role awareness to look for incidents of separation of duties violations?

To achieve enterprise-wide visibility and easily answer the questions above, banks must be able to monitor and correlate activity across all users and infrastructure, including desktops, servers, databases, network and security devices, applications, legacy systems, and more. This raises the question – how can banks comprehensively and efficiently monitor activity across the entire enterprise?

Logs and Monitoring

What many enterprises don't realize is that they already have the information needed to detect breaches in a timely manner and to cost effectively address regulatory requirements. Every second of the day, servers, laptops, applications, network infrastructure, and security devices leave a trail of activity behind in the form of logs. Every login and logout, every badge swipe, and every action in an application can be tracked through its trail of logs. By consolidating and analyzing logs across the enterprise, banks can effectively monitor all activity for threats, breaches, and compliance violations.

The challenge is keeping up with the millions of log events that can be generated on a daily basis by even a small bank. To compound the problem, each device logs data in a different format which makes monitoring activity across devices even more challenging. SIEM (Security Information and Event Management) solutions address those challenges through pre-built adapters for collection of logs from all sources; easy expansion and support for legacy

sources; efficient centralized storage and retention; and most importantly, powerful and scalable log analysis. Even so, most commercial SIEM solutions lack the capabilities that are needed to effectively and comprehensively monitor bank IT infrastructure for security threat detection and more efficient regulatory compliance. To that end, a list of key requirements to aid the selection and evaluation of a SIEM solution follows:

- Pre-built content to address common regulatory drivers (SOX, BASEL II, country-specific privacy laws) and security threats that banks face (malware, hacking, fraud, anti-money laundering, etc.)
- Complete monitoring across all bank assets, including branch office infrastructure, legacy applications, online portals, outsourced operations, and emerging technology investments (database activity monitoring, data leak prevention, identity management systems, etc.)
- Activity profiling or discovery of activity patterns by user role or group
- Efficient, long-term storage and automated enforcement of log retention policies based on the various regulations impacting banks
- Scalable, real-time correlation and historical analysis (forensics search, reporting) of logs with minimal impact on log collection rates and log storage efficiency
- A robust asset model to contextualize activity from logs with the role, location, criticality, and other attributes of any system, database, or application
- A comprehensive user model to contextualize activity from logs with user roles and privileges
- Session tracking to detect the user when user context is missing within activity logs
- Identity mapping for awareness of all physical and logical identities of a given user
- Identity adapters to populate the user model and leverage existing identity technology investments
- Tracking and escalation of users and systems to detect low and slow attacks
- Rules-based response automation at the network (port disablement, VLAN isolation) and user (account disablement) level to stop breaches, compliance violations, and fraud

The ArcSight SIEM Platform

The ArcSight SIEM Platform is an integrated set of products for collecting, analyzing, and managing enterprise event information. The ArcSight SIEM Platform is used across a wide variety of industries, including finance and insurance, to manage and monitor security, business risk, and compliance. The platform includes products for event collection, real-time event management, long-term retention, and compliance reporting. The logical layers of platform are described below.

Event Collection

For complete visibility into user and system activity, any financial institution will need to collect logs from a wide variety of sources and log formats including network devices, security devices, hosts, databases, and a range of homegrown and commercial applications. ArcSight Connectors solve the problem of managing log records in hundreds of different formats.

This unique architecture is supported across hundreds of commercial products out-of-the-box, as well as legacy systems which are widespread in the banking sector. ArcSight Connectors also offer various audit quality controls including secure, reliable transmission and bandwidth controls which are important considerations for bank branch offices. In addition to software-based deployments, ArcSight Connectors are available in a range of plug-and-play appliances that can cost effectively scale from bank branch office locations to large data centers. Connector appliances enable rapid deployment and eliminate delays associated with hardware selection, procurement, and testing.

Log Management

Connectors pass the data up to ArcSight Logger for efficient long-term storage, forensics, and compliance reporting. Once collected, the data is compressed and stored efficiently, but remains easily accessible for forensic searches and reporting. Financial institutions are subject to numerous regulations with distinct log retention requirements and ArcSight Logger can automate the enforcement.

ArcSight Logger is available in a range of performance options. At the high end, a single appliance can capture raw logs at rates of up to 100,000 events per second, can compress and store up to 35TB of logs, and can execute searches and reports at up to 3 million events per second—essentially eliminating the classic tradeoff between performance and efficiency imposed by other commercial or home grown solutions. A SAN-based variation of the appliance enables large banks to leverage their existing storage area network as the primary data store.

Event Management

The market-leading ArcSight real-time correlation engine, ArcSight ESM, provides advanced analysis of log event data to discover cyber-security threats, fraud, and compliance violations. ArcSight ESM uses a variety of sophisticated techniques to sift through millions of events to find the incidents that can have real business impact. ArcSight ESM also uniquely provides visibility into hidden patterns through its Pattern Discovery module. Through the application of mathematical algorithms over large log data sets, ArcSight enables discovery and visualization of low and slow, as well as unknown attack vectors. In turn, the patterns can be converted into correlation rules to detect future occurrences of suspicious activity that may represent a new fraud scheme or suspicious user behavior.

When ArcSight ESM finds a potential problem via event correlation, the optional guided response engine, ArcSight Threat Response Manager (TRM) provides administrators with workflow-driven advice for containing the problem. For example, if ArcSight ESM detects a broker accessing customer records of another broker without authorization, ArcSight TRM can determine which active directory account to disable, which VPN session to disconnect, etc. and then guide an administrator through the proper steps.

ArcSight IdentityView is a specialized solution module built on the ArcSight ESM capabilities. It is designed to enhance the value of identity-related technology investments by combining the broad activity collection and correlation capabilities within the context of user and role awareness.

Compliance Automation

Small and large banks alike are subject to numerous regulations across countries in which they operate. ArcSight Compliance Insight Packages enable financial institutions to rapidly address regulatory compliance audit requirements with pre-built content clearly mapped to specific regulations and based on best practices such as ISO 27002. ArcSight compliance solutions include real-time rules, as well as historical reports and dashboards to visualize compliance status. In addition to best practices that apply horizontally across regulations, ArcSight has purpose-built content for major regulations like Sarbanes Oxley and PCI which impact numerous banks.

Key Use Cases

The capabilities of the ArcSight platform described in the previous section enable a broad range of monitoring use cases relevant to banks. In fact, banks of all sizes and across the globe use the ArcSight SIEM Platform to address regulatory audit requirements and monitor their networks for continuous protection against internal and external threats and breaches. A few key use cases uniquely enabled by ArcSight for the banking industry are described in this section.

Customer Data Theft/Confidential Data Access

Client data, earnings data, and trading positions are stored in databases and accessed by applications. However DBAs responsible for managing the infrastructure can access the databases directly and use the information for

personal gain. ArcSight can be used to track confidential data access in the database and correlate that access with other actions, such as email or file transfers of the queried information. Through its unique ability to model roles and privileges, ArcSight can report on data access by job type, as well as access by roles that have no business need to query confidential data.

Privileged/At Risk User Monitoring

Privileged users have access to sensitive data and applications as part of their job definitions. These users include database administrators, network administrators, and client service staff. Such users can access confidential systems and also place fraudulent transactions. ArcSight can be used to track all activity by such privileged users, including building badge-ins and badge-outs, email sent, databases queried, and system rights changes. Using role monitoring, ArcSight can compare a user's activity to trends for other privileged users in the same role. For example ArcSight can monitor traders with high trading limits more closely for potentially abnormal transaction patterns.

Terminated User Activity

Due to mergers and acquisitions, financial firms are likely to have more turnover and therefore terminated users, both full-time employees and contractors. However, because of the network integration that mergers require, these same firms may have difficulty confirming that a terminated user is actually completely locked out of all systems. For example, is a particular ex-IT contractor accessing a specific Linux file server directly? ArcSight can compare a user's account status, as indicated in the human resources or identity management system, with activity on all servers in the IT environment. As a result, ArcSight can detect local system activity by users who should be locked out.

Shared Account Tracking

Many legacy applications have embedded generic accounts (e.g., "admin" accounts) that are shared across users. It is therefore difficult to determine who actually entered a specific application transaction and many people may be logged in simultaneously using the same shared ID. Due to regulations that require proper internal controls to be in place, the only option for many firms is to re-write/replace the application to remove embedded IDs. This may be very difficult, expensive, and in some cases impossible, due to other critical processes that may depend on the legacy application. ArcSight can correlate each user's local machine account and IP address with activity on the legacy system for complete accountability and attribution of activity to the correct user.

Online Fraud

Online fraud, especially as a result of account hijacking, is on the rise as organized criminals execute more sophisticated attacks. For example, credit card numbers can be stolen and used to execute many small transactions, draining the owner's credit limit. Or, a hacker may gain access to a user's online bank account and execute repeated wire transfers, draining the account without tripping any alarms. ArcSight can evaluate multiple risk factors, such as the country of origin, transaction country, or account status, etc. to generate a risk score for each transaction. This risk score can be used by bank fraud detection systems to block transactions or delay them for further examination.

Call Center Fraud

Call center fraud is another common problem in banking environments because of the outsourced, low wage, and contractual nature of employment. The normal pattern of activity for a CSR (customer service representative) is to access a single account during an incoming call from a customer. If a CSR accesses several accounts during an outbound phone conversation or a call that was not routed through the PBX pool, it may be a fraud indicator. ArcSight can detect such activity through correlation of logs across the phone system and the customer account application. This scenario can also be applied more generally to any third-party group (common in banking) that has access to customer data.

Multi-Channel Fraud

Multi-channel fraud is increasingly prevalent in banking environments and requires monitoring and correlating activity across customer touch points. For example, compromised bank accounts are often used to conduct basic reconnaissance, such as viewing old checks and signatures. Cyber-criminals then use that information to conduct a wire transfer or to withdraw money in person using forged signatures and blank checks. Often such online access is from a new location or a location not normally associated with the account owner. Such a deviation in the account usage pattern can trigger ArcSight to automatically place the account on a watch list for closer activity monitoring. A fraud alert can be generated when additional activity, such as a wire transfer or a withdrawal from a branch differing from recent withdrawal locations occurs.

Money Laundering

Money laundering is one of the common problems banks must tackle today and ArcSight can detect various forms of such activity. For example, if the bank account of an all cash business which normally receives two monthly deposits of $5,000 suddenly receives a significantly larger amount, it may suggest a problem. Alternatively, if money is transferred to accounts or banks in certain countries which are known money laundering havens, ArcSight can automatically raise an alert.

Compliance Automation

Although banks are already highly regulated, they continue to see increased oversight from new laws at a local, national, or trans-national level. Each of these regulations comes with its own requirements to demonstrate due diligence. ArcSight offers pre-packaged best practices content based on widely used frameworks, such as ISO 27002, to efficiently automate compliance across regulatory requirements.

Conclusion

Despite early adoption of security technology, the financial industry continues to account for a majority of data breaches because it is also the most lucrative target for identity theft, fraud, and cyber crime. The threat to banks and other financial institutions is significant from external sources as well as insiders. This challenge is only compounded by the multi-channel, distributed, legacy, and heterogeneous nature of bank IT infrastructure.

Effectively addressing those challenges in step with growing security and privacy-related regulatory oversight requires visibility into all activity on the network. Point technology investments, while valuable, have not given banks that visibility, and as this white paper demonstrates, the solution lies in continuous and automated monitoring of all user, system, and application activity. ArcSight offers a scalable, minimally intrusive, log-based monitoring platform optimized to address the monitoring challenges unique to financial institutions.

In the face of increased cyber-threat and commoditization, banks that can effectively combat breaches stand to build a strong brand, a competitive advantage, and to extract more value from their existing IT investments. Banks of all sizes and throughout the globe are successfully using the ArcSight SIEM Platform to achieve those goals.