White Paper

information security & technology • cybersecurity

enhance your cybersecurity now

What Your Institution Needs to Know to Mitigate Today's Cyber Threats

jack henry™

contents

introduction

You have most likely heard the quote, “A body in motion stays in motion, a body at rest stays at rest.” This is true for your cybersecurity program as well. Today’s banking security dilemma can be boiled down to three primary elements: the sophistication of threats, the complexity of IT environments, and the shortage of IT and InfoSec talent. This combination is eroding your institution’s abilities to protect consumer account information, corporate confidential data, and the availability of your computing infrastructure to serve your customers or members. The hard truth is that you are more exposed today than ever before. The good news is that there are new tools and practices being implemented to help.

It’s time to embrace today’s advances in technology to protect your institution from the pervasive and persistent cyberthreats. Over the last couple of years, we have seen the emergence of new technologies and capabilities that can counter the proliferation of malware and thwart cyberattacks. These technologies include UTM enhancements (Unified Threat Management), SIEM (Security Incident and Event Management), Machine Learning, Behavioral Analytics, and SOAR (Security, Orchestration, Automation and Response). This white paper will elaborate on this banking security dilemma and share with you how to embrace these new technologies to protect your institution against omnipresent cyberthreats and malware.

today’s banking security dilemma

sophisticated threats

According to CyberSecurity Ventures, damage related to cybercrime was projected to hit $6 trillion annually by 2021. A host of new and evolving cybersecurity threats has the information security industry on high alert. Ever-more sophisticated cyberattacks involving malware, phishing, machine learning and artificial intelligence, cryptocurrency, and more have placed the data and assets of financial institutions (FIs) at constant risk. One thing the experts agree on is that cybercrime is here to stay. In fact, as our dependence on technology continues to grow, it will get even worse.

According to CyberSecurity Ventures, damage related to cybercrime was projected to hit **$6 trillion annually by 2021.**

The recent “IntSights Financial Institutions Threat Landscape Report” shows an increase in attacks on FIs in 2019 over 2018. Below are some highlights from their report:

- 151% - in FI assets on the dark web.
- 135% - in the selling of online banking information and banking records on the black market.
- 91% - in targeted phishing attacks against FIs.
- 40% - in employee credential theft.

The nonprofit Information Security Forum, which describes itself as “the world’s leading authority on cyber, information security and risk management,” warns in its annual study of the cybersecurity landscape (Threat Horizon 2019) of increased potential for:

- **Disruption** – Over-reliance on fragile connectivity creates the potential for premeditated internet outages capable of bringing trade to its knees and heightened risk that ransomware will be used to hijack the Internet of Things.
- **Distortion** – The intentional spread of misinformation, including by bots and automated sources, causes trust in the integrity of information to be compromised.

Cybercriminals are successful in large part because many institutions are not carrying out due diligence in addressing the problems of business email compromise, phishing, spear phishing, ransomware, and other threats. The increasing sophistication of cyberattacks means stronger strategies are needed at FIs. Looking forward, we'll see a continued rise in malicious activity in the following areas:

Phishing Gets More Sophisticated

Phishing attacks, in which carefully targeted digital messages are transmitted to fool people into clicking on a link that can then install malware or expose sensitive data, are becoming more sophisticated. Now that employees at most institutions are more aware of the dangers of email phishing or of clicking on suspicious-looking links, hackers are upping the ante. For example, they're using machine learning to much more quickly craft and distribute convincing fake messages in the hopes that recipients will unwittingly compromise their institutions' networks and systems. Such attacks enable hackers to steal user logins, credit card credentials, and other types of personal financial information as well as gain access to private databases.

Ransomware Strategies Evolve

Ransomware attacks cost victims billions of dollars every year, as hackers deploy technologies that enable them to literally kidnap an individual or institution's databases and hold all of the information for ransom. The rise of cryptocurrencies like bitcoin is credited with helping to fuel ransomware attacks by allowing ransom demands to be paid anonymously. As institutions continue to focus on building stronger defenses to guard against ransomware breaches, some experts believe hackers will increasingly target other potentially profitable ransomware victims such as highnet- worth individuals.

State-Sponsored Attacks

Beyond hackers looking to make a profit through stealing individual and institution data, entire nation-states are now using their cyber skills to infiltrate other governments and perform attacks on critical infrastructure. Cybercrime today is a major threat, not just for the private sector and for individuals, but for the government and the nation as a whole. Going forward, state-sponsored attacks are expected to increase, with attacks on critical infrastructure of significant concern. Computer security giant McAfee has predicted that: "Nation-state cyberwarfare will become an equalizer, shifting the balance of power in many international relationships just as nuclear weapons did starting in the 1950s. Small countries will be able to build or buy a good cyber team to take on a larger country. In fact, cyberwarfare skills have already become part of the international political toolkit, with both offensive and defensive capabilities."

Third Parties (Vendors, Contractors, Partners)

Third parties such as vendors and contractors pose a huge risk to institutions, many of which have no secure system or dedicated team in place to manage these third-party employees. As cybercriminals become increasingly sophisticated and cybersecurity threats continue to rise, institutions are becoming more and more aware of the risk third parties pose.

The financial services industry today forms an important backbone of the world economy. The banking sector in particular is identified as one of the Critical Infrastructure Sectors by the U.S. Department of Homeland Security, which believes that the sector is so vital to the United States that "its incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." The banking sector is, by the nature of its business, a highly interconnected sector as well. Greater interconnectivity introduces greater cybersecurity risks given that (a) there are too many things to secure and monitor, and (b) the interconnected entities are likely connected to additional entities which could also be the source of cybersecurity risk. Add to this the fact that third-party vendors are an accepted reality today.

> Cybercriminals are successful in large part because many institutions **are not carrying out due diligence** in addressing the problems of business email compromise, phishing, spear phishing, ransomware, and other threats.

This increased reliance on third-party vendors has also meant added exposure to cybersecurity risks and vulnerabilities. Regulators and regulatory authorities have grown increasingly concerned about third-party vendor risk management practices, especially in the banking industry. While there have been several data breaches over the years where the thirdparty vendor was clearly at fault, more recent ones have shown that these still happen and will continue to. In April 2017, Scottrade Bank acknowledged a data breach that exposed the personal information of 20,000 of its customers because a third-party vendor uploaded a file to a server without adequate cybersecurity protections.

IoT Attacks

The Internet of Things is becoming more ubiquitous by the day (according to Statista.com, the number of devices connected to the IoT will reach almost 31 billion by 2020). It includes laptops and tablets, of course, but also routers, webcams, household appliances, smart watches, medical devices, manufacturing equipment, automobiles, and even home security systems. Connected devices are handy for consumers, and many institutions now use them to save money by gathering immense amounts of insightful data and streamlining businesses processes. However, more connected devices mean greater risk, making IoT networks more vulnerable to cyber invasions and infections. Once controlled by hackers, IoT devices can be used to create havoc, overload networks, or lock down essential equipment for financial gain.

complex IT environments

Technology is changing the way people live and work. While many of these changes are designed to make our lives easier, managing today's complex IT environment can be challenging. This is especially true for FIs. Cloud computing is gaining traction as a platform to help institutions keep pace. Cloud computing spans a range of classifications, types, and architecture models. The transformative networked computing model can be categorized into three major types: public cloud, private cloud, and hybrid cloud. The technology service can be accessed in various models and deployment strategies, including the most popular Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The underlying infrastructure architecture can take various forms and features, including virtualized, software-defined, and hyper-converged models, among others. Let's take a closer look at the three.

Public Cloud

Public cloud refers to the cloud computing model in which the IT services are delivered across the internet. The service may be free, freemium, or a subscription-based offering based on the computing resources consumed. The computing functionality may range from common services such as email, apps, and storage to the enterprise-grade OS platform or infrastructure environments used for software development and testing. The cloud vendor is responsible for developing, managing, and maintaining the pool of computing resources shared between multiple tenants from across the network. The defining features of a public cloud solution include high elasticity and scalability for IT-enabled services delivered at a low-cost, subscription-based pricing tier.

There are a couple of key challenges Institutions have in deploying public cloud solutions:

- Not the most viable solution for security and availability sensitive mission-critical IT workloads.
- Low visibility and control into the infrastructure, which may not suffice to meet regulatory compliance.

Private Cloud

Private cloud refers to the cloud solution dedicated for use by a single institution. The data center resources may be located on-premise or operated by a third-party vendor offsite. The computing resources are isolated and delivered via a secure private network and not shared with other institutions. Private cloud is customizable to meet the unique business and security needs of the institution. With greater visibility and control into the infrastructure, institutions can operate compliance-sensitive IT workloads without compromising on the security and performance previously only achieved with dedicated on-premise data centers.

There are many advantages for FIs to deploy private cloud computing solutions.

- Dedicated and secure environments that cannot be accessed by other institutions.
- Compliance to stringent regulations as institutions can run protocols, configurations, and measures to customize security based on unique workload requirements.
- High scalability and efficiency to meet unpredictable demands without compromising on security and performance.
- High SLA performance and efficiency.
- Flexibility to transform the infrastructure based on ever-changing business and IT needs of the institution.

Hybrid Cloud

Hybrid cloud refers to a cloud infrastructure environment that is a mix of public and private cloud solutions. The resources are typically orchestrated as an integrated infrastructure environment. Apps and data workloads can share the resources between public and private cloud deployment based on institutional business and technical policies around security, performance, scalability, and cost and efficiency among other aspects. For instance, institutions can use private cloud environments for their IT infrastructure and complement the infrastructure with public cloud resources to accommodate specific applications. A good example of this is the leveraging a private cloud computing provider to host your Microsoft Windows infrastructure while using a public cloud to host your institution's email with Microsoft Office 365.

Some key advantages of a hybrid cloud are:

- Flexible policy-driven deployment to distribute workloads across public and private infrastructure environments based on security, performance, and cost requirements.
- Scalability of public cloud environments is achieved without exposing sensitive IT workloads to the inherent security risks.

talent shortage

A war is raging for cybersecurity talent. The financial, government, and private sectors are scrambling for it. Thousands of information-security jobs are going unfilled as the industry in the U.S. struggles with a shortage of properly trained professionals. By one estimate, there were 3.5 million unfilled cybersecurity jobs by 2021. The talent problem is not new. The problem has become highlighted in the last five to 10 years with the increase in cyberattacks. Not only have cyberattacks grown in frequency and intensity, but also cybersecurity has risen to become a board-level issue. After the Target 2013 attack, boards and executives realized cybersecurity was a business issue and some started putting more money behind it. The aftermath is that everyone is hiring, all at the same time.

What has caused this rise in cyberattacks? There are a few variables. The first is the connectedness of everything, "IoT" – cars, refrigerators, TVs, etc. Then there's the monetary incentive for attacks – financial records, for example, sell for almost $150 per record. Add to that poor coding of products that leave them vulnerable to cyberattacks. Finally, the shortage of skilled and experienced security practitioners' forces companies to use less skilled and experienced IT personnel to try and protect sensitive data and intellectual property.

Cybersecurity Talent Shortage Is a Systemic Issue

The fundamental problem facing the skills gap, however, is there aren't enough people coming into the field to begin with. It starts and ends with education. Not enough interest is being generated at the middle school and high school levels in STEM. This leads to less graduates in technical disciplines, and less graduates in PhD-level technical disciplines. Cybersecurity should have been a bachelor of science degree 15 years ago. Today we're seeing this in some universities, but it's not enough.

These are all systemic issues needing systemic answers that could take years to resolve. Still, these shortage problems need to be addressed, and they won't be until we change how cybersecurity experts are hired, retained, and educated.

So now, we're faced with a set of problems:

- Lack of qualified staff. Finding skilled security engineers takes way too long. One report says it takes up to six months to find security engineers.
- Using under-skilled practitioners. When companies can't find qualified cybersecurity personnel, they're forced to use
- their existing IT/network teams. These teams generally don't have a "security first" mindset – they have an "availability first" mindset. Uptime is usually prioritized over security.
- Too many security tools. With the average enterprise using 45+ security-specific tools to protect data and intellectual property, understaffed security teams are forced to manage tool sets they don't know or understand.

The Implications for Business Resilience

Cybersecurity talent is hard to recruit and retain for every institution. Small institutions located in rural areas are struggling to find talent. While the talent pool is larger in metropolitan areas, institutions can find talent but are struggling to keep these employees, as the demand for talent outweighs the supply. The implications for business resilience are worrisome.

- Security positions are going unfilled for months. Unfilled positions lead to negative impact across the board: on productivity, customer service, security, innovation, speed to market, and profitability.
- Tools are not being used effectively. Support teams (usually not security teams) are installing,

managing, and monitoring security tools without the background to make them effective.

- Security oversight is lacking. Projects and products are being deployed without security oversight, leading to potential risks for their companies.
- Falling behind in cybersecurity training.
- The lack of skilled cybersecurity personnel is doing more than putting institutions at risk; it's affecting the job satisfaction of existing staff. This is a dangerous side effect that affects morale.

Talent Shortage Today and Beyond

Cybersecurity is obviously a job sector of the future. That's the good news. It's also the bad news. The main reason it's a job of the future is because the security risks of a connected world keep expanding and evolving. Hackers and bad actors will continue to go after our data and intellectual property. Without the right people (skilled and experienced) and the right tools, this problem will continue to grow. As you might imagine, we're fighting the war for cybersecurity talent every day.

combating today's cyberthreats

Traditional methodologies for protecting financial institutions (FIs) against cyberthreats become less effective over time. Addressing security in silos provides an incomplete picture, as it's difficult to gain visibility across the entire institution. Cyberattacks can often only be detected through a holistic view and analysis of events occurring on your network. It's more important than ever to gain a comprehensive view of your entire institution. Aggregation and correlation of events across all systems and networks provides management with better visibility of potential cyberthreats. More visibility leads to a better assurance that your security controls are effective, which will lower your risk profile and reduce your total cost to mitigate cyberthreats.

There have been several advancements in cyberthreat protection technology over the past few years that is just starting to make its way down to FIs. These solutions are documented below.

UTM (Unified Threat Management) Enhancements

UTM consolidates multiple security and networking functions with one unified appliance that protects institutions and simplifies infrastructure. Simplified security and networking capabilities in one box reduces the risk of cyberthreats. Recent advancements in the UTM security appliances have provided the ability to further protect your institution from cyberthreats and malware. These advances include SSL DPI, Sandbox Inspection, and DLP.

> Traditional methodologies for protecting financial institutions (FIs) against cyberthreats become **less effective over time.**

SSL DPI

Web and application-based traffic comprise a higher volume of total traffic, with much of that traffic including sensitive data. To accommodate this change, institutions are increasing their reliance on encryption, primarily secure sockets layer (SSL) and transport layer security (TLS), to protect their data in motion. It is estimated that over 72% of all network traffic is encrypted, and that figure is expected to grow. There are many benefits to this strategy, the most important of which is that it allows data, applications, workflows, and transactions initiated by both employees and consumers to travel wherever business requirements demand. In turn, this enables our global transition to a digital economy.

SSL DPI (Continued)

Although there are many benefits to encrypting internet sessions, such as protecting the privacy and integrity of personal information for data exchange, we are also seeing a less positive trend emerge as malware writers exploit this encryption capability as a way of hiding their attacks from firewalls. Not only can attackers bypass firewalls and capitalize on blind spots to sneak in malware that opens doors directly into any network, they are also using TLS/SSL to hide command and control traffic to manipulate compromised systems from virtually anywhere. Institutions not inspecting encrypted traffic are missing a lot of the value of their firewall systems. They are unable to view what is inside that traffic, spot malware downloads, identify harmful files, or see unauthorized transmission of privileged information to external systems. Unfortunately, very few security devices can inspect encrypted data without severely impacting network performance. This is rendering the UTM increasingly less capable of defending against threats, as encrypted data cannot be inspected. Encrypted traffic must be decrypted in order to be inspected.

SSL DPI (Secure Socket Layer – Deep Packet Inspection) has been available for a few years. SSL DPI supports the decryption of the data flow at UTM. Unfortunately, according to recent test results from NSS Labs, very few security devices can inspect encrypted data without severely impacting network performance. On average, the performance hit for deep packet inspection is 60%, connection rates dropped by an average of 92%, and response time increased by a whopping 672%. As a result, much of today's encrypted traffic is not being analyzed for malicious activity – making it an ideal mechanism for criminals to spread malware or exfiltrate data.

Over the past couple of years, UTM providers have released affordable UTMs capable of decrypting data at wire speeds without impacting performance. It's important to work with the manufacturer to size the UTM accordingly to enable SSL DPI without impacting performance and throughput.

Sandbox - Early Breach Detection

Sandboxing, also referred to as early breach detection, is fundamentally different from anti-virus. It goes beyond traditional malware defense by testing and inspecting the content on your network to recognize threats and help identify an attack or breach faster. The key difference in strategy offered by this unique tool is that rather than searching for a specific file, it safely tests the behavior of files in a separate emulation environment. Early breach detection alerts you of suspicious activity and provides advanced, detailed warnings. By testing files in emulation, even unknown malware can be detected. This helps to quickly recognize zero-day and advanced persistent threats. Leading UTM providers such as Fortinet and SonicWALL provide this functionality as part of their UTM devices. Just like SSL DPI, it is important to work with the manufacturer to ensure the UTM is sized correctly to support Sandboxing at wire speeds without impacting performance.

How it Works

The UTM examines incoming and outgoing network traffic and uses packet capture technology to find potentially harmful content. Files such as executables and macros are run in the sandbox environment that can safely emulate Windows®, Mac, or Office applications. Results of the testing are then analyzed by your security team or MSSP (Managed Security Service Provider) to find indications of malicious effects. Even highly targeted and evasive malware can be identified. Detailed information of the malware's behavior is obtained, which enables quick assessment and response. The goal is to detect malware and cyberthreats early, so your security professionals can take action.

The Power of Prevention

Zero-day threats can be especially pernicious because they are new and often unrecognized. Sandbox file testing creates a wall of protection against these and other dangers. In addition, if you leverage a MSSP, their team of skilled engineers are there to provide assistance 24/7.

What It Does

- Examines network traffic for potentially harmful malware. ests files in emulation to detect even unknown malware.
- Inspects endpoint data to identify behavior patterns that indicate a system compromise.
- Alerts your institution to the presence of malware.

What It Does for Your Institution

- Provides an additional layer of defense beyond traditional malware protection.
- Boosts your own security efforts with expert analysis and cutting-edge technology.
- Helps prevent damaging security breaches by reducing the time to discovery.
- Eases anxiety about zero-day and advanced persistent threats by bolstering your defense-in-depth strategy.

DLP (Data Loss Prevention)

UTMs also support data leak prevention (DLP). This functionality allows you to prevent sensitive data from leaving your network. When you define sensitive data patterns, data matching these patterns will be blocked, or logged and allowed, when passing through UTM unit. You configure the DLP system by creating individual filters based on file type, file size, a regular expression, an advanced rule, or a compound rule, in a DLP sensor and assign the sensor to a security policy.

Although the primary use of the DLP feature is to stop sensitive data from leaving your network, it can also be used to prevent unwanted data from entering your network and to archive some or all of the content passing through the UTM.

SIEM (Security Information and Event Management)

SIEM is an approach to security management that combines SIM (security information management) and SEM (security event management) functions into one security management system. Uptime is a mandate for today's digital business and end users don't care if their application's problems are performance- or security-related. The underlying principles of every SIEM system is to aggregate relevant data from multiple sources, identify deviations from the norm, and take appropriate action. For example, when a potential issue is detected, a SIEM might log additional information, generate an alert, and instruct other security controls to stop an activity's progress.

At the most basic level, a SIEM system can be rules-based or employ a statistical correlation engine to establish relationships between event log entries. Advanced SIEMs have evolved to include user and entity behavior analytics (UEBA) and security orchestration and automated response (SOAR).

You must use the functionality of today's advance SIEM to gain comprehensive visibility into your institution's network. Today, SIEM platforms use an architecture that enables unified data collection and analytics from diverse information sources including logs, performance metrics, SNMP Traps, security alerts, and configuration changes. They essentially take the analytics traditionally monitored in separate silos – SOC and NOC – and bring that data together for a more holistic view of the security and availability of the business. Every piece of information is converted into an event, which is first parsed and then fed into an event-based analytics engine for monitoring real-time searches, rules, dashboards, and adhoc queries.

SIEM - Machine Learning

Machine learning (ML) is a category of algorithm that allows software applications to become more accurate in predicting outcomes without being explicitly programmed. The basic premise of machine learning is to build algorithms that can receive input data and use statistical analysis to predict an output while updating outputs as new data becomes available.

The processes involved in machine learning are similar to that of data mining and predictive modeling. Both require searching through data to look for patterns and adjusting program actions accordingly. Many people are familiar with machine learning from shopping on the internet and being served ads related to their purchase. This happens because recommendation engines use machine learning to personalize online ad delivery in almost real time. Beyond personalized marketing, other common machine learning use cases include fraud detection, spam filtering, network security threat detection, predictive maintenance, and building news feeds.

With the flood of data available to us, FIs are turning to analytics solutions to extract meaning from the huge volumes of data to help improve decision-making. Predictive analytics companies that are attempting to optimize their security efforts need capabilities to analyze historical data and forecast what might happen in the future.

> Cyberattacks can often only be detected through a **holistic view and analysis of events** occurring on your network.

Looking at all the analytic options can be a daunting task. However, these analytic options can luckily be categorized at a high level into three distinct types. No one type of analytic is better than another, and in fact they co-exist with, and complement, each other. In order for a business to have a holistic view of the market and how a company competes efficiently within that market requires a robust analytic environment which includes:

- Descriptive Analytics, which use data aggregation and data mining to provide insight into the past and answer, "What has happened?"
- Predictive Analytics, which use statistical models and forecasting techniques to understand the future and answer, "What could happen?"
- Prescriptive Analytics, which use optimization and simulation algorithms to advise on possible outcomes and answer, "What should we do?"

Correctly implemented, your SIEM should use machine learning to detect UEBA without requiring an administrator to write complex rules. It should identify insider and incoming threats that would pass traditional defenses and create high-fidelity alerts to prioritize which threats need immediate attention.

SIEM - Applied Threat Intelligence

A threat intelligence feed (TI feed) is an ongoing stream of data related to potential or current threats to an institution's security. Intelligence, in the military and other contexts like business and security, is information that provides an institution with decision support and possibly a strategic advantage. Threat intelligence data feeds provide users with constantly updated information about potential sources of attack. To be impactful, a threat data feed should be specific to the vertical your company occupies. For FIs, the threat data must be related to the banking industry.

Five Common Reasons Why Threat Intelligence Can Fail the Security Team

1. *Misunderstanding the Value to the Business*
   What type of threat intelligence is important to the business? For example, are business problems being solved by a particular threat feed – or did someone subscribe to the threat intelligence service because the data looks interesting and the charts look cool? If the

intelligence isn't tied to a business problem, chances are, the service is a waste of money.

2. *Do I Have the Wrong Feed?*
There are many threat intelligence feeds available. For an FI, a feed consumed by community colleges may not be right for you. If you operate in particularly troublesome regions of the world, your needs are different from those of a company operating in a safer environment. Figure out what you need, and make sure you have the right coverage – and minimize redundancy. Seeing the same threat reported on two similar feeds doesn't make it twice as important. Getting too much information can be worse than having too little. If the feeds overwhelm your staff, too many false alarms and too many fire drills will cause them to lose interest…and perhaps miss something important.

3. *Focusing on the Wrong Thing*
Do you stay focused on the feeds themselves, or do you actually look at your entire collection of data as a result of ingesting the feed? It's not trivial to mash them all together. Do you have enough data and metadata? Are you missing the nugget that's going to give you the value you're looking for by heading off a real threat? Are you missing the connection/correlation? Consuming intelligence on a regular (real-time) basis is critical. Sorry, but just looking at the data once a week, or expecting automated alarms to catch all the hazards for you, won't cut it.

4. *Drowning in Too Much Data*
According to a recent study by ESG, nearly 74% of cybersecurity professionals surveyed already ignore security events and alerts because there's too much to consume. The teams can't keep up with the volume and end up with security data overload. We've discussed some of the causes already, and they include feeds that are intended for the wrong industries, wrong types of companies, and even for inappropriately sized security teams. Another cause is redundancy. Figure out what you need: Do you want raw data on threats and risks? Or do you want actionable intelligence that can help your teams set policies, fine-tune firewall rules, and comb your log files for patterns that match new attacks?

5. *Inability to Operationalize the Data*
About 65% of IT leaders surveyed by the Ponemon Institute said that threat intelligence could have prevented or minimized an attack on their institution. That's encouraging. 46% said the information is not well categorized according to threat type or attacker. Threat intelligence alone does not trigger a response to a breach. Yes, threat intelligence can help drive more tactical actions, but the security team needs to know what the nuances are, why they matter, and how to use the data to drive the necessary action. Some types of threat intelligence are perfect for correlating with existing data in a SIEM, and this makes for a great starting point. But a true proactive defense will involve the right tools, processes, and people. To put it another way: Tools and feeds alone are not sufficient. Effective threat intelligence processes that are aligned with the business are also required.

Your MSSP or internal security team must configure your SIEM to ingest and apply threat intelligence specifically designed for FIs to combat cyberthreats and malware. Having the correct feeds will provide you with a significantly increased level of security. Using the right threat intelligence sources will create a consortium effect that allow you to deliver a powerful reputational and behavioral based system capable of detecting even the most obscure breach attempts.

Intelligent feeds for the financial industry should include the following resources to glean threat intel:

FBI	FSISAC	UTM Provider
FireEye iSIGHT	US-CERT	SIEM Provider
NCFTA	3rd Party Security Vendors	DNS Monitoring

CVE - Common Vulnerabilities and Exposures | NCFTA – (The National Cyber-Forensics and Training Alliance)

SOAR

Most institutions have at least basic cybersecurity protocols in place, such as requiring strong passwords and controlling access to vital systems. Unfortunately, cybercriminals are evolving and using constantly shifting tactics to gain unauthorized access to private data. For years, many cybersecurity protocols were based on SIEM. To address the shortcomings of a SIEM approach more MSSPs are turning to SOAR (Security Orchestration and Automation), which offers an effective way to build on and augment your institution's SIEM systems. SOAR was developed by the research company Gartner and is a system that seamlessly combines three distinct cybersecurity approaches: Security orchestration and automation, security incident response platforms (SIRP), and threat intelligence platforms (TIP). SOAR allows institutions to not only collect large quantities of security data from a wide range of sources, like a patchwork of SIEM products does, it also provides a way to sort through and aggregate this vast amount of information in ways that both increase efficiency and make it easier for your cybersecurity team to quickly find the information they need.

Quality, Not Just Quantity

An effective response to a sophisticated cybersecurity attack is built on your cybersecurity team's ability to:

- Gain an in-depth understanding of the cybercriminal's tactics, procedures, and techniques.
- Identify which areas of your institution's cybersecurity defenses are being targeted and know what their potential weaknesses are.
- Have a solid plan already in place to address this particular type of cybersecurity incident.

Since SOAR is able to aggregate vast quantities of data, it is able to help your cybersecurity team quickly validate incoming intelligence and identify and prioritize important information. SOAR draws information from a wide variety of sources such as firewalls, SIEM, and intrusion detection systems so that your team can make more informed decisions and work quickly to identify and eradicate cybersecurity attacks.

More Efficient and More Effective with SOAR

Your cybersecurity team needs to be efficient in order to identify and respond to cybersecurity threats quickly. If your team needs to manage several different programs and spend time sorting through vast quantities of data, it slows them down and gives your attackers a distinct advantage. Another serious problem in cybersecurity is fatigue. Not only do cybersecurity teams at many MSPs need to monitor and maintain multiple systems, but a barrage of daily alarms can cause alert fatigue. Constantly switching between systems is a waste of both time and energy and increases the likelihood of mistakes. A SOAR approach allows your institution to automate many mundane and day-to-day tasks. SOAR filters incoming intelligence using AI and machine learning and delivers the relevant facts to your team in an easy-to-understand package.

This helps reduce the amount of context switching your team members need to do and can increase both productivity and efficiency. A team that has the tools to allow it to work at peak efficiency is able to catch more potential problems and handle incidents better without the need to hire more personnel. SOAR lets your team work smarter, not harder.

Improved Incident Responses

A rapid response is vital to minimizing the risk of breaches and limiting damage and disruption if a breach should occur. SOAR makes it easier for your cybersecurity team to detect threats early and respond quickly. SOAR also offers the ability to automate some response procedures, such as blocking IP addresses using a firewall or IDS system, suspending compromised user accounts, and quarantining infected endpoints. By automating these simple yet important tasks, SOAR frees up your team to deal with more pressing matters that require a human touch.

More Robust Reporting

Once an incident has been dealt with, many cybersecurity personnel are pulled away from their daily tasks to document the incident and generate reports. Since SOAR allows institutions to aggregate their intelligence, this means that your team will spend less time sorting through data. This reduces the amount of paperwork that needs to be done and can improve communication between frontline cybersecurity personnel, the C-suite, and other key players. This means that your team can focus on continuing to protect your institution's digital assets as well as create more comprehensive incident reports more quickly. SOAR is an effective way to streamline your cybersecurity response, give your team the tools it needs to improve efficiency, make their responses more effective, reduce the amount of time spent on incident reports, and improve communication between all key players and departments. If you are unsure how you can implement SOAR at your institution, you may want to reach out to a cybersecurity expert. Good cybersecurity experts will not only help you take stock of your current cybersecurity procedures and suggest improvements, they can also help you refine your response protocols and teach your team how to use new cybersecurity programs effectively.

security operations and engineering staffing

All the great security technology options discussed above are only as good as the people you have to run your security operations. Having the right people, performing the right tasks at the right time, is critical to your institution's ability to design, implement, maintain, and monitor your security. There are three security roles required to effectively implement the technology discussed in this whitepaper: Security Architects, Engineering, and Analysts. Security Architects and Engineers are responsible for developing, configuring, and implementing your institution's security infrastructure, including your UTMs and SIEM platform. Conversely, Security Operations requires analysts to perform the monitoring, alerting, and reporting of all security incidents and events.

Security Architect

A Security Architect is responsible for designing, building, testing and implementing security systems within an institution's IT network. A Security Architect is expected to have a thorough understanding of complex IT systems and stay up to date with the latest security standards, systems and authentication protocols, as well as best practice security products.

Security Architect Duties and Responsibilities

In addition to anticipating possible security threats and identifying areas of weakness in a network system, a Security Architect must respond promptly and effectively to possible breaches of security. A Security Architect job description generally includes:

- Reviewing current system security measures and recommending and implementing enhancements.
- Conducting regular system tests and ensuring continuous monitoring of network security.
- Developing project timelines for ongoing system upgrades.
- Ensuring all personnel have access to the IT system limited by need and role.
- Establishing disaster recovery procedures and conducting breach of security drills.
- Promptly responding to all security incidents and providing thorough post-event analyses.

As a senior member of the IT team, a Security Architect job description should also include cultivating a culture of security awareness and arranging continuing education of personnel to ensure security policies are adhered to at all times.

Security Architect Job Qualifications and Requirements

A degree in information technology, computer science, or related field is highly desirable. Some employers may require additional advanced security qualifications such as SABSA (Sherwood Applied Business Security Architecture) or CISSP (Certified Information Systems Security Professional) certifications. As well as formal qualifications, a Security Architect job description should include the following qualities:

- Extensive experience in information security and/or IT risk management with a focus on security, performance, and reliability.
- Solid understanding of security protocols, cryptography, authentication, authorization, and security.
- Good working knowledge of current IT risks and experience implementing security solutions.Experience implementing multi-factor authentication, single sign-on, identity management, or related technologies.
- Ability to interact with a broad cross-section of personnel to explain and enforce security measures.
- Excellent written and verbal communication skills as well as business acumen and a commercial outlook.

Security Engineer

Faced with an ever-increasing cybersecurity threats, institutions need to maintain a vigilant approach to protect their systems and data, and Security Engineers play a key role in this process. Security Engineers can be responsible for a number of functions associated with IT security – from ensuring the security of software, through to selecting and/or constructing and deploying broader network security systems. The security engineers are the resource required to implement and configure your institutions security systems.

Security Engineer Duties and Responsibilities

A Security Engineer job description should include the responsibility of completing a thorough risk assessment, identifying vulnerabilities within a network, and creating firewalls, or configuring systems to enhance existing security features.

Security Engineers are expected to respond to, and document, any security threats, resolve technical faults, apply and update system configurations and allocate resources to deliver real solutions. They must also be proficient in:

- Understanding complex technical issues and managing them within a fast-paced business environment.
- Maintaining all the software and hardware in relation to security.

- Documenting security certification.
- Identifying current and emerging technology issues including security trends, vulnerabilities, and threats.
- Applying threat intelligence.
- Sourcing and implementing new security solutions to better protect the institution.
- Conducting proactive research to analyze security weaknesses and recommend appropriate strategies.
- Liaising with vendors to implement security solutions.

Security Engineer Job Qualifications and Requirements

Holding an IT-related degree and a technical background is essential for a Security Engineer role. Individual institutions may have additional requirements for a Security Engineer, including security certifications such as CISSP, GISP, and CISM.

As well as formal qualifications, a Security Engineer job description should include the following qualities:

- Expertise across a variety of security products including firewalls, URL filtering, information security, and virus protection.
- The commercial acumen to provide cost-effective security solutions.
- An enthusiasm for staying up to date with the very latest updates about security threats and solutions.
- Outstanding communication skills that go beyond “tech talk” – the ability to translate complex IT matters to those without an IT background.
- Strong time management and organizational skills.
- Previous exposure to Linux and/or Windows operating systems, coding languages, and/or networks.

Security Analyst

A Security Analyst is responsible for ensuring the security of the FI’s information, making sure cybersecurity is being monitored, maintained, automated, improved, documented, and protected to the highest standard.

A person in this position must possess very good analytical skills, which are needed for triaging and investigating sophisticated security incidents. This role is suited for individuals with well-developed security documentation skills and a keen interest in automation.

Security Analyst Duties and Responsibilities

- Collect, analyze, interpret, and investigate event logs.
- Manage and execute multi-level responses on detected incidents.
- Involvement in incident response as needed.
- Documentation of tasks/processes in preparation for automation.
- Design & development of dashboards for metrics and reporting.
- Involvement in SOC automation and orchestration.
- Contributing to the implementation of security tools, architecture, and standards.

Security Analyst Job Qualifications and Requirements

- Proven experience analyzing, interpreting, and investigating security event logs with SIEM tools.
- Network security background/understanding (TCP/IP, routing, network intrusion methods, network containment, and segregations techniques).
- IDS and IPS experience.
- Experience with security orchestration and automation tools.
- Scripting experience is beneficial (Python, PowerShell, SQL).
- Excellent verbal and written communication skills.
- Great documentation skills.

summary

Today's consumers expect their assets and information to be available and secure 24/7. They trust your institution to protect and secure their finances against cyberthreats. It's imperative that your institution continues to invest in technology and people to meet this need. The "Security Dilemma" is real and you need to attack it head on.

For most institutions under 10 billion in assets, it is not practical to staff and retain qualified security professionals to mitigate today's pervasive cyber threat landscape. A MSSP should be engaged to augment your internal technology and security team. MSSP's can be an invaluable resource for institutions that want to maximize their network security but don't have the resources to build a large cybersecurity team internally. However, the choice to use managed security services should not be taken lightly. Institutions need to consider the benefits of managed security services (as well as their specific cybersecurity requirements) before choosing which MSSP to partner with. If you elect to use a MSSP, there are some critical requirements. Your MMSP must be staffed 24/7 and have a SOC II Audit performed annually. If they are focused on servicing FIs, they may be under FFIEC oversight. If so, you can request a copy of their ROE (Report of Examination). What are some managed security service benefits that FIs can leverage? Why should a FI use an outsourced network security team instead of an in-house one?

Here's a short list of some benefits of using managed security services:

- MSSPs have extensive cybersecurity knowledge and experience.
- MSSPs may use security tools In-House teams aren't familiar with.
- Using managed security services frees in-house IT for value-driven work.
- MMSPs help reduce the cost of labor for managing cybersecurity solutions.

connect with next-generation technology

Learn more about our cybersecurity solutions.

For more information about Jack Henry, visit jackhenry.com.