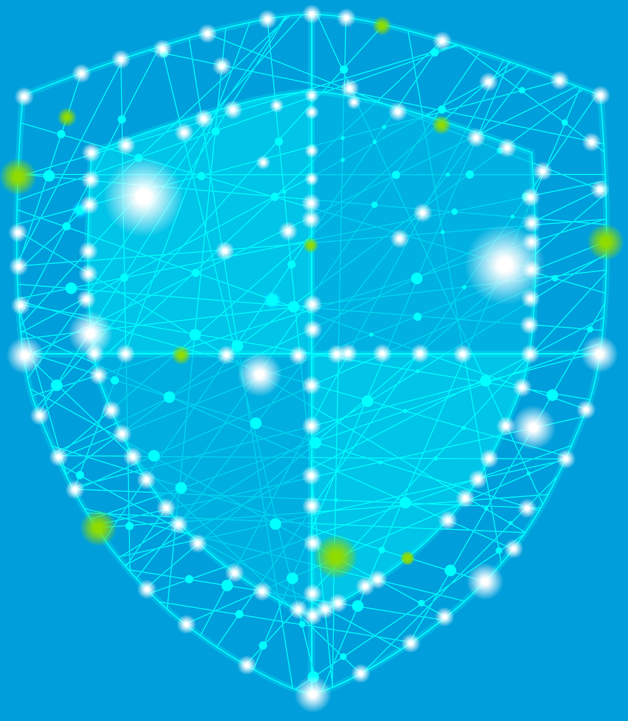


How to build a

Security Operations Center

(on a budget)

AT&T Cybersecurity

AT&T Business

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 protecting your network. Controlling access with tools like passwords, access control lists (ACLs), firewall rules, and others aren't quite good enough. You still have to constantly monitor your critical infrastructure so that you can spot anomalous 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 cybersecurity 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 a Security Operations Center

Security Operations Center (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, and the appropriate remediation.

SOC roles and responsibilities have continued to evolve as the frequency and severity of incidents continue to increase.

Building a SOC with limited resources is 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 security monitoring technologies and near-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, the AlienVault® Unified Security Management® (USM) platform provided by AT&T Cybersecurity provides the foundation you need to build a SOC—without requiring costly implementation services or large teams to manage it. With AlienVault® USM™, powered by threat intelligence from the AT&T Alien Labs™ Security Research Team and AlienVault® Open Threat Exchange® (OTX™), you can quickly achieve a well-orchestrated combination of people, processes, tools, and threat intelligence. Virtually all the key ingredients for building a SOC.

> In each chapter of this eBook, we'll go into detail on 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 and triage; prioritization and analysis; remediation and recovery; and assessment and audit. Examine how AlienVault 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 AlienVault USM.

Chapter 4: **Intelligence**

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

Chapter 1: **People**

Just like people, every security organization is different. In some companies, the executive team recognizes the importance of cybersecurity 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.

Creating 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.

So how do we get there?

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

Setting up the SOC foundation

The quick basics

There are 2 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 AlienVault 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; and sharing your findings with the threat intelligence community.

Key Takeaways Knowing what it takes to build a SOC will help you determine how to staff your team. For assistance with recruiting and staffing, examine our SOC skillset matrix in the chart on the next page to review the roles and responsibilities for building a 4-5 person SOC team that will give your SOC a solid foundation.

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 (IDS, correlation rules, etc.).
Tier 2 **Security Analyst**	**Incident Responder** (IT's version of the First Responder)	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.	Reviews trouble tickets generated by Tier 1 Analyst(s). Utilizes 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.
Tier 3 **Expert Security Analyst**	**Threat Hunter** (Hunts vs. defends)	All of the above + familiar with using data visualization tools and penetration testing tools.	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 and 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 (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).

How do I know if I need an MSSP?

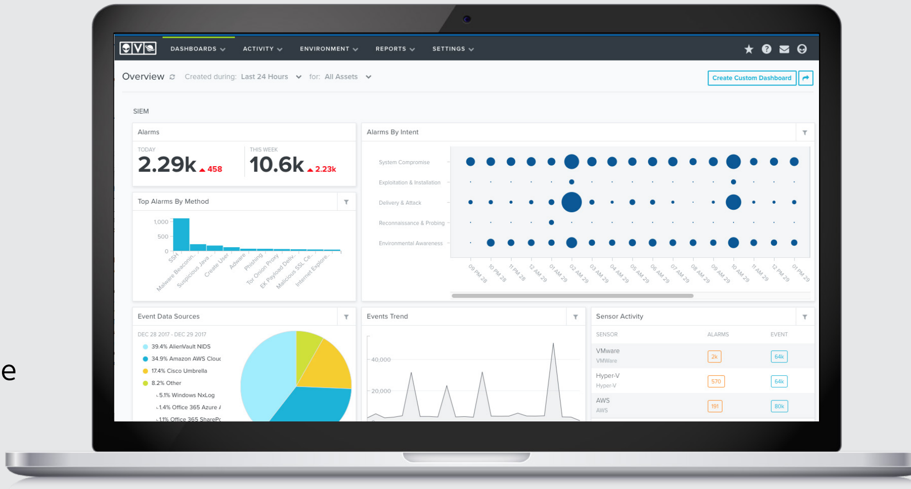
We wish that there was a hard and fast rule to knowing precisely if/when you'd need to outsource your SOC to a service provider. Staff size and skillset is certainly a factor. At the same time, some of the largest enterprises rely on MSSPs instead of building their own SOCs. The choice really comes down 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 utilize an MSSP to manage your SOC.

Learn more about Managed Security offerings from AT&T Cybersecurity here.

Next up

Chapter 2: 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.



SENSOR	ALARMS	EVENT
VMware VMWare	2k	64k
Hyper-V Hyper-V	570	64k
AWS AWS	191	80k

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 provides that you can get to your final destination without spilling any peanuts.

> Checklists are essential to security operations center processes.

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 AlienVault USM to help power your SOC processes.

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

SOC processes

Answering the big question for each SOC stage

1 Event classification and 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 you 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 Unified Security Management (USM)?

AlienVault USM , offered by AT&T Cybersecurity, collects, parses, and analyzes your log data against the latest threat intelligence, which is delivered to the platform automatically and continuously from the Alien Labs Security Research Team and the AlienVault Open Threat Exchange (OTX). As threats and anomalous activities are detected in your environment, AlienVault USM generates alarms, which are mapped to the MITRE ATT&CK™ framework and also automatically prioritized by intent according to the Lockheed Martin Cyber Kill Chain®. This “chain” is a sequence of actions an attacker needs to take in order to infiltrate an environment and exfiltrate data from it. This event categorization helps to highlight the most serious threats facing your assets. This alarm prioritization allows you to focus your attention on the most severe threats first, rather than having to manually review all alarms to know where to start.

The Cyber Kill Chain in Practice

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.

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 weekly basis)
Delivery and attack	Behavior indicating an attempted delivery of an exploit	Low/Med	Review activity from OTX (on a weekly basis)
Exploitation and installation	Behavior indicating a successful exploit of a vulnerability or backdoor/RAT (remote-access trojan) 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), and which events are false positives. AlienVault USM makes this part of the process easy. From any alarm, event, or vulnerability that AlienVault USM detects within your environments, you can easily open and track tickets with third-party productivity tools like ServiceNow® and Jira®, without leaving the USM platform. You can also use labels within USM to classify, track, and search vulnerabilities and alarms. Documenting the investigation provides 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.

2 Prioritization and analysis

Why is this important?

Prioritization is the key to success in any endeavor, and it's even more critical in cybersecurity. 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 responsibility entrusted to the SOC team.

What do SOC analysts do at this stage?

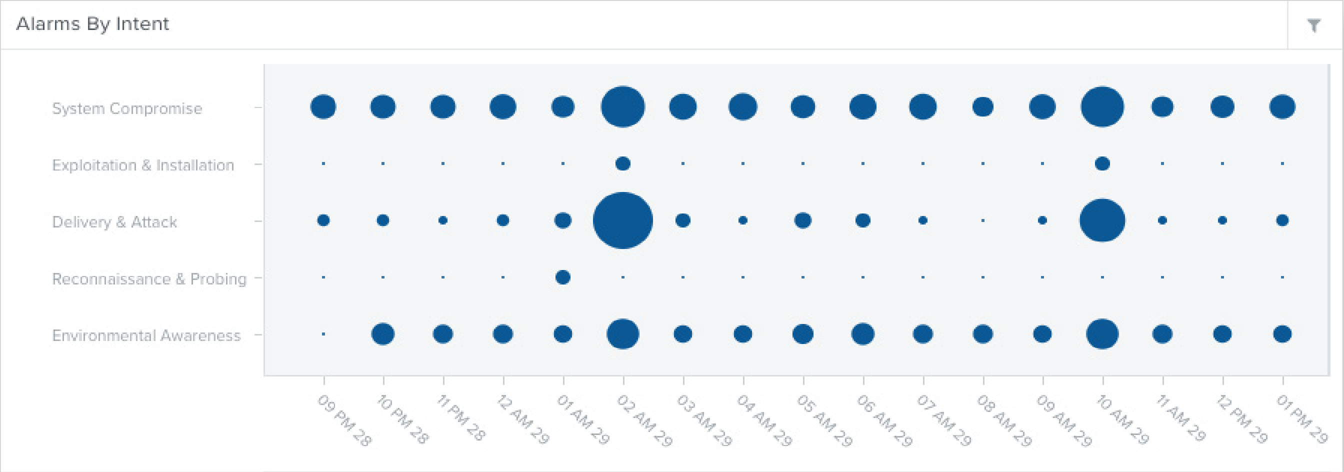
Review and respond to any activity that indicates an adversary has infiltrated your environment. This can range from the installation of a rootkit/RAT or backdoor taking advantage of an existing vulnerability to network communications between an internal host and a known bad IP address associated with a cyber adversary's C2 (command-and-control servers) infrastructure.

How do I do it with AlienVault USM?

Powered by threat intelligence from the Alien Labs Security Research Team, AlienVault 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 AlienVault 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 and installation and system compromise categories, SOC analysts zero in on the threats that have already advanced beyond primary security defenses. With AlienVault USM, analysts can determine the best way to address these attacks using response templates from threat intelligence updates provided by Alien Labs. Because Alien Labs draws insights from the community-powered threat data in OTX, the threat intelligence within AlienVault USM reflects the collective experiences of tens of thousands security practitioners 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 help 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 (tactics, techniques, and procedures) 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 AlienVault USM



Know your network and all its assets

Asset discovery and inventory is one of the most important and yet most overlooked cybersecurity capabilities. When you're on the SOC team, having access to an updated and automated asset inventory is invaluable.

AlienVault USM continuously scans your cloud and on-premises environments to discover assets to monitor. On premises, you can discover all the IP-enabled devices on your network, as well as identify what software and services are running on them, and whether they include potential vulnerabilities. For your Amazon Web Services (AWS®) and Microsoft® Azure® cloud infrastructure, the USM platform provides 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 AlienVault USM asset discovery capabilities.

3 Remediation and 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 have a remediation plan.

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 AlienVault USM?

AlienVault USM simplifies remediation and recovery by helping you detect events quickly so you can respond in time to help prevent further damage. Additionally, AlienVault 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.

To keep track of incident response activities across a team, you can also open tickets within Jira® or ServiceNow® directly from alarms, events, or vulnerabilities within the USM platform. AlienVault USM also enables automatic notification through multiple channels, including Amazon SNS, Slack, PagerDuty®, and Datadog, making it fast and simple to notify stakeholders when incidents occur.

Learn more about AlienVault USM vulnerability assessment capabilities.

4 Assessment and 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 AlienVault USM?

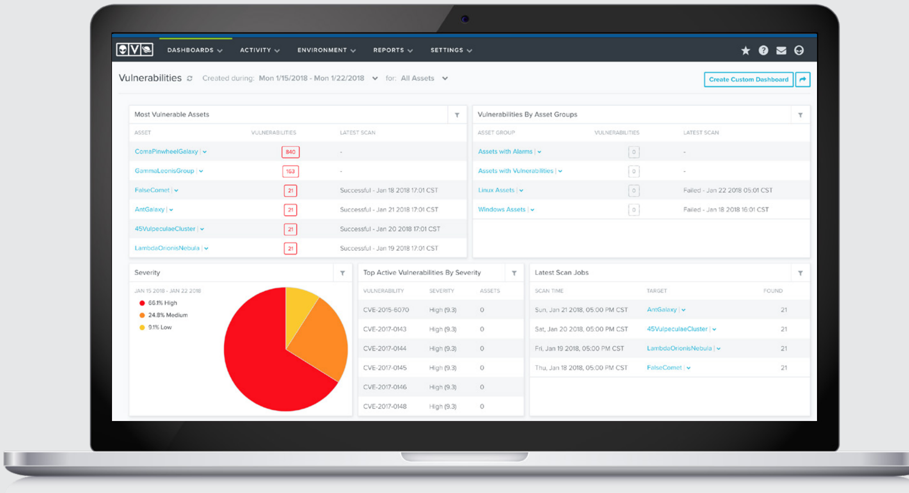
With AlienVault USM, you can run continuous vulnerability scans against all of your assets (internal and external assets, as well as those in your cloud environments) to help detect any system changes that may signal an exposure. These vulnerability reports can be shared with auditors, executive management,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

Next up

Chapter 3:

SOC tools

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



Vulnerabilities Created during: Mon 1/15/2018 - Mon 1/22/2018 for: All Assets

Most Vulnerable Assets

ASSET	VULNERABILITIES	LATEST SCAN
ComaPinwheelGalaxy	840	-
GammaLeonisGroup	163	-
FalseComet	21	Successful - Jan 18 2018 17:01 CST
AntGalaxy	21	Successful - Jan 21 2018 17:01 CST
45VulpeculaeCluster	21	Successful - Jan 20 2018 17:01 CST
LambdaOrionisNebula	21	Successful - Jan 19 2018 17:01 CST

Vulnerabilities By Asset Groups

ASSET GROUP	VULNERABILITIES	LATEST SCAN
Assets with Alarms	0	-
Assets with Vulnerabilities	0	-
Linux Assets	0	Failed - Jan 22 2018 05:01 CST
Windows Assets	0	Failed - Jan 18 2018 16:01 CST

Top Active Vulnerabilities By Severity

VULNERABILITY	SEVERITY	ASSETS
CVE-2015-6070	High (9.3)	0
CVE-2017-0143	High (9.3)	0
CVE-2017-0144	High (9.3)	0
CVE-2017-0145	High (9.3)	0
CVE-2017-0146	High (9.3)	0
CVE-2017-0148	High (9.3)	0

Latest Scan Jobs

SCAN TIME	TARGET	FOUND
Sun, Jan 21 2018, 05:00 PM CST	AntGalaxy	21
Sat, Jan 20 2018, 05:00 PM CST	45VulpeculaeCluster	21
Fri, Jan 19 2018, 05:00 PM CST	LambdaOrionisNebula	21
Thu, Jan 18 2018, 05:00 PM CST	FalseComet	21

Chapter 3: **SOC tools**

Sometimes security pros use the term “defense-in-depth” to describe how to best protect critical data and systems against cyber threats.

Think of this concept as 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 cybersecurity 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 cybersecurity budgets and highly skilled teams, this approach has worked—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 providing that vulnerabilities are patched among other prevention-type activities (e.g. security of desktop configurations and account management and strict password policies, 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 the AT&T Marketplace Pulse: Global State of Cybersecurity*, they found that it was common for victims to learn that they'd been breached from a third party versus discovering these breaches themselves.

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 AlienVault USM combines these essential capabilities for building a SOC into a single platform. Finally, we'll cover how the Alien Labs Threat Intelligence Subscription 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. Help achieve SOC success with limited time and resources by utilizing a single platform like AlienVault USM that consolidates these tools into one place.

* https://www.business.att.com/content/dam/attbusiness/reports/vol4-threatlandscape.pdf

1 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.

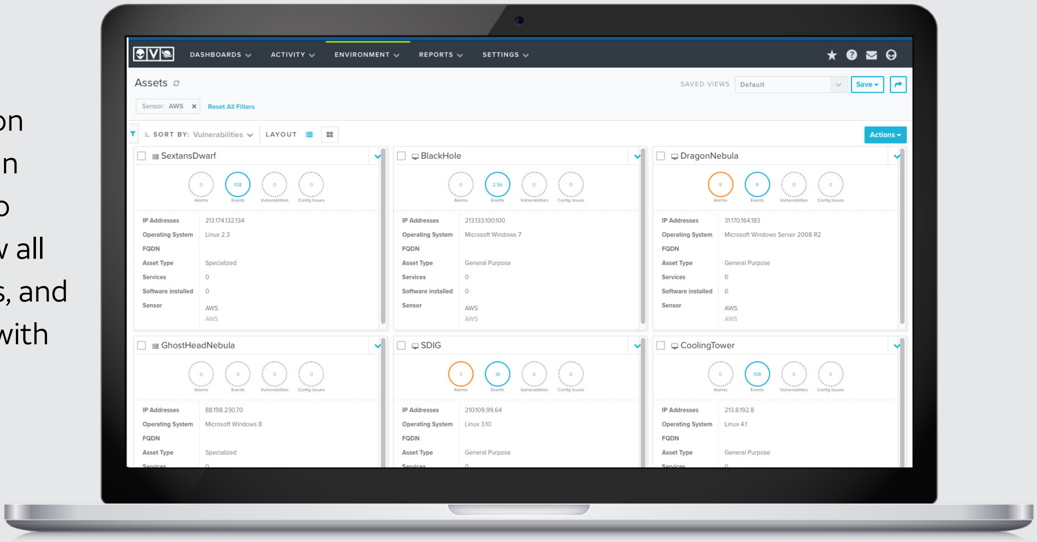
How do I do it with AlienVault USM?

AlienVault USM captures accurate, near-real-time information on all the assets in your on-premises and cloud environments. On-premises, the USM platform 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, the USM platform hooks directly into cloud providers' APIs to give you immediate visibility of your cloud infrastructure. AlienVault USM utilizes native cloud services like AWS® CloudWatch® and Microsoft Azure® Monitor to collect data from your cloud environments and begin detecting threats.

Feature spotlight Asset detail

The asset discovery and inventory capabilities within AlienVault USM are explicitly designed for SOC analysts. The asset inventory tool provides a high 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.



Assets

Sensor: AWS ✖ Reset All Filters

SAVED VIEWS: Default

SORT BY: Vulnerabilities

□ SextansDwarf
Alarms 0 · Events 108 · Vulnerabilities 0 · Config Issues 0

IP Addresses	213.174.132.134
Operating System	Linux 2.3
FQDN	
Asset Type	Specialized
Services	0
Software installed	0
Sensor	AWS AWS

□ BlackHole
Alarms 0 · Events 2.5k · Vulnerabilities 0 · Config Issues 0

IP Addresses	213.133.100.100
Operating System	Microsoft Windows 7
FQDN	
Asset Type	General Purpose
Services	0
Software installed	0
Sensor	AWS AWS

□ DragonNebula
Alarms 9 · Events 9 · Vulnerabilities 0 · Config Issues 0

IP Addresses	31.170.164.183
Operating System	Microsoft Windows Server 2008 R2
FQDN	
Asset Type	General Purpose
Services	0
Software installed	0
Sensor	AWS AWS

□ GhostHeadNebula
Alarms 0 · Events 0 · Vulnerabilities 0 · Config Issues 0

IP Addresses	88.198.230.70
Operating System	Microsoft Windows 8
FQDN	
Asset Type	Specialized
Services	0

□ SDIG
Alarms 3 · Events 18 · Vulnerabilities 0 · Config Issues 0

IP Addresses	210.109.99.64
Operating System	Linux 3.10
FQDN	
Asset Type	General Purpose
Services	0

□ CoolingTower
Alarms 0 · Events 108 · Vulnerabilities 0 · Config Issues 0

IP Addresses	213.8.192.8
Operating System	Linux 4.1
FQDN	
Asset Type	General Purpose
Services	0

2 Vulnerability assessement

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 AlienVault USM?

AlienVault USM includes a built-in vulnerability assessment tool that allows you to 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, AlienVault USM takes a different approach. It provides a unified and easy-to-use platform that bolsters vulnerability scanning software with asset discovery, a streamlined user interface, and easy scheduling so you can have 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, AlienVault USM offers cloud vulnerability scanning capabilities using cloud-native sensors for your Azure and AWS environments, giving you virtually complete visibility into your cloud and on-premises environments from a single pane of glass.

A closer look: Vulnerability assessment in USM

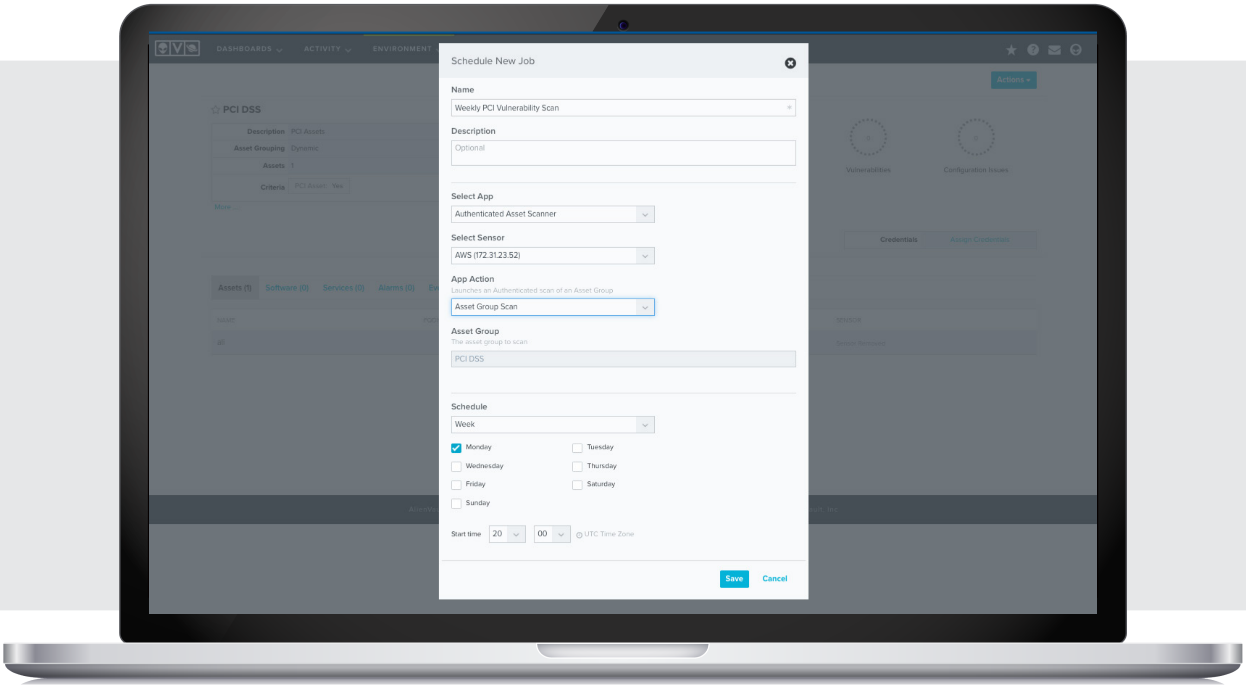
Regularly scheduled auto-scanning: Create scans that run daily, weekly, or monthly during your off-peak hours. Automated scanning allows for continuous visibility of your vulnerabilities as your IT landscape changes.

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 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.

Feature spotlight:

Vulnerability scan scheduler



Schedule New Job

Name: Weekly PCI Vulnerability Scan

Description: Optional

Select App: Authenticated Asset Scanner

Select Sensor: AWS (172.31.23.52)

App Action — Launches an Authenticated scan of an Asset Group: Asset Group Scan

Asset Group — The asset group to scan: PCI DSS

Schedule: Week

☑ Monday ☐ Tuesday
☐ Wednesday ☐ Thursday
☐ Friday ☐ Saturday
☐ Sunday

Start time 20 00 UTC Time Zone

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, AlienVault USM offers SOC analysts control and flexibility when setting up ad-hoc and scheduled vulnerability scans.

With USM Anywhere, 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

3 Behavioral monitoring

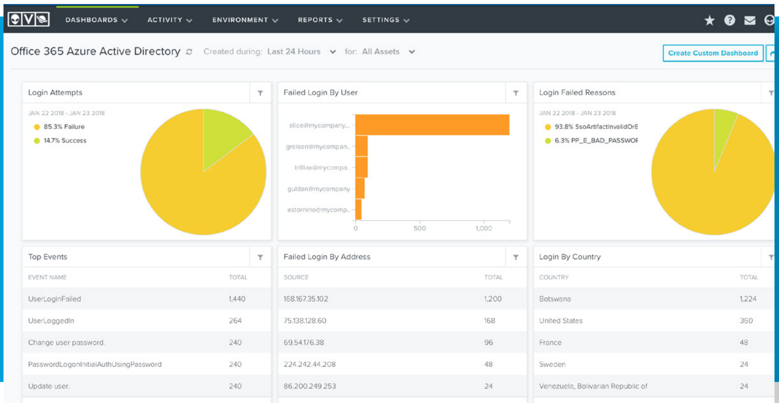
Why is this important?

At its most basic, effective cybersecurity 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's 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 AlienVault USM?

AlienVault USM provides fully integrated behavioral monitoring technologies within its platform, including visibility of user behavior in your cloud environments and applications. USM provides cloud access logs (Microsoft Azure® Monitor, AWS® CloudTrail®, S3, ELB); AWS VPC flow monitoring; asset access logs; and VMware access logs.



Office 365 Azure Active Directory   Created during: Last 24 Hours   for: All Assets

Top Events

EVENT NAME	TOTAL
UserLoginFailed	1,440
UserLoggedIn	264
Change user password.	240
PasswordLogonInitialAuthUsingPassword	240
Update user.	240

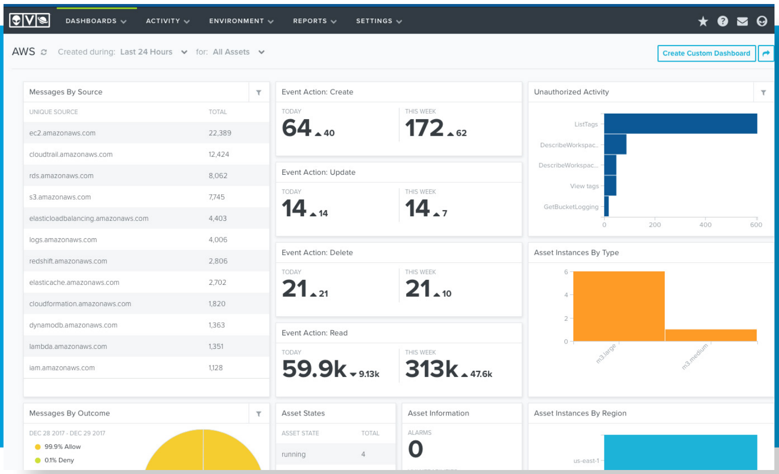
Failed Login By Address

SOURCE	TOTAL
168.167.35.102	1,200
75.138.128.60	168
69.54.176.38	96
224.242.44.208	48
86.200.249.253	24

Login By Country

COUNTRY	TOTAL
Botswana	1,224
United States	360
France	48
Sweden	24
Venezuela, Bolivarian Republic of	24

Cloud application monitoring for applications like Office 365™ allows you to track user and admin activity that might indicate a data breach.



AWS   Created during: Last 24 Hours   for: All Assets

Messages By Source

UNIQUE SOURCE	TOTAL
ec2.amazonaws.com	22,389
cloudtrail.amazonaws.com	12,424
rds.amazonaws.com	8,062
s3.amazonaws.com	7,745
elasticloadbalancing.amazonaws.com	4,403
logs.amazonaws.com	4,006
redshift.amazonaws.com	2,806
elasticache.amazonaws.com	2,702
cloudformation.amazonaws.com	1,820
dynamodb.amazonaws.com	1,363
lambda.amazonaws.com	1,351
iam.amazonaws.com	1,128

Event Action: Create
TODAY 64 ▲40   THIS WEEK 172 ▲62

Event Action: Update
TODAY 14 ▲14   THIS WEEK 14 ▲7

Event Action: Delete
TODAY 21 ▲21   THIS WEEK 21 ▲10

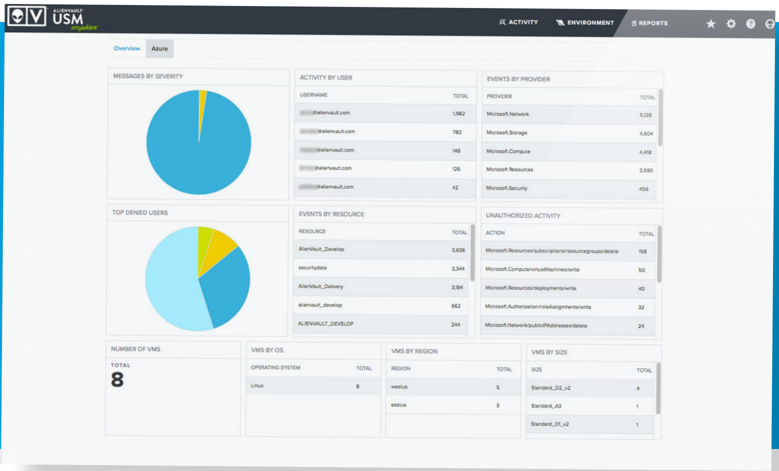
Event Action: Read
TODAY 59.9k ▼9.13k   THIS WEEK 313k ▲47.6k

Asset States

ASSET STATE	TOTAL
running	4

Asset Information
ALARMS 0

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



ACTIVITY BY USER

USERNAME	TOTAL
[redacted]@alienvault.com	1,982
[redacted]@alienvault.com	782
[redacted]@alienvault.com	148
[redacted]@alienvault.com	126
[redacted]@alienvault.com	42

EVENTS BY PROVIDER

PROVIDER	TOTAL
Microsoft.Network	5,128
Microsoft.Storage	4,604
Microsoft.Compute	4,418
Microsoft Resources	3,590
Microsoft.Security	456

EVENTS BY RESOURCE

RESOURCE	TOTAL
AlienVault_Develop	3,636
securitydata	3,344
AlienVault_Delivery	3,184
alienvault_develop	662
ALIENVAULT_DEVELOP	244

UNAUTHORIZED ACTIVITY

ACTION	TOTAL
Microsoft.Resources/subscriptions/resourcegroups/delete	158
Microsoft.Compute/virtualMachines/write	50
Microsoft.Resources/deployments/write	40
Microsoft.Authorization/roleAssignments/write	32
Microsoft.Network/publicIPAddresses/delete	24

NUMBER OF VMS
TOTAL 8

VMS BY OS

OPERATING SYSTEM	TOTAL
Linux	8

VMS BY REGION

REGION	TOTAL
westus	5
eastus	3

VMS BY SIZE

SIZE	TOTAL
Standard_D2_v2	4
Standard_A3	1
Standard_D1_v2	1

Cloud management plane integration provides that you are able to monitor your AWS and Azure instances automatically.

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 (IDSs) are considered one of the "must-have" SOC tools for identifying known attacks and known attacker activity. The keyword is "known." On-premises, an IDS operates 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 AlienVault USM?

AlienVault USM offers 3 types of IDS technologies that you can enable on a per-network, per-asset group, or per-server basis. Network intrusion detection (NIDS) analyzes on-premises network traffic to detect known attack patterns that indicate malicious activity (e.g. malware infections, policy violations, port scans, etc.).

The USM platform's host-based intrusion detection (HIDS) analyzes system behavior and configuration that could indicate system compromise. This includes the ability to recognize common rootkits, detect rogue processes, and detect modification to critical configuration files. Additionally, AlienVault USM delivers **cloud intrusion detection system (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 Alien Labs Security Research Team keeps AlienVault USM 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 Alien Labs is a critical extension to your SOC team, allowing you to focus on response.

Feature spotlight:

AlienVault USM integration with AT&T Alien Labs threat intelligence

Before explaining how this integration works, it's important to understand how the Alien 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 AlienVault Open Threat Exchange (OTX), the Alien Labs Security Research Team collects millions of threat indicators every day, including malicious IP addresses and URLs, domain names, malware samples, and suspicious files. The Alien Labs team aggregates data from a wide range of sources, including:

- External threat vendors (such as McAfee®, Emerging Threats, VirusTotal®)
- 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)
- AlienVault USM and AlienVault 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 Alien Labs 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 Alien Labs 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 Alien Labs team delivers all information about the threats and the attack infrastructure to the USM platform via the Alien Labs Threat Intelligence Subscription. The team regularly updates 8 coordinated rulesets, including correlation directives, IDS signatures and 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 Alien Labs Team's 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 help 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.

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 built the platform (AlienVault USM), the community (OTX), and the threat research team (Alien Labs) to create a SOC for virtually all teams to implement—no matter the size.

How do I do it with AlienVault USM?

AlienVault 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 Alien 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, the USM platform's correlation logic translates into rich and highly detailed compliance-ready 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 may not have the time, budget, or resources to constantly research the global threat landscape, don't worry. The Alien Labs security research team does it for you. With its built-in threat intelligence subscription, the AlienVault USM platform is regularly updated with:

- **New and advanced correlation directives** to help find the latest threats among the activity on your network
- **New IDS signatures** to help detect emerging threats on your network and servers
- **New vulnerability checks** to provide that systems and apps are effectively patched
- **New asset discovery signatures** for an accurate asset inventory
- **Dynamic IP reputation data** to help detect activity with the latest known bad adversaries
- **New data source plugins** to consume more raw event log data
- **Updated report templates** to help demonstrate compliance with PCI DSS, HIPAA, and more
- **Up-to-the-minute guidance** to help discover emerging threats and context-specific remediation
- **A contribution system** for malware to be analyzed

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

The Alien Labs security research team helps maximizes the efficiency of security monitoring programs 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:

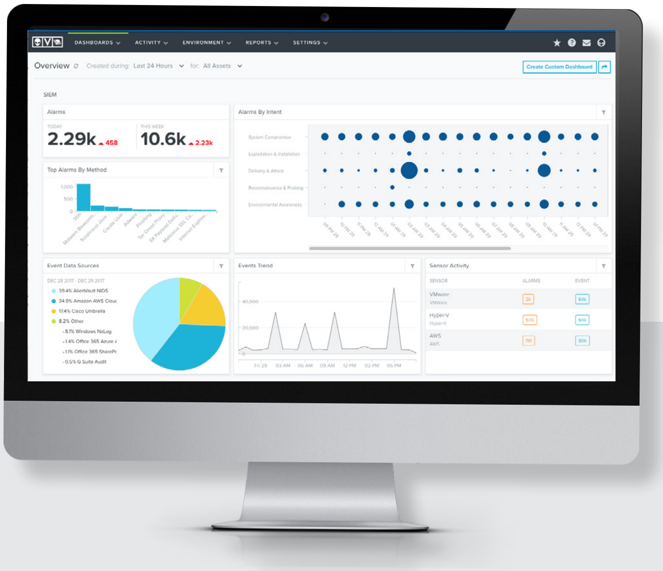
AlienVault USM security dashboards and visualizations

If you can't measure it, you can't manage it. That's a favorite saying 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, AlienVault USM includes intuitive dashboards and clean visualizations. The USM platform 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 in the USM platform to see details about the threats and vulnerabilities affecting your critical infrastructure.



SENSOR	ALARMS	EVENT
VMware VMWare	2k	64k
Hyper-V Hyper-V	570	64k
AWS AWS	191	80k

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 activity 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 high quality threat intelligence that is essential for building a SOC.

Key Takeaways Understand the differences among tactical, strategic, and 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 the Alien Labs Security Research Team.

Know thyself. Know thy enemy.
A thousand battles. A thousand victories.

– Sun Tzu, The Art of War

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 cybersecurity 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 the upper hand 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 3 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.

Three types of threat intelligence for SOC teams

The following table outlines how each of the 3 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 cybersecurity 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 provide alignment between their cybersecurity strategy and real-world risk.	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.
How it works in AlienVault USM	AlienVault USM Anywhere receives continuous updates with the latest indicators from the AlienVault Labs Security Research Team. These updates utilize threat data from the larger community in AlienVault OTX, so they reflect in-the-wild attacks on organizations of all sizes from around the world.	Alien Labs Security Research Team members spend countless hours researching the latest threat actors and their methods. These discoveries are integrated into the USM Anywhere platform through continuous threat intelligence updates, which include rich, context-specific guidance on how to respond to threats detected in your environments.	The Alien Labs Security Research Team regularly publishes threat intelligence updates to the USM Anywhere 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 utilizes the power of Alien Labs OTX, the world’s largest crowdsourced repository of threat data to provide global insight into attack trends and bad actors.
Key benefits	• Constantly updated in near-real time • Easily searchable • Easily shared • Easily integrated	• Educates and empowers SOC team and leadership decision-making • Helps communicate the urgency of cybersecurity issues to execs, board members, and other stakeholders	• Automatically detects the latest threats • Guides SOC analyst actions • Powered by near-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 AT&T Cybersecurity has incorporated each one of these approaches into the USM platform.

Crowdsourced

One of the best innovations in the industry has been driven by the cybersecurity 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, virtually seamless integration with the USM platform, 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 cybersecurity hardware and software vendors (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 Alien 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 AlienVault 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)

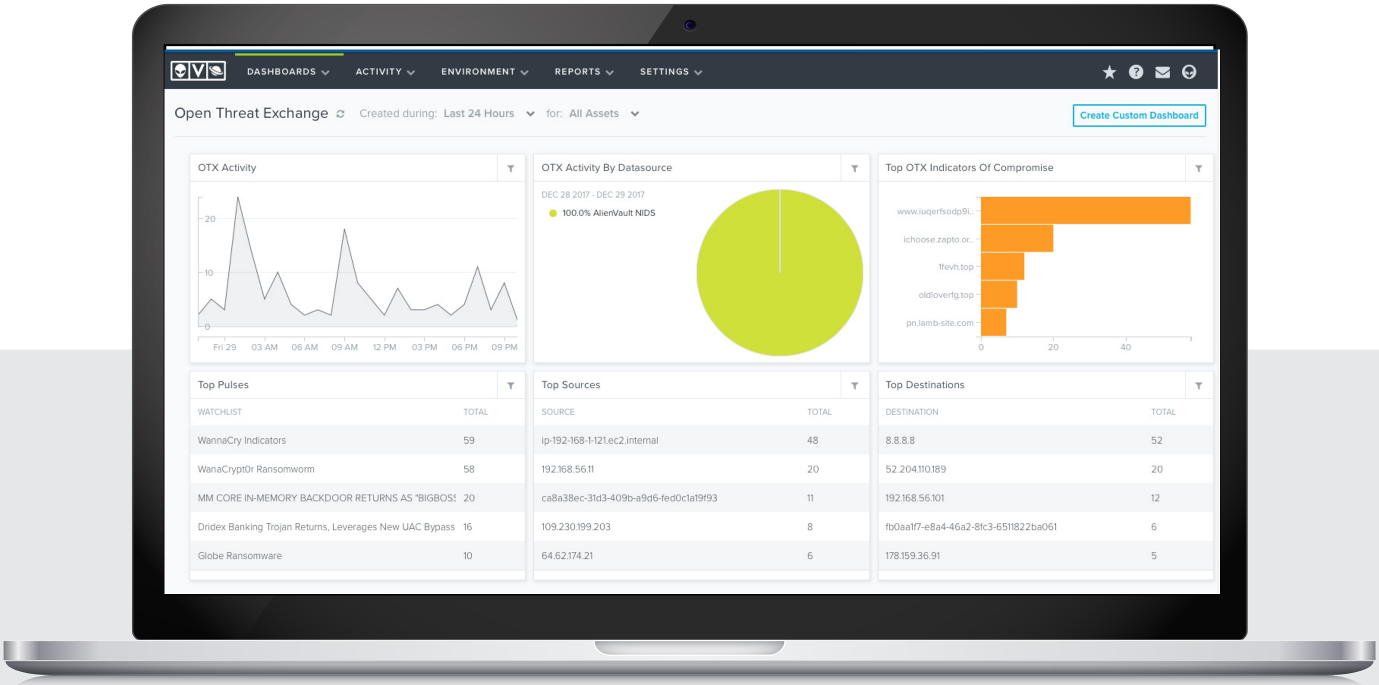
With the number of OSINT (open source intelligence or public intelligence) sources available, it is theoretically possible to "write your own" correlation rules or signatures to detect specific exploits or attack patterns. You can download IOCs from AlienVault OTX or submit malware samples to VirusTotal®, 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:

Alien Labs OTX threat data

Real-time threat sharing and collaboration is one of the best ways that lean and mean SOC teams can help 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 cybersecurity threats as well as how active collaboration can improve security for all. Because the Alien Labs Security Research Team analyzes OTX threat data to generate the continuous threat intelligence updates they curate for AlienVault USM, SOC analysts using the USM platform can know 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.



Open Threat Exchange   Created during: Last 24 Hours   for: All Assets

Top Pulses

WATCHLIST	TOTAL
WannaCry Indicators	59
WanaCrypt0r Ransomworm	58
MM CORE IN-MEMORY BACKDOOR RETURNS AS "BIGBOS!	20
Dridex Banking Trojan Returns, Leverages New UAC Bypass	16
Globe Ransomware	10

Top Sources

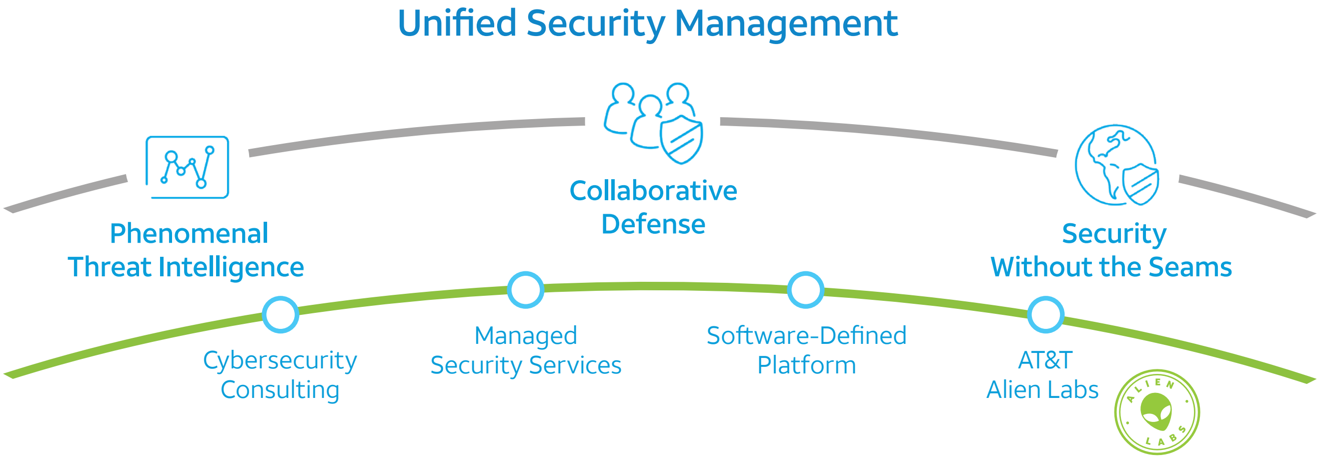
SOURCE	TOTAL
ip-192-168-1-121.ec2.internal	48
192.168.56.11	20
ca8a38ec-31d3-409b-a9d6-fed0c1a19f93	11
109.230.199.203	8
64.62.174.21	6

Top Destinations

DESTINATION	TOTAL
8.8.8.8	52
52.204.110.189	20
192.168.56.101	12
fb0aa1f7-e8a4-46a2-8fc3-6511822ba061	6
178.159.36.91	5

About AT&T Cybersecurity

AT&T Cybersecurity's edge-to-edge technologies provide phenomenal threat intelligence, collaborative defense, security without the seams, and solutions that fit your business. Our unique, collaborative approach integrates best-of-breed technologies with unrivaled network visibility and actionable threat intelligence from Alien Labs researchers, Security Operations Center analysts, and machine learning — helping to enable our customers around the globe to anticipate and act on threats to protect their business.


Unified Security Management
Phenomenal Threat Intelligence
Collaborative Defense
Security Without the Seams
Cybersecurity Consulting
Managed Security Services
Software-Defined Platform
AT&T Alien Labs
ALIEN LABS

This document is intended to include general overview information. Use of third party companies in the document are for informational purposes only and do not constitute any endorsements by AT&T Cybersecurity.

AT&T Business

www.alienvault.com