WHITE PAPER

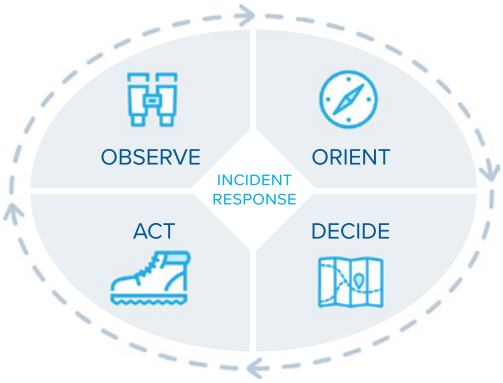
The AlienVault Incident Response Toolkit:

PUTTING THE OODA LOOP TO WORK IN THE REAL WORLD

When it comes to data breaches, most agree that it's not a matter of if, but when. In CyberEdge Group's 2017 Cyberthreat Defense Report, an astounding 79% of surveyed organizations admitted being victims of cyber attacks, up from 76 percent in 2016 and 70 percent in 2015.1

Given that intrusions are inevitable, it's important to have the right tools in place to spot an event quickly and to minimize its impact on your organization with an effective response plan.

We believe the best way to approach Incident Response is to deploy the OODA Loop method, developed by US Air Force military strategist John Boyd. The OODA Loop focuses on the key essential tactics for responding to any crisis: Observe, Orient, Decide, and Act.



In this paper, you'll read about a few specific use cases where AlienVault® Unified Security Management® (USM) helps you Observe, Orient, Decide, and Act for effective incident response.

When observing for potential risks and impending threats, there are three essential success factors that should guide your activity as an incident responder.

OBSERVE:

Use security monitoring to identify anomalous behavior that may require investigation.

- OBSERVE FROM ALL ANGLES.
- APPLY PRIORITIZATION BASED ON THE LATEST THREAT INTELLIGENCE.
- CONTINUOUSLY FINE-TUNE SECURITY MONITORING TOOLS.

[1] http://cyber-edge.com/2016-cdr/

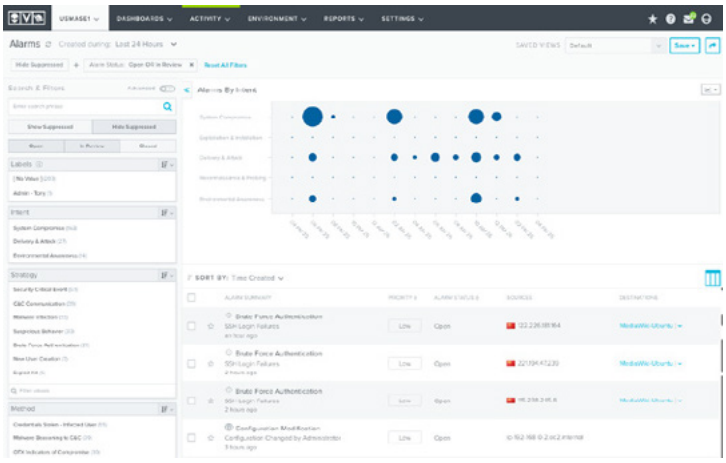
OBSERVE FROM ALL ANGLES WITH ALIENVAULT® UNIFIED SECURITY MANAGEMENT® (USM)

For your incident response plan to be effective, you need to consider your organization's security from a holistic perspective. For example, it's impossible to detect threats effectively if your security plan doesn't account for the entirety of your organization's critical infrastructure. Similarly, a plan that doesn't include threat intelligence updates leaves your organization vulnerable to emerging threats.

AlienVault USM provides the 360-degree security visibility that you need for full situational awareness across your cloud, and on-site environments. The USM platform's approach combines the essential capabilities your organization needs into a single solution, including asset discovery, vulnerability scanning, intrusion detection, behavioral monitoring, SIEM, log management, and threat intelligence.

PRIORITIZE EFFECTIVELY WITH THREAT INTELLIGENCE FROM ALIENVAULT

Threat detection starts with an awareness of the constantly-evolving threat landscape, which is a challenge for any organization without its own dedicated research team. With AlienVault USM, the latest threat intelligence is built into the platform itself through continuous updates from the AlienVault Labs Security Research Team in the form of correlation rules, vulnerability signatures, response templates, and more. As a result, AlienVault USM is always ready to detect the latest threats.



To help you effectively prioritize each security alarm, the USM platform automatically classifies each alarm that occurs within your environments according to the AlienVault Cyber Kill Chain. The Kill Chain is a representation of the level of risk associated with that alarm, with System Compromise representing the greatest risk. With this information, along with information including attack strategy, method, and more, you have the context you need to understand the nature of the threat and how to respond.

The AlienVault® Cyber Kill Chain is modeled after the Lockheed Martin Cyber Kill Chain taxonomy,[2] which we have simplified from seven steps to a five-step process based upon the Security Research Team's research into emerging attacker tools, techniques, and tactics.

When your goal is to hunt down attacks quickly, minimize damage, and rapidly recover – quick prioritization is the key to your success. By automating event analysis and classification with the AlienVault Cyber Kill Chain, AlienVault USM arms your security team with automated prioritization for effective incident response.

CONTINUOUSLY UPDATE AND TUNE SECURITY MONITORING TOOLS.

Malicious actors are constantly coming up with new threats. Between researching new threats, applying that information to threat detection efforts, prioritizing intrusions, and figuring out how to respond, most organizations are ill-equipped to stay up-to-date on their own.

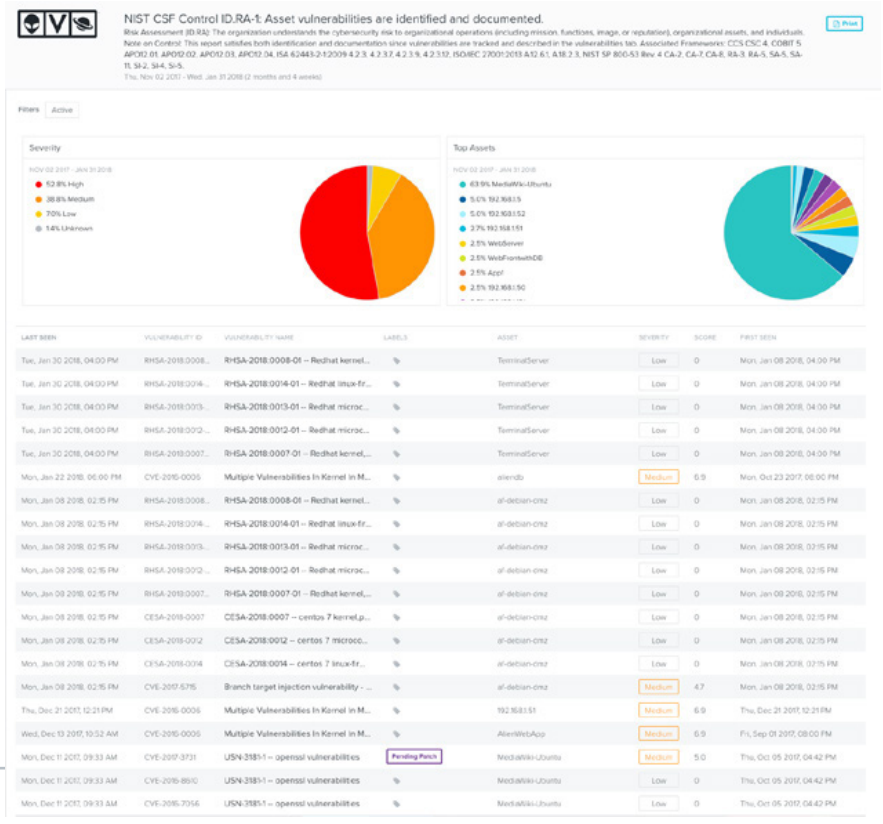
To address that challenge, the AlienVault Labs Security Research Team delivers continuous threat intelligence updates to the USM platform itself so that your team is always equipped to detect, prioritize, and respond to the latest threats affecting your critical infrastructure.

Here's an example of what it looks like to address a new threat within AlienVault USM:

What happened? A new OpenSSL vulnerability has been announced publicly.

WHAT DO YOU DO?

First, ensure initiate or schedule an automated vulnerability scan. You can analyze the scan results to detect the presence of the SSL vulnerability and view guidance on how to respond.



[2] *http://cyber.lockheedmartin.com/solutions/cyber-kill-chain*

Observe: Summary

KEY TAKEAWAY #1: OBSERVE FROM ALL ANGLES

How does AlienVault help? AlienVault Unified Security Management® (USM) unifies the following distinct layers of security monitoring telemetry to provide a full 360-degree view of your assets:

- **Emerging threat detection** – The AlienVault Security Research Team combines proprietary research with crowd-sourced insights from the AlienVault Open Threat Exchange® (OTX™)[3] to craft actionable threat intelligence updates for the USM platform, assuring that AlienVault USM can help you detect and respond to new threats.
- **Behavioral monitoring** – Correlation rules enable you to spot suspicious user and administrator activity and act quickly when potential threats are identified.
- **Vulnerability assessment** – Vulnerability scans and continuous vulnerability monitoring help you identify risks and prioritize remediation fast.
- **Event log analysis / SIEM** – Unifies and performs analysis of events from across your entire infrastructure. This includes your firewalls, servers, routers, domain controllers, cloud workloads, public cloud services, and more to fuel your incident response program.

KEY TAKEAWAY #2: APPLY PRIORITIZATION WITH ALIENVAULT LABS THREAT INTELLIGENCE

How does AlienVault help? AlienVault USM maps each security alarm against the AlienVault Cyber Kill Chain so that security analysts understand the intent of the malicious behavior and know which incidents to investigate first. The AlienVault Labs Security Research Team powers this prioritization by monitoring and analyzing the latest attack techniques, tools, and tactics, and by applying this analysis to the USM platform's correlation engine.

KEY TAKEAWAY #3: TUNE SECURITY MONITORING TO YOUR ENVIRONMENT'S NEEDS

How does AlienVault help? The USM platform allows you to tailor the alarms you receive to better reflect your organization's specific observational requirements.

[3] OTX is the world's first truly open threat intelligence community that enables collaborative defense with open access, collaborative research, Integration with AlienVault USM and OSSIM, as well as ability to export IoCs to almost any security product. OTX enables everyone in the OTX community to actively collaborate, strengthening their own defenses while helping others do the same. To learn more, go to https://otx.alienvault.com

ORIENT:

Evaluate what's going on in the cyber threat landscape & inside your company. Make logical connections & real-time context to focus on priority events.

All the information you've collected during the observation phase is essential for detecting a security event that requires your investigation. But information without context is not sufficient for closedloop incident response.

That's where the **Orient** phase comes in.

Contextual information is essential for orientation. All the data in the world is useless without having the necessary context to understand the significance of that data. For example, a system outage in your data center could either be an innocuous event (unexpected power failure) or something more serious (denial of service attack). Without the necessary context to orient you—for example, an email announcement from your ISP about the outage—you can't implement an effective response.

YOUR INCIDENT RESPONSE GOALS DURING THE ORIENT PHASE INCLUDE:

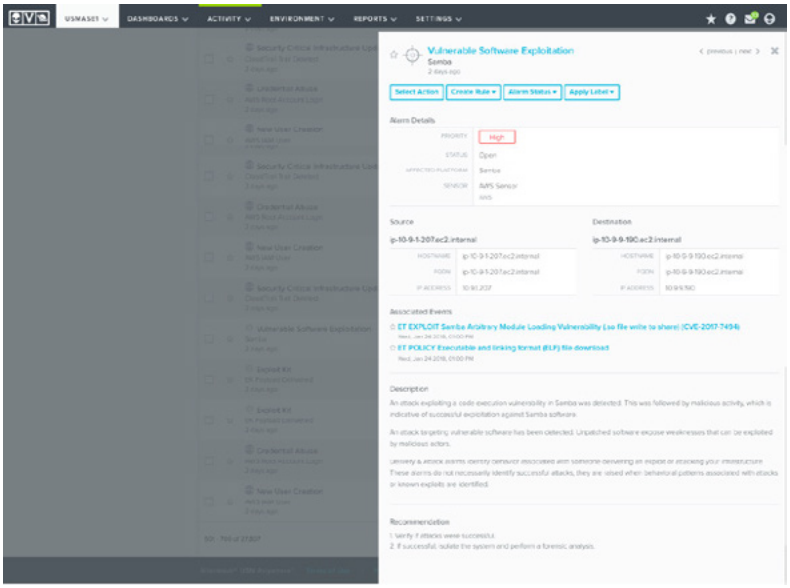
- DETERMINE THE SCOPE AND IMPACT OF AN ATTACK BASED ON THE LATEST THREAT INTELLIGENCE.
- REVIEW EVENTS IN THE CONTEXT OF OTHER ACTIVITY ON THE NETWORK TO ESTABLISH A TIMELINE.
- INVESTIGATE THE SOURCE OF THE ATTACK TO DETERMINE ATTRIBUTION (IF POSSIBLE) AND ANY ADDITIONAL INTELLIGENCE THAT CAN ASSIST DECISION-MAKING.

DETERMINE THE SCOPE AND IMPACT OF AN ATTACK BASED ON THE LATEST THREAT INTELLIGENCE.

The AlienVault Labs Security Research Team draws on threat data from the global AlienVault Open Threat Exchange® (OTX™) community as they research, monitor, and analyze the latest attacker tools and tactics. They convert this intelligence into automated actions (correlated rules, alarms, and response templates) within AlienVault USM so that you can effectively respond.

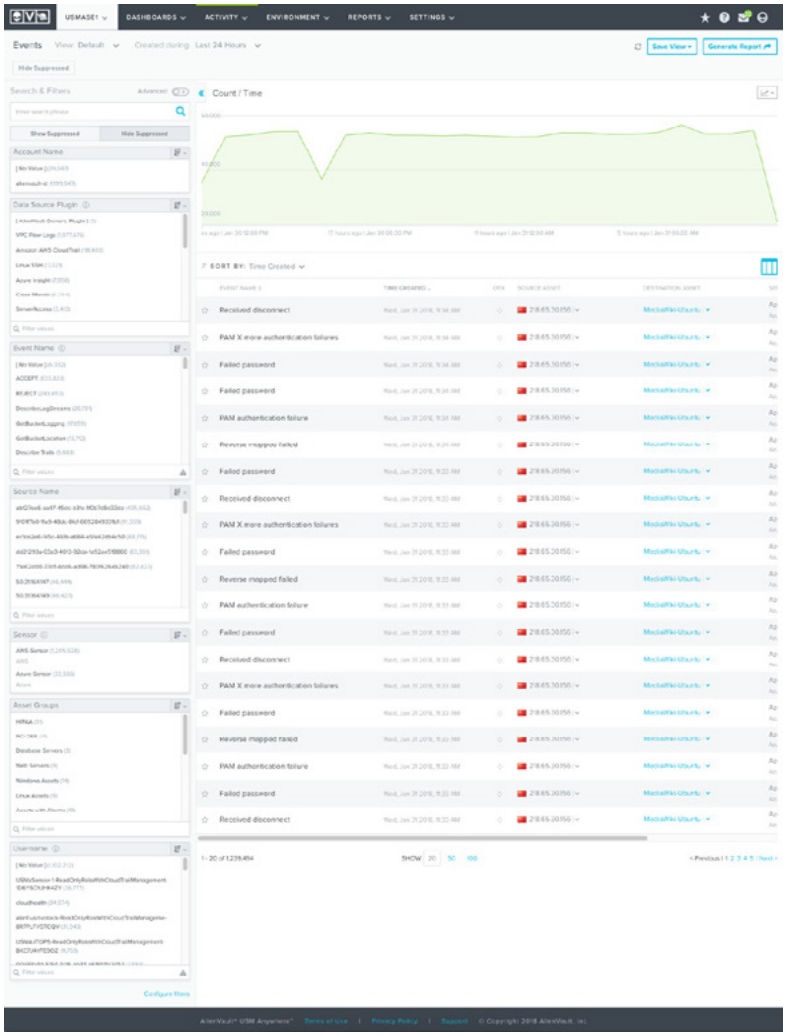
These tools enable you to quickly determine which assets are affected and the severity of the activity or attack.

Here's a specific example. In your AlienVault USM environment, you see an alarm for a vulnerable software exploitation event. In investigating further, you see that this involves an asset that's running a vulnerable version of Samba, and it may not be the only asset that's vulnerable. Directly from the alarm within AlienVault USM, you're able to orchestrate response actions to isolate the endpoint until it can be patched, collect forensic data to help you investigate whether the exploit was successful, and run a vulnerability scan to identify other systems with this type of vulnerability.



REVIEW EVENTS IN THE CONTEXT OF OTHER ACTIVITY ACROSS YOUR ENVIRONMENTS TO ESTABLISH A TIMELINE

AlienVault USM provides a unified timeline for all events to easily make connections between and among disparate-but-related events. By viewing all events across a visual timeline, you can easily scan all the security events and activity



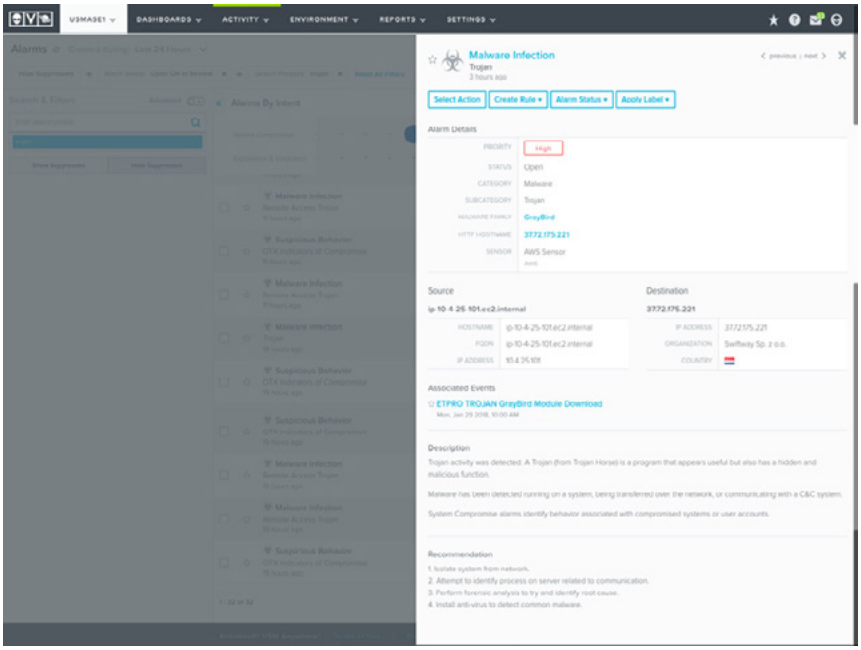
By viewing all events across a visual timeline, you can easily scan all the security events and activity across your network—without having to consult multiple consoles, apps, or databases.

The simplified data visualization approach makes it easy to make quick conclusions about which events require further investigation. In order to provide enough context yet not to overwhelm your team, AlienVault chose to use a simplified design for the USM platform's event timeline.

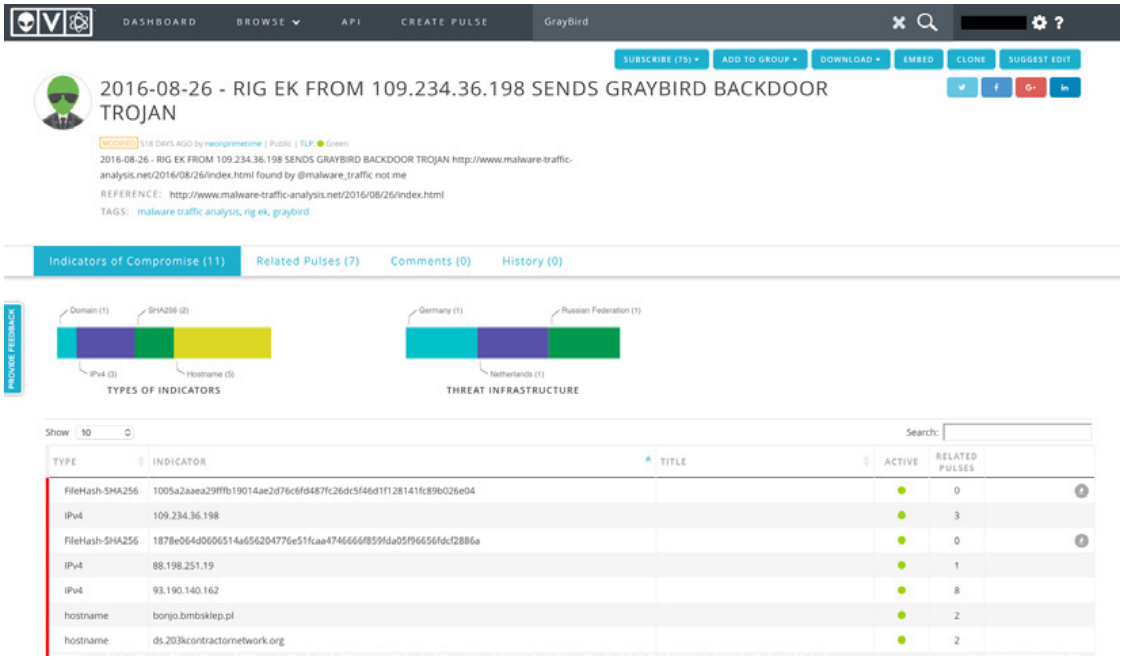
INVESTIGATE THE SOURCE OF AN ATTACK TO DETERMINE ATTRIBUTION (IF POSSIBLE) AND ANY ADDITIONAL INTELLIGENCE THAT CAN ASSIST DECISION-MAKING

According to cyber security expert Bruce Schneier,4 strong attribution can lead to deterrence. It can also provide the essential context to help detect and prevent future attacks and attackers that may share those same motivations, tools, and techniques. The AlienVault Security Research Team's use of AlienVault OTX threat data from around the world to inform the threat intelligence updates to AlienVault USM enables our customers to use this intelligence for more reliable incident response.

Here's an example from the trenches. In the AlienVault USM demo environment, we don't mind a bit of poking and prodding from the ne'er-do-wells in cyber space. In fact, it helps us capture interesting events that we can share with our customers and partners. As you can see in this screenshot, AlienVault USM shows that this malware infection is a trojan from the GrayBird family. Clicking on the malware family name will present threat intelligence pulses within OTX that have been created by OTX users around the world, and will give additional context on the threat. You can also search your own environment for other activity associated with this malware.



[6] https://www.schneier.com/blog/archives/2015/03/attack



Additionally, you can search for this particular malware family across all your events to find activity that may have affected other assets. You can also orchestrate an action such as the collection of forensic data to help your investigation with just a few clicks from within the alarm.

ORIENT: Summary

KEY TAKEAWAY #1: DETERMINE SCOPE AND IMPACT OF AN ATTACK USING THE LATEST THREAT INTELLIGENCE

How does AlienVault help? The AlienVault Labs Security Research Team orients AlienVault USM customers by identifying the latest threats, resulting in the broadest view of threat vectors, attack techniques, and effective defenses. The insights the team draws from AlienVault OTX widen the threat context by using crowd-sourced and community-verified threat intelligence on the latest attacks. Through continuous threat intelligence updates in the form of correlation rules, vulnerability signatures, and remediation templates, the Security Research Team helps you convert intelligence into action within AlienVault USM.

KEY TAKEWAY #2: REVIEW EVENTS IN THE CONTEXT OF OTHER ACTIVITY ON NETWORK TO ESTABLISH A TIMELINE

How does AlienVault help? AlienVault USM provides a unified view of all events to easily make connections between and among disparate-but-related events. The simplified design and userfriendly dashboard makes it easy to see and search events within a contextual timeline to assist in effective decision-making.

KEY TAKEAWAY #3: INVESTIGATE THE SOURCE OF AN ATTACK TO DETERMINE ATTRIBUTION (IF POSSIBLE) AND ANY ADDITIONAL INTELLIGENCE THAT CAN ASSIST DECISION-MAKING

How does AlienVault help? Working with other cyber security industry leaders, the AlienVault Labs Security Research Team works tirelessly to uncover and analyze details on attack campaigns for reliable attribution. Community-driven resources, like the AlienVault® Open Threat Exchange® (OTX™) and OTX pulses (collections of IoCs generated by the OTX community) enable defenders to describe and submit any type of online threat including malware, fraud campaigns, and even state-sponsored hacking. These discoveries are tightly integrated into AlienVault USM in the form of correlation directives for automated event analysis and more informed incident response.

The first two stages in the OODA loop—Observe and Orient—are all about security monitoring essentials. OTX Labs helps by gathering as much data as possible and then placing it in the context of local and global risk so that you can make the best decision possible.

DECIDE:

Based on observations & context, choose the best tactic for minimal damage & fastest recovery.

These first two phases benefit from using automated tools for data collection and analysis, but deciding what to do based on this intelligence unfortunately can't be outsourced to non-humans. At least not yet.

That said, the AlienVault Labs Security Research Team, AlienVault USM, and the AlienVault OTX community provide guidance to support the best possible decisions and outcome.

THE KEY INCIDENT RESPONSE GOALS FOR THE DECIDE PHASE INCLUDE THE FOLLOWING:

- DETERMINE THE IMMEDIATE NEXT STEPS IN RESPONDING TO THE INCIDENT.
- REVIEW ASSET DETAILS AND PRIORITIZE YOUR RESPONSE.
- DOCUMENT ALL REMEDIATION TACTICS PLANNED FOR THE AFFECTED ASSETS.

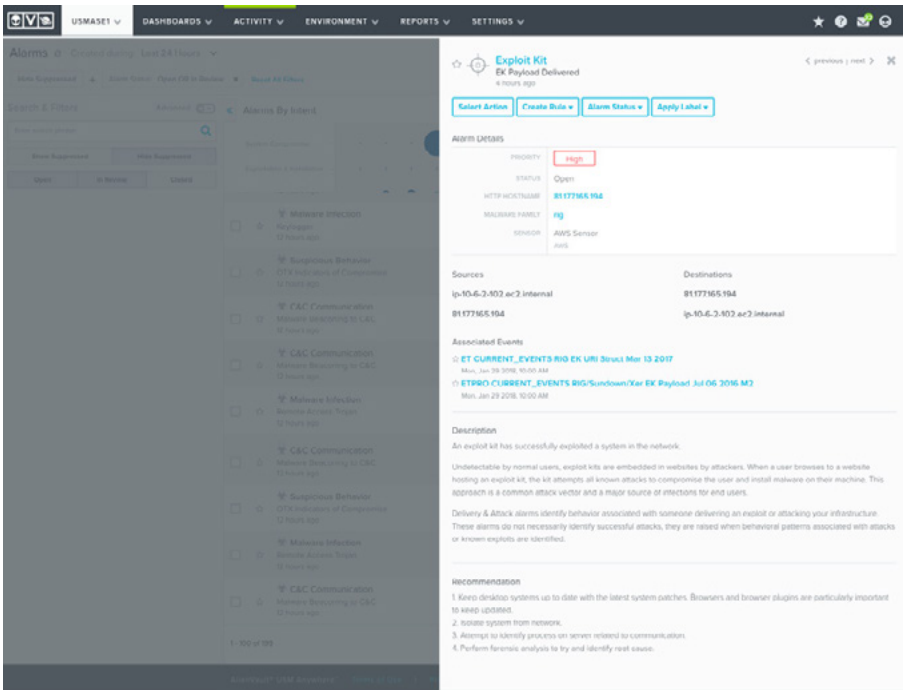
DETERMINE THE IMMEDIATE NEXT STEPS IN RESPONDING TO THE INCIDENT

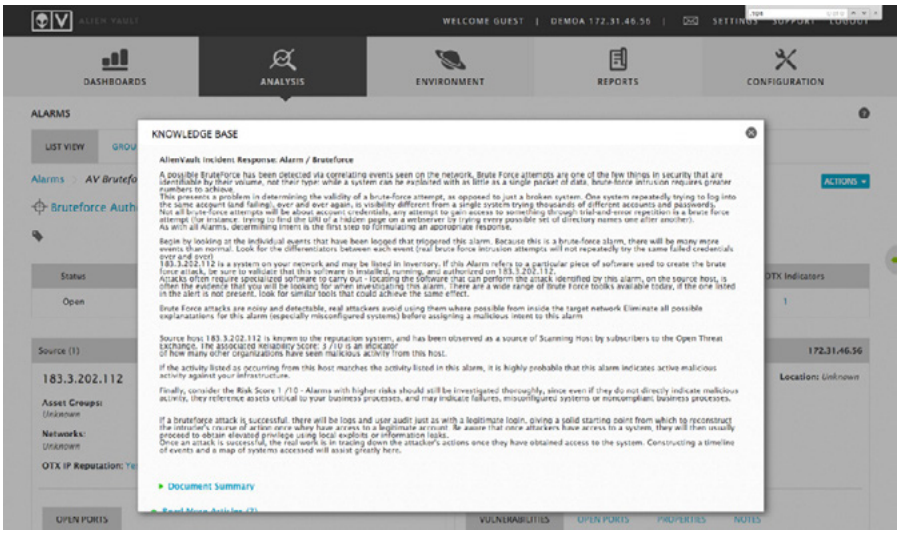
One of the biggest decisions that incident responders have is how to navigate the balancing act between the need to preserve evidence versus the need to recover quickly.

This decision is best handled well in advance of your first incident. In fact, the standard operating procedure about handling incidents should come directly from senior management and the Board of Directors, with guidance from your legal team. Whether or not to preserve evidence versus simply recover is not an easy decision to make, but one that you'll need to work out as soon as possible.

And please note, which way to go will often vary based on the industry you're in, the governing local and state laws, the type of data in question, the method in which it was obtained, and whether this was an inside job versus an outside one. As you can see, this is not a decision to take lightly, and we urge you to ask for guidance on this question.

In the meantime, AlienVault is here to make your life easier, especially when it comes to the security events we're analyzing and detecting throughout your critical infrastructure. For each alarm within AlienVault USM, incident responders are provided specific guidance in how to interpret each threat and how to respond.





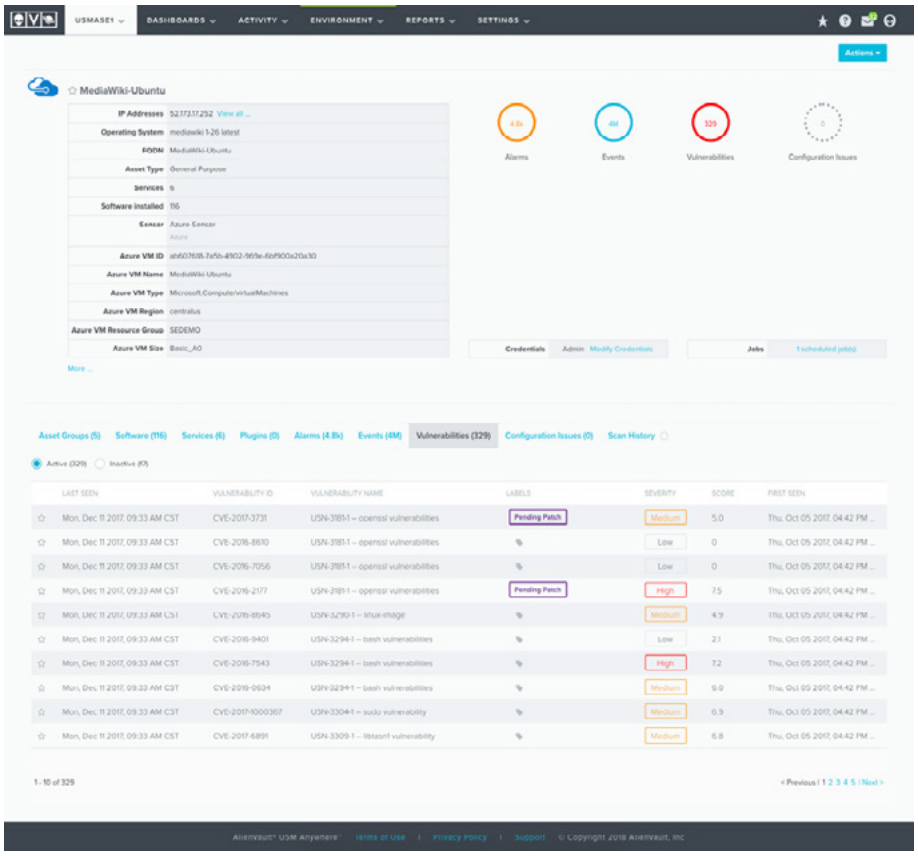
REVIEW ASSET DETAILS AND PRIORITIZE YOUR RESPONSE

When you're an incident responder, the more you know about the assets on your network, the better you'll be at investigating incidents that involve them. This is true especially of the servers in your environment.

It's often not clear who owns an asset, how it's configured, or what software is installed, despite checking a variety of management tools, spreadsheets, and other documents. With AlienVault USM, you can document and review who owns an asset and what to do and contact in the event of an incident, as well as rich data on the vulnerabilities that exist, the software that's installed and running, and any recent changes to critical files.

DOCUMENT ALL REMEDIATION TACTICS PLANNED FOR THE AFFECTED ASSETS

Once you've confirmed the impact and scope of the incident, you'll need to remediate as quickly as possible to contain the damage and recover. It's a good idea to document these remediation steps with information on the specific assets as well as what was done, by whom, and when. An audit trail like this is very helpful, especially since at this point you don't know what kind of questions you'll get management in the future.



Because AlienVault® Unified Security Management® (USM) provides response templates to help IT professionals address each incident, it's easy to take action right away and keep track of steps you've taken, rather than getting sidetracked with research to figure out what to do next.

DETERMINE WHICH ALARMS TO RESPOND TO ACCORDING TO YOUR ORGANIZATION'S POLICIES

Sometimes the unique needs of your organization require customized alarms. Based on your organization's specific needs, you can fine-tune controls within AlienVault USM to increase or limit the alarms you receive. For example, you can:

- Create an alarm for all events with a certain destination IP
- Suppress alerts about the use of Dropbox on employees' PCs because your organization has approved the application for business use

DECIDE: Summary

KEY TAKEAWAY #1: DETERMINE THE IMMEDIATE NEXT STEPS IN RESPONDING TO THE INCIDENT

How does AlienVault help? AlienVault® Unified Security Management® (USM) integrates emerging threat intelligence with operational guidance written by security experts on the AlienVault Labs Security Research Team. This guidance is customized for each alarm, so you can make better decisions in the heat of the moment.

KEY TAKEAWAY #2: REVIEW ASSET DETAILS AND PRIORITIZE YOUR RESPONSE

How does AlienVault help? AlienVault USM's rich asset inventory capability allows IT admins to view details about each asset, to guide responders about what to do in case of an incident.

KEY TAKEAWAY #3: DOCUMENT ALL REMEDIATION TACTICS PLANNED FOR THE AFFECTED ASSETS

How does AlienVault help? AlienVault USM provides actionable response templates for alarms within the platform, enabling IT admins to focus on implementing their remediation efforts rather than hunting down answers.

KEY TAKEAWAY #4: DETERMINE WHICH ALARMS TO RESPOND TO ACCORDING TO YOUR ORGANIZATION'S POLICIES

How does AlienVault help? AlienVault USM allows you to adjust the alarms you receive within the platform based on your organization's specific needs.

ACT:

Remediate & recover. Improve incident response procedures based on lessons learned.

By now, we've walked you through each of the first three phases of an effective incident response plan. We've shown how AlienVault USM, the AlienVault Labs Security Research Team, and the AlienVault OTX community provide the foundation you need to OBSERVE, ORIENT, and DECIDE how to respond to incidents.

Now it's time to **ACT**.

But first... In the previous section, we talked about the need to decide whether your IR team should focus on preserving evidence (in order to prosecute a data breach) vs. recovering quickly (and potentially lose transient forensic artifacts). This decision is far beyond the scope of this paper, and it's an important one. In the meantime, if you're interested in preserving data for further investigation, SIFT (SANS Investigative Forensics Toolkit) is a collection of various open source tools that can assist you in performing forensics analysis tasks.[5]

For the purposes of this paper, we focus on recovery and remediation as well as the specific ways that

AlienVault helps you achieve these essential incident response goals within the Act phase:

- QUICKLY IMPLEMENT REMEDIATION ON ALL AFFECTED ASSETS AND VERIFY THAT REMEDIATION HAS BEEN IMPLEMENTED PROPERLY.
- REVIEW AND UPDATE SECURITY AWARENESS TRAINING PROGRAMS OR SECURITY POLICIES AS APPROPRIATE.
- REVIEW (AND POTENTIALLY RECONFIGURE) SECURITY MONITORING CONTROLS BASED ON LESSONS LEARNED FROM THE INCIDENT.

[5] An international team of forensics experts, led by SANS Faculty Fellow Rob Lee, created the SANS Incident Forensic Toolkit (SIFT) Workstation for incident response and digital forensics use and made it available to the whole community as a public service. Check it out at: http://digital-forensics.sans.org/community/downloads#overview

It's difficult to cover all the possible remediation activities that you may need to implement, since it will largely depend on the specific threat, impact, targeted assets, and scope. That said, chances are that this will likely include activities such as:

- Patching systems (OS, applications, firmware, etc.)
- Removing unnecessary or unauthorized software
- Reconfiguring system files (e.g. removing DLLs, registry settings, etc.)
- Applying new ACLs on routers or adding firewall rules
- Enabling or installing personal firewall rules
- Revoking access privileges
- Resetting passwords
- Terminating unused or unnecessary accounts
- ... and more

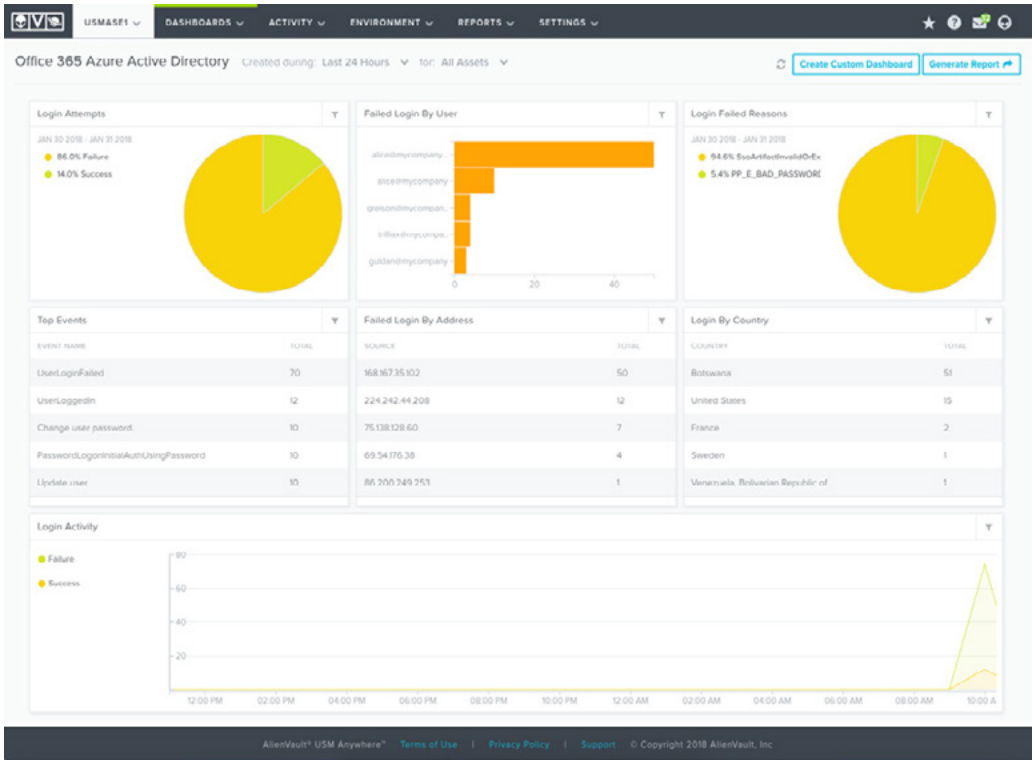
AlienVault USM helps you to verify that remediation has been implemented properly in a variety of ways. First, our vulnerability assessment can be used to scan remediated hosts immediately after they've been patched to verify fixes have worked and haven't introduced additional risks.

Additionally, the asset inventory capability captures and collects all asset data including installed software and services. These two capabilities combined help you confirm—at a glance—if a patch has been applied or a personal firewall installed or enabled.

REVIEW AND UPDATE SECURITY AWARENESS TRAINING PROGRAMS OR SECURITY POLICIES AS APPROPRIATE

Every security incident investigation provides you with the opportunity to assess how well your security program is working (in terms of security awareness, policies, procedures, and technology effectiveness). Users are to be blamed for every security incident, but the more vigilant your users can be about cyber security, the more likely the risk of incidents will decrease, both in terms of frequency and overall impact.

A good first step is to investigate user activity to gain an understanding of how users at your organization typically behave. AlienVault USM provides visibility into user and administrator activity on the assets in your environment so that you can verify that security policies are being followed and any violations are documented and investigated. For example, the screenshot below shows authentication and administrative activities through Azure Active Directory, and other dashboards for Office 365, G Suite, and more show user and administrator activities across those productivity suites.



REVIEW (AND POTENTIALLY RECONFIGURE) SECURITY MONITORING CONTROLS BASED ON LESSONS LEARNED FROM THE INCIDENT

Once you've completed and verified all necessary remediation steps (and this goes for patching systems as well as tweaking security policies), it's now time to do a critical analysis of the entire incident for essential lessons learned. Ask yourself and your team:

- What went well?
- What did we miss?
- What could we have done better?

During this analysis, you may discover the need to increase monitoring on certain assets or asset groups. With AlienVault USM, you can enable host-based IDS on specific assets to monitor activities and processes on those assets, as well as changes to critical system files.

Additionally, you may decide to do weekly versus monthly vulnerability scans. AlienVault USM allows you to schedule vulnerability scans at any frequency, and offers a lot of options for how to execute these scans.

ACT: Summary

KEY TAKEAWAY #1: QUICKLY IMPLEMENT REMEDIATION ON ALL AFFECTED ASSETS AND VERIFY THAT REMEDIATION HAS BEEN DONE PROPERLY

How does AlienVault help? The AlienVault USM platform's integrated vulnerability assessment checks for software weaknesses or misconfigurations that could expose systems to increased risk. The USM platform's asset inventory capability gives you granular data about your assets, so you can verify that the necessary patches have been installed or that specific services have been disabled.

KEY TAKEAWAY #2: REVIEW AND UPDATE SECURITY AWARENESS TRAINING PROGRAMS OR SECURITY POLICIES AS APPROPRIATE

How does AlienVault help? AlienVault USM provides a big-picture overview of your security posture, making it easy for you to see the results of your security awareness and policy compliance training over time.

KEY TAKEAWAY #3: REVIEW (AND POTENTIALLY RECONFIGURE) SECURITY MONITORING CONTROLS BASED ON LESSONS LEARNED FROM THE INCIDENT

How does AlienVault help? The AlienVault USM platform makes it easy to fine-tune security monitoring capabilities based specifically on what you glean from a post-mortem analysis.

SUMMARY

AlienVault USM, the AlienVault Labs Security Research Team, and AlienVault OTX provide the foundation you need for effective incident detection and response. From Observing and Orienting to Deciding and Acting, AlienVault is your partner in detecting and responding to the latest threats against your on-site and cloud environments. Thanks to our all-in-one approach to security monitoring, you and your fellow incident responders will have more time to spend on active threat hunting and less time on managing individual point products.

LEARN MORE ABOUT ALIENVAULT UNIFIED SECURITY MANAGEMENT

- Watch a 2-Minute Demo
- Explore the Online Demo Environment