WHITE PAPER

Incident Response Orchestration

Leverage Automation for Faster, More Effective Incident Response

According to the SANS 2017 Incident Response Capabilities Survey, 47% of organizations reported taking more than 24 hours to move from detecting an incident to containing it. From the moment a security incident occurs within one of your environments, the clock is ticking. Given the kind of damage an attacker can inflict within a matter of minutes or hours, the speed of your incident response has a tremendous impact on your organization's security.

Relying on manual incident response processes means repeating many of the same set of tasks every time an incident occurs, often requiring multiple tools and numerous individuals to complete. For example, opening a ticket to have another team update a firewall with a new rule to block a malicious IP can take time that may be exacerbated by the other team's priorities or miscommunications. Security teams don't have that kind of time to waste.

By using automated incident response to reduce simple and repetitive tasks, security teams can save time and focus on security, not process. An orchestrated, automated incident response can remove much of the friction and improve efficiencies when it comes to incident detection, response, and remediation. Security teams of every size should consider how the right orchestration solutions can help their IR processes run quickly and efficiently.

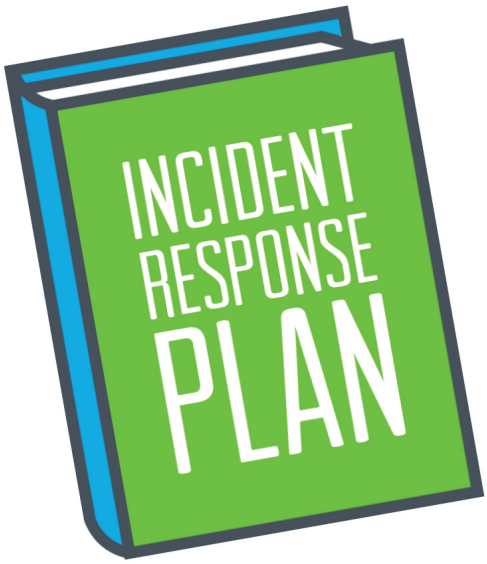
In this whitepaper, we will explore what security orchestration is and how it can help you speed up your incident response (IR) processes. Next, we'll look at examples of IR automation in action to give you a taste of what's possible for your organization.

Part One: Understanding Orchestration

Automation vs Incident Response Orchestration

Automation refers to replacing one or more manual tasks, which typically slow down incident response, with immediate reactions to security events identified across your environments. Automating certain repetitive tasks can ease the security operations burden and help you respond to threats more quickly—and more effectively.

However, let's be clear: Just as you wouldn't want a machine to take over your favorite restaurant, the human element of incident response isn't going away any time soon. There are certain pieces that require human judgment, which means complete automation may not be preferred for some scenarios.



Instead, security teams should focus on orchestrating the incident response processes that help human security analysts respond to threats as quickly and efficiently as possible.

Elements of incident response orchestration get left out of discussions that focus explicitly on automating individual tasks. For example, switching between an intrusion detection solution and an application where you need to take an action in the event of a breach can slow down the entire incident response process. To take full advantage of incident response orchestration and improve processes across multiple steps and toolsets, look for solutions that help you unify your IR activities within a single solution, like AlienVault® USM Anywhere™.

What Incident Response Orchestration Can Do for You

Incident response orchestration will look slightly different at every organization—that's where the human element I mentioned earlier comes into play. As you consider your organization's incident response plans and compare different solutions that might help you streamline them, there are a few key IR orchestration and automation capabilities you should look for.

- **Prioritized Security Alerts** – For incident response teams, automatic alarm prioritization reduces the burden of researching alarms individually and focuses security resources where they're most needed. As you evaluate solutions, look for one that helps you focus your attention in the right places right out of the gate.
- **Threat Context** – Understanding the full picture is one of the biggest challenges when investigating incidents. To support the incident response process, some solutions, like USM Anywhere, allow you to centrally investigate events aggregated from multiple data sources to help speed up forensic investigation. USM Anywhere also builds context and response guidance into alarms, helping you streamline your response efforts.
- **Automated Incident Response Actions** – When malware infects one of your systems, you can employ automated IR actions like isolating or shutting down the system to keep it from infecting other assets. Consider solutions that give you granular control over what you want automated, which allows you to tailor them to fit your organization's needs and infrastructure.
- **Threat Intelligence Updates** – As the threat landscape changes, your incident response plan should adapt accordingly to provide the most optimal response to the threat. For up-to-date threat detection and enough context for effective forensics, seek out a solution that includes actionable threat intelligence updates. Keep in mind that some threat intelligence solutions just provide threat data, meaning you still need to figure out how to apply it. Security teams should look for a solution that continually incorporates new threat intelligence into product updates that assure you're ready to detect and respond to emerging threats.

› **Bidirectional Response** – Some IR orchestration products can interact with each other to streamline your incident response actions. A solution like USM Anywhere, for example, can incorporate and analyze log data from Cisco Umbrella to detect threats, then respond to threats by sending the IP addresses of malicious domains back to Cisco Umbrella to block traffic between the domain and your employees and assets.

While all these capabilities are helpful individually, the power of IR orchestration comes from pulling them together in a way that makes sense for your organization's workflows and infrastructure. As you compare solutions, consider how they will affect the entire incident response process at your organization. For example, a unified solution like USM Anywhere can shorten the time between detection and response by centralizing your IR activities in one place.

Part Two: Automated Incident Response in Action

While automation can't replace human security analysts, it can help IT security teams save time and resources. With the right automated incident response tools, IT security teams can stay in control of their incident response activities and respond to threats and intrusions swiftly and effectively, with less manual work—no wire-ripping required.

In this section, we'll take a look at examples of incident response automation in action, comparing them to what it would take to handle them manually. As you read through these examples, consider what kinds of automated IR capabilities would have the greatest impact on your own organization's incident response processes and timelines.

1. One of your users interacts with a malicious IP address. You need to update your firewall to block the IP.

Firewalls help protect you from bad actors by filtering network traffic. Still, they have limits. Most firewalls aren't connected to your other security tools and their rules are infrequently updated, meaning they may not be current to address the latest threats. Addressing this situation might entail detecting the problem using other security software, prioritizing the event, and manually updating a firewall with a new rule to block the malicious IP. At some organizations, you might even need to open a ticket to have another team or team member take action, further slowing down the response process.

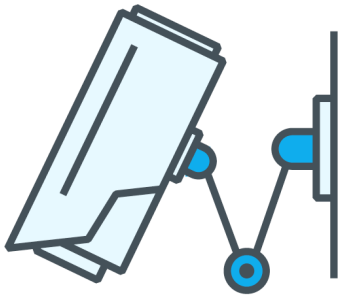
With automated incident response, you can automatically update your firewall to block malicious IPs as they are detected. For example, USM Anywhere detects traffic to and from an external IP address that, through its integrated threat intelligence, it knows is malicious. USM Anywhere can instruct your Palo Alto Networks next-generation firewalls to block or isolate the IP address, using an automatic or manual incident response action.

2. One of your systems has been infected with malware. You need to limit the damage and find out how many systems are vulnerable before it spreads.

Relying on manual processes to contain and investigate a malware intrusion means you're faced with a long to-do list of tedious tasks: identifying all the infected systems, researching the threat, gathering event logs from different locations to investigate, and more. Just as importantly, if your security solution bombards you with noisy alarms, you might not realize you have something significant on your hands until the damage has progressed.

Automated incident response tools can shorten your to-do list. With orchestration and automation tools like the ones in USM Anywhere, you can automate actions like fetching additional forensics data, disabling networking on an infected system, running automated vulnerability scans to identify other at-risk systems, and isolating those as well until you have a chance to patch or otherwise address them. By automating the incident response activities that do not impact or disrupt business operations, you can work faster and more efficiently.

3. You've contained a breach, but what was the scope of the damage? Whether for compliance purposes or just to understand what happened, you need to investigate.

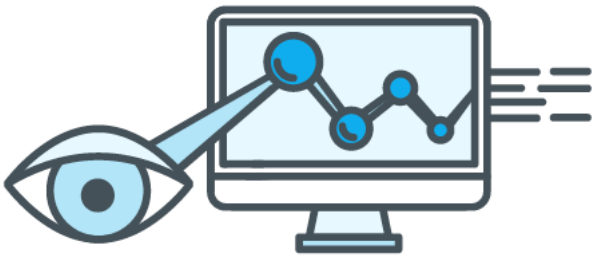


Understanding the scope of a breach provides critical information about what happened and how it affects your organization. If sensitive customer data has been exposed or corrupted, you need to know right away. However, getting the information you need often means engaging in repetitive, manual actions like going into each system to review its events and logs to try to piece together how the breach took place and what was compromised.

As a starting point, having a solution with log management capabilities would allow you to search for relevant alarms and events instead of combing through them manually. For example, USM Anywhere aggregates events and logs from across all your systems and networks, so you can get the information you need right away using powerful search and filtering capabilities. You can search for events or alarms based on criteria like event type, source name, username, and asset group, and you can examine detailed information on each event including the original log entries and network packet payloads. If there's a specific system you want to get additional forensic data from, you can do that directly from within USM Anywhere using the Forensics and Response App in just a few clicks.

4. One of your systems interacts with a Command & Control server for a remote administration tool (RAT). You need to block any further communication with the malicious domain.

If your IDS tool detects traffic to or from a known malicious domain, such as a C2 server, you need to take a range of actions to contain the situation and investigate the scope of the potential intrusion. One of those actions is to block the known malicious domain to prevent further communication. To do so, just jot down the domain from your IDS on a Post-It note, then open Cisco Umbrella to copy the domain into your blocked list. Or...



With automation capabilities, you can move immediately from detection to response by blocking the domain automatically when your intrusion detection system detects the threat. For example, if USM Anywhere detects communication with a known malicious host, you can send the IP or domain information of that malicious host to Cisco Umbrella using an automated incident response action or a manual action, so it can block communications with that domain not just from the infected system, but from any employees or other systems that may try to communicate with that domain.

5. Breaking news: New ransomware has emerged that exploits a vulnerability in a common Operating System. You need to know if your systems are vulnerable and, if so, take action.

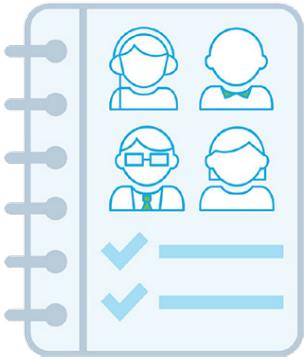
When your security plan relies on a lot of manual work, learning about new ransomware variants and how to protect your assets can inspire headaches – or even panic. Not only do you need to make sure your organization stays secure, you may also have to reassure other stakeholders who might not put cybersecurity at top of mind. If you don't have visibility of the state of security across your infrastructure, these challenges can be significant.

In this case, automation can help you before an incident even occurs. A product that builds actionable threat intelligence updates into your security plan can ensure you're up-to-date to detect new vulnerabilities and threats without needing to do your own research and setting up your own threat detection rules. With automated vulnerability scans scheduled to run at regular intervals, you can stay aware of at-risk systems across your infrastructure as new vulnerabilities emerge, allowing you to either patch them or limit their exposure to the rest of your network. (Note that built-in asset discovery and vulnerability assessment capabilities like the ones in USM Anywhere help ensure that you're continually discovering and scanning all of your assets.)

By the time you hear about new malware in the news, you can feel confident that you know your organization's level of risk exposure.

6. A breach occurs in one of your environments. You have a team of people handling the investigation, but you (and they) need to keep track of the incident response activities they're taking on.

Even with automation tools, the incident response can involve a lot of different actions for a team of security analysts (or for one person wearing a lot of hats). With threat information in one set of products and ticketing in another—or with no workflow ticketing whatsoever—keeping track of the tasks on each person's plate poses a challenge. Without a way to track IR activities, it's easy to lose track of key priorities or focus on the wrong tasks. For example, two team members might find out belatedly that they've been working on the same issue, wasting time a resource-strapped team can't afford to lose.

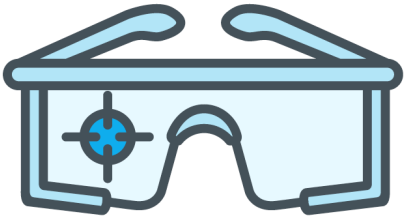


Luckily, some solutions include tools to help you keep track of your team's IR efforts. To track activity within USM Anywhere, you can apply a label directly inside an alarm to identify whether a task is open or closed, or which analyst is working on it. You can also open a ticket in ServiceNow without leaving the USM Anywhere interface or use email alerts to generate a ticket within other systems, saving you time and reducing wasted effort.

7. You detect ransomware activity on a server storing critical customer data – and the alarm occurs in the middle of the night.

Each organization has its own unique infrastructure needs and priorities, making one-size-fits-all security automation impractical and potentially disruptive. You wouldn't want to shut down business-critical systems every time a false-positive alarm popped up in one of your environments. For certain situations, however, an immediate response can prevent you from waking up in the middle of the night to do damage control, or finding out in the morning that customer information has been corrupted or exposed for the past eight hours or more.

With the right automated incident response tools, you can tailor automated responses to protect your most critical data. For example, if evidence of ransomware appears on a particular server, USM Anywhere enables you to set up a rule to automatically disable networking to contain the intrusion and protect your data, whether or not you're awake to trigger the action. For a business-critical server that can't be shut down, in contrast, you could send an automated notification via email or SMS to your cell phone. You retain control of when and how to apply these rules based on your organization's specific security needs.



Part Three: Reduce Your Incident Response Time with USM Anywhere

Automated incident response capabilities like the ones within USM Anywhere can accelerate your incident response processes and reduce headaches across your organization. Most importantly, it can help you limit the potential damage an incident can cause to your organization and customers.

USM Anywhere makes the entire incident response process faster and more efficient by consolidating your IR activities within the same solution as your other security monitoring and compliance management needs. Out-of-the-box, USM Anywhere delivers essential capabilities like asset discovery, vulnerability scanning, intrusion detection, behavioral monitoring, SIEM, and log management. From the same pane of glass, you

can manage IR activities within the other technologies you use, including Cisco Umbrella, Palo Alto Networks next-generation firewalls, ServiceNow, Carbon Black, and more.

Learn more about AlienVault's unified approach to incident response orchestration:

- Read an overview of AlienVault USM Anywhere
- Explore our online demo now – no setup required
- Watch the Webcast: "Stop Malware in its Tracks with Security Orchestration"
- Join the Open Threat Exchange

About AlienVault

AlienVault has simplified the way organizations detect and respond to today's ever evolving threat landscape. Our unique and award-winning approach, trusted by thousands of customers, combines the essential security controls of our all-in-one platform, AlienVault Unified Security Management, with the power of AlienVault's Open Threat Exchange, the world's largest crowd-sourced threat intelligence community, making effective and affordable threat detection attainable for resource-constrained IT teams. AlienVault is a privately held company headquartered in Silicon Valley and backed by Trident Capital, Kleiner Perkins Caufield & Byers, Institutional Venture Partners, GGV Capital, Intel Capital, Jackson Square Ventures, Adara Venture Partners, Top Tier Capital and Correlation Ventures.