Building a Business-driven Financial SOC

CYBERBIT

PROTECTING A NEW DIMENSION

May 2017

Table of Contents

4 Towards a More Mature Financial Security Stance

5 Banks Have the Money

6 Challenges in the Cyber Climate

- Dynamic Threat Landscape
- Widening Attack Surface
- Business Goals Versus Security
- Information Overload
- Lack of Visibility into all Data
- Skill Shortage
- Insider/Outsider Threats
- Heterogeneous Products
- Multiple Procedures

10 Identifying the High-Risk Areas for Financial Services

- Dealing/Trading Rooms
- Third Party/Supply Chain Vendors
- Business Goals Versus Security
- ATM Skimming and Jackpotting
- Dormant/Orphaned Account Hijacking

11 Considerations for the Financial Services Security Team

- Reduce Time to Detect (TTD) and Time to Recovery (TTR)
- Face the Reality of The Skills Shortage
- Implement Efficiency Measures
- Understand the Importance of Self-Governance
- Investigate the Past to Understand the Future
- Involve Analysts in Ongoing Training Exercises
- Develop a Plan to Manage Crisis Effectively
- The Human Factor

13 Characteristics of the Business-driven SOC

One Platform

Big Data Collection and Correlation

Canonized Data Structure

Threat Intel and External Interfaces

Automation or Semi-Automation of Workflows

Anomaly Detection

Forensics

Access Control Monitoring

Knowledge Management

Analysis Engines

Collaboration Tools

Auditing and Change Management

14 The Business-driven Transformation

15 About Cyberbit

Towards a More Mature Financial Security Stance

In 2016, the financial services industry found itself occupying slot number three on the list of industries most targeted by cyber crime. Though it climbed down from the number one spot it had previously occupied, don't let the figures mislead you: Attacks against banks and financial services have not declined. On the contrary, they continue to grow in occurrence and sophistication, becoming more targeted with each iteration.

It's clear that protecting clients' confidential information and assets must be the top priority of every financial service company. It's really no wonder that security leaders are doing their best to compel the C Suite to pour whatever resources they can into creating a stable and strong infrastructure that cannot be breached.

But it seems as though there is little to show for all their spending as the financial industry continues to face a constant barrage of attacks. C-level executives are motivated to invest in tightened security but it can be difficult to clearly understand the bottom line value of security spending and know which actions to take to efficiently reduce risk to the organization.

It's high time to reassess the old methods. Security leaders in the financial services industry need to understand how attaining a higher level of security maturity will help further the goals of the business to facilitate understanding and collaboration between security teams and execs. And at the same time, reaching a heightened security maturity will help your organization become better fortified against attacks.

Banks Have the Money

The security operations center (SOC) of any financial institution, in truth isn't all that different than any other SOC. It is (under)staffed by overworked analysts who must tease out meaningful information from the myriad of tools they use to monitor, collect and process data. They must be able to see past the useless noise created as a byproduct of the multitude of security tools. And they need to relate the importance of their mission to the C suite who don't always quite understand how or why any of it is relevant.

This is where the similarities end;

As they say, "Banks are where the money is" and naturally, attackers won't stop until they get what they want. In fact, banks are attacked and breached often, with each incident costing on average $4 million according to the 2016 Ponemon Cost of Data Breach Study. Traditional defense methods have not deterred hackers, they have just prodded them to become more persistent and creative in their attack methods.

And as more financial institutions embrace new technological innovations to cater to customer's evolving digital habits, banks place themselves in an even more precarious position.

Challenges in the Cyber Climate

There are many factors that further contribute to an already complex security environment

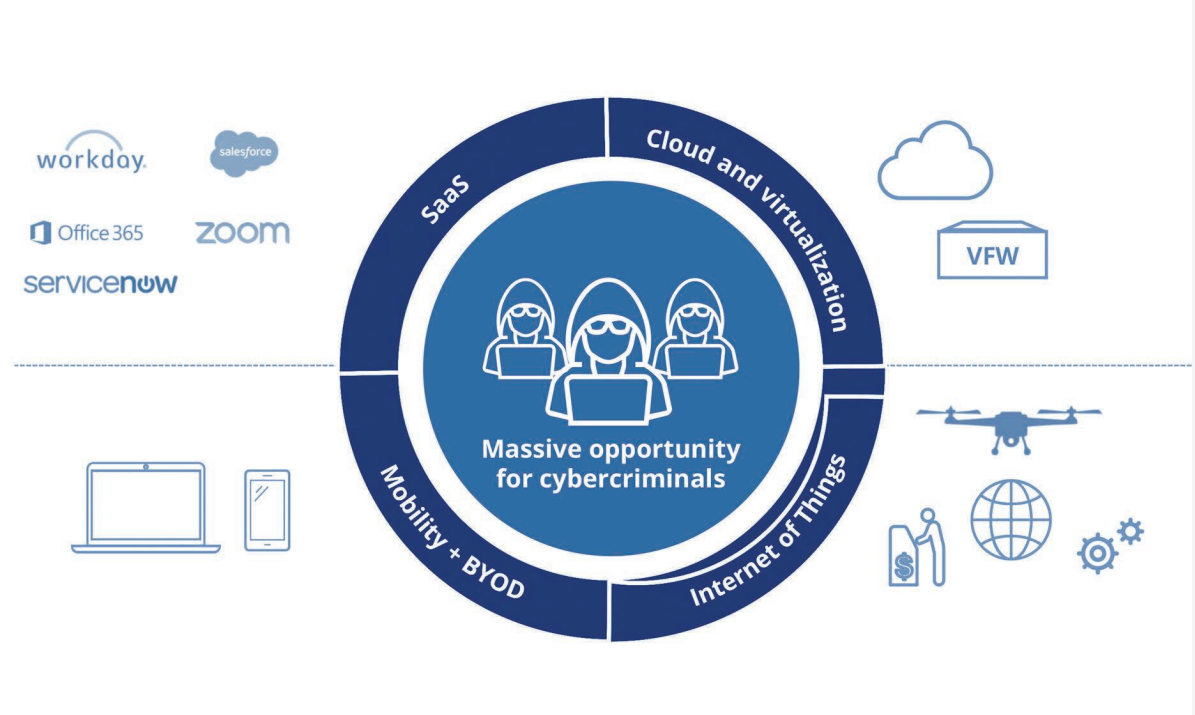
Dynamic Threat Landscape

Not only is the industry dealing with new and previously unknown malware threats like GozNym, the sophisticated trojan that's a combination of two already very potent pieces of malware, the attack model itself is changing. For example, though no bank is willing to admit it, 2016 brought with it amplified ransomware attacks perpetrated against financial institutions. We also saw attacks against Point of Sale (POS) vendors, ATMs and third parties such as the SWIFT terminal. Their eye on the prize, attackers can quickly pivot and find new ways to get what they want.

Widening Attack Surface

Today, attackers have their pick of many ways with which to launch their attack. Whether the entry point is via a phishing email sent to bank employees, via a vulnerability in a mobile banking app, or via a weakness in one of the bank's third party suppliers, these are all areas that serve as clear targets in an evolving and widening attack surface.

Tectonic Shift Creates the Perfect Storm



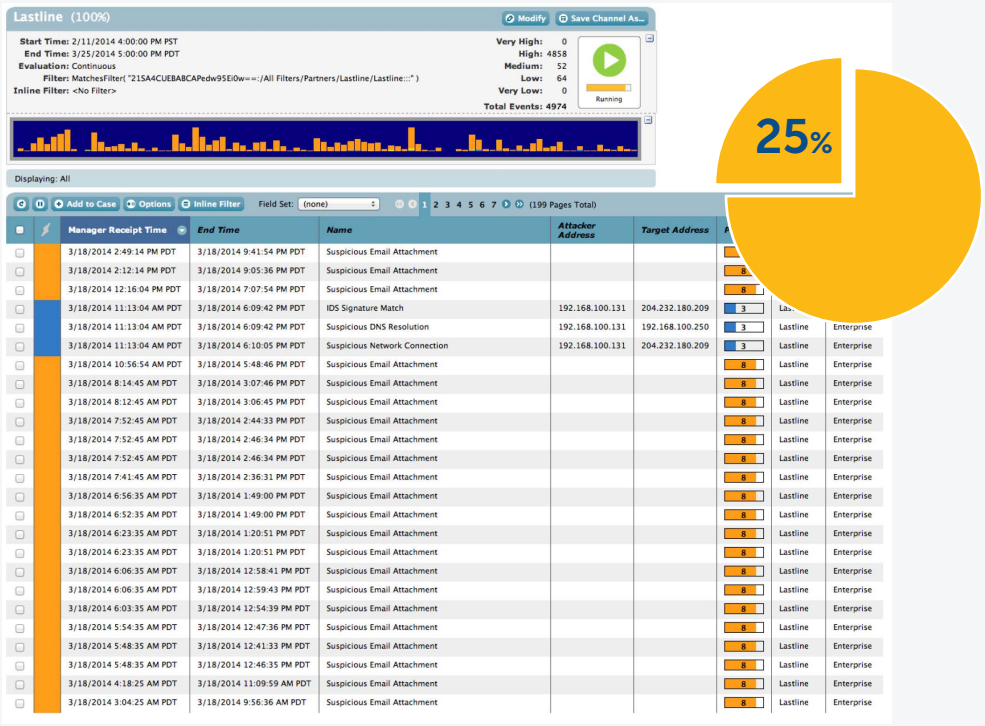
Business Goals Versus Security

The financial service C-suite usually has clear and mappable goals: to deliver services to customers at a profit and ensure customers will continue to select their bank/insurance company/investment fund, etc. over the competition. What the security team wants is to ensure the security and integrity of the bank's own information and that of its customers. Often these goals don't exactly align, with business leaders feeling that they are being unnecessarily restrained by the security team, preventing the company from being competitive.

Information Overload

With so many security tools and processes at work, each one creating additional alerts, it can be challenging to say the least for analysts to find the real correlation between events. This overabundance of noise leads to more busywork, more frustration and ultimately, more analysts who quit.

25% of security alerts not sufficiently investigated



Source:McAfee Labs Threats Report December 2016

Lack of Visibility into all Data

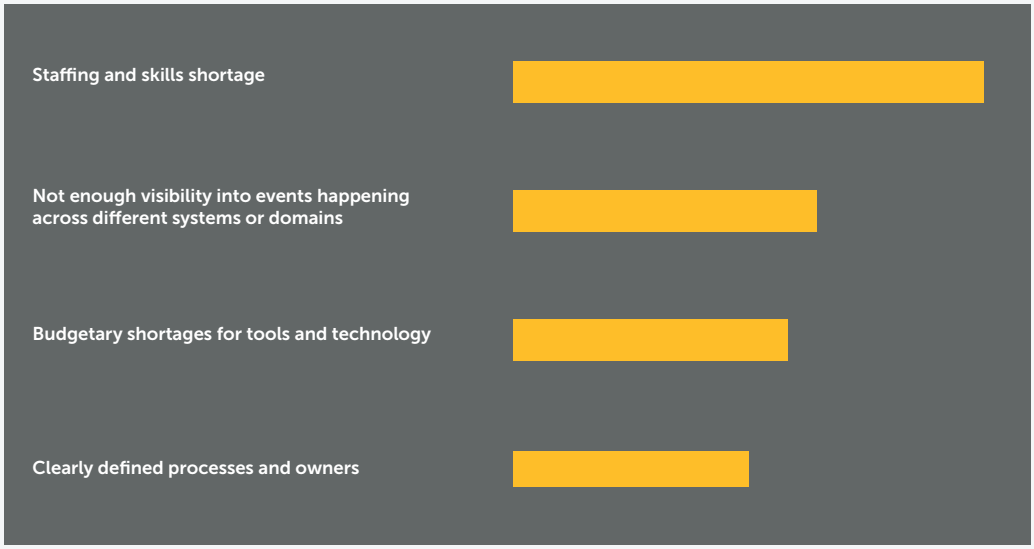
Security teams don't always have access to all the data they need to make fully informed security decisions. For example, there may be pertinent business data coming from sources like ATM transactions or the dealing room, but the security team might never get their hands on that data. This impairs their ability to make the best possible security decisions.

Skill Shortage

The security industry-wide skills shortage affects financial services just as much as any other industry but with all that's at stake in this setting, the consequences can be dire. And even accounting for all the newbies who are set to enter the field, there still won't be enough skilled professionals who can tackle an adversary as nefarious and agile as the ones the finance industry faces.

> *45% of organizations report a problematic shortage of cybersecurity skills today.*
>
> ESG Research

What do you believe are the key impediments to effective IR at your organization?



Source: "Hacking the Skill Shortage", CSIS and Intel Security, July 2016

Insider/Outsider Threats

All industries face threats from malicious actors. But when the stakes are high, morals often fall by the wayside. And nowhere are the stakes higher than in the financial services industry. Insider threats may come in the form of the disgruntled ex-employee or the star employee gone rogue. Outsiders can infiltrate by using privileges and learning patterns, adapting behavior to fly under the radar.

Heterogeneous Products

There are so many disparate tools and so many processes at work in the financial security center. They don't integrate smoothly with each other which creates crippling blind spots. This fragmented information lives in its own silo, leading to the cracks that events eventually fall through.

Multiple Procedures

Securing a bank or financial service is replete with complexities. The security team needs to keep considerations regarding compliance and regulations at the forefront at all times. They have to account for the growing involvement from the C Suite and relevant stakeholders. And they must be thinking about risk management at every stage.

Identifying the High-Risk Areas for Financial Services

Risks abound in Finance but some facets of the industry come with more room for potential vulnerabilities than others and these are the areas most lucrative for attackers. Pay special attention to the potential vulnerabilities that come from the following areas.

Dealing/Trading Rooms

As the central hub of all trading and dealing taking place, trading rooms present one of the greatest potentially vulnerable areas in any bank. In the quest to process more transactions with better precision, the trading room has typically become an early adopter of technology. There are many ways processes can be manipulated, for example via fictitious trades made via the automated system.

ATM Skimming and Jackpotting

ATMs may present banks and customers with a tidy way to conduct simple transactions but to hackers, they are a pot of gold waiting to be collected. The slow adoption of EMV technology, combined with lack of physical security and outdated and unpatched hardware and software means that they are easily breachable.

Skimming is a lucrative proposition for attackers, netting about $5000 to $100,000 per incident according to the ATM Industry Association (ATMIA). Skimming is simple to pull off; all a hacker needs to do is successfully insert an overlay on top of the real ATM reader which reads the information stored on the card's magnetic strip. And a new threat, dubbed Jackpotting, involves code that forces ATMs to spit out large amounts of cash in strategic locations where accomplices collect the plunder.

Third Party/Supply Chain Vendors

February 2016's series of attacks on the SWIFT Terminal sent shockwaves through the financial world and beyond. Though the terminal itself wasn't compromised, and rather, it was through valid credentials obtained by hackers that attackers were able to appear as if they were actual bank employees initiating transactions, the issue highlighted the very real problem of third party risks. Supply chain vendors often have VPN access to critical assets such as access to the mainframe, core finance applications and algo-trading platforms. Even if institutions themselves have done all they can on their end to ensure a solid infrastructure, vulnerabilities in third parties can have devastating effects. Remember, if they are vulnerable, so is your institution.

Dormant/Orphaned Account Hijacking

Dormant bank accounts or accounts with an undetermined owner can be manipulated by attackers with some insider help. That insider surreptitiously changes the status from dormant to active and initiates transfers that eventually reach the hands of the hackers.

Considerations for the Financial Services Security Team

We don't want to simply deal with the complicated financial services cyber attack climate. That's the approach organizations have been taking for years and clearly, that model isn't working too well. The goal should be for the SOC to evolve into a mature business unit that aligns the priorities of the security team with the overall priorities of the business.

Some key considerations that should be addressed on the journey to creating a mature business-driven SOC:

Reduce Time to Detect (TTD) and Time to Recovery (TTR)

We already know that it takes mere minutes to breach a network but it can take weeks to detect that breach. More time given to hackers in your network means more data and assets exfiltrated. Banks must invest more in detection and response to reduce the extent of damage.

Face the Reality of the Skills Shortage

The shortage of skilled analysts that exists across the industry isn't going to fix itself. The focus must shift from scouting highly seasoned analysts to join your team to utilizing the team and tools you already have more efficiently and effectively. A lower barrier to entry must also be adopted with an eye towards on-the-job training, to provide fresh-out-of-school analysts with the experience they need to withstand the myriad of challenges they will inevitably face.

Understand the Importance of Self-governance

The SOC takes the business's people, processes and technology into account, but there is another important facet that should be woven in throughout all of these elements: Governance, the process of ensuring that efficient and effective control and measurement mechanisms are being used to help people and processes achieve their organizational goals and responsibilities.

Investigate the Past to Understand the Future

Investigating historical logs helps analysts see clearly context of events and understand root causes with more accuracy. Logs help analysts build a complete and transparent picture from fragmented events that previously went unnoticed.

Develop a Plan to Manage Crisis Effectively

In the face of a crisis, having a predefined management plan to fall back on makes all the difference. And the CISO and security team will likely become the mouthpiece of that plan, delivering directives to the C Suite, stakeholders, board, IT team and managers. When a major breach happens, and it will happen, it creates full on organizational crisis that involves all executive management and several internal and external departments. Crisis management must be well planned and practiced to ensure the entire financial institution responds in an effective, coordinated manner.

Implement Efficiency Measures

It's important to ensure that the right measurement mechanisms are in place so we can find our less-efficient processes, predict where bottlenecks may occur and systematically route them out before they happen. When it comes to service level agreements (SLAs) with outside contractors, make sure to include metrics for: application response time, availability, help desk response time and a plan to address downtime. Delineate KPIs to make sure things are on track, and understand where processes can be automated or semi-automated to enhance speed and accuracy.

Ongoing Analyst Training Exercises

Analysts with real life experience fare much better in the face of crisis than those without. But thankfully, major events don't happen everyday, which can make it difficult for new hires to get the experience they need. This is where simulation training comes in. Analysts should train for events through a system of exercise and mentoring, where skills are continuously enhanced, refreshed and sharpened. It will help new hires get up to par faster while keeping veteran analysts engaged and aware of new developments.

The Human Factor

No organization can say that their people never make mistakes that can lead to breaches. Every malicious link that gets opened, every password that gets shared are all ways that attackers make their way into corporate networks. So it doesn't matter how many endpoint detection, mitigation or investigation tools your bank has installed; at the end of the day, it's the humans who must be aware. Periodic notices about best practices are not enough. Create opportunities for every user in the organization to practice good security habits and familiarize themselves with how to identify clever phishing emails and malicious websites.

Characteristics of the Business-driven SOC

Most security teams at financial services are entrenched in the world of SERP and SIEM-based SOCs. They are seeing their events without context and security runs counter to the business's overall goals.

Evolving from the SERP and SIEM based SOC is a change that won't and can't happen overnight - Gartner describes the evolution from a traditional SOC to a mature one as a five step journey and all levels build on the previous one. But with the right time, effort and direction, the business priorities and security priorities will become one in the same.

Let's look at the elemental building blocks needed to align security priorities with those of the entire business:

One Platform

A single frame that all tools plug into, providing one streamlined and accurate view at a glance.

Big Data Collection and Correlation

The ability to ingest and view all information coming off all data sources. Using big data analysis, teams can then sort, filter and draw meaningful conclusions from the information to understand correlation between events.

Canonized Data Structure

Provides the ability to normalize data from various sources to a structure in which it can be read, processed and analyzed by a single platform or algorithm. This way, data from multiple feeds or vendors can be correlated, compared or integrated by a single platform. As a result, users gain insights across the various feeds, channels and data source.

Threat Intel and External Interfaces

External feed to provide common information about threat behaviors, signatures or IOCs (indicators of compromise) from community resources or external vendors.

Automation or Semi-automation of Workflows

Provides analysts with recommended actions based on context and automates responses, allowing teams to control situations and improve speed, flexibility and effectiveness.

Anomaly Detection

Helps analysts detect and observe events that are not in line with expectations.

Forensics

Provides tools to uncover and interpret data effortlessly.

Access Control Monitoring

Monitors whether a certain entity may access a certain device, file or activate a process.

Knowledge Management

Manages the organizational knowledge and communicates it across the organization to keep everyone informed. For example, when encountering a similar incident to the one analyst may be dealing with now, it is worthwhile to know how it was handled previously, what worked well and what did not.

Analysis Engines

Programs and algorithms to produce insights and context from data. For example, behavioral analysis engines can process network and endpoint data to assess whether a security incident has occurred.

Collaboration Tools

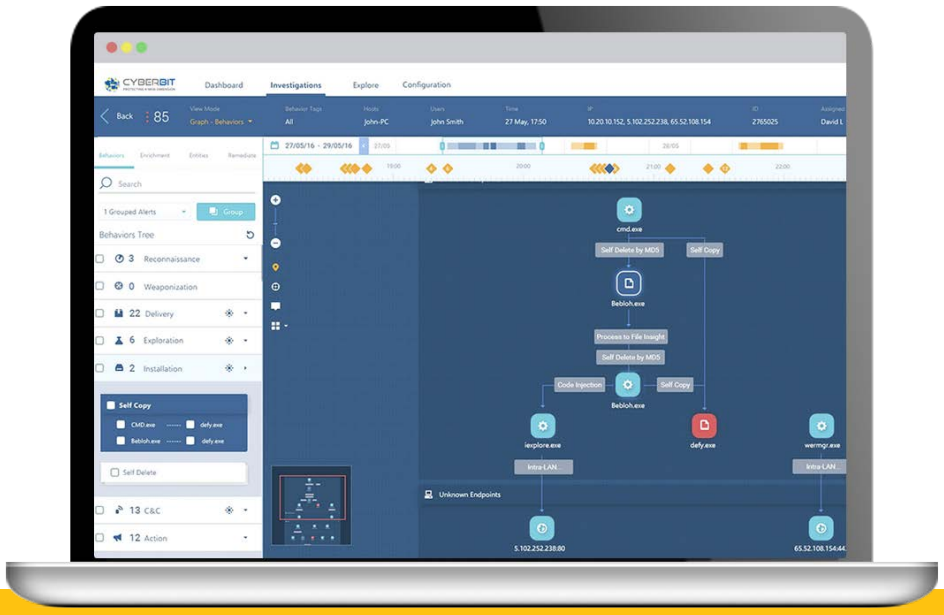
Sharing threat intel with others in the industry is critical to reducing the window of time it takes to curb attacks and threats. This is even more crucial in financial services since attackers will likely target several institution within the sector and where each additional moment attackers have in your system means greater loss.

Auditing and Change Management

Auditing capabilities assess various processes in the organization for compliance and certification purposes. For example, having systems in place that produce well defined dashboards and reports can significantly simplify and accelerate an auditing process.

Change management allows the security team to see if any settings have been changed and which members of the organization changed them. This helps keep tabs on movement across the organization.

Forensics - Cyberbit EDR



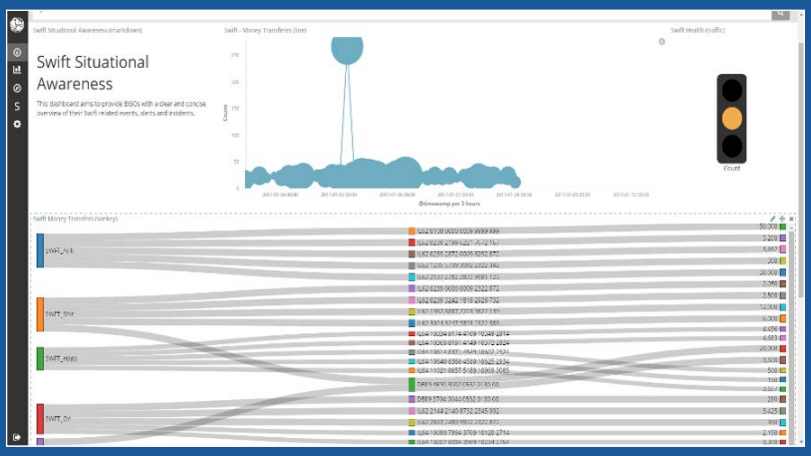
The Business-driven Transformation

Now it's time to take this knowledge and put it into action. Creating a plan of defense that will take your organization into the future depends upon turning your traditional, reactive SOC into one that furthers the overall goals of the business while adopting a risk-based and proactive security stance.

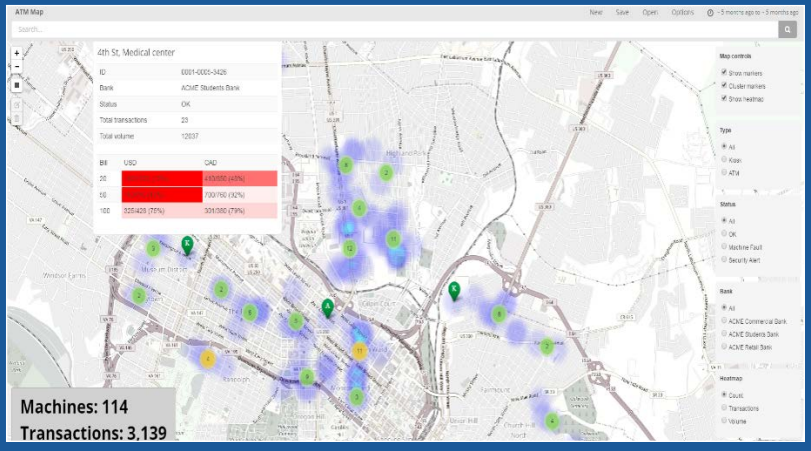
To evolve your SOC into a business-driven proactive one:

1. Understand/determine the business critical processes.
2. Create visibility for relevant data in order to implement the right controls for detection.
3. Engage relevant leaders throughout the business and build communication channels and a mitigation plan that involves both security and business stakeholders.
4. Run drills and exercises to make sure everything runs smoothly, everyone knows their job and can execute under pressure.

Monitoring business-critical processes



Visibility - ATM security status - Cyberbit SOC 3D



About Cyberbit

Cyberbit's battle-hardened cybersecurity solutions detect, analyze and respond to the most advanced, complex and targeted threats. A subsidiary of defense systems provider Elbit Systems Ltd. (NASDAQ: ESLT), Cyberbit has more than 500 personnel on three continents helping organizations protect sensitive assets and maximize security operations performance.

Cyberbit solutions empower enterprises to detect advanced threats in seconds, protect critical infrastructure, automate security operations center (SOC) workflows and train staff. With machine learning, big data and continuous technology advancements, Cyberbit maximizes protection against today's signature-less threats and arms organizations for tomorrow's new dimension of attack.

3800 N. Lamar Blvd.
Suite 200
Austin, TX 78756

Tel: +1.737.717.0385
info@cyberbit.net
www.cyberbit.net

CYBERBIT
PROTECTING A NEW DIMENSION