Empowering Incident Response via Automation

Matt Bromiley

SANS

A SANS Whitepaper

Empowering Incident Response via Automation

Written by **Matt Bromiley**

February 2019

Sponsored by:

Cisco

Introduction

"Fool me once, shame on you. Fool me twice, shame on me."

That's how the old saying goes, and it's especially true in the realm of information security, and more specifically, incident response. In SANS' experience, the past few years have sent at least one clear message about incident response: There's still plenty of room to grow and plenty of things to fix. Here's the kicker: We've been down this road before. It's time to finally make the necessary changes.

Now, we're not saying incident response is in dire straits. Quite the contrary—the 2018 SANS Incident Response Survey[1] (which we'll discuss more in depth later) showed that incident response detection and response metrics are improving. While we are making noticeable increases in some areas, such as dwell times, there's still significant room for improvement in automation. A definitive overhaul of some processes is needed to further the success of response teams, while limiting the success of attackers.

Automation doesn't mean replacing jobs. It means empowering your employees and making them more successful.

In this paper, we examine some of the critical issues that are facing incident responders today. These issues, which may vary in your organization, typically include:

- The inability to move from remediation/eradication to recovery
- Monotonous and/or laborious processes that eat up time that could be spent dealing with incidents

[1] "It's Awfully Noisy Out There: Results of the 2018 SANS Incident Response Survey," www.sans.org/reading-room/whitepapers/incident/paper/38660

- Lack of data enrichment to help make investigative decisions
- Lack of investigative tracking mechanisms to help teams learn from the past

We will examine where incident response automation can be used to empower your teams and bring their level of productivity and investigations to never-before-seen heights. Your analysts should be focused on solving the problems that require human intervention, not tripped up by technical hurdles that a computer could easily solve. With this paper, we challenge our incident response readers and team leaders to look for areas within their organization that could use optimization or automation, and work on implementing accordingly.

Incident response can be stressful, with practitioners constantly engaging in combat with attackers from foreign nations who may have a wide range of capabilities. However, if incident response teams have the right automation, even the most wily and resourceful of attackers may find themselves up against an unstoppable force. It's time to level up.

Critical Problems

In SANS' experience, there are a handful of problems that increase the burden on incident response teams. Although we cannot address (or solve) them all, we will focus on a few specific, consistent issues that could benefit from implemented automation.

Incident Scoping and Remediation

In the SANS 2018 Incident Response Survey,[2] the one metric that concerned us the most was the percentage of reoccurring attacks. Approximately 44 percent of the survey respondents indicated they had suffered attacks from the same threat actor at least twice, and 77 percent of those indicated that the attacker had returned with similar or the same tactics, techniques, and procedures (TTPs). Figure 1 defines the two most important phases of the six-step incident response process: scoping and eradication/remediation.

These statistics from the Incident Response Survey represent a clear gap in either incident scoping or remediation—or both. We begin to question the effectiveness of remediation events when an attacker returns with the exact same TTPs. Did the attacker ever actually leave in the first place? The issue is effective scoping, which leads to effective remediation/eradication. And effective scoping ties back to visibility—something that many incident responders wish they had more of.

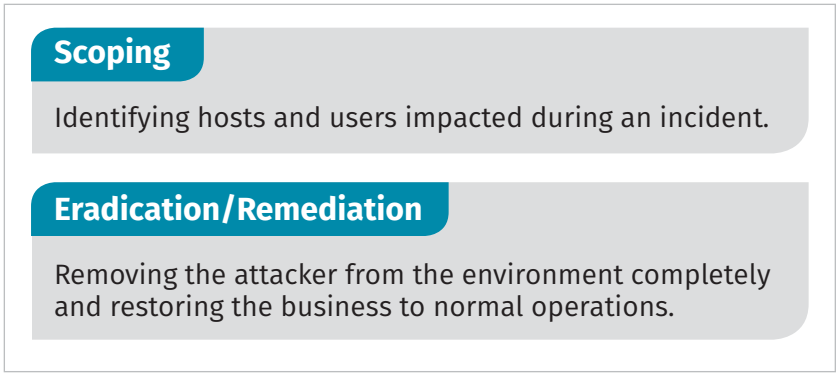

Figure 1. Two Most Crucial Phases of the Six-Step IR Process

[2] "It's Awfully Noisy Out There: Results of the 2018 SANS Incident Response Survey," www.sans.org/reading-room/whitepapers/incident/paper/38660

In our experience, even with appropriate visibility, the process of performing host correlations and lookups may not only be too cumbersome but also provide attackers an opportunity to move faster than the incident response team. Furthermore, even with host-network correlation (which may be shaky at best), by the time incident responders have made the link, the attackers have bought themselves extra minutes or hours within the organization. This is time responders simply cannot afford to give away.

The Pain of Monotony

One of the more significant pain points for many incident responders is the repetitive tasks required to further the knowledge and scope of an investigation. These may include tasks such as data enrichment, host-to-network correlation or malware analysis/triage, just to name a few among many. Incident responders who must spend minutes or hours tracking hosts through their own corporate network are likely missing other threats within the environment. Those minutes and hours add up—and buy more time for the attackers.

Data enrichment and user-host and host-network correlation are easily scriptable and should be automated. Some SIEM platforms can assist with this correlation—once again, automating lookups that analysts *shouldn't have to perform*. Additionally, the movement of data, such as a file from the network sensor to the malware analysis engine, is another area for automation.

Our 2018 IR survey indicated that organizations saw the same attacker return with the same TTPs. Incident response should learn from previous incidents, making it more difficult for an attacker to return.

Learning from the Past

An additional pain point we see at multiple organizations is a lack of investigative data retention. Organizations of all sizes, especially those with a full-time incident response team, experience multiple security events per year. They are likely seeing a myriad of attack types and malware families. However, despite the wealth of experience, some incident response teams are not recording details for future applicability.

Even worse, when a similar (if not the exact same) type of incident occurs in the future, that team may be caught without proper documentation from the previous investigation. Without the ability to reference their previous, applicable work, responders may find themselves performing tasks that were already completed—or investigating an attacker that was already eradicated. This type of "In-house threat intelligence" (derived from internal investigations and their impact on the organization) is among the more crucial data points that incident response teams should be collecting. Not only do they point to areas that the organization needs to improve, but they are also excellent candidates to identify areas for automation and future team success.

Improving IR Through Automation

The painful part is over. Now that we've analyzed some of the critical issues that incident response teams deal with on a daily basis, it's time to say, "Enough is enough." Figure 2 shows quick-win areas where we can increase automation and empower our incident response teams.

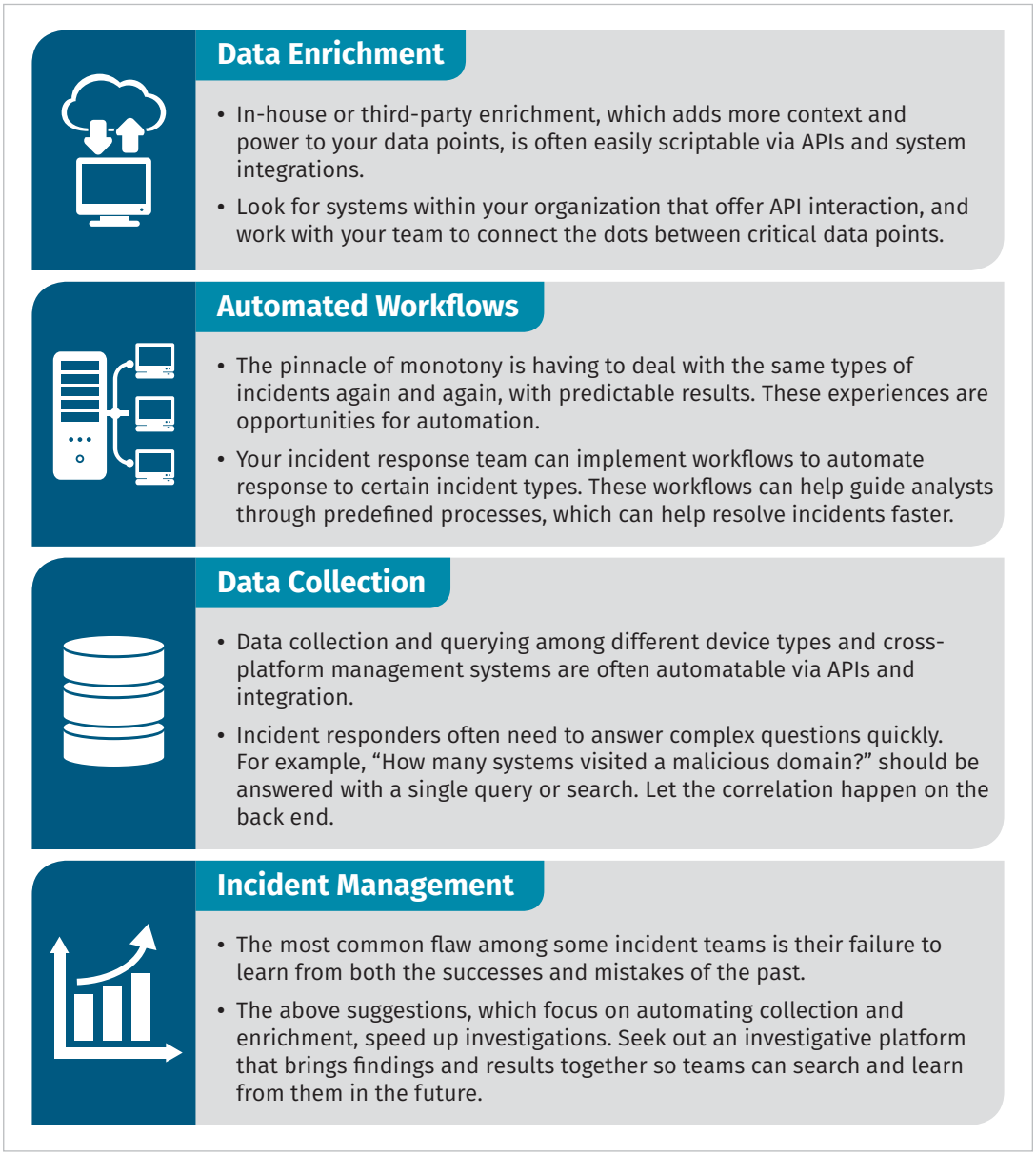

Figure 2. Quick-Win Areas for Increased Automation

Case Study: Swimming Up Niagara Falls

Let's examine a sample scenario where analysts could benefit greatly from having automation on their side. This is a fictional scenario, but my guess is that some of the issues it highlights will seem familiar to many analysts and organizations.

Problem: Multiple Tools/Ad Hoc Processes

Dade is an incident responder at Murphy Industries. Dade is passionate about digital forensics and incident response and loves protecting the organization. He is one of the more trustworthy responders on the team and has been a key player in identifying and eradicating advanced threats from the environment. This expertise and commitment have afforded Dade's managers the budget to purchase a wide range of security tools, all of which sport their own accounts, dashboards, limitations—and hindrances.

As much as Dade loves the idea of his job, the day-to-day effort of finding and accessing relevant data to support his investigations is taxing. In some cases, it's so laborious that Dade finds himself repeating searches and pulling back data he already examined—sometimes from a previous case! To help keep the chaos organized, Dade has come up with a personal investigative tracking mechanism that he—and only he—understands. Figure 3 provides an example of Dade's typical investigative workflow.

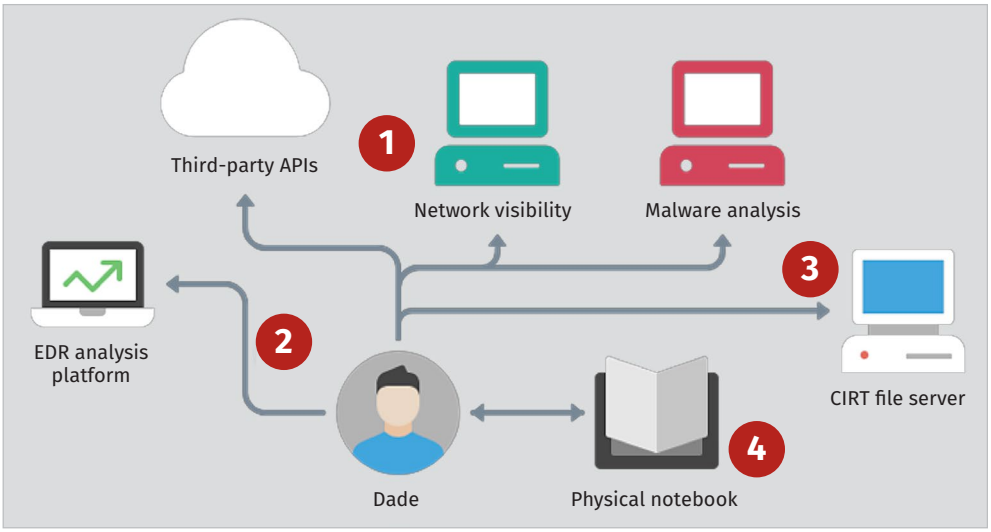

Figure 3. Dade's Typical Investigative Workflow

Let's walk through a typical investigation workflow for Dade:

1. An alert is elevated from the security operations center (SOC) that requires Dade's investigation. He begins by examining the network logs for the source system, so he can correlate the alert with IP addresses and a time frame.
2. Dade figures out the source host and hops over to the EDR analysis platform. By this time, the alert is almost 10-15 minutes old, and host-based evidence may be in danger of rolling. Fortunately, however, Dade can identify the chain of events that led to a potential system infection. He still hasn't determined whether this is a true infection.
3. Dade extracts the malware from the EDR tool and copies the file to the malware analysis system for semi-automated malware triage. That will help him determine the behavior and intentions of the malware. He also places a file on the IR team file server for posterity.
4. After the initial steps of the investigation have been determined, Dade returns to his physical notebook to record the findings from the steps taken above. Note that all along the way, he has had to manually enrich and record various data points.

Pro Tip

When purchasing tools, be sure they fit with your organizational needs as well as integrate within your analyst workflows. Automation should be a critical thought process *before* checks are signed.

Automating the boring tasks lets your analysts focus on the stuff that matters—the tasks that require humans.

Dade's life is about to get even more complex—Murphy Industries just purchased a company that will bring approximately 500 new systems, more security software and required capabilities to Dade's investigative purview.

A Solution: Letting Automation Take the Wheel

As much as Dade loves his job, it is laborious and requires interaction with multiple systems. You've probably already identified several areas where Murphy Industries could empower Dade with some automation. Let's examine a few.

The Hand-off

Note that Dade receives an alert from the SOC that provides him little to no details. He must manually track down the alert and correlate to the host. Not only should this have been done prior to escalation, but it should also be an automated feature.

The Platforms

Dade must jump between multiple platforms to get initial insight. A network alert that leads to host-based insight is nothing novel, but there's no reason to be living in a world of multiple dashboards. Instead, there should be a single, integrated view providing the data Dade needs right up front.

The Analysis

Once Dade can do some correlation—the thing that humans *should* be doing—he extracts a malware sample and submits it for analysis. Submitting a static file that tripped a rule for malware analysis? That can also be automated. Data enrichment (which Dade was performing and recording manually)? That is ripe for automation.

The Notebook

Dade is recording things in a physical notebook. This works great for him but is useless for maintaining future investigative notes for folks *other* than Dade. What happens if the same type of malware hits the environment tomorrow, when Dade is off? That's right—the organization would be starting over from square one.

The Timing

Timing is the most crucial, underlying issue with Dade's setup. The time it takes him to make a correlation, extract a sample and make an informed decision is nearly 20 minutes after the alert is fired. Twenty minutes may not seem like much, but to an attacker, it can be plenty of time to move laterally, infect other systems with ransomware or delete evidence that could help responders make confident decisions. So, if there's any final argument to automation, it's that speed must be an *ace up the incident responder's sleeve, not the attacker's*.

Speed must be an ace up the incident responder's sleeve, not the attacker's.

Implementation and Automation Working Together

Let's revisit Dade's environment after a bit of automation is put into place (see Figure 4).

OK, that looks even more confusing! But wait—life is much easier for Dade. Let's analyze a few of the changes made to his environment.

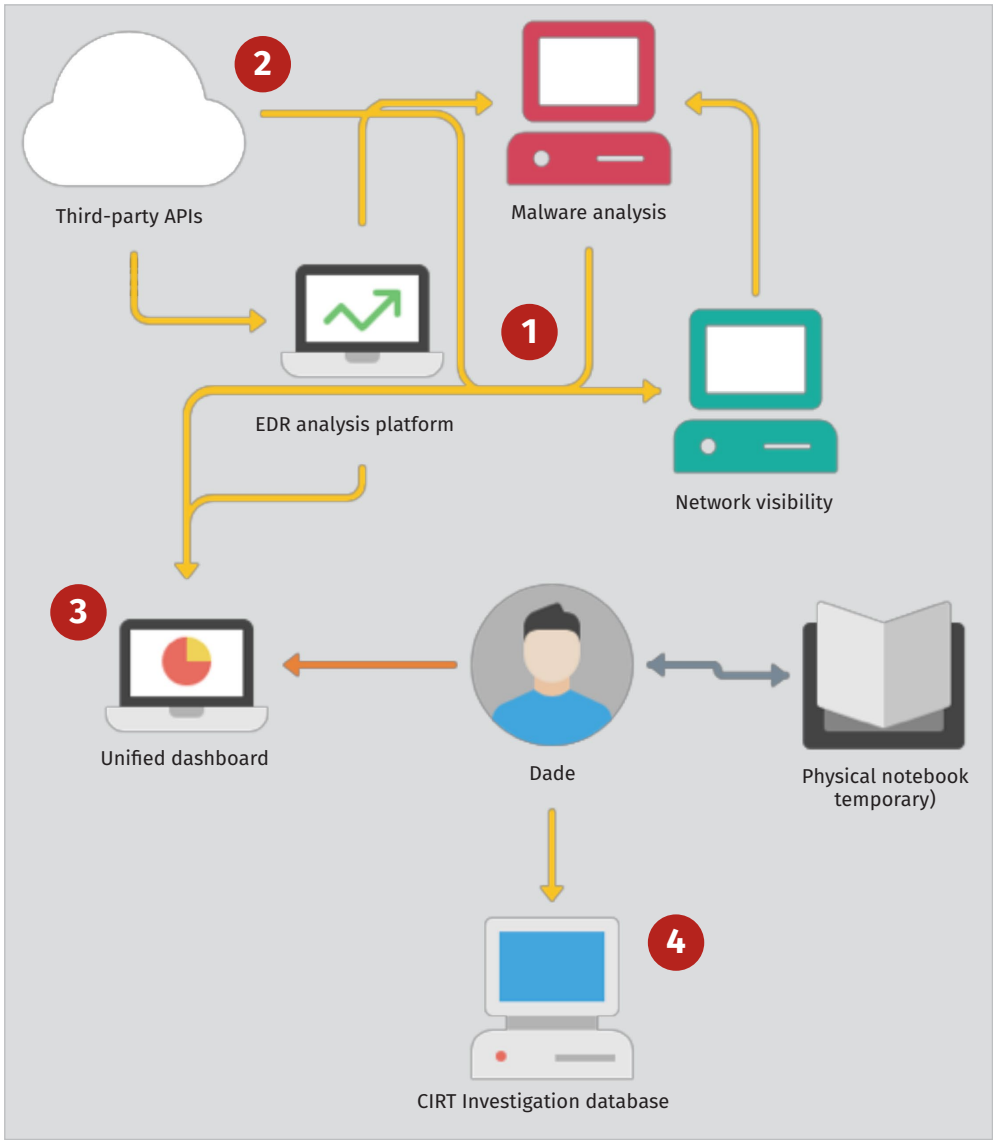

Figure 4. Dade's Environment After Some Automation Is Implemented

1) All of the gold connections are now automated pushes or pulls initiated by the appropriate devices. Every system is talking to every other system—for the benefit of the incident response team. For example:

   a. If the network IDS encounters a file that trips a malicious signature, it automatically sends it to the malware analysis engine for processing. A similar process exists for the EDR platform. Dade can view malware analysis results immediately, instead of waiting to dig to uncover a sample. Automation allows him to assess criticality faster.

   b. The network- and host-based platforms work together to provide a holistic, automated view into endpoints. For example, as new DHCP leases are issued, endpoint detection is automatically tuned into the new endpoints and reflects the correct change.

   c. If it looks as if there is a lot of overlap, that's correct! We've optimized the paths along which data travels and enrichments are performed. Despite all the complex computing on the back end, however, Dade is still limited to one central point of analysis.

2) Third-party APIs are used for automatic enrichment of data—not for use after the fact. Furthermore, third-party APIs can include things such as geographical or ASN (autonomous system number) lookups or enrichment via custom and third-party threat intelligence feeds.

3) Dade no longer must hop between multiple dashboards. Every tool feeds into one place. While having "one pane of glass" is old advice, it's not being followed as often as we'd like. Furthermore, the unified dashboard is not necessarily a SIEM. It could be a collaboration platform that not only allows Dade to view data, but also to take action off it.

4) Lastly, we have upgraded Dade's investigation tracker to an investigation database accessible to the critical incident response team (CIRT). These benefits are twofold:

   a. As Dade works through his investigation, all his results and key findings are automatically piped to the database. He no longer needs to pause to write things down.

   b. If Dade wants to take vacation, another analyst can easily pick up right where he left off.

If Dade's new diagram seems like a dream to your incident response team, it's time to wake up. These types of integration and automation tools already exist. Unfortunately, they are not leveraged as much as they could, or should, be. Automating incident response can empower even smaller teams to handle more incidents and make critical decisions faster.

Conclusion

Incident response should not be a game where the attackers always win. However, it can often feel like an endless loop with little success. Without the right processes in place, it's very easy for IR teams to get stuck in loops of adversarial combat. Eventually, the incident response team is worn down, and the attackers may find a sliver of success. While this may seem like an edge case, it's not an uncommon situation. *It should never become the norm.*

Hope is not lost. To identify areas where incident response is in desperate need for improvement, we must first identify some of the core problems:

- How much time are responders spending on tasks that could largely be automated?
- How confident are responders that the decisions they are making are backed by solid foundations?
- Are responders' containment and/or remediation efforts working? If so, do the adversaries keep coming back?

When your core problems have been identified, it's time to explore options for automation. To help you assess whether a tool or platform can help your team, here are a few features we'd like to see included:

- **Data import/export capabilities—**Can the incident response team easily get data in and out of the tool/platform? You don't want to hire a data scientist just to ingest a spreadsheet. Furthermore, let's make sure that standard data formats (JSON, STIX, TAXII, etc.) are supported.

- **API access—**What good is the tool/platform if it cannot talk to anyone or anything else? Look for API access with *good* documentation.
- **Collaboration—**Can your tool/platform easily incorporate into your team collaboration? Can users share links/findings with one another, and if so, how easy is it to manage those ACLs?
- **Third-party integration—**Depending on your organization's needs, this may or may not be a requested feature. Whereas API access will allow your team to automate, you should also consider what integrations the tool may already have. For example, some tools will tie into the common vulnerabilities and exposures (CVE) database by default, allowing your team to have that data without the need to write the code.
- **Ease of use—**This last feature is the most crucial. Too many organizations invest in technology that often requires extensive training to use correctly. This does not help a busy IR team, and also sets up an artificial barrier to entry for junior analysts. Have your team test-drive the tool for *weeks* or *months*. No two-hour presentations.

Regardless of whether your organization faces only a few—or a lot more—problems for your incident response teams, the time to start making impactful changes is now!

Let's go back to our example of Dade again. Notice that when we walked through his new incident response setup, we did not implement a system that replaced Dade. Instead, we made him powerful, faster and more informed. The goal of automated setups is simple: **Let the human focus on solving the complex problems. Let the machines focus on answering the boring ones.**

About the Author

Matt Bromiley is a SANS Digital Forensics and Incident Response instructor, teaching Advanced Digital Forensics, Incident Response, and Threat Hunting (FOR508) and Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response (FOR572), and a GIAC Advisory Board member. He is also a principal incident response consultant at a major incident response and forensic analysis company, combining experience in digital forensics, incident response/triage and log analytics. His skills include disk, database, memory and network forensics, as well as network security monitoring. Matt has worked with clients of all types and sizes, from multinational conglomerates to small, regional shops. He is passionate about learning, teaching and working on open source tools.

Sponsor

SANS would like to thank this paper's sponsor: