HOW TO BUILD A

SECURITY OPERATIONS CENTER

(ON A BUDGET)

ALIEN VAULT

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 network. Controlling access with tools like passwords, ACLs, firewall rules and others aren't quite good enough. You still have to constantly monitor that these security controls continue to work across all of your devices, so that you can spot strange activity that may indicate a possible exposure.

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.

Unfortunately, unlike with CCTV cameras, you can't just look into 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.

Building an SOC:

SOC teams are responsible for monitoring, detecting, containing and remediating IT threats across applications, devices, systems, networks, and locations.

Using a variety of technologies and processes, SOC teams rely on the latest threat intelligence (e.g. indicators, artifacts, and other evidence) 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 WITH LIMITED RESOURCES IN A RACE AGAINST TIME

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 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, AlienVault™ provides the foundation you need to build a SOC - without requiring costly implementation services or large teams to manage it. With AlienVault USM™, AlienVault Labs Threat Intelligence, and AlienVault OTX™, you'll 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.

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 AlienVault USM, AlienVault Labs, and AlienVault OTX support these critical processes.

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 AlienVault 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 and proprietary data sources and explore key aspects of AlienVault OTX and AlienVault Labs Threat Intelligence.

Chapter 5

REAL WORLD

Building a SOC in the Real World. Examine real-world use cases where AlienVault'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 has realized the significance of cyber security to the business bottom line. In these cases, the SOC team is in a great position: enough budget for good tools and enough staff to manage them, and the “human” capital of executive visibility and support.

But that’s not the reality in most cases, unfortunately.

SOC teams are fighting fire 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, using the least amount of resources - all while gaining visibility into active and emerging threats. That’s our goal.

So how do we get there?

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

Key Takeaways 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.

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 servers and security devices (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 - 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, scope of impact, evaluating attribution and adversary details, as well as sharing your findings with the threat intelligence community etc.

Knowing what it will take for building a SOC will help you determine how to staff your team. In most cases, for security operations teams of 4-5 people, the chart on the next page will relay our recommendations.

ROLE	DESCRIPTION	SKILLS	RESPONSIBILITIES
 Tier 1 **Security Analyst**	**Triage Specialist** (Separating the wheat from the chaff)	Sysadmin skills (Linux/Mac/Windows); Programming skills (Python, Ruby, PHP, C, C#, Java, Perl, and more); Security skills (CISSP, GCIA GCIH, GCFA, GCFE, etc.)	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, IDSes, correlation rules, etc.).
 Tier 2 **Security Analyst**	**Incident Responder** (IT's version of the First Responder)	All of the above + natural ability and dogged curiosity to get to the root cause. The ability to remain calm under pressure. Being a former White Hat Hacker is also a big plus.	Reviews trouble tickets generated by Tier 1 Analyst(s). Leverages emerging threat intelligence (IOCs, updated rules, etc.) to identify impacted 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.
 Tier 3 **Expert Security** Analyst	**Threat Hunter** (Hunts vs. Defends)	All of the above + be familiar with using data visualization tools (e.g. Maltego) and penetration testing tools (e.g. Metasploit).	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.
 Tier 4 **SOC Manager**	**Operations & Management** (Chief Operating Officer for the SOC)	All of the above + strong leadership and communication skills	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.

Do I Need a Threat Intelligence Team Too?

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 (less 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).

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? There's no shame in leveraging an MSSP to manage your SOC - in fact, we'd recommend starting with one of many AlienVault-powered MSSPs. You can find one here.

NEXT UP

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.

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.

The cyber security world isn't all that different, yet the stakes are even higher.

There are 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 & quickly. At every step along the way, we'll show you how you can use AlienVault USM, AlienVault OTX, and AlienVault Labs Threat Intelligence to power your SOC processes.

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 AlienVault® USM™, AlienVault Labs, and AlienVault OTX™ support these critical processes.

SOC PROCESSES

Answering the Big Questions for Each SOC stage

1 EVENT CLASSIFICATION & TRIAGE

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 AlienVault?

AlienVault USM applies plugins and correlation logic - delivered via the AlienVault Labs Threat Intelligence subscription - 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, AlienVault 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 the ransom by a certain period of time.

How do I do it with AlienVault?

The critical key to success is identifying attacker activity in the early stages of an attack, before sensitive data and systems are impacted. Because as an attacker moves up these kill chain stages, it becomes more likely they'll be successful in their attacks. By looking at network and system activity from an attacker's perspective, you'll be able to determine which events require your attention now.

ALARM TYPE	DESCRIPTION	PRIORITY LEVEL	TIER 1 ANALYST TASKS
 **Reconnaissance and Probing**	Behavior indicating an actor attempting to discover information about the organization	 Low	Review Activity from OTX (on a monthly basis)
 **Delivery and Attack**	Behavior indicating an attempted delivery of an exploit	 Low/Med	Review Activity from OTX (on a weekly basis)
 **Exploitation & Installation**	Behavior indicating a successful exploit of a vulnerability or backdoor /RAT being installed on a system	 Med/High	Verify and Investigate (escalate to Tier 2)
 **System Compromise**	Behavior indicating a compromised system	 High	Verify and Investigate (escalate to Tier 2)

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, AlienVault USM 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 into 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 self-assessments no longer suffice once you've been breached).

2 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 (this requires knowing which assets are the most critical, and flagging these as business critical - see how to do this in AlienVault USM below). 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 network. 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 AlienVault?

Powered by AlienVault Labs Threat Intelligence, AlienVault USM can detect the specific indicators that signal activity of specific adversary tools, methods, and infrastructure. Correlation directives, developed by AlienVault Labs, are rules that are applied against the raw event log data that USM collects. Once applied, these directives identify and categorize these 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. AlienVault OTX helps you identify attribution for cyber attacks targeted against you.

It's essential to understand who is behind a particular attack, because this will inform how you should respond, as well as how to 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, you make that adversary's job much more difficult and costly. Everybody wins.

View threat details within the kill chain context in AlienVault USM

Know Your Network and All Its Assets

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. AlienVault USM gives you the ability to discover assets through passive network monitoring and active network scanning. Additionally, USM can identify the presence of installed software as well as running services. All of which help inform the SOC team when investigating security incidents. That said, you'll also need to answer some tricky questions about your assets that can't be discovered with technology.

- 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 systems rely on?
- Which systems manage and store sensitive information?

Learn more about AlienVault USM asset discovery capabilities.

3 REMEDIATION & RECOVERY

Why is this important?

The quicker 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. So make sure that you work closely and communicate clearly and often with your management team. 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 network 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 AlienVault?

AlienVault USM simplifies remediation and recovery by helping you detect events quickly so that you can respond in time to prevent further damage. Additionally, AlienVault USM's Asset Discovery and Vulnerability Assessment capabilities deliver updated and detailed information on 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 AlienVault USM vulnerability assessment capabilities

4 ASSESSMENT & AUDIT

Why is this important?

It's always optimal to find and fix vulnerabilities before an attacker exploits them in order to gain access to your network. 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 network vulnerability assessments and generating compliance reports are some of the most common audit activities for SOC team members. Additionally, SOC team members may also 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 AlienVault?

With AlienVault USM, you can run continuous vulnerability scans against all of your assets (internal and external assets, as well as those in your AWS environment) 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.

You can also monitor SOC team performance using USM Dashboards and Reports. AlienVault USM customers and partners use these reports to communicate the value of the SOC team, by demonstrating all of the work that goes into SOC operations: all of the tickets, events, network traffic, user activity, and analysis done on behalf of the company and its assets.

NEXT UP

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

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.

Think of this concept like a jawbreaker.

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 for them - more or less.

Prevention vs Detection

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.

For smaller organizations, with limited budget and time, a new approach is needed. One that combines the essential SOC 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 AlienVault USM combines these essential capabilities for building a SOC into a single platform. Finally, we'll cover how AlienVault Labs Threat Intelligence and AlienVault OTX power these essential capabilities within AlienVault 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 AlienVault Unified Security Management (USM) that consolidates these tools into one place.

1 ASSET DISCOVERY

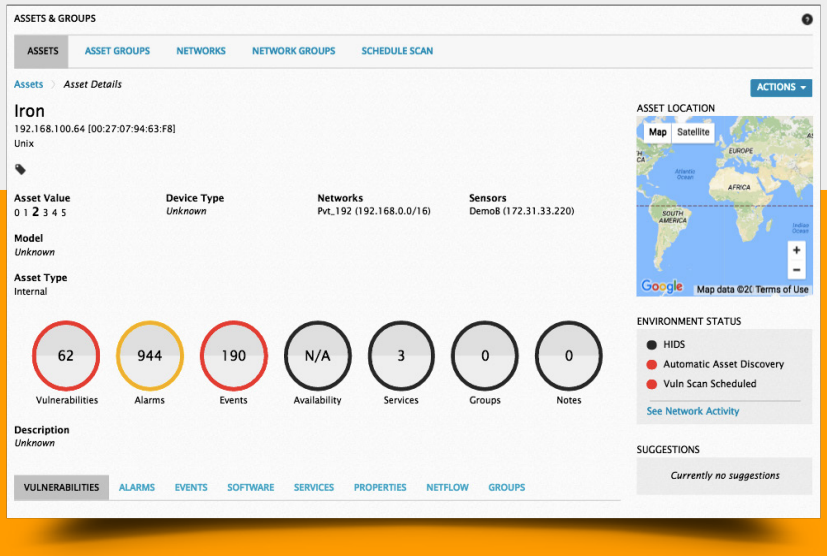
Why is this important?

Knowing what's on your network is the first step in protecting what's on your network. You need to know what systems exist - laptops 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 AlienVault?

Using both active and passive techniques, AlienVault USM captures accurate and real-time information on all the assets in your network and cloud environments. Active network scanning gently probes your network to coax and interpret responses from devices that help determine the OS, running services, and installed software (often without requiring any credentials). By passively monitoring and capturing host traffic on the network, AlienVault USM analyzes these communications and then enumerates the services on these hosts. This enables you to quickly spot unauthorized applications, misconfigurations, or other attributes that may signal an intrusion or leave you exposed to one.

FEATURE SPOTLIGHT:
Asset Detail



The Asset Discovery & Inventory capabilities within AlienVault 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.

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. Additionally, you can examine all of the installed software and running services on it. With one click, you can create a ticket that helps you delegate and escalate items when they require it.

When you're investigating an incident, you can also document what you discover directly within the asset details (in the Notes section) so that the next time this asset is targeted, you have a reliable audit trail.

2 VULNERABILITY ASSESSMENT

Why is this important?

Vulnerabilities represent the tiny cracks that an attacker uses to infiltrate your networks, apps, devices, and 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 network for vulnerabilities. Additionally, you may be subject to a variety of contractual and regulatory mandates (e.g. PCI DSS, SOX, etc.) that requires periodic vulnerability assessment to demonstrate compliance.

How do I do it with AlienVault?

AlienVault includes a built-in vulnerability assessment tool that allows you to both meet your compliance obligations and effectively detect those tiny cracks. Whenever you run a vulnerability scan, you have to balance between doing an in-depth and accurate assessment with how much that may require (user credentials) and how much it may impact your business (network and system performance). With AlienVault USM, you have full control over how and when vulnerability assessments are done. For example, you can choose authenticated scans for certain asset groups and run an unauthenticated scan on those systems that don’t require as in-depth of an analysis. Additionally, AlienVault USM combines active network scanning and host-based assessment for continuous vulnerability discovery, assessment, and validation when the vulnerabilities are resolved.

A Closer Look:

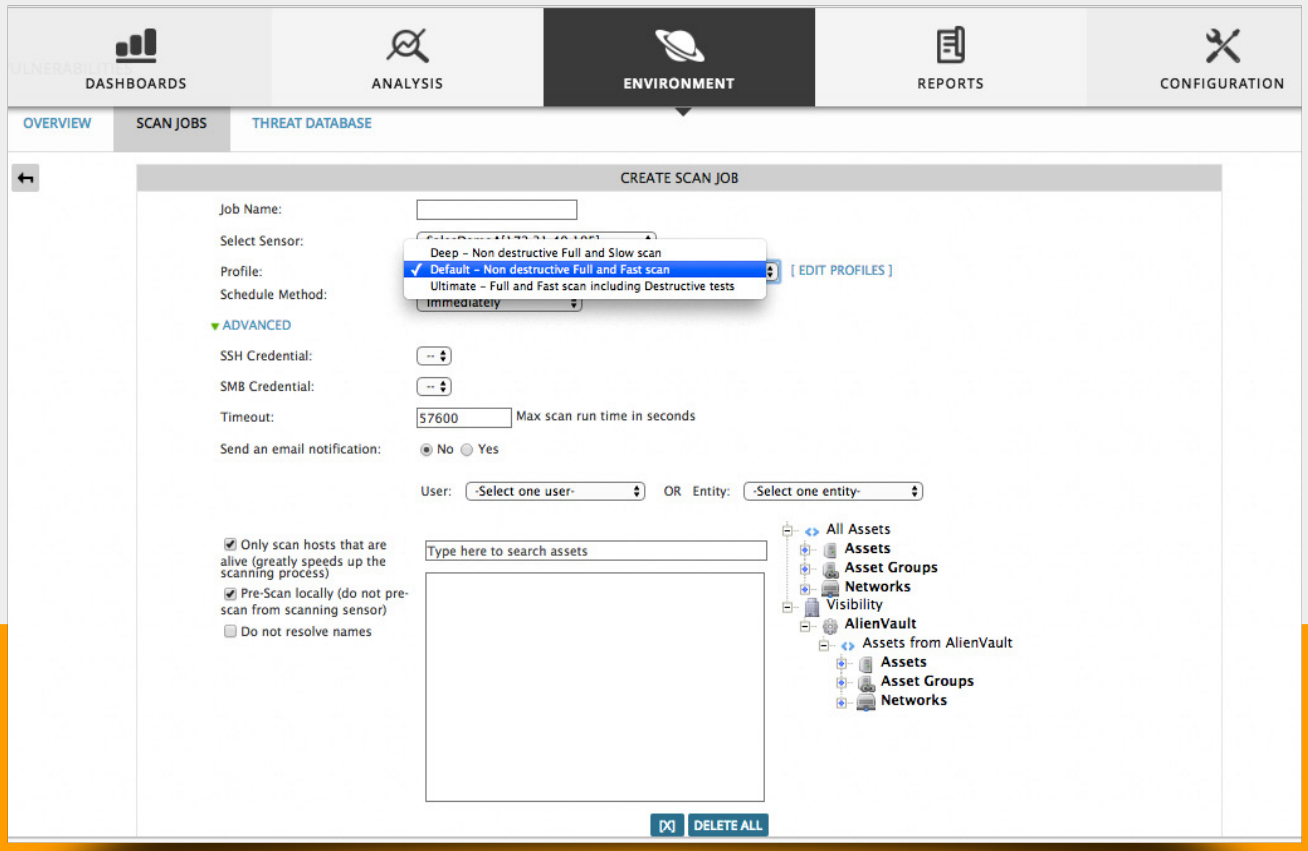
VULNERABILITY ASSESSMENT IN USM

Active Network Scanning (unauthenticated) actively probes hosts using carefully crafted network traffic to elicit a response and analyze these responses to determine the presence of a vulnerability (e.g. misconfiguration or unpatched software).

Host-based Assessment (authenticated) accessing the system’s file system, our analysis engine performs a more accurate and comprehensive detection of vulnerabilities by inspecting installed software and continuously comparing it against a list of known vulnerable software.

FEATURE SPOTLIGHT:

Vulnerability Scan Scheduler



Flexibility is one of the most important aspects of doing vulnerability assessment well. When not carefully calibrated, vulnerability scans can often disrupt network and system performance. At the same time, if they're not done in an in-depth way, you may end up with too many false positives due to superficial probing and incomplete reconnaissance. AlienVault USM offers SOC analysts complete control and flexibility when setting up ad-hoc and scheduled vulnerability scans.

You can choose to apply pre-set profiles that range from the default non-intrusive to deep and ultimate for more in-depth vulnerability verification. Additionally, you can apply each of these profiles to specific asset groups or network segments based on their compliance relevance, business criticality, or other important considerations.

3 BEHAVIORAL MONITORING

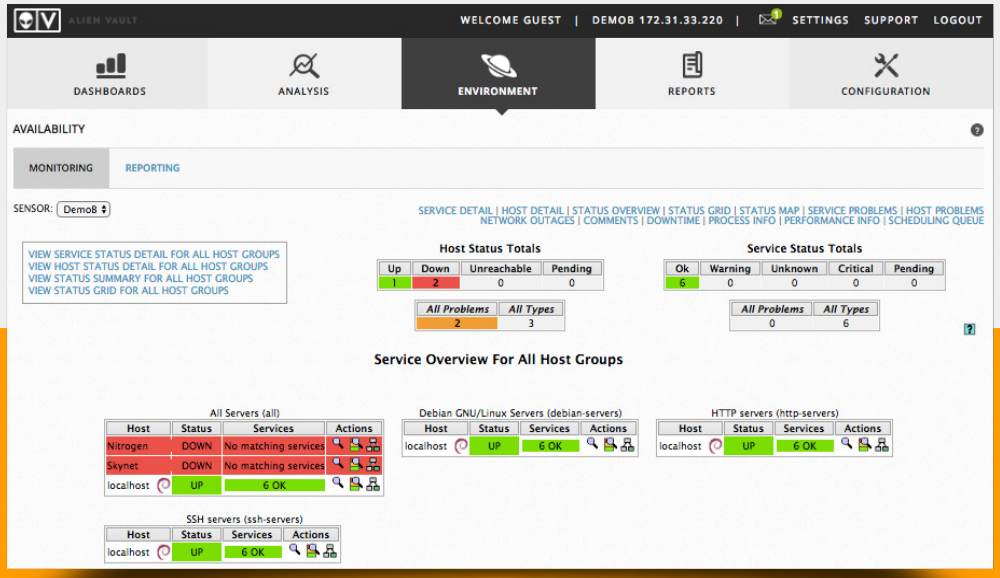
Why is this important?

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 on your network.

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.

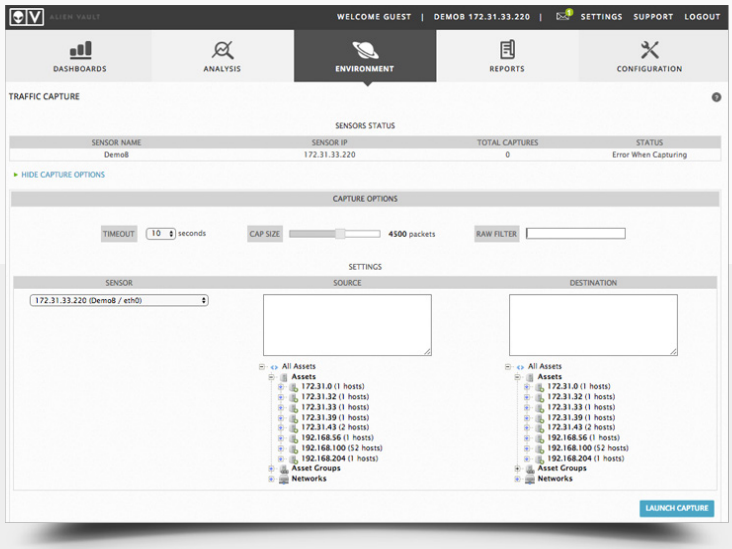
How do I do it with AlienVault?

AlienVault USM combines four fully integrated behavioral monitoring technologies within its platform: active service monitoring; NetFlow analysis; network traffic capture and host-based intrusion detection. (HIDS).

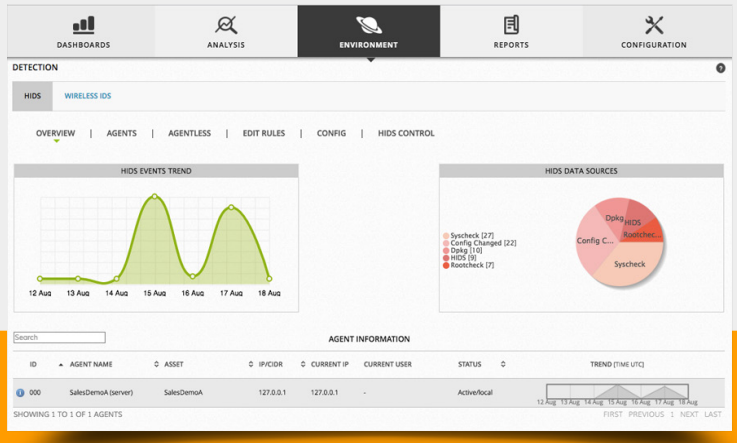


Active Service Monitoring validates that the services running on hosts are continuously available.

NetFlow Analysis captures metadata from the TCP/IP stream and analyzes the protocols and calculates the bandwidth used by each protocol.



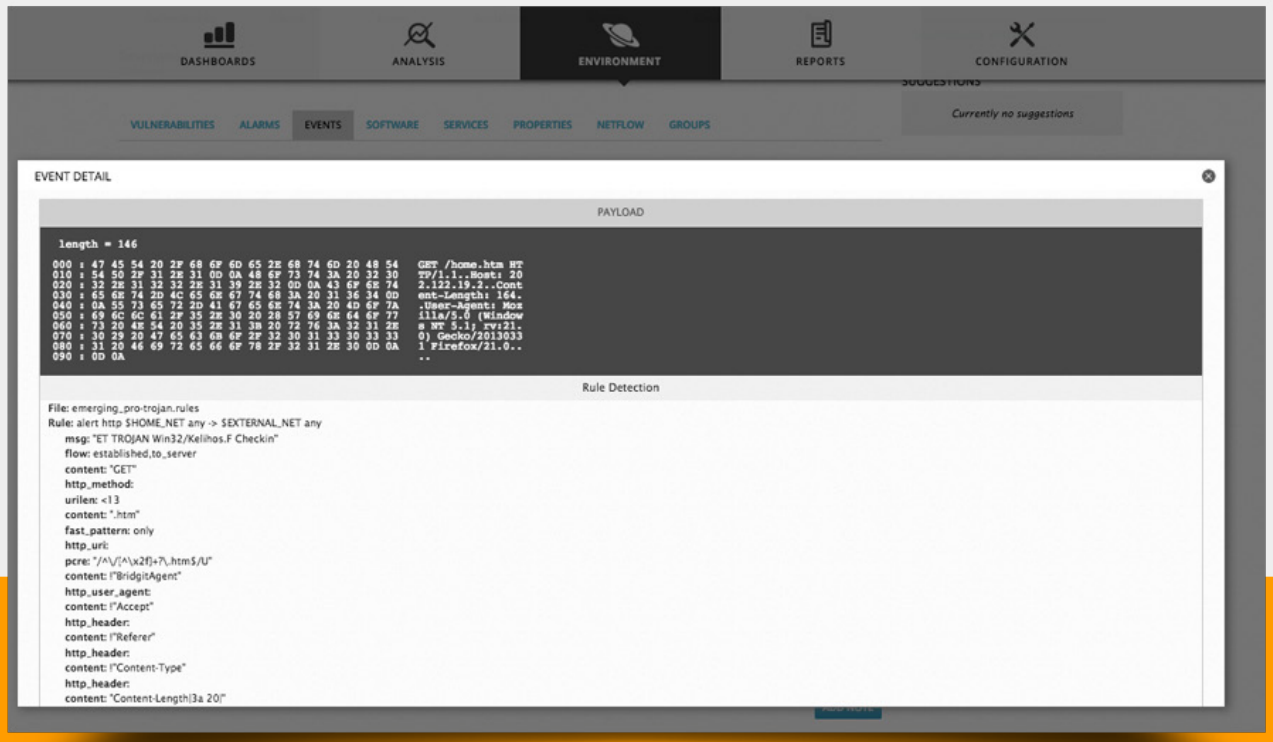
Network Traffic Capture allows for forensic storage of the packet stream so that detailed inspection can be performed if necessary.



Host-Based Intrusion Detection continuously monitors running processes and resource utilization on hosts in order to detect indicators of compromise (IOCs) in real-time.

FEATURE SPOTLIGHT:

Packet Capture & Payload Analysis



Examining the payload of each event within the USM portal will enable 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 AlienVault Labs Threat Intelligence.

4 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". IDS, unlike the behavior monitoring tools we covered above, operate based on signatures, or rules, that look for known patterns of suspicious network traffic and system activity that could signal an intrusion. When that activity or traffic is found on your network, you'll need to know about it immediately in order to investigate and contain any damage.

How do I do it with AlienVault?

AlienVault USM offers two types of intrusion detection technologies (IDS) that you can enable on a per-network, per-asset group, or per-server basis. The Network Intrusion Detection System (NIDS) analyzes network traffic to detect known attack patterns that indicate malicious activity (e.g. malware infections, policy violations, port scans, etc.). The Host-based Intrusion Detection System (HIDS) 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.

AlienVault Labs Threat Intelligence provides updated signatures on a continuous basis as threats change for the built-in network IDS and updated signatures for OSSEC for host-based IDS. This threat intelligence and the work performed by the AlienVault Labs team is a critical extension to your SOC team, allowing you to focus on response.

FEATURE SPOTLIGHT:

USM Integration with AlienVault Labs Threat Intelligence

Before explaining how this integration works, it's important to understand how AlienVault Labs Threat Intelligence is developed. First, AlienVault collects over 4 million threat indicators every day, including malicious IP addresses and URLs, domain names, malware samples, and suspicious files. AlienVault aggregates this data in the Open Threat Exchange (OTX) platform, AlienVault's Big Data platform, 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, we have set up automated systems and processes which leverage machine learning to 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 AlienVault Labs team, which also leverage machine learning, 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 AlienVault Labs research team then conducts deeper qualitative and quantitative analysis on the threats. For example, reverse-engineering a malware sample, or conducting extensive research on particular threat actors and their infrastructure, to detect patterns of behavior and methods.

The AV Labs team delivers all information about the threats and the attack infrastructure to the USM platform via the USM Threat Intelligence Subscription. The team regularly updates 8 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 AlienVault Labs analytical systems and tools, enabling them to make future correlations of threat indicators.

5 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 cyber attack 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 (i.e. Correlation Directives) against a mountain of disparate and varied event log data - to find the latest threats.

SIEM Secret Sauce: **Threat Intelligence**

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 we at AlienVault are so happy to provide the platform (USM), the community (OTX), and the threat intelligence (AlienVault Labs) to build a SOC for all teams to implement - no matter the size.

How do I do it with AlienVault?

AlienVault USM combines all of 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 AlienVault Labs to find and classify potential threats. When an alarm is triggered by a correlation directive, 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, AlienVault's SIEM correlation logic also translates into rich and highly detailed compliance reports. 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 AlienVault Labs Threat Intelligence do it for you. With AlienVault Labs Threat Intelligence, 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 AlienVault Labs 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. AlienVault's team of security experts analyze, validate, and curate the global threat data collected by the OTX community.

The AlienVault Labs Threat 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.

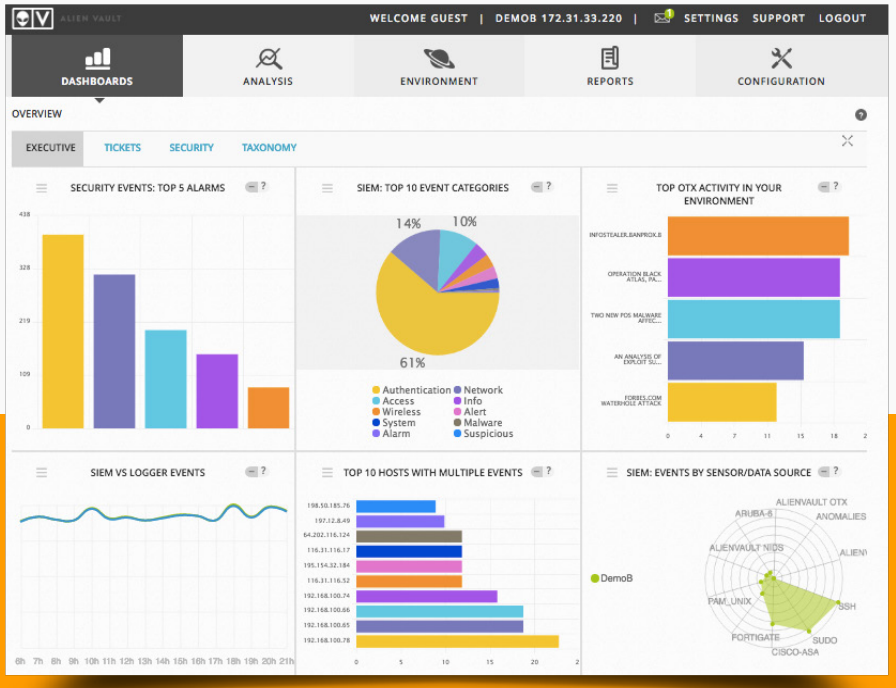
FEATURE SPOTLIGHT:

USM Security Dashboards & Reports

If you can't measure it, you can't manage it. That's one of the most favorite quotes of millions of business people - across industries and regions. It's especially true now that we find ourselves in the age of Big Data. I haven't met an executive who doesn't like a pretty chart, have you? But in all seriousness, speaking "business" is one of the most successful skills that SOC analysts can have to promote themselves and the overall SOC team mission.

We understand this, and that's why we've built intuitive executive-level dashboards and reports on key SOC metrics such as:

- Top 5 Alarms
- Top 10 Event Categories
- Top OTX Activity in Your Environment
- Top 10 Hosts with Multiple Events
- Top 10 Promiscuous Hosts



Additionally, you can also use the dashboards and reports USM provides for evaluating SOC team operations and performance, by viewing key trouble ticket statistics.

NEXT UP

Chapter 4
Threat Intelligence:
Learn more about threat intelligence: the key characteristics, approaches, and use cases for building a SOC.

Chapter 4

THREAT INTELLIGENCE

The Recipe for Threat Intelligence = Context + Attribution + Action

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 assets, devices, and networks. The "bread crumbs" that these adversaries leave are usually of the same sort: IP addresses, host and domain names, email addresses, filenames, and file hashes.

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 high quality threat intelligence that are essential for building a SOC.

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 AlienVault OTX and AlienVault Labs Threat Intelligence.

> Know thyself. Know thy enemy.
> A thousand battles. A thousand victories.
>
> -Sun Tzu, The Art of War

CONTEXT

It's a cliche, 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 piece of tradecraft (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. Attacker's 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.

3 TYPES OF THREAT INTELLIGENCE FOR SOC TEAMS

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.

	TACTICAL Offers clues (without Context and Attribution)	STRATEGIC Provides Context and Attribution to Inform Action	OPERATIONAL Applies Context and Attribution to Enable Action
Description	Indicators, artifacts, and other evidence (e.g. IOCs) about an existing or emerging threat to assets.	"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.	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.
Use Case	SOC analysts use these artifacts to detect emerging risks and share information about them with others to improve security for all.	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.	SOC analysts get notified of the latest threats in their environment based on automated updates to their SIEMs, IDSes, vulnerability scanners, and other SOC tools.
How it Works in AlienVault	AlienVault USM automatically gets updated with the latest indicators from AlienVault Labs. You can also sign up for immediate updates (OTX Pulses) from the larger community in AlienVault OTX. You'll receive a USM alarm every time an OTX indicator shows up in your environment.	AlienVault Labs team members spend countless hours researching the latest threat actors and their methods. These discoveries are shared via the AlienVault Labs blog providing in-depth, strategic analysis of threat trends, threat actors, and their infrastructure and tools (e.g. reverse engineering malware or exposing a threat actor's methodology or infrastructure set-up).	The AlienVault Labs threat 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 AlienVault Labs team also leverages the power of AlienVault OTX, the world's largest crowd-sourced repository of threat data to provide global insight into attack trends and bad actors.
Key Benefits	• Constantly updated in real-time • Easily searchable • Easily shared • Easily integrated	• Educates and empowers SOC team and leadership decision-making • Helps communicate the urgency of cyber security issues to execs, board members and other stakeholders	• 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 AlienVault 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.

AlienVault 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, IDSes, 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.

AlienVault Labs Threat Intelligence helps IT practitioners who don't have the time to research the latest threats and write the rules to detect those threats. The AlienVault Labs threat research team spends countless hours mapping out the different types of attacks, the latest threats, suspicious behavior, 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 AlienVault OTX or submit malware samples to VirusTotal and 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. Because doing that manually 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.

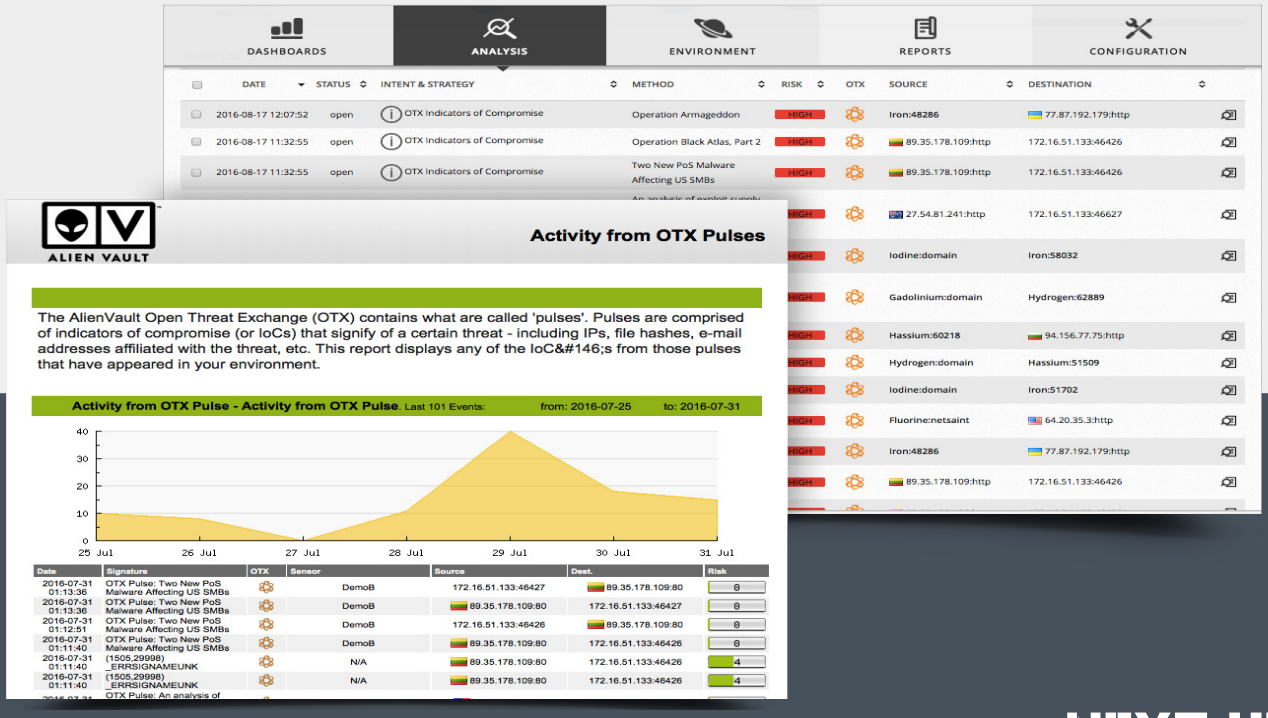
FEATURE SPOTLIGHT:

AlienVault USM and AlienVault OTX Integration

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. AlienVault USM will immediately trigger an alarm as soon as any OTX-reported actor is discovered interacting with your network or assets.

USM Reporting includes detailed lists of all of the activity associated with threat actors and indicators that have been collected, shared and reviewed by thousands of OTX community members. 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.



NEXT UP

Chapter 5

Building a SOC in the Real World

Examine real-world use cases where AlienVault's technologies, communities, and threat intelligence provide the perfect set-up for building a SOC.

Chapter 5

REAL WORLD

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 AlienVault 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 AlienVault, 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.

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

REAL WORLD LESSON 1

Become Informed. Not Overwhelmed

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 of 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.

> I was doing a web search, looking for something like Security Onion but with a better UI. That's when I found AlienVault'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 for Council Rock School

After a few months, Matthew migrated from OSSIM to USM, 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 can share throughout the district as well as with auditors - to demonstrate compliance with requirements for vulnerability assessment, log analysis and other security controls. USM scans, reports, and dashboards are constantly updated with threat intelligence from AlienVault Labs.

In fact, the AlienVault Labs 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.

KEY TAKEAWAYS & NEXT STEPS:

- Consolidate all of 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 AlienVault Labs (which includes asset database updates, updated vulnerability checks, updated rules, and more).
- Integrate USM with dynamic & collaborative threat indicators from **AlienVault OTX.**
- Learn more about the **Council Rock School District case study**.

REAL WORLD LESSON 2

Know When to Ask for Help.

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 AlienVault USM, AlienVault OTX, and AlienVault Labs 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 AlienVault USM as the foundation for monitoring and maintaining network security for their business customers.

Most of their business customers lack the cyber security skills needed to manage security operations on a 24x7 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.

> Hawaiian Telcom offers our customers the most up-to-date network security services supported by AlienVault Labs, which actively tracks & analyzes millions of threats to deliver the latest intelligence directly to the USM platform."

Matt Freeman, **Senior Manager**
IP & Managed Services, Hawaiian Telcom

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.

Hawaiian Telcom uses the AlienVault 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 AlienVault Labs is constantly updating these services based on an analysis of emerging risks. And finally, many of their SOC analysts rely on AlienVault OTX pulses for the latest threat indicators and countermeasures.

KEY TAKEAWAYS & NEXT STEPS:

- When your business requires 24x7x365 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 who uses AlienVault.
- **Learn more about the Hawaiian Telcom case study**.
- **Apply to become an AlienVault-certified MSSP partner.**

REAL WORLD LESSON 3

Use USM to Broaden Impact

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, 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 being seen as a leader 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.

Brier & Thorn first began searching for an all in one security solution in early 2013 when, as a risk management consultancy, they were tasked with conducting an incident response investigation into a spear phishing attack targeting one of their clients. Brier & Thorn attempted to conduct additional research into this attack and the associated communications, but ran into an obstacle. They lacked an incident response forensics tool to see traffic going in and out of the network. They wanted to be able to deploy something quickly that could detect and alert on communication with known malicious hosts, and broaden their impact as a security services provider.

In their search for the right solution, Brier & Thorn came across AlienVault's Unified Security Management (USM) platform and its Open Threat Exchange™ (OTX). After a few conversations with AlienVault, Brier & Thorn determined that the functionality provided by USM delivered the ideal tool set for their incident response investigation.

Once deployed, AlienVault USM 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,

Alissa Knight
Group Managing Partner at Brier & Thorn

After the investigation, Brier & Thorn were inspired to expand beyond their existing portfolio of risk management consulting services and establish a new managed security services offering. Using AlienVault USM, AlienVault OTX, and AlienVault Labs threat intelligence, they built their first SOC to support this new offering. And because they serve customers around the world, Brier & Thorn appreciates the fact that USM federates all of the network security events from their customers' networks into a single console.

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

Whether you're a consultant looking to broaden your impact for your clients, or a SOC analyst looking to broaden your impact internally, AlienVault provides the full and unified view of cyber security you need for operational tactics as well as strategic success.

KEY TAKEAWAYS & NEXT STEPS:

- When you're looking to broaden your impact internally, AlienVault 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 AlienVault-certified MSSP partner.**
- **Find an MSSP in your area who uses AlienVault.**

ABOUT ALIENVAULT

AlienVault 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, AlienVault Unified Security Management, with the power of AlienVault's Open Threat Exchange, the world's largest crowd-sourced threat intelligence community, making effective and affordable threat detection attainable for resource-constrained IT teams. AlienVault is a privately held company headquartered in Silicon Valley and backed by Trident Capital, Kleiner Perkins Caufield & Byers, Institutional Venture Partners, GGV Capital, Intel Capital, Jackson Square Ventures, Adara Venture Partners, Top Tier Capital and Correlation Ventures.

NEXT STEPS: PLAY, SHARE, ENJOY!

- Learn more about AlienVault USM
- See the 90-second demo
- Start detecting threats today with a free 30-day trial
- Join the Open Threat Exchange (OTX)

www.alienvault.com