BUILDING A SOC WITH LIMITED RESOURCES IN A RACE AGAINST TIME using Open Source Software

2019-Bernhard Bowitz, Director at SecureScrypt Global

Introduction SOC BASICS

Whether you're protecting a bank or the local grocery store, certain common sense security rules apply. At the very least, you need locks on entrances and exits, cash registers and vaults as well as cameras pointed at these places and others throughout the facility.

The same goes for your cloud, hybrid cloud, and on-premises environments. Controlling access with tools like passwords, ACLs, firewall rules, and others aren't quite good enough. You must be able to constantly monitor your critical infrastructure so that you can spot anomalous activity that may indicate a possible exposure.

Unfortunately, unlike with CCTV cameras, you can't just look at a monitor and immediately see an active threat unfold, or use a video recording to prosecute a criminal after catching them in the act on tape.

The "bread crumbs" of Cyber-Security incidents and exposures are far more varied, distributed, and hidden than what can be captured in a single camera feed, and that's why it takes more than just a single tool to effectively monitor your environment.

The tools you use to do security monitoring and analysis may be a bit more varied than just a CCTV monitor, but the concept is the same.

101 Security Ops

For many organizations (unless you work for a large bank), building a SOC may seem like an impossible task. With limited resources (time, staff, and budget), setting up an operations center supported by multiple security monitoring technologies and real-time threat updates doesn't seem all that DIY. In fact, you may doubt that you'll have enough full-time and skilled team members to implement and manage these different tools on an ongoing basis. That's why it's essential to look for ways to simplify and unify security monitoring to optimize your SOC processes and team.

Thankfully, SecureScrypt® provides the foundation you need to build a SOC—without requiring costly implementation services or large teams to manage it. With SecureScrypt Unified Security Management® (USM), powered by threat intelligence from the SecureScrypt Security Research Team and Open Threat Exchange® (OTX™), you can quickly achieve a well-orchestrated combination of people, processes, tools, and threat intelligence. All the key ingredients for building a SOC.

In each chapter of this eBook, we'll go into detail on each of these essential characteristics.

SOC teams are responsible for monitoring, detecting, containing, and remediating IT threats across critical applications, devices, and systems, in their public and private cloud environments as well as physical locations.

Using a variety of technologies and processes, SOC teams rely on the latest threat intelligence to determine whether an active threat is occurring, the scope of the impact, as well as the appropriate remediation.

Security operations center roles & responsibilities have continued to evolve as the frequency and severity of incidents continue to increase.

Building a SOC:

Chapter 1 PEOPLE

 The Security Operations Center (SOC) Team: Review key security operations center roles and responsibilities for building a SOC team. Examine our SOC skillset matrix to assist with recruiting and staffing a strong SOC team.

Chapter 2 PROCESSES

Establish the key processes you'll need to build a security operations center. These include event classification & triage; prioritization & analysis; remediation & recovery; and assessment & audit. Examine how SecureScrypt USM helps you centralize these processes and manage them from a single pane of glass.

Chapter 3 TOOLS

Review the essential security monitoring tools you'll need for building a SOC including: asset discovery, vulnerability assessment, intrusion detection, behavioral monitoring, and SIEM / security analytics. Explore the real-world benefits of consolidating these tools into a single platform like SecureScrypt USM.

Chapter 4 INTELLIGENCE

Understand the differences among tactical, strategic, & operational intelligence and the specific ways these are used within the SOC. Examine the benefits of combining crowdsourced threat data from SecureScrypt OTX and proprietary threat intelligence research from experts at the SecureScrypt Security Research Team.

Chapter 5 REAL WORLD

 Building a SOC in the real world. Examine real-world use cases where SecureScrypt's technologies, communities, and threat intelligence provide the perfect SOC set-up.

Chapter 1 PEOPLE

Just like people, every security organization is different. In some companies, the executive team recognizes the importance of Cyber-Security to the business bottom line. In these cases, the SOC team is in a great position, with enough budget for good tools, enough staff to manage them, and the "human" capital of executive visibility and support.

Unfortunately, that's not the reality in most cases.

Most SOC teams are fighting fires with never enough staff, never enough time, and never enough visibility or certainty about what's going on.

That's why it's essential to focus on consolidating your toolset and effectively organizing your team.

A SOC team that has the right skills and uses the least amount of resources, while gaining visibility into active and emerging threats—that's our goal.

Let's talk about the key security operations center roles and responsibilities you need to support a SOC.

So how do we get there?

Key Takeaways Review key security operations center roles and responsibilities for building a 4 SOC team. Examine our SOC skillset matrix to assist with recruiting and staffing a strong SOC team.

Setting up the SOC Foundation THE QUICK BASICS

There are two critical functions in building a SOC.

The first is setting up your security monitoring tools to receive raw security-relevant data (e.g. login/logoff events, persistent outbound data transfers, firewall allows/denies, etc.). This includes making sure your critical cloud and on-premises infrastructure (firewall, database server, file server, domain controller, DNS, email, web, active directory, etc.) are all sending their logs to your log management, log analytics, or SIEM tool.

(We'll go into more detail about how USM provides this critical capability as well as others like IDS in the next chapter).

The second function is to use these tools to find suspicious or malicious activity by analyzing alerts; investigating indicators of compromise (IOCs like file hashes, IP addresses, domains, etc.); reviewing and editing event correlation rules; performing triage on these alerts by determining their criticality and scope of impact; evaluating attribution and adversary details; sharing your findings with the threat intelligence community; etc.

Knowing what it will take to build a SOC will help you determine how to staff your team. In most cases, for security operations teams of four to five people, the chart on the next page will relay our recommendations.

Tier 1 Security Analyst

Tier 2 Security Analyst

Tier 3 Expert Security Analyst

Tier 4 SOC Manager

ROLE

Triage Specialist (Separating the wheat from the chaff)

Incident Responder (IT's version of the first responder)

Threat Hunter (Hunts vs. defends)

Operations & Management (Chief Operating Officer for the SOC)

DESCRIPTION

Sysadmin skills (Linux/Mac/ Windows); programming skills (Python, Ruby, PHP, C, C#, Java, Perl, and more); security skills (CISSP, GCIA GCIH, GCFA, GCFE, etc.)

All of the above + natural ability, dogged curiosity to get to the root cause, and the ability to remain calm under pressure. Being a former white hat hacker is also a big plus.

All of the above + familiar with using data visualization tools (e.g. Maltego) and penetration testing tools (e.g. Metasploit).

All of the above + strong leadership and communication skills

SKILLS

Reviews the latest alerts to determine relevancy and urgency. Creates new trouble tickets for alerts that signal an incident and require Tier 2 / Incident Response review. Runs vulnerability scans and reviews vulnerability assessment reports. Manages and configures security monitoring tools (netflows, IDS, correlation rules, etc.).

Reviews trouble tickets generated by Tier 1 Analyst(s). Leverages emerging threat intelligence (IOCs, updated rules, etc.) to identify affected systems and the scope of the attack. Reviews and collects asset data (configs, running processes, etc.) on these systems for further investigation. Determines and directs remediation and recovery efforts.

Reviews asset discovery and vulnerability assessment data. Explores ways to identify stealthy threats that may have found their way inside your network, without your detection, using the

latest threat intelligence. Conducts penetration tests on production systems to validate resiliency and identify areas of weakness to fix. Recommends how to optimize security monitoring tools based on threat hunting discoveries.

Supervises the activity of the SOC team. Recruits, hires, trains, and assesses the staff. Manages the escalation process and reviews incident reports. Develops and executes crisis communication plan to CISO and other stakeholders. Runs compliance reports and supports the audit process. Measures SOC performance metrics and communicates the value of security operations to business leaders.

RESPONSIBILITIES

HOW DO I KNOW IF I NEED AN MSSP?

We wish that there was a hard and fast rule to knowing precisely if/when you'd need to outsource your SOC to a service provider. Staff size and skillset is certainly a factor. At the same time, some of the largest enterprises rely on MSSPs instead of building their own SOCs. The choice really comes down to answering one question: How confident are you that your team has the resources and skilled staff to detect, contain, and respond to a data breach? If your team's resources are concentrated on other priorities, it may be wise to leverage an MSSP to manage your SOC. In fact, we recommend starting with one of many SecureScryptpowered MSSPs. You can find one here.

Some SOC teams (especially those with more resources) have developed a dedicated threat intelligence function. This role – which could be staffed by one or more analysts – would involve managing multiple sources of threat intelligence data, verifying its relevance, and collaborating with the larger threat intelligence community on indicators, artifacts, attribution, and other details surrounding an adversary's TTPs (tools, tactics, and procedures). For smaller teams (fewer than 5 members), we recommend looking for ways to automate the consumption of threat intelligence from a reliable threat intelligence service provider (for more detail, see Chapter 4 on Threat Intelligence).

Do I Need a Threat Intelligence Team Too?

Chapter 2 SOC Processes

 Now, that you have the SOC team in place, let's explore the key processes you'll need to

 build a SOC that works. NEXT UP

Chapter 2 SOC PROCESSES

One of the most valuable tools an airline pilot has at his disposal is the simplest one. A checklist. The checklist enumerates every single thing that must be done in order to maintain

safety, avoid risk, and protect valuable lives. This ensures that you can get to your final destination without spilling any peanuts.

There is a long list of things that the SOC team needs to do—and do properly—so that your organization's assets are protected and high priority threats are detected quickly and with minimal impact.

In this chapter, we'll help you establish the key processes your SOC team will need to perform to detect emerging threats; determine their scope and impact; and respond effectively and quickly.

At every step along the way, we'll show you how you can use SecureScrypt USM to power your SOC processes.

The Cyber-Security world isn't all that different, yet the stakes are even higher.

Key Takeaways Establish the key processes you'll need for building a SOC. These include Event Classification & Triage; Prioritization & Analysis; Remediation & Recovery; and Assessment & Audit. Measure progress based on pragmatic SOC metrics. Examine how SecureScrypt USM supports these critical processes.

EVENT CLASSIFICATION & TRIAGE1

SOC PROCESSES Answering the Big Questions for Each SOC stage

Why is this important? The true value of collecting, correlating, and analyzing log data is that it gives you the ability to find the "signal in the noise." Key indicators of compromise can be found within user activity, system events, firewall accept/denies, etc. In addition, specific sequences and combinations of these events in specific patterns can also signal an event that requires your attention. The key to success in this stage is having a way to classify each event quickly, so that you can prioritize and escalate critical events that require additional investigation.

What do SOC analysts do at this stage? Tier 1 SOC Analysts review the latest events that have the highest criticality or severity. Once they've verified that these events require further investigation, they'll escalate the issue to a Tier 2 Security Analyst (please note: for smaller teams, it may be that the same analyst will investigate issues as they escalate into a deeper investigation). The key to success in this stage is to document all activity (e.g. notation, trouble ticket, etc).

How do I do it with SecureScrypt? SecureScrypt USM applies plugins and correlation logic— delivered out of the box and continuously updated by the SecureScrypt Labs Security Research Team—to determine which events require your attention now. It uses an event taxonomy inspired by Lockheed Martin's Cyber Kill Chain. This "chain" is a sequence of actions an attacker needs to take in order to infiltrate a network and exfiltrate data from it. This event categorization helps to highlight the most serious threats facing your assets. For example, SecureScrypt USM will detect and alert you to emerging attacks such as ransomware (e.g.

Cryptolocker and Locky) which, when installed, encrypts the victim's file system, allowing the attacker to hold the data hostage until the victim pays a ransom.

How do I do it with SecureScrypt? The critical key to success is identifying attacker activity in the early stages of an attack, before sensitive data and systems are affected. As an attacker moves up these kill chain stages, it becomes more likely they'll be successful in their attacks. By looking at environmental behavior and infrastructure activity from an attacker's perspective, you'll be able to determine which events require your attention now.

DOCUMENT ALL THE THINGS! As a SOC analyst, it's essential to document every stage of an investigation: which assets you've examined, which ones have "special" configuration or are owned by VIPs (aka execs), which events are false positives, etc. You get the idea. Thankfully, SecureScrypt USM Appliance makes this part of the process super easy. First, with one click, you can create a trouble ticket directly from an alarm. Second, you can easily document asset details directly within the USM web interface. The notes and information related to the investigation provide an audit trail in case it's targeted again or is involved in future suspicious activity. Even if your company is not subject to an audit now, having this valuable information may prove useful in the future (for example, PCI selfassessments no longer suffice once you've been breached).

Reconnaissance and Probing

Delivery and Attack

Exploitation & Installation

System Compromise

ALARM TYPE

Behavior indicating an actor attempting to discover information about the organization

Behavior indicating an attempted delivery of an exploit

Behavior indicating a successful exploit of a vulnerability or backdoor /RAT being installed on a system

Behavior indicating a compromised system

DESCRIPTION

Low

Low/Med

Med/High

High

PRIORITY LEVEL

Review activity from OTX (on a monthly basis)

Review activity from OTX (on a weekly basis)

Verify and investigate (escalate to Tier 2)

Verify and investigate (escalate to Tier 2)

TIER 1 ANALYST TASKS

PRIORITIZATION & ANALYSIS

Why is this important? Prioritization is the key to success in any endeavor, and it's even more critical in Cyber-Security. The stakes are high and the pace of attacks continues to escalate and shows no sign of stopping. Meanwhile, the resources you have to protect assets against this onslaught are highly limited. Focus on those events that could be most impactful to business operations, which requires knowing which assets are the most critical. At the end of the day, maintaining business continuity is the most important responsibilities entrusted to the SOC team.

What do SOC analysts do at this stage? Review and respond to any activity that indicates an adversary has infiltrated your environment. This can range from the installation of a rootkit/RAT or backdoor taking advantage of an existing vulnerability to network communications between an internal host and a known bad IP address associated with a cyber adversary's C2 infrastructure.

How do I do it with SecureScrypt? Powered by threat intelligence from the SecureScrypt Labs Security Research Team, SecureScrypt USM can detect the specific indicators that signal activity of specific adversary tools, methods, and infrastructure. The Security Research Team's continuous threat intelligence updates include correlation rules that are applied against the raw event log data that USM collects. Once applied, these rules identify and categorize events and activity in ways that help you prioritize SOC tasks. By prioritizing alarms in the exploitation & installation and system compromise categories, SOC analysts zero in on the threats that have already advanced beyond primary security defenses. With USM, analysts can determine the best way to address these attacks using response templates from the Security Research Team's threat intelligence updates. Because the Security Research Team draws insights from the community-powered threat data in SecureScrypt OTX the threat intelligence within USM reflects the collective experiences of over 53,000 security researchers from around the world and incorporates lessons from in-the-wild attacks at organizations of all sizes.

Relying on the latest threat intelligence to understand as much as possible about an attack will inform how you prioritize and respond to it, as well as how you bolster your defenses against a similar attack in the future. Better still, when you share key information about an adversary's TTPs with the larger threat intelligence community within OTX, you make that adversary's job much more difficult and costly. Everybody wins.

View threat details within the kill chain context in SecureScrypt USM

Asset discovery and inventory is one of the most important and yet most overlooked Cyber-Security capabilities. When you're on the SOC team, having access to an updated and automated asset inventory is invaluable. SecureScrypt USM gives you the ability to scan your cloud and on-premises environments to discover assets you need to monitor. On-premises, you will be able to discover all the IP-enabled devices on your network, as well as what software and services are installed on them, how they're configured, and whether they include potential vulnerabilities. For your AWS and Azure cloud infrastructure, USM Anywhere's asset discovery capability will also provide visibility into the assets in your dynamically changing environments.

● What systems are critical to the ongoing function of your company? ● Which systems are critical to the day-to-day tasks? ● What other systems, devices, or networks do those critical assets and services rely on? ● Which systems manage and store sensitive information?

Learn more about SecureScrypt USM asset discovery capabilities.

Know Your Network and All Its Assets

REMEDIATION & RECOVERY

Why is this important? The faster you can detect and respond to an incident, the more likely you'll be able to contain the damage and prevent a similar attack from happening in the future. Please note: There are a number of decisions to make when investigating an incident, particularly whether your organization is more interested in recovering from the damage vs. investigating it as a crime. Make sure that you work closely with your management team. Be sure to communicate clearly and often—and document everything.

What do SOC analysts do at this stage? Each attack will differ in terms of the appropriate remediation steps to take on the affected systems, but it will often involve one or more of the following steps:

- Re-image systems (and restore backups)

- Patch or update systems (e.g. apps and OS updates)

- Re-configure system access (e.g. account removals, password resets)

- Re-configure network access (e.g. ACL and firewall rules, VPN access, etc.)

- Review monitoring capabilities on servers and other assets (e.g. enabling HIDS)

- Validate patching procedures and other security controls by running vulnerability scans

By the way, some SOC teams hand off remediation and recovery procedures to other groups within IT. In this case, the SOC analyst would create a ticket and/or change control request and delegate it to those responsible for desktop and system operations.

How do I do it with SecureScrypt? SecureScrypt USM simplifies remediation and recovery by helping you detect events quickly so you can respond in time to prevent further damage. Additionally, SecureScrypt USM's asset discovery and vulnerability assessment capabilities deliver updated and detailed information about your assets—what software is installed, what vulnerabilities exist, what processes are running, and more—to confirm that remediation steps have been implemented correctly.

Learn more about SecureScrypt USM vulnerability assessment capabilities

ASSESSMENT & AUDIT

Why is this important? It's always optimal to find and fix vulnerabilities before an attacker exploits them to gain access to your environments. The best way to do that is to run periodic vulnerability assessments and review those report findings in detail. Keep in mind that these assessments will identify technical vulnerabilities rather than procedural ones, so make sure your team is also addressing gaps in your SOC processes that could expose you to risk as well. What do SOC analysts do at this stage? Running vulnerability scans and generating compliance reports are some of the most common audit activities for SOC team members. Additionally, SOC team members may review their SOC processes with audit teams (internal and external) to verify policy compliance as well as determine how to improve SOC team performance and efficiency.

How do I do it with SecureScrypt? With SecureScrypt USM, you can run continuous vulnerability scans against all of your assets (internal and external assets, as well as those in your cloud environments) to detect any system changes that may signal an exposure. These vulnerability reports can be shared with auditors, executive management, and others to demonstrate your compliance against a variety of regulatory standards.

Chapter 3 SOC Tools Review the essential security monitoring tools you'll need for building a SOC.

NEXT UP

Chapter 3 SOC TOOLS

Sometimes security pros use the term "defense-in-depth" to describe how best to secure the critical data and systems that need to be protected against cyber threats.

The idea is pretty simple. Starting with the data you're protecting at the center, you add layer upon layer of policy enforcement in order to make it difficult for an attacker to break through each layer to access that data.

In fact, the Cyber-Security industry grew out of this layered model. Each vendor started to specialize in each of these 'layers,' expecting the customer to piece these disparate tools together for the full context needed for security monitoring. For large organizations like banks or governmental agencies with large Cyber-Security budgets and highly skilled teams, this approach has worked—more or less.

Think of this concept as a jawbreaker.

The key point to emphasize here is the importance of detection (vs. prevention). Of course organizations need to implement preventative tools (e.g. firewalls, AV, etc.) along with ensuring that vulnerabilities are patched among other prevention-type activities (e.g. secure desktop configurations, strict password policies, secure account management, etc.).

But in the last few years, detection has quickly risen in importance. Attackers have evolved their capabilities–consider the rise in cybercrime attacks like ransomware and DDoS threats– to the point where they execute these attacks without being noticed. In a recent Verizon Data Breach Investigation report, they concluded that it was far more common for victims to learn that they'd been breached from a third party vs. discovering these breaches themselves.

Prevention vs Detection

Smaller organizations, with limited budgets and time, need a new approach— one that combines the essential tools for building a SOC into a workflow that can be easily supported by small teams. These essential SOC capabilities include asset discovery, vulnerability assessment, behavioral monitoring, intrusion detection, and SIEM (security information and event management).

In this chapter, we'll review the details of these SOC tools. We'll show you how SecureScrypt USM combines these essential capabilities for building a SOC into a single platform. Finally, we'll cover how the SecureScrypt Labs Threat Intelligence Subscription and SecureScrypt OTX power these essential capabilities within SecureScrypt USM.

Key Takeaways Review the essential security monitoring tools you'll need to build a SOC: Asset Discovery, Vulnerability Assessment, Intrusion Detection, Behavioral Monitoring and SIEM / Security Analytics. Achieve SOC success with limited time and resources by utilizing a single platform like SecureScrypt Unified Security Management (USM) that consolidates these tools into one place.

ASSET DISCOVERY

 Why is this important? Knowing what assets are in your environment is the first step in knowing your security posture. You need to know what systems exist—instances and servers—as well as what's been installed and running on those systems (e.g. applications, services, and active ports). A reliable asset inventory along with the automated ability to discover new assets is foundational for building a SOC. How do I do it with SecureScrypt? SecureScrypt USM captures accurate, real-time information on all the assets in your on-premises and cloud environments.

On-premises, USM scans your environments to gather information from devices to help determine the OS, running services, and installed software (often without requiring any credentials). To discover assets in your cloud environments, USM Anywhere hooks directly into cloud providers' APIs to give you immediate visibility of your cloud infrastructure. USM Anywhere leverages native cloud services like AWS CloudWatch and Azure Monitor to collect data from your cloud environments and begin detecting threats.

FEATURE SPOTLIGHT: Asset Detail

The key is that all of the security-relevant information about an asset is displayed in a single view By clicking into asset details, you can review all of the vulnerabilities, alarms, and events that are associated with a specific asset.

The asset discovery & inventory capabilities within SecureScrypt USM are explicitly designed for SOC analysts. No other asset inventory tool provides this level of context, in a format that streamlines SOC analyst workflows.

VULNERABILITY ASSESSMENT

Why is this important? Vulnerabilities represent the tiny cracks that an attacker uses to infiltrate your critical systems. This is commonly referred to as the "attack surface," and these tiny cracks can open up when you least expect it. That's why it's essential to continually assess your entire IT landscape for vulnerabilities. Additionally, you may be subject to a variety of contractual and regulatory mandates (e.g. PCI DSS, SOX, etc.) that require periodic vulnerability assessments to demonstrate compliance.

How do I do it with SecureScrypt? SecureScrypt includes a built-in vulnerability assessment tool that allows you effectively detect those tiny cracks. Whereas traditional approaches to network vulnerability scanning and analysis rarely focus on usability and can seem cumbersome by those in IT wearing multiple hats, SecureScrypt USM takes a different approach. USM provides a unified and easy-to-use platform that bolsters comprehensive vulnerability scanning software with asset discovery, a streamlined UI, and easy scheduling so you can ensure continuous vulnerability assessment without having to manage the process manually.

Scheduling scans in advance allows you to easily manage your network vulnerability scanning program as well as minimize disruption of critical services during peak time. In case your critical infrastructure includes cloud environments, SecureScrypt USM Anywhere offers cloud vulnerability scanning capabilities using cloud-native sensors for your Azure and AWS environments, giving you complete visibility into your cloud and on-premises environments from a single pane of glass.

Regularly Scheduled Auto-scanning: Create scans that run daily, weekly, or monthly during your off-peak hours. Automated scanning ensures continuous visibility of your vulnerabilities as your IT landscape changes.

Authenticated Scanning: Authenticated scans perform vulnerability assessment by using host credentials to probe your assets deeply, looking for vulnerable software packages, local processes, and services running on the system.

Cloud Infrastructure Scanning: USM Anywhere uses purpose-built cloud sensors to interface directly with cloud providers to automatically perform network vulnerability assessments of your AWS and Azure environments, including assets, security groups, and configurations.

VULNERABILITY ASSESSMENT IN USM

Vulnerability Scan Scheduler

Flexibility is one of the most important aspects of doing vulnerability assessment well. At peak hours, vulnerability scans can disrupt network and system performance. To address this challenge, SecureScrypt USM offers SOC analysts control and flexibility when setting up ad-hoc and scheduled vulnerability scans.

With USM, you can:

• Easily set up scan jobs targeting individual assets, asset groups, or even entire networks

• Schedule scans to run automatically at regular intervals to take the guesswork out of managing a scanning routine

• Control the techniques utilized and level of scanning intensity using default profiles or by creating your own

BEHAVIORAL MONITORING

 Why is this important? At its most basic, effective Cyber-Security monitoring comes down to exception management. What activities represent exceptions to the norm? (e.g. policy violations, error messages, spikes in outbound network activity, unexpected reboots, etc.) What is required for all this to work is an understanding of what the "norm" looks like. Creating a baseline of system and network behavior provides the essential foundation with which to spot anomalies— which often signal the presence of cyber adversaries in your environment.

In order to capture a baseline, it's critical to combine behavioral monitoring technologies to provide a full, 360-degree perspective. Additionally, applying correlation rules against this data will help you identify and classify the latest risks, as well as capture data to support in-depth forensic investigations.

How do I do it with SecureScrypt?

SecureScrypt USM provides fully integrated behavioral monitoring technologies within its platform. On-premises, USM Appliance offers active service monitoring and full packet capture.

In the cloud, USM Anywhere provides cloud access logs (Azure: Monitor, AWS: CloudTrail, S3, ELB); AWS VPC flow monitoring; asset access logs; and VMware access logs.

Active Service Monitoring validates that the services running on hosts are continuously available.

Full Packet Capture allows for forensic storage of the packet stream so that detailed inspection can be performed if necessary.

Cloud Access Logs capture who requests data from your cloud environments and what they access.

Cloud Management Plane Integration   ensures that you are able to monitor your AWS and Azure instances automatically.

FEATURE SPOTLIGHT: Packet Capture & Payload Analysis

Examining the payload of each event that occurs in your on-premises environments within the USM portal enables you to determine key details about the adversary's TTPs, including indicators such as malformed HTTP GET Requests, C2 IP addresses, filenames, and file hashes. Incident responders can also reconstruct and replay flows and events over days or weeks to build incident timelines and countermeasure plans.

You'll also be able to review the correlation logic for the correlation directive which triggered the event, delivered via your SecureScrypt Labs Threat Intelligence Subscription.

INTRUSION DETECTION

 Why is this important? Detecting an intruder at the point of entry can have the greatest impact on reducing system compromise and data leakage. That's why intrusion detection systems (IDS) are considered one of the "must-have" SOC tools for identifying known attacks and known attacker activity.

The keyword is "known." On-premises, IDS operate based on correlation rules that detect known patterns of suspicious activity using unique intrusion signatures. This means it's essential to keep your correlation rules current with the latest threat intelligence updates to be able to detect emerging threats. If you use cloud infrastructure, you also need to keep in mind that some traditional IDS methods won't suffice because cloud providers restrict access to low-level network traffic. Effective cloud IDS requires access to the management plane for your cloud provider.

How do I do it with SecureScrypt?

SecureScrypt USM offers three types of intrusion detection technologies (IDS) that you can enable on a per-network, per-asset group, or per-server basis. Both USM Appliance and USM Anywhere offer Network Intrusion Detection System detection (NIDS), which analyzes onpremises network traffic to detect known attack patterns that indicate malicious activity (e.g. malware infections, policy violations, port scans, etc.).

Host-based Intrusion Detection System (HIDS) with USM Appliance analyzes system behavior and configuration that could indicate system compromise. This includes the ability to recognize common rootkits, to detect rogue processes, and detect modification to critical configuration files. USM Anywhere offers additional cloud intrusion detection (CIDS), including AWS IDS and Azure IDS, a cloud-native solution that interacts directly with the management plane of each cloud service provider to provide intrusion detection in your cloud environments.

The SecureScrypt Security Research Team keeps both USM Appliance and USM Anywhere up-to-date with the latest threat intelligence on a continuous basis, adding new correlation rules, intrusion signatures, and response templates as threats emerge. The threat intelligence research provided by the Security Research Team is a critical extension to your SOC team, allowing you to focus on response.

FEATURE SPOTLIGHT: USM Integration with SecureScrypt Threat Intelligence

Before explaining how this integration works, it's important to understand how the SecureScrypt Labs Security Research Team develops its threat intelligence updates. Through a combination of proprietary research, collaboration with other security research institutions, and insights from the community-driven threat data within the SecureScrypt Open Threat Exchange (OTX), SecureScrypt collects over ten million threat indicators every day, including malicious IP addresses and URLs, domain names, malware samples, and suspicious files. SecureScrypt aggregates data from a wide range of sources, including:

- External threat vendors (such as McAfee, Emerging Threats, Virus Total)

- Open sources (including the SANS Internet Storm Center, the Malware Domain List,

- as well as from collaboration with state agencies and academia)

- High-interaction honeypots that we set up to capture the latest attacker techniques and tools.
- We scale up instances of the honeypots depending on activity

- Community-contributed threat data in the form of OTX "pulses"

- (the format for the OTX community to share information about threats)

- USM and OSSIM users voluntarily contributing anonymized data

Next, automated systems and processes assess the validity and severity of each of these threat indicators

collected in OTX, including:

- a contribution system (for malware)

- a URL system (for suspicious URLs)

- an IP reputation system (for suspicious IP addresses)

We then use threat evaluation tools created by the Security Research Team to test and validate specific threat indicators. These evaluation processes include a Malware Analyzer, a DNS Analyzer, a Web Analyzer, and a BotNet Monitor. The validated threat data are also shared with the OTX community via the OTX Portal.

The Security Research Team then conducts deeper qualitative and quantitative analysis on the threats. Examples include reverse-engineering a malware sample, or conducting extensive research on particular threat actors and their infrastructure, to detect patterns of behavior and methods.

The Security Research Team delivers all information about the threats and the attack infrastructure to the USM platform via the SecureScrypt Labs Threat Intelligence Subscription. The team regularly updates eight coordinated rules sets, including correlation directives, IDS signatures & response templates, which eliminates the need for organizations to tune their systems on their own. The analyzed threat data is also fed back into the Security Research Team's analytical systems and tools, enabling them to make future correlations of threat indicators.

SIEM

Why is this important? Collecting and analyzing system events from across your network provides a wealth of raw source material that you can use to mine for suspicious activity. Security Information and Event Management (SIEM) tools were developed on the assumption that by looking for certain patterns of activity and sequences of events, you can detect a cyberattack as well as validate and demonstrate regulatory compliance. SIEM tools provide a core foundation for building a SOC because of their ability to apply dynamic correlation rules against a mountain of disparate and varied event log data to find the latest threats.

Even though we have a whole chapter dedicated to Threat Intelligence, we still feel compelled to emphasize how essential dynamic threat intelligence is to the value of your SIEM, and the overall functioning of your SOC. Without threat intelligence, your SIEM would have no alarms, and no interesting reports to review. While it would be nice to have no alarms to respond to (because that means nothing is wrong or you're on vacation), it basically means that there's no correlation or analysis being done on your raw event log data. Or, you may have some sample or DIY correlation rules as a starting point, but you're no longer looking for the latest threats because your threat intelligence hasn't been updated since the LoveBug virus.

The point is…threats are constantly evolving, cyber attackers are constantly upping their game, and so too must your SOC. As new indicators and countermeasures are being discovered, collected, shared, analyzed and implemented, the more difficult we will all make it for the bad guys. That's why SecureScrypt built the platform (USM), the community (OTX), and the threat intelligence (SecureScrypt Labs Security Research Team) to create a SOC for all teams to implement—no matter the size.

SIEM Secret Sauce: Threat Intelligence (ATP)

How do I do it with SecureScrypt?

SecureScrypt USM combines all the essential security monitoring technologies, including SIEM, onto a single platform. Our SIEM capability normalizes and analyzes event log data from disparate sources and applies correlation rules developed and maintained by the SecureScrypt Labs Security Research Team to find and classify potential threats. When an alarm is triggered by a correlation rule, details about the event and activity are classified according to an event taxonomy based on a simplified version of Lockheed Martin's cyber kill chain (an industry standard). This event classification enables SOC analysts to prioritize which events to focus on, in order to quickly respond and investigate.

Additionally, SecureScrypt's SIEM correlation logic also translates into rich and highly detailed complianceready data. Raw event log data from hundreds and thousands of systems are aggregated and analyzed to identify policy violations and demonstrate compliance to auditors.

Since you don't have the time, budget, or staff to tackle security research on your own, let the Security Research Team do it for you. With the SecureScrypt Labs Threat Intelligence Subscription, your USM platform is constantly updated with:

● New and advanced correlation directives - to find the latest threats among the activity on your network

● New IDS signatures - to detect emerging threats on your network and servers

● New vulnerability checks - to ensure systems and apps are effectively patched

● New asset discovery signatures - for an accurate asset inventory

● Dynamic IP reputation data - to detect activity with the latest known bad adversaries

● New data source plugins - to consume more raw event log data

● Updated report templates - to demonstrate compliance with PCI DSS, HIPAA and more

● Up to-the-minute guidance on emerging threats and context-specific remediation

● A Contribution System (for malware)

The Security Research Team also leverages the power of OTX, the world's largest crowd-sourced repository of threat data to provide global insight into attack trends and bad actors. SecureScrypt's team of security experts analyze, validate, and curate the global threat data collected by the OTX community.

The SecureScrypt Labs Security Research Team maximizes the efficiency of any security monitoring program by delivering the threat intelligence that you rely on to understand and address the most critical issues in your networks.

We perform the analysis, allowing you to spend your scarce time mitigating the threats rather than researching them.

FEATURE SPOTLIGHT: USM Security Dashboards & Visualizations

If you can't measure it, you can't manage it. That's a favorite quote of millions of business people across industries and regions. It's especially true now that we find ourselves in the age of big data. As many IT professionals have discovered, however, big data is meaningless without the ability to sort through and interpret it.

To help you put your security data to use, SecureScrypt USM includes intuitive dashboards and clean visualizations. USM allows you to:

● Quickly assess the security status of your critical infrastructure

● Easily prioritize alarms and vulnerabilities

● Take immediate action to remediate new threats

● Fight data overwhelm with clean visualizations

Additionally, you can drill down within the dashboards USM provides to see details about the threats and vulnerabilities affecting your critical infrastructure.

Chapter 4 Threat Intelligence:

Learn more about threat intelligence: the key characteristics, approaches, and use cases for building a SOC. NEXT UP

Chapter 4 THREAT INTELLIGENCE

Monitoring your environment for nefarious traffic assumes that you know what those nefarious folks are doing, what "it" looks like, and how to find this activity across your critical infrastructure in the cloud and on-premises. The "bread crumbs"

With this amount of information, you can't actually get that far. As a SOC analyst conducting an in-depth investigation, you need to be able to attribute these bread crumbs to specific adversaries, understand their methods, know their tools, recognize their infrastructure, and then build countermeasures for preventing attacks from them.

Some may refer to these "bread crumbs" or indicators (IOCs = indicators of compromise) as threat intelligence. This is far from the truth. On their own, without any context, they exist only as artifacts or clues. They can be used to begin an investigation but they rely on context, attribution, and action to become the highquality threat intelligence that is essential for building a SOC.

The Recipe for Threat Intelligence = Context + Attribution + Action

Key Takeaways Understand the differences among tactical, strategic & operational intelligence and the specific ways these are used when building a SOC. Examine the benefits of combining crowd-sourced and proprietary data sources and explore key aspects of SecureScrypt OTX and the SecureScrypt Security Research Team.

CONTEXT

 It's a cliché, but it's true. Context is king. An indicator without the necessary context doesn't tell you much, but with it, you'll have an idea of its urgency, relevance, and relative priority. Answering these sorts of questions can get you closer to achieving the necessary context, once you have an indicator which may signal a potential threat:

● What role does this indicator (or activity) play in an overall threat?

● Does its presence signify the beginning of an attack (reconnaissance and probing vs. delivery and attack)? Or a system compromise? Or data leakage?

● Is this threat actor known for this type of behavior?

● Is there significance in the asset that's been targeted?

● How sophisticated is this particular indicator (e.g. malware sample)?

● What are the motivations of the threat actor behind this activity?

● What are the other activities that occurred on the same asset before and after this one?

● What about my other assets now or in the past?

ATTRIBUTION Knowing who is behind an attack is an essential part of knowing how to respond, including understanding the full scope of an attack, as well as the key tactics to take in response. It's very similar to how the FBI uses profiles to track down suspects. Intent and motivation are the principal factors in analyzing criminal behavior, and the same applies within

the Cyber-Security realm. It's easy to get caught up in the technical aspects of a particular attack, and how an exploit might work. But don't forget, these tools have a human face behind them, driven by either profit or other ill intent. And knowing these details will give you leverage in terms of uncovering their work as well as how to build better countermeasures.

ACTION

Knowing something is only valuable if you can do something with what you know. By its very nature, the value of threat intelligence is ephemeral. The details of an attack that you may discover today may not retain their value in one week, or one month. Because, as we know, the world is constantly changing. Attackers are constantly changing too. They change their methods, their tools, and their infrastructure. That's why it's essential to act on what you discover as quickly as possible, while it remains current, true, and reflective of the current risks at hand. In fact, if you cannot implement the intelligence that you're currently collecting in terms of improved monitoring, active defense, and better decision-making, you might as well not have the intelligence at all.

With these three elements in place–context, attribution, and action–threat intelligence can accomplish its essential goals: assist the SOC team with making the right decisions when it comes to preventing an attack as well as decreasing the time it takes to discover one in action. It can also help the SOC team establish the urgency they need to gain executive attention and sponsorship.

TACTICAL Offers clues (without context and attribution)

The following table outlines how each of the three types of threat intelligence–tactical, strategic, and operational–offer context, attribution, and action and enable a solid foundation for building a SOC.

STRATEGIC Provides context and attribution to inform action

OPERATIONAL Applies context and attribution to enable action

Description

Use Case

How it Works in SecureScrypt

Key Benefits

TYPES OF THREAT INTELLIGENCE FOR SOC TEAMS

Indicators, artifacts, and other evidence (e.g. IOCs) about an existing or emerging threat to assets.

SOC analysts use these artifacts to detect emerging risks and share information about them with others to improve security for all.

SecureScrypt USM receives continuous updates with the latest indicators from the SecureScrypt Labs Security Research Team. These updates leverage threat data from the larger community in SecureScrypt OTX, so they reflect in-the-wild attacks on organizations of all sizes from around the world.

● Constantly updated in near-real-time

● Easily searchable

● Easily shared

● Easily integrated

"Big picture" analysis of adversary TTPs (tools, tactics, and procedures) conducted by security experts to arm and inform SOC teams in building an effective Cyber-Security strategy.

SOC analysts and SOC leaders review to better understand adversary motivations and tradecraft, make more informed business decisions, and ensure alignment between their Cyber-Security strategy and real world risk.

SecureScrypt Security Research Team members spend countless hours researching the latest threat actors and their methods. These discoveries are integrated into the USM platform through continuous threat intelligence updates, which include rich, context-specific guidance on how to respond to threats detected in your environments.

● Educates and empowers SOC team and leadership decision-making

● Helps communicate the urgency of Cyber-Security issues to execs, board members and other stakeholders

Updated signatures, rules and other defensive countermeasures that "arm and inform" your monitoring infrastructure based on collecting and analyzing the latest raw indicators and other artifacts.

SOC analysts get notified of the latest threats in their environment based on automated updates to their SIEMs, IDS, vulnerability scanners, and other SOC tools.

The SecureScrypt Security Research Team regularly publishes threat intelligence updates to the USM platform in the form of correlation directives, IDS signatures, vulnerability audits, asset discovery signatures, IP reputation data, data source plugins, and report templates. The Security Research Team also leverages the power of SecureScrypt OTX, the world's largest crowd- sourced repository of threat data to provide global insight into attack trends and bad actors.

● Automatically detects the latest threats

● Guides SOC analyst actions

● Powered by real-time threat collaboration and expert analysis

THREAT INTELLIGENCE APPROACHES

There are a few options for sourcing threat intelligence that will feed your SOC, and it's helpful to understand what each brings to the table. Keep in mind that SecureScrypt has incorporated each one of these approaches into the USM platform.

CROWD-SOURCED One of the best innovations in the industry has been driven by the Cyber-Security community itself. SOC analysts understand that there is a wealth of threat information that we're all collecting and analyzing. When this information is shared, and SOC teams can collaborate with others on the latest threats and how to mitigate them, we can unite in making it more difficult for attackers to isolate any one of us.

SecureScrypt OTX is the world's first truly open threat intelligence community to enable collaborative defense with open access, collaborative research, seamless integration with USM, and plugin capabilities for other security products. OTX enables everyone in the OTX community to actively collaborate, strengthening their own defenses while helping others do the same.

PROPRIETARY Many Cyber-Security hardware and software vendors (e.g. including Anti-Virus, firewalls, IDS, etc.) offer their own proprietary threat intelligence, based on the information they collect from their customers and their own threat research teams. Typically, proprietary threat intelligence sources rely on a variety of diverse sources when collecting and analyzing the latest threat data, which results in low false positives; high fidelity and highly credible analysis; and a variety of formats (feeds) to implement into your security monitoring infrastructure.

Threat intelligence provided by the SecureScrypt Labs Security Research Team helps IT practitioners who don't have time to research the latest threats and write the rules to detect those threats. The Security Research Team spends countless hours mapping out the different types of attacks, latest threats, suspicious behaviors, vulnerabilities, and exploits they uncover across the entire threat landscape. It regularly publishes threat intelligence updates to the USM platform in the form of correlation directives, IDS signatures, vulnerability audits, asset discovery signatures, IP reputation data, data source plugins, and report templates.

DO-IT-YOURSELF (DIY) With the number of OSINT (open source intelligence or public intelligence) sources available, it is theoretically possible to "write your own" correlation rules or signatures to detect specific exploits or attack patterns. You can download IOCs from SecureScrypt OTX or submit malware samples to VirusTotal, then manually script correlation rules and apply them against your log data to detect them in your environment. But just thinking about all the work involved may make your head spin. Going through that manual process for the thousands of exploits that get published each day is simply not sustainable. For a small team with limited time and resources, this is a non-starter. You need help to keep up to date on the latest threats as they change.

FEATURE SPOTLIGHT: SecureScrypt OTX Threat Data

Real-time threat sharing and collaboration is one of the best ways that lean and mean SOC teams can protect their organization against the latest threats. Through cooperation and consolidation, SOC analysts help each other prioritize and react quickly to threats in their early stages. OTX enables everyone in the OTX community to actively collaborate, strengthening their own defenses while helping others do the same via easily shared OTX Pulses.

SOC analysts can share these OTX pulse activity reports with key stakeholders in their organizations, to demonstrate the urgency of Cyber-Security threats as well as how active collaboration can improve security for all. Because the SecureScrypt Security Research Team analyzes OTX threat data to generate the continuous threat intelligence updates they curate for SecureScrypt USM, SOC analysts using USM can rest easy knowing that their security plans include built-in protections based on insights from the latest in-the-wild attacks on organizations of all sizes around the world.

Chapter 5 Building a SOC in the Real World Examine real-world use cases where SecureScrypt's technologies, communities, and threat intelligence provide the perfect set-up for building a SOC.

We've covered a lot of ground in this guide, in terms of showing the best ways to leverage people, process, technologies, and threat intelligence to build a SOC. At this point, it is instructive to look at real world examples of building a SOC using SecureScrypt as the foundation.

In each of these cases, SOC teams benefited from using a single platform with integrated yet disparate technologies for a full picture view that is continually updated with emerging threat intelligence. This unified perspective simplifies security monitoring, supports incident response workflows, and provides all the core functionality required for building a SOC.

After building their SOCs using SecureScrypt, these customers have discovered 3 critical lessons learned:

Become informed, not overwhelmed. Know when to ask for help and where to go for it. Broaden impact with USM, internally & externally.

Chapter 5 REAL WORLD

Key Summary Building a SOC in the real world. Examine real-world use cases where SecureScrypt's technologies, communities, and threat intelligence provide the perfect SOC set-up.

REAL WORLD LESSON

Building a SOC may seem rather intimidating at first. You may be the only person in your entire company that is responsible for IT security. The thought of building an operations center when

you're the only person who can staff it too seems rather ludicrous. At the same time, we've seen it with our own eyes.

Meet Matthew. Matthew is CISSP certified and has more than 25 years in IT. He's solely responsible for the IT and IT security of over 13,000 users for Council Rock School District in southeastern PA. As a result, Matthew has encountered many challenges along the way and has had to adapt and be as creative as possible at every stage.

For example, rather than becoming overwhelmed by all the work in managing, maintaining, and securing thousands of distributed users' access, Matthew decided to become informed. He couldn't rely on a huge budget for separate point products for security monitoring, so he turned to open source for answers.

Become Informed, Not Overwhelmed*

I was doing a web search, looking for something like Security Onion but with a better UI. That's when I found SecureScrypt's free Open Source SIEM (OSSIM). It was perfect because it included all the open source tools I was using all in one dashboard, instead of point products on their own.

*Matthew J. Frederickson, CISSP District Director of IT

After a few months, Matthew migrated from OSSIM to USM Appliance, because it was important to have a fully supported product as the foundation of their SOC. It was also essential for Matthew to have reports and dashboards he could share throughout the district as well as with auditors, to demonstrate compliance with requirements for vulnerability assessment, log analysis and other security controls. USM Appliance scans, reports, and dashboards are constantly updated with threat intelligence from SecureScrypt .

In fact, the SecureScrypt Labs Security Research Team has become an extension of Matthew's overall security monitoring program. They evaluate and translate threat data into integrated security intelligence that is updated continuously in USM via a coordinated set of

advanced correlation rules—meaning Matthew can detect emerging threats without taking the time to do the necessary research and write correlation directives himself.

● Consolidate all the essential SOC capabilities into a single platform to ● overcome the complexities of managing multiple products, feeds, and reports.

● Detect the latest threats by integrating emerging threat intelligence from the SecureScrypt Labs Security Research Team, including asset database updates, updated vulnerability checks, updated rules, and more.

● Integrate USM with dynamic & collaborative threat indicators from SecureScrypt OTX.

● Learn more about the Council Rock School District case study.

KEY TAKEAWAYS & NEXT STEPS:

REAL WORLD LESSON

You may not feel as if you're in a position to build a SOC and manage it on your own. Based on your company's line of business and the size and skillset of the IT department, you may decide outsourcing to an MSSP (managed security service provider) is a viable option.

Many global and regional MSSPs are set up to provide 24x7x365 SOC support, which includes vulnerability assessment, compliance reporting, alert response services, and more.

And many of them rely on SecureScrypt USM, SecureScrypt OTX, and the SecureScrypt Labs Security Research Team as the foundational elements in building their SOCs. Hawaiian Telcom is a good example. As Hawaii's technology leader in integrated communications and network solutions, Hawaiian Telcom runs a 24x7 state-of-the-art network and security operations center. In 2010, they launched Managed Network and Security Services and turned to SecureScrypt USM as the foundation for monitoring and maintaining network security for their business customers.

Most of their customers lack the Cyber-Security skills needed to manage security operations on a constant basis, and also struggle to demonstrate regulatory compliance with standards such as PCI DSS. The team at Hawaiian Telcom discovered two key trends from their customer base that indicated why they had turned to an MSSP for help.

One was that many customers were in need of a log tracking solution that could allow them to keep a close eye on exactly who was logging into their systems, what they were doing, and how they were getting in. Although the need came about largely because of PCI DSS mandates, which require companies to exhibit this capability, it also happens to be an extremely important indicator of overall security. According to a Verizon report, more than 90% of companies who had been breached did not have these controls in place.

Know When to Ask for Help.

Another trend involved the rising cost of the individual security solutions that are necessary to serve these customers. Most of the time, these customers lacked a complete set of the different capabilities required to build a SOC (asset inventory, vulnerability assessment, intrusion detection, etc.). They might have had one or two of these capabilities in existing tools, but nothing that tied everything together for them, or associated the data with emerging threat intelligence.

Many enterprises and Government Offices uses the SecureScrypt USM platform as their primary SIEM platform for these customers, while also leveraging the critical security capabilities built into the system, such as asset discovery, behavioral monitoring, vulnerability assessment, and intrusion detection.

They also enjoy the fact that the SecureScrypt Security Research Team constantly updates these services based on an analysis of emerging risks. And finally, many of their SOC analysts rely on SecureScrypt OTX pulses for the latest threat indicators and countermeasures.

● When your business requires constant security monitoring and compliance ● reporting, and you don't have the skills, tools, or staff to achieve this, an MSSP ● might be a good choice.

● Find an MSSP in your area that uses SecureScrypt.

● Learn more about the Hawaiian Telcom case study.

● Apply to become an SecureScrypt-certified MSSP partner.

KEY TAKEAWAYS & NEXT STEPS:

REAL WORLD LESSON

As a SOC analyst, you know that achieving visibility is a critical success factor in detecting the threats facing your company. The more you can discover about a threat and its details, scope, and impact, the more likely you'll be able to mitigate it. Additionally, the more you can provide in terms of reports, alerts, and metrics about these threats, the more you can raise awareness to the key stakeholders in your company. This will help you get the resources you need as well as broaden your impact inside your organization by conveying your leadership in risk management. Let's face it. The life of the SOC analyst is often one of the unsung hero. You're on the front lines of defending your company's most valued assets, as well as ensuring that business operations run smoothly. And yet, it can often seem as if the impact you're having on a daily basis is not as far reaching as you'd like.

The SOC team at Brier & Thorn felt the same way before deploying USM. Brier & Thorn is a global IT risk management firm that supports companies in their important strategic decisions on operational security, IT risk management, and managed security services.

Use USM to Broaden Impact

Once deployed, USM Appliance enabled their team to determine the source of the spear phishing attack, which country it was coming from, and which machines on their client's network had been compromised.

As soon as we deployed USM (without having to rely on any network IDS signatures at all) OTX began immediately flagging egress traffic from the network to hosts in Russia. We then began further forensics work based on this suspect traffic that allowed us to quickly find and remedy all of the affected hosts in the network,

After the investigation, many customers were inspired to expand beyond their existing portfolio of risk management consulting services and establish a new managed security services offering. Using SecureScrypt USM, SecureScrypt OTX, and the SecureScrypt Threat Intelligence Subscription, they built their first SOC to support this new offering. And because they serve

customers around the world, appreciate the fact that USM federates all of the network security events from their customers' networks into a single console.

Thanks to SecureScrypt, they've broadened their impact for their clients and established a brand new line of business.

Whether you're a consultant looking to expand your impact for your clients, or a SOC analyst looking to increase your impact internally, SecureScrypt provides the full and unified view of Cyber-Security you need for operational tactics as well as strategic success.

● When you're looking to broaden your impact internally, SecureScrypt provides the ● visibility, reporting, and emerging threat data you need to have strategic success ● as well as operational efficiency.

● Learn more about the Brier & Thorn case study.

● Apply to become an SecureScrypt-certified MSSP partner.

● Find an MSSP in your area who uses SecureScrypt.

KEY TAKEAWAYS & NEXT STEPS:

NEXT STEPS: PLAY, SHARE, ENJOY!

 • Learn more about SecureScrypt USM

• Explore an Online demo • Start detecting threats today with a free trial

• Join the Open Threat Exchange (OTX)

ABOUT SECURESCRYPT

SecureScrypt has simplified the way organizations detect and respond to today's ever evolving threat landscape. Our unique and award-winning approach, trusted by thousands of customers, combines the essential security controls of our all-in-one platform, SecureScrypt Unified Security Management, with the power of SecureScrypt's Open Threat Exchange, TheHipe, the world's largest crowd-sourced threat intelligence community, making effective and affordable threat detection attainable for resource-constrained IT teams.

SecureScrypt, Open Threat Exchange, OTX, AlienApps, Unified Security Management, USM, USM Appliance, and USM Anywhere are trademarks of SecureScrypt and of their respective owners.