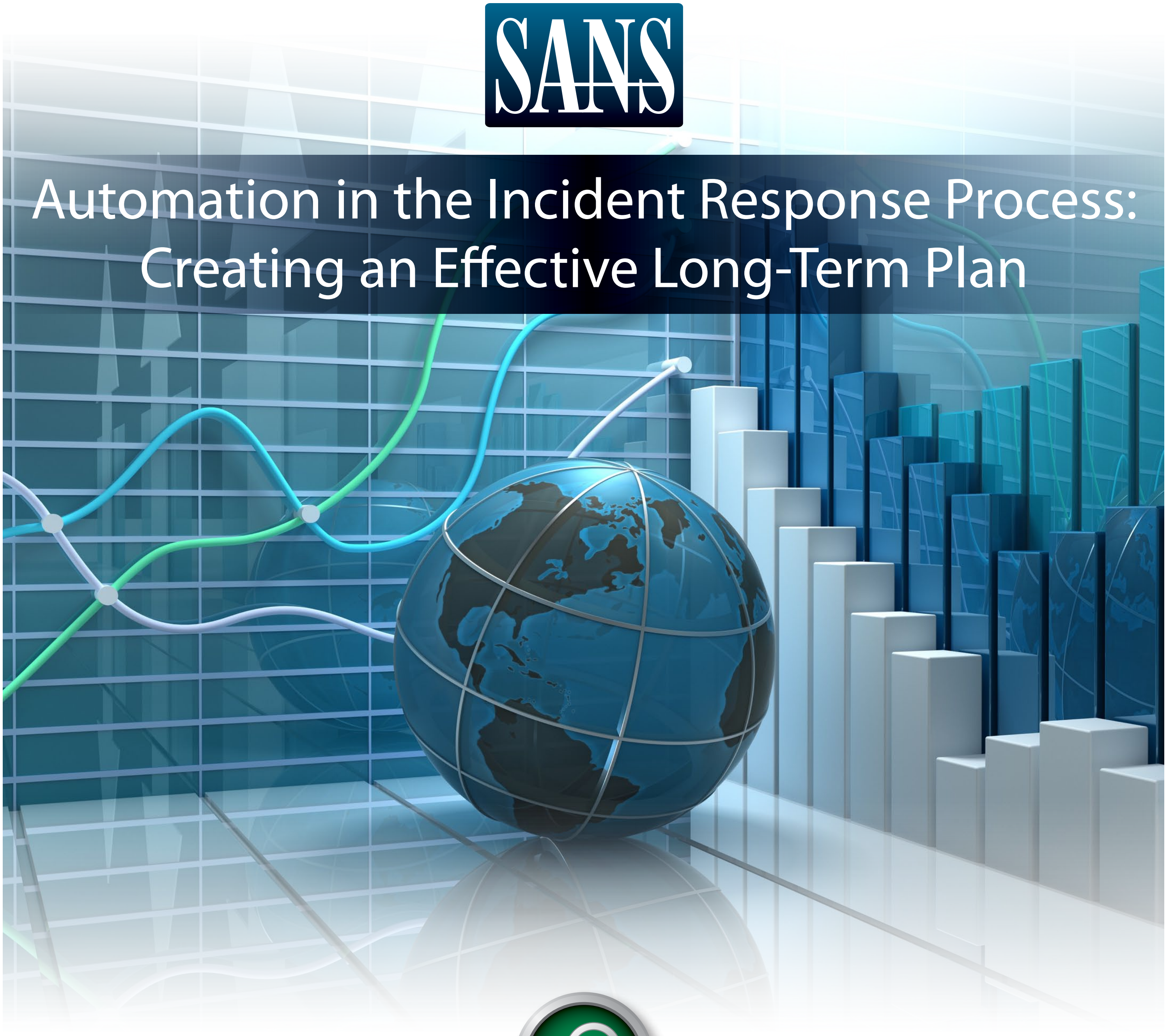
Automation in the Incident Response Process: Creating an Effective Long-Term Plan

With the right resources in place, attackers can be detected more accurately and efficiently, mitigating damage and data loss from inevitable network attacks. This paper presents a proper process and procedure for incident response that includes the use of automation tools.



Automation in the Incident Response Process: Creating an Effective Long-Term Plan

A SANS Whitepaper

Written by Alissa Torres

February 2015

Sponsored by
Bit9 + Carbon Black

Introduction

If 2014 was the year of the *mega breach*, with corporate giants falling prey to hackers and suffering significant data breaches, 2015 may very well be known as the year of *proactive vigilance*. None of our networks is immune to a motivated attacker. As Joseph Demarest, assistant director of the cyberdivision of the Federal Bureau of Investigation, told members of Congress at the end of December 2014, "[T]he malware that was used would have gotten past 90 percent of the Net defenses that are out there today in private industry."[1]

[1] "FBI official calls Sony attackers 'organized,' 'persistent,'"
www.cnet.com/news/fbi-official-calls-sony-attackers-organized-persistent

Present Weaknesses in the Incident Response Process

Security professionals have grown to accept certain irrefutable truths:

- The adversary is already in the network.
- Detection is *theoretically* possible with the *right* technology, process and expertise.
- Security teams are limited by organizational constraints (budget, trained personnel and effective technology) and how much risk avoidance the company is willing to pay for.

With the right resources in place, security professionals can detect attacks more accurately and efficiently, mitigating damage and data loss. And today's chief information security officers (CISOs) are under tremendous pressure to craft a proactive strategy for defense and detection. At the same time, security pros are dealing with limited budgets, staff and other resources.

Mixed into this challenging environment are increasingly tough data breach and compliance regulations that require enterprises to protect proprietary data and customer personally identifiable information to avoid legal fines.

Creating and implementing effective measures to prevent a data breach in 2015 are in the forefront of security team agendas in organizations of all sizes. According to the Ponemon Institute "2014: A Year of Mega Breaches" survey results, 55 percent of respondents reported that their organization created an incident response (IR) capability as a result of the recent large-scale data breaches covered in the media.[2]

[2] www.identityfinder.com/us/Files/2014TheYearOfTheMegaBreach.pdf

What Is the Role of Automation and Why?

Six Steps of Incident Response

1. Preparation
2. Detection
3. Containment
4. Eradication
5. Remediation
6. Follow-up

Working from an IR plan allows for structure and organization when the unexpected occurs. Because the circumstances of critical events vary widely, a team with the proper process and procedure in place will move smoothly through the six steps of the IR process. These steps include preparation, detection, containment, eradication, remediation and follow-up.

Even as security challenges have multiplied, many organizations' current IR plans rely on both the availability and affordability of third-party IR and breach mitigation support, either employed via retainer or service contract. These third-party companies specialize in detailed scoping of an intrusion as well as mitigation, enabling other organizations to call upon them as needed instead of establishing their own full-time IR staff.

But with the recent spike in demand for IR services, the outsourced model has fallen under intense scrutiny. And exponentially increasing demand for premier level service prioritization from these service providers means that meeting any acceptable "boots on the ground" SLA timeframe is becoming increasingly more difficult. Few breach victims can wait days, much less weeks, for service providers to arrive on site when an attacker is actively stealing sensitive data.

Few breach victims can wait days, much less weeks, for service providers to arrive on site when an attacker is actively stealing sensitive data.

As a consequence, CISOs in many organizations are realizing faster response times and financial advantages of moving these capabilities in-house. By taking ownership of the IR process and customizing the response process to the specific needs and infrastructure of their organization, an internal IR team will grow increasingly more proficient at handling its own critical incidents.

Typical efficiency gains of automating and owning IR include deeper knowledge of the implemented technology, faster false-positive reductions, shorter duration of detection to containment time and, subsequently, less significant data loss when a breach occurs. According to the 2014 SANS Incident Response survey, 59 percent of respondents reported their employers have a dedicated internal team focused on IR, reporting and remediation, and 61 percent of respondents' employers have identified surge IR support team members from internal staff.[3] These statistics (see Figure 1) support the recent trend of establishing in-house IR capabilities.

[3] www.sans.org/reading-room/whitepapers/analyst/incident-response-fight-35342

What resources does your orginization utilize in responding to incidents?

Select the best answer.

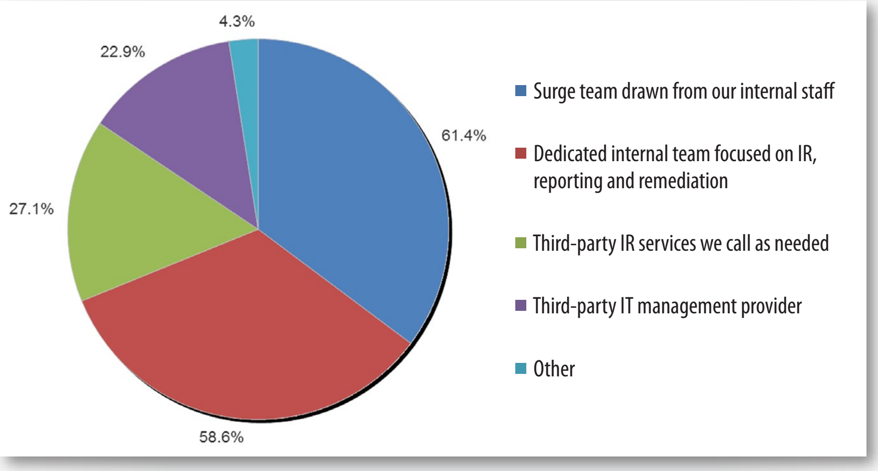


Figure 1. Dedicated Versus Third-Party IR Capability (Source: SANS 2014 IR Survey)

There is no shortage of obstacles for those teams developing an internal IR capability. Time from initial infection to detection is thought to be the most critical matter and greatest failing of today's IR teams.[4] The 2014 Verizon Data Breach Investigations Report shows that the majority of attacks require less than a week to break into a network, yet only approximately 25 percent of the breach detection occurs in the same span of time.[5]

To target this Achilles heel of the six-step IR process, security information and event management (SIEM) and endpoint security and intrusion detection technologies were reported as the top security investments companies are making, according to the 2014 Ponemon Institute survey.[6] Fifty percent of survey respondents reported that their organization's top security investment was in SIEM, with endpoint security a close second, named by 48 percent of respondents.

[4] "Lessons From 2014 Mega Breaches: It's Time To Shift To A Post-Breach Mindset," www.forbes.com/sites/frontline/2015/01/07/lessons-from-2014-mega-breaches-its-time-to-shift-to-a-post-breach-mindset/2

[5] www.verizonenterprise.com/DBIR/2014

[6] www.ponemon.org/library/2014-a-year-of-mega-breaches

Acknowledging the substantial investment involved with weighing, selecting and implementing an endpoint and network monitoring system, it is essential that organizations consider their present and future security needs. These tools enable the security team to aggregate critical endpoint system information and log to a SIEM technology. With access to a continuous system-state data feed, the security team can configure a SIEM to identify a pattern or sequence of activities (such as serial attempts seen associated with a domain user attempting to connect to a system across the network via share).

Enterprises that want to increase their internal automated IR capabilities face several potential challenges, including a lack of time, skills and roadmap. Those organizations creating a proactively vigilant environment from nothing also face several potential obstacles, including whether to add testing and installation of endpoint protection software.

In addition, enterprises going in-house will need to evaluate whether workstations, servers and mobile devices should be within the scope of system monitoring and what data they should aggregate from each of these types. Often the absence of skilled personnel experienced with the chosen technology makes customizing a tool for a unique environment a time-consuming and frustrating trial-and-error effort.

A View into the State of Current IR Processes

Automation provides deeper insight into endpoint and network traffic and facilitates detection of execution of malicious software or anomalous activity. In addition to improving detection, efficiency gains provided by automation can improve response time significantly, allowing for swift triage and containment. Fast response affects the impact of incident after detection, mitigating the organization's data loss and/or destruction.

Consider the inefficiencies of the following scenario, representative of the state of current IR processes in many organizations:

> A Tier 2 IR analyst spots anomalous entries on a few workstations while performing targeted data aggregation and stacking analysis. In studying the *least frequently occurring* AppCompatCache registry entries from a sample set of hundreds of systems, three systems show an **`scvhost.exe`** having executed from a peculiar **`C:\Users\Public\Biforder`** directory. Based on the time and date stamps embedded in these registry values, the analyst isolates the initial time of execution as being approximately two months ago. How does this analyst proceed with triage and investigation of these potentially suspicious findings?

When encountering possible signs of malicious code execution on a system, one must consider the various possible stages of attack at which incident responders may discover an intrusion. In the best-case scenario, the malicious **`scvhost`** binary attempted to execute on these systems and failed to download, in which case few additional artifacts would exist both on these systems and in capture network traffic.

But consider a successful exploitation and stage 2 malware delivery completed on all three systems. After two months on the network, a sophisticated adversary would have gained intelligence survey of the internal network and notable directory structures as well as had the opportunity to harvest local system, application and domain credentials. How will the analyst determine at what stage in the attacker kill chain he has encountered the adversary?[7]

Naturally, the responder's investigative methodology would lead him to interrogate each system of interest to gather more information on the suspicious binaries. Unfortunately, in most organizations, this analysis would be limited to the current state of the system with no historical understanding of system volume, Windows registry or native Windows artifacts. After all, a security team cannot be precognitive about what will be pertinent to the investigation before the breach occurs. The team could not possibly predict which artifacts on which specific system would hold the key to unraveling the initial vector of infection.

The examiner's view of the current contents of the file system, based on the sophistication of his attacker, may or may not include the **`C:\Users\Public\Biforder`** directory at this point. What about volume shadow copies (VSS)? They may have a past snapshot of the directory of interest, yet a roll of the dice occurs for such a possibility because the timeframe of VSS creation is every seven days. The current system's **`prefetch`** directory, local event logs, $USNJournal, $LogFile and Windows Search Index may shed some light on the existence and timeline of these binaries as well, but have an element of *brittleness* based on the rate of *churn* on the systems.

Incident responders encounter this all-too-common scenario every day. Even those who don't just react to alerts but proactively hunt for behavioral indicators of adversary behavior find it difficult—if not impossible—to reconstruct the sequence of events that led to infection. And without access to relevant archived system or network data, the most skilled examiners can be left without insight into how the system volume, Windows registry, and native logs and artifacts looked last week, or last month, or at any other period.

[7] www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

As this example illustrates, the level of expertise required to manually acquire the target dataset from the potentially compromised systems requires considerable training and experience. Many organizations just growing their response capability are not able to employ such an expert, because such expertise is unavailable, too expensive or otherwise not feasible. Given this reality, a case can be made for automated data management technology, which can standardize data collection in a triage situation so nothing is missed.

Because one of the biggest challenges for incident responders is just *getting the data*, automated continuous monitoring of endpoints and network traffic provides such data. Therefore, analysis can begin immediately to help move the IR investigation forward.

Developing a more automated, and therefore more effective, IR approach can be broken into three specific strategies:

- Continuous data collection
- Aggregate and apply threat intelligence
- Streamlining live response capabilities

Figure 2 illustrates these strategies.

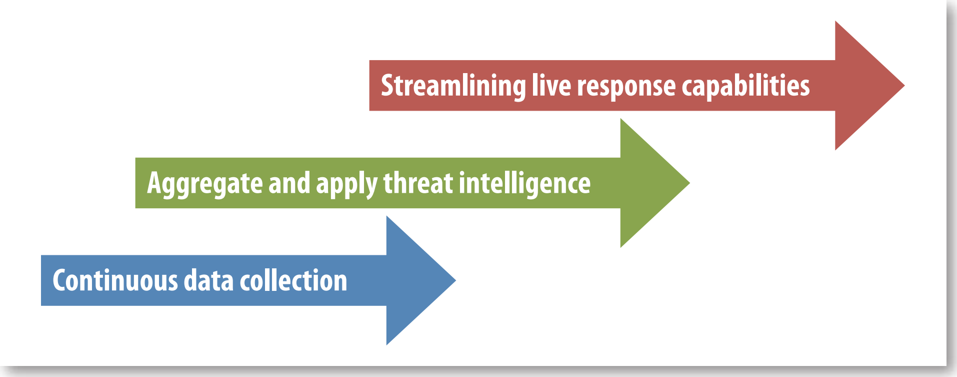

Streamlining live response capabilities
Aggregate and apply threat intelligence
Continuous data collection

Figure 2. The Three Steps to an Automated IR Plan

Continuous Data Collection

According to the SANS 2014 Log Management survey, 97 percent of respondents collect logs, yet only 42 percent send logs to an SIEM system.[8] In implementing automated continuous data collection strategies, a security team gains deeper insight into historical system state, event logs and network traffic.

How does automated continuous data collection compare to the standard data collection performed when an incident is detected? In traditional IR, evidence gathering takes place after a potential incident, leaving the investigator with blind spots regarding how the system was compromised and what the attacker did prior to detection.

In contrast, continuous proactive data collection ensures that evidence of execution, file access, lateral movement, network connections and logons are collected *continuously*. This data is archived for future use in incidents that have not yet occurred or been identified—a form of IR *precognition*.

[8] www.sans.org/reading-room/whitepapers/analyst/ninth-log-management-survey-report-35497

In the preceding example, with ongoing enterprise endpoint monitoring in place, the examiner could have rolled right into response, having overcome the greatest hurdle to the investigative process—just getting the data. The skilled examiner has the data immediately within arms' reach instead of having to extract evidence manually. This approach saves significant time.

Prioritizing ongoing data collection offers some additional benefits. For example, large-scale enterprise data aggregation tools provide the capability to baseline user behavior. By creating *patterns of life* for legitimate users on the network, deviations from a user's typical activity would be flagged as anomalous behavior. The examiner can then create automated alerts for events such as unusually timed logons, network resource accesses and VPN activity, allowing visibility into possible activity of the attackers already inside the network.

By collecting the right data, signs of an attacker's lateral movement under the guise of legitimate credentials may be identified.

In addition, by collecting the right data, signs of an attacker's lateral movement under the guise of legitimate credentials may be identified—a technique commonly employed by attackers to move among remote systems. Relying on logon audit failures or manual log review would make this type of identification nearly impossible.

It is important to note here that SIEMs are only as intelligent as the data they are fed, pointing to the expertise involved in selecting what data to aggregate in the first place. Yet if configured correctly, the automated collection can allow security teams to know what normal system and user behavior looks like—and therefore recognize anomalous activity when it occurs.

Aggregate and Apply Threat Intelligence

With continuous data monitoring in place, enterprises now can move to step two of our three-step plan. By centralizing continuous endpoint and network data collection, powerful correlations can be drawn with regards to threat activity, attack and reconnaissance techniques and threat actors. Threat intelligence is a capability that in the past has often been associated with more mature security teams and is underutilized in most organizations today. As seen in the SANS Incident Response survey conducted in June 2014, only 31 percent of organizations polled perform adversary/attacker attribution based on the data they collect during the IR process (see Figure 3).[9]

With automated data aggregation, threat intelligence and attribution becomes easier from an institutional perspective.

Does your organization perform adversary/attacker attribution based on the data/signatures collected during the incident response process?

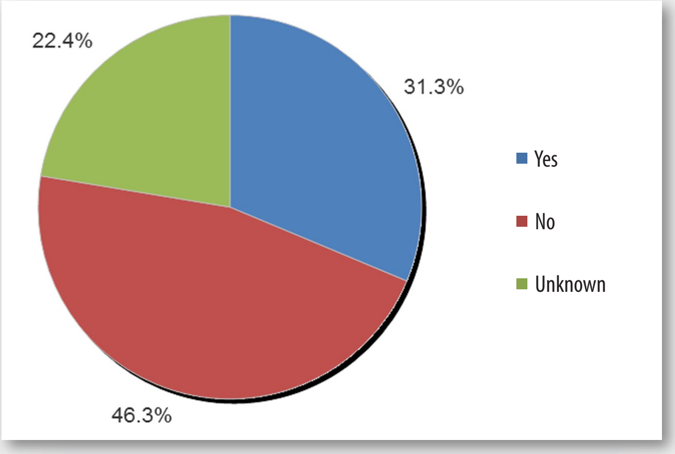


Figure 3. Respondents Who Perform Adversary/Attacker Attribution with IR Data
(Source: SANS 2014 IR Survey)

How can an organization incorporate threat intelligence capability into their IR process? With automated data aggregation, *threat intelligence and attribution* becomes easier from an institutional perspective, using data from past incidents to identify current attacks, as well as through partnerships developed with endpoint/network security vendors. Threat intelligence feeds can be obtained from SIEM vendors, community feeds and commercial threat intelligence providers and aggregators capable of packaging feeds in SIEM-ready preformatted rules. Through automation, the barrier to making use of past incident data from the organization and others in the community is lowered, allowing for greater proactive detection and response.

[9] www.sans.org/reading-room/whitepapers/analyst/incident-response-fight-35342

Streamline Live Response Capability

Lack of historical data was not the only difficulty that the examiner in our example ran into during his investigation, because the life of an incident responder is littered with obstacles. From the start, he struggled to rapidly perform system triage due to his organization's inefficient response technology, giving the attacker more dwell time uncontained on his network. Streamlining of the IR process and reduction of inefficiencies such as the one described is another critical element of an effective automated plan.

In our example of an attack, gaining access to the three geographically disparate systems of interest required laborious configuration changes because the environment lacked a remote enterprise triage tool. This problem is an easy fix because many of today's remote endpoint analysis tools offer automated triage capabilities. In connecting to the remote system via a software agent, these tools enable an examiner to perform triage swiftly upon request or to set triage to trigger automatically in reaction to an alert. Remote system interrogation provides a solution for getting the data to the examiner for faster triage of potentially compromised systems. However, not all organizations take advantage of these tools at this time.

A notable percentage of companies are paying for automated endpoint detection and mitigation technology and not making effective use of their investment due to lack of time, trained staff or incompatible network architecture. "Much of the new spending, however, may be on process improvements and staffing to get the most value out of existing security technologies already in place," according to the 2014 Ponemon Institute survey.[10]

Most computer incident response team (CIRT) members agree that every day on the job brings different and widely varying challenges. Devising a standard operating procedure when each incident could require uniquely specific actions is exceedingly difficult. For example, the measures taken to contain the effects of equipment theft compared to those put in place to combat a distributed denial of service (DDoS) against a web server can hardly be described in one standing document, let alone expected to be handled comprehensively by the same skillset of professionals. The need for automation and efficiency of process and procedure exists no matter what type of incident an organization encounters.

[10] "Data Breaches Drive Investments In Security Response, Data Protection," www.crn.com/news/security/300075493/data-breaches-drive-investments-in-security-response-data-protection.htm

Summary

As many organizations seek to increase their response capabilities, future implementations of streamlining evidence collection from the endpoints and crafting intelligently baselined event threshold alerts will become more imperative due to budget, time and manpower constraints. A forward leaning focus on automated security implementations that incorporates endpoint data/log collection, network device log aggregation and packet capture will offer an organization the capability to expand to its future demands of an ever-changing, increasingly sophisticated threatscape.

About the Author

Alissa Torres is a certified SANS instructor, specializing in advanced computer forensics and incident response (IR). Her industry experience includes serving in the trenches as part of the Mandiant Computer Incident Response Team (MCIRT) as an incident handler and working on an internal security team as a digital forensic investigator. She has extensive experience in information security, spanning government, academic and corporate environments, and holds a bachelor's degree from University of Virginia and a master's from University of Maryland in information technology. Alissa has taught as an instructor at the Defense Cyber Investigations Training Academy (DCITA), delivering IR and network basics to security professionals entering the forensics community. She has presented at various industry conferences and numerous B-Sides events. In addition to being a GIAC Certified Forensic Analyst (GCFA), she holds the GCFE, GPEN, CISSP, EnCE, CFCE, MCT and CTT+.

Sponsor

SANS would like to thank this paper's sponsor:

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.

Last Updated: April 29th, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Automotive Cybersecurity Summit & Training 2018	**Chicago, ILUS**	**May 01, 2018 - May 08, 2018**	**Live Event**
SANS SEC504 in Thai 2018	**Bangkok, TH**	**May 07, 2018 - May 12, 2018**	**Live Event**
SANS Security West 2018	**San Diego, CAUS**	**May 11, 2018 - May 18, 2018**	**Live Event**
SANS Melbourne 2018	**Melbourne, AU**	**May 14, 2018 - May 26, 2018**	**Live Event**
SANS Northern VA Reston Spring 2018	**Reston, VAUS**	**May 20, 2018 - May 25, 2018**	**Live Event**
SANS Amsterdam May 2018	**Amsterdam, NL**	**May 28, 2018 - Jun 02, 2018**	**Live Event**
SANS Atlanta 2018	**Atlanta, GAUS**	**May 29, 2018 - Jun 03, 2018**	**Live Event**
SEC487: Open-Source Intel Beta Two	**Denver, COUS**	**Jun 04, 2018 - Jun 09, 2018**	**Live Event**
SANS London June 2018	**London, GB**	**Jun 04, 2018 - Jun 12, 2018**	**Live Event**
SANS Rocky Mountain 2018	**Denver, COUS**	**Jun 04, 2018 - Jun 09, 2018**	**Live Event**
DFIR Summit & Training 2018	**Austin, TXUS**	**Jun 07, 2018 - Jun 14, 2018**	**Live Event**
Cloud INsecurity Summit - Washington DC	**Crystal City, VAUS**	**Jun 08, 2018 - Jun 08, 2018**	**Live Event**
Cloud INsecurity Summit - Austin	**Austin, TXUS**	**Jun 11, 2018 - Jun 11, 2018**	**Live Event**
SANS Milan June 2018	**Milan, IT**	**Jun 11, 2018 - Jun 16, 2018**	**Live Event**
SANS Crystal City 2018	**Arlington, VAUS**	**Jun 18, 2018 - Jun 23, 2018**	**Live Event**
SANS Oslo June 2018	**Oslo, NO**	**Jun 18, 2018 - Jun 23, 2018**	**Live Event**
SANS ICS Europe Summit and Training 2018	**Munich, DE**	**Jun 18, 2018 - Jun 23, 2018**	**Live Event**
SANS Philippines 2018	**Manila, PH**	**Jun 18, 2018 - Jun 23, 2018**	**Live Event**
SANS Cyber Defence Japan 2018	**Tokyo, JP**	**Jun 18, 2018 - Jun 30, 2018**	**Live Event**
SANS Paris June 2018	**Paris, FR**	**Jun 25, 2018 - Jun 30, 2018**	**Live Event**
SANS Vancouver 2018	**Vancouver, BCCA**	**Jun 25, 2018 - Jun 30, 2018**	**Live Event**
SANS Minneapolis 2018	**Minneapolis, MNUS**	**Jun 25, 2018 - Jun 30, 2018**	**Live Event**
SANS Cyber Defence Canberra 2018	**Canberra, AU**	**Jun 25, 2018 - Jul 07, 2018**	**Live Event**
SANS London July 2018	**London, GB**	**Jul 02, 2018 - Jul 07, 2018**	**Live Event**
SANS Charlotte 2018	**Charlotte, NCUS**	**Jul 09, 2018 - Jul 14, 2018**	**Live Event**
SANS Cyber Defence Singapore 2018	**Singapore, SG**	**Jul 09, 2018 - Jul 14, 2018**	**Live Event**
SANSFIRE 2018	**Washington, DCUS**	**Jul 14, 2018 - Jul 21, 2018**	**Live Event**
SANS Cyber Defence Bangalore 2018	**Bangalore, IN**	**Jul 16, 2018 - Jul 28, 2018**	**Live Event**
SANS Malaysia 2018	**Kuala Lumpur, MY**	**Jul 16, 2018 - Jul 21, 2018**	**Live Event**
SANS Pen Test Berlin 2018	**Berlin, DE**	**Jul 23, 2018 - Jul 28, 2018**	**Live Event**
SANS SEC460: Enterprise Threat Beta Two	**OnlineVAUS**	**Apr 30, 2018 - May 05, 2018**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**