

Threat Detection Best Practices in AWS

Compiled from works completed by

J. Michael Butler | Dave Shackleford | David Szili

with an introduction by **John Pescatore**

December 2019

Table of Contents

3	Introduction
4	How to Build a Security Visibility Strategy in the Cloud
5	Introduction
5	Types of Security Visibility Needed in the Cloud
6	Security Visibility Today
7	What Is Different About Visibility in the Cloud?
8	Building a Cloud Security Visibility Strategy
9	Case Study: The Modern Cloud-Aware SOC
10	Architecture Planning
10	Enabling Security Controls
12	Adapting Existing Processes and Functions
13	Summary
15	JumpStart Guide for SIEM in AWS
16	Introduction
17	Understanding Your Needs
18	Implementation Options in AWS
18	Cloud-Optimized
18	Managed Services
19	Consulting Partner Private Offers
19	Needs and Capabilities: The Business Case for SIEM and SOAR in the Cloud
20	General Cloud SIEM and SOAR Considerations
20	Business Considerations
21	Technical Considerations
21	Operational Considerations
22	AWS Implementation Considerations
25	Making the Choice
25	Have a Plan
26	Consider Partners
26	Conduct a Proof-of-Concept Test and Evaluate Options for Desired Features
27	Conclusion
29	How to Build a Threat Detection Strategy in AWS
30	Introduction
31	Data Collection
31	Flow Logs
33	API and Account Activity Logs
34	Intrusion Detection and Prevention Systems
35	Network IDS/IPS
35	Traffic Mirroring
36	Host-Based IDS/IPS
37	Event Management and Analysis
38	Putting It All Together
39	Automation
40	Security Monitoring Best Practices in AWS
40	AWS Security Monitoring Best Practices
41	The Process
42	Conclusion
44	Next Steps

“By blocking as many attacks as possible while also detecting those that get through first-level defenses, businesses are able to significantly improve on three key metrics that are critical to secure operations.”

Cyber threats may be a constant on the internet, but cyber incidents don't have to be. Many organizations have evolved their cybersecurity strategies and architectures to effectively and efficiently protect their online business applications and sensitive customer information against sophisticated hackers. The common denominators across those success stories are the abilities to:

- Avoid or mitigate most vulnerabilities
- Block all common attacks seeking to exploit remaining vulnerabilities
- Quickly detect sophisticated attacks that couldn't be blocked
- Rapidly and accurately respond to incidents, and minimize or avoid business disruption

These same factors are key to staying secure as organizations migrate to cloud-based operations. In earlier e-books in this series, we addressed the first two factors: focusing on endpoint security for vulnerability reduction and configuration management, along with network security to protect endpoints that remained at risk and monitor for other malicious traffic on networks. By blocking as many attacks as possible while also detecting those that get through first-level defenses, businesses are able to significantly improve on three key metrics that are critical to secure operations: mean time to detect, mean time to mitigate and mean time to restore business operations.

To gain these improvements, the security architecture must be able to process large amounts of alerts and log data coming from firewalls, intrusion detection systems and endpoint security agents. While not enough data can allow hackers to exploit blind spots, too much data can cause high “noise” levels that mask serious events. Tools, such as security information and event management (SIEM) systems, are available to manage this torrent of security data and reduce both false positives and false negatives. Because staffing is often constrained, organizations can use products such as security orchestration, automation and response (SOAR) tools to augment skilled staff to manage the volume and enable that staff to focus on the highest value alerts.

The following papers describe best practices and techniques for creating security visibility and threat detection strategies in Amazon Web Services (AWS):

- **How to Build a Security Visibility Strategy in the Cloud**, written by Dave Shackleford, defines the key elements of assuring both event- and behavior-driven visibility into the current security state. The whitepaper also details the security architectural elements needed to make sure that visibility extends across networks, endpoints, applications, containers and cloud infrastructure.
- In **JumpStart Guide for SIEM in AWS**, J. Michael Butler provides a tutorial on event monitoring and management terminology in general, and SIEM and SOAR products in particular. It also details a methodology that explores the business, technical and operational considerations to architect the SIEM deployment strategy for protecting your organization's AWS services.
- Finally, **How to Build a Threat Detection Strategy in AWS**, by David Szili, ties everything together by detailing the specific features AWS provides for visibility and log management, along with how to merge and analyze that information with threat information and data from security controls. The end result is a set of best practices for rapid and accurate detection of threats to your AWS-based services.

By increasing visibility, leveraging large-scale analytics and automation, and building solid threat detection strategies, organizations have the power to vastly improve security when doing business in the cloud.



How to Build a Security Visibility Strategy in the Cloud

Written by **Dave Shackleford**

March 2019

Sponsored by:

AWS Marketplace

Webcast

You can access the associated webcast at:
<https://pages.awscloud.com/AWSMP-SANS-Training-Security-Visibility>

Introduction

Today organizations are storing sensitive information ranging from business intelligence to personally identifiable information, health records, credit cards and other regulated data in the cloud. It is obvious that cloud is here to stay, and security professionals need to manage the threats and vulnerabilities that go along with cloud deployments. The good news is that more powerful tools and capabilities are available in the cloud than ever before, and this all starts with increasing visibility for cloud implementations, both with cloud-native tools and services and third-party tools and products that have been adapted to cloud provider environments.

In this paper, we look at a variety of controls to ensure network, application, instance/container, database/storage, and control plane visibility and build upon them to create a security visibility strategy for the cloud.

Types of Security Visibility Needed in the Cloud

The two major types of visibility that security teams need to focus on in the cloud today are:

- **Event-driven visibility**—The most common types of visibility that security teams have traditionally focused on are events. These events can be derived from a wide variety of sources, including operating system logs, application logs, network device and platform logs and events, and security system events (intrusion detection and prevention, data protection tools, anti-malware platforms and more). In the cloud, all of these events still have merit and all can (and should) be collected as needed. However, the cloud service environment itself can also track events occurring across infrastructure, so security teams have a new category of events they can use to monitor for unusual or suspicious activity. For example, a security operations center (SOC) can monitor AWS CloudTrail¹ events for an Amazon Elastic Compute Cloud (EC2) instance spawned from a non-approved machine image or a user attempting to deactivate multifactor authentication (MFA).
- **Behavior-driven visibility**—The other major types of visibility needed in many environments are more driven by events occurring over time, indicating a pattern of behavior. Particularly in cases of insider abuse, account hijacking and illicit use of cloud resources, organizations need insight into larger datasets over longer periods of time to really see whether unusual or malicious activities are afoot. An example might be an unusual pattern of workloads trying to communicate to other workloads within a subnet, potentially indicating system compromise and

The importance of visibility into what the environment looks like and the inventory of available assets cannot be overstated.

¹ This paper mentions product names to provide real-life examples of how visibility tools can be used. The use of these examples is not an endorsement of any product.

attempted lateral movement. This may be noted by observing large datasets of flow logs aggregated and monitored by a network monitoring solution or event management platform.

With these two types of visibility in mind, the next section describes the types of controls you will need to ensure security visibility.

Security Visibility Today

The importance of visibility into what the environment looks like and the inventory of available assets cannot be overstated. The first of the Center for Internet Security (CIS) Critical Security Controls² focuses entirely on shoring up this lack of visibility through maintaining a sound inventory of systems operating within the environment.

The security concept “You can’t secure what you don’t know about” holds true in any environment, and this control has been the highest-priority control since the list’s inception. The second CIS Critical Security Control focuses on gathering and maintaining an inventory of software running on systems. Both of these controls fit into the identify function of the NIST Cyber Security Framework (CSF), which is illustrated in Figure 1.

While these controls serve as a sound starting point for any conversation about visibility and tracking assets in a cloud environment, there’s much more to do. Today, most organizations rely on many types of controls for security visibility. All of these are readily available in the cloud, often in both cloud-native formats and third-party vendor solutions:

- **Network visibility**—The types of controls often used to achieve network visibility include network firewalls, network intrusion detection and prevention, load balancers, proxying tools, and network flow data (behavioral) collection and monitoring. Leading network vendors have adapted products in all of these categories to integrate into a virtual private cloud (VPC) architecture, granting network and security teams the same security capabilities and insight into network traffic they’ve attained internally. Cloud-native access controls such as security groups and flow logs enable security teams to monitor and track network events and behaviors.

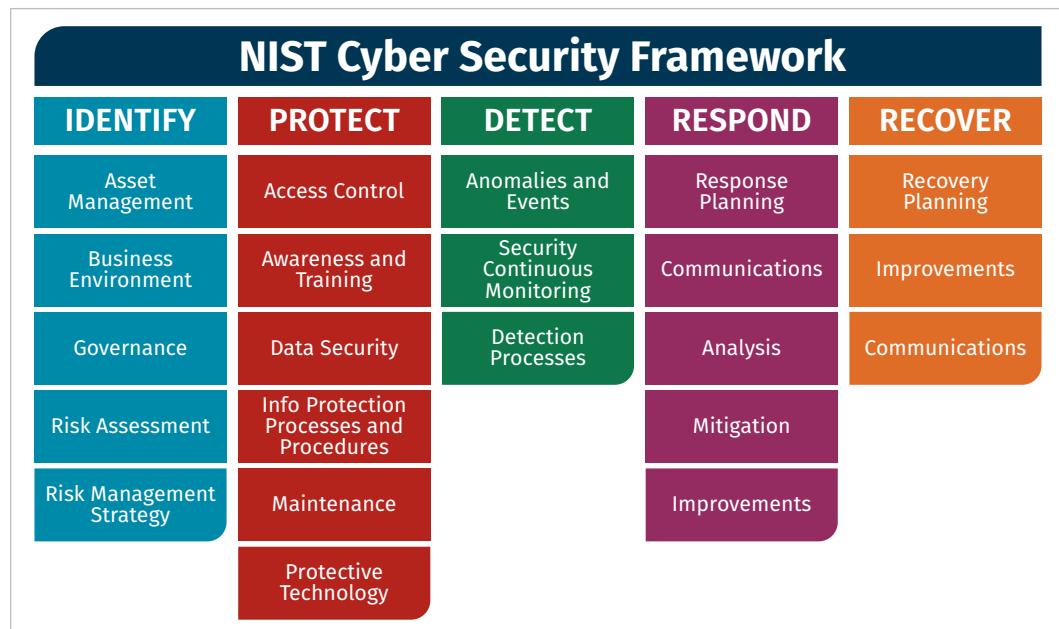


Figure 1. The NIST Cyber Security Framework³

² www.cisecurity.org/controls

³ “Introduction to the NIST CyberSecurity Framework for a Landscape of Cyber Menaces,” Security Affairs, April 20, 2017, <https://securityaffairs.co/wordpress/58163/laws-and-regulations/nist-cybersecurity-framework-2.html>

- **Application visibility**—Application visibility relies on tracking events and behaviors at scale as workloads communicate within the cloud environment as a whole, in addition to the local application logs on individual systems and containers.
- **Instance/container visibility**—Logs and events generated by services, applications and operating systems within cloud instances should be automatically collected and sent to a central collection platform. Automated and remote logging is something many security teams are already comfortable with, so organizations implementing robust cloud security designs really just need to ensure that they are collecting the appropriate logs, sending them to secure central logging services or cloud-based event management platforms, and monitoring them closely using SIEM and/or analytics tools. In the case of containers and container management tools, many new and well-known providers of vulnerability scanning and configuration assessment services have adapted their products to work in the cloud, granting deep visibility into both container image configuration and runtime event monitoring.
- **Database/storage visibility**—Many cloud deployments employ a wide variety of storage types, including block storage, blob-type storage, databases and more. Security visibility for storage components often revolves around access controls and permissions, as well as events related to encryption and other protective measures implemented within the storage platform. All major cloud storage types include various forms of logging, and many include access control measures. Many encryption and data monitoring tools are available for public cloud storage, as well.
- **Control plane visibility**—Another type of visibility that is now available in the cloud is of the cloud environment itself: the control plane. In addition to extensive logging of all activity within the environment itself, a number of new services are available to continuously monitor cloud accounts and environments for best practices configuration and security controls status. Imagine a single service to monitor the entire data center and its configuration all at once!

Myths About Cloud Security Visibility

As cloud adoption has increased, a couple of myths about cloud security visibility linger.

“We can’t get adequate logging in the cloud.”

Today, this statement is blatantly false, because major infrastructure-as-a-service (IaaS) providers have enabled extensive logging of all activity within the environment, essentially recording every API call made in any way.

“Network security visibility is less capable in the cloud.”

With the right mix of tools and architecture, this is also untrue. More and more, leading network security providers are adapting products to integrate into leading IaaS clouds, and coupled with cloud-native network controls, this provides plenty of opportunity to see and control traffic.

What Is Different About Visibility in the Cloud?

One major development in cloud security that immediately benefits security teams is the reality that cloud-based assets are inextricably linked to the provider’s environment, making them always visible. Through a combination of integrated APIs, scanning and local agents, it is possible to improve upon inventory and asset management strategies more than ever. In essence, there’s an “always-on” level of visibility that teams can query and monitor, and there’s really nowhere to hide in the cloud.

In addition, as noted earlier, a comprehensive control plane is now part of the mix for security-related tasks and operations. What does this mean to visibility? In essence, the environment (and APIs offered by the cloud provider) becomes a unified backplane that organizations can attach monitoring tools to, generate event data from, and set event and behavior “triggers” around that puts this control plane to work for security teams in an automated fashion. By building out policies for event monitoring, continuous scanning of workloads and events, and potentially responding through automated actions, the cloud platform lends itself to deeper levels of visibility than were possible in traditional data center environments. Imagine having a single control plane for your entire data center, where all tools could be connected, events generated and monitored, access managed and so on—this is truly what’s possible in the cloud.

All of this is possible, of course, because the entire environment is software-defined. In addition to adapting existing tools and services to work within the new control environment, many services from the cloud providers themselves are emerging to augment security operations strategies. It is possible to have more than one tool or service monitoring various facets of cloud environments at all times—with minimal additional overhead.

Building a Cloud Security Visibility Strategy

The first function outlined in the NIST CSF is Identify, which consists primarily of asset management, governance and risk assessment practices and controls within the environment. Accordingly, the first step to building a cloud visibility strategy is to determine what types of event data and information are available in the cloud environment you’re operating within, which can immediately help to achieve the goals of the identify phase. Aside from agent-based tools that can help to collect workload and container events, and other third-party platforms that organizations may choose to implement (discussed shortly), logs and events that contribute to cloud visibility also include environment logs that describe interesting API activity (which would also align under the investigate function of the NIST CSF). Take, for example, an AWS CloudTrail event that indicates a cloud user trying to deactivate an MFA device, as shown in Figure 2.

Be sure to evaluate these log types carefully to understand what types of information they provide you.

Another major element of the NIST CSF is Protect, which emphasizes many security controls that would be involved in improving security visibility. Such controls include firewalls and security agents that can aid in

```
"eventTime": "2017-01-20T18:53:02Z",
"eventSource": "iam.amazonaws.com",
"eventName": "DeactivateMFADevice",
"awsRegion": "us-east-1",
"sourceIPAddress": "1.2.3.4",
"userAgent": "signin.amazonaws.com",
"requestParameters": {
  "userName": "dave",
  "serialNumber": "arn:aws:iam::000012345678:mfa/dave"
},
"responseElements": null,
"requestID": "d1a9ebf8-5fc8-11e5-9d8f-1bc7c6757e61",
```

Figure 2. Suspicious AWS CloudTrail Event

protecting from malware, network behavior monitoring, event management tools and more. Consider the following process to select and implement the most effective cloud security visibility strategy:

1. Be sure to investigate third-party options from vendors and service providers that can enhance and augment your monitoring and visibility strategy.
2. Before considering the latest cloud-native tools and capabilities from cloud providers, consider the critical factors that may dictate when you should keep your in-house vendor products in place (or possibly choosing entirely different third-party tools versus those you've had) as opposed to moving to new cloud service provider offerings. Sticking with your current tools makes sense if:
 - You have a well-supported vendor product that has been adapted to the cloud and scales well.
 - You have a highly distributed cloud deployment and need to keep operational overhead and skills to a bare minimum.
 - Your vendor product has clear and distinct advantages over the cloud provider services offered and these make a difference to you.

In some cases, however, a combination of both vendor and cloud provider services/controls may make more sense than one solution alone. To that end, be sure to evaluate cloud-native controls that the provider offers. In-house services may offer simpler operations, better performance, improved capabilities, or deeper and more natural integration than existing tools. For many large enterprises, though, cloud-native solutions will be better implemented to augment and enhance security visibility alongside third-party tools.

Finally, make sure you tie together event monitoring, vulnerability scanning/monitoring and control plane visibility to create a true continuous monitoring strategy.



Figure 3. Planning Steps for a Cloud-Aware SOC

Case Study: The Modern Cloud-Aware SOC

What does a modern cloud-enabled SOC look like for hybrid architectures? Figure 3 illustrates key issues a cloud-aware SOC should be prepared to work through.

Architecture Planning

The SOC team needs to align with cloud architecture and engineering teams that have built the hybrid architecture and maintain it. DevOps teams will also be involved in governance and oversight of cloud activity monitoring and visibility, because they will be responsible for application development and deployments into a platform-as-a-service (PaaS) or IaaS environment. The SOC team should strive to understand the following with the assistance of these teams:

- **What connectivity does the public cloud provider have back to the data center or primary operations location?** In many hybrid architectures, this connection is either a point-to-point IPSec VPN tunnel (or several of them), a dedicated telecommunications circuit of some fixed bandwidth, or a combination of both. The means of connectivity will determine accessibility into the cloud network environment, as well as bandwidth constraints on event data and other visibility information the SOC needs.
- **Are the appropriate tools enabled?** Discuss whether any deployment tools in use for managing and promoting infrastructure as code (code repositories, deployment tools like Jenkins, or template formats like CloudFormation, Terraform, etc.) should be enabled for auditing activities and access logging.
- **How will deployment images and container builds be deployed?** Discuss deployment images and container builds, so that the SOC understands where and how these will be deployed. Team members need to understand topics including image update cycles, storage locations and workload lifecycle to better enable contextual monitoring.
- **What are our plans for elasticity and scaling?** Discuss any plans for elasticity and automatic scaling operations that could increase or decrease activity and operations in the cloud environment. SOC teams must understand these issues so that they can better prepare to monitor the events and track changes accordingly.

Enabling Security Controls

The SOC should then enable the following options in various security control categories to ensure visibility is maximized in the cloud:

OS Hardening and Logging

Enable auditing and logging of all instances and containers to be forwarded to a central in-cloud storage location, where the data can then be streamed to an on-premises or in-cloud SIEM. Ideally, CIS guidelines and other industry benchmarks are built into deployment templates and images, and additional logging and hardening scripts can be created by experience over time.

Control Plane Logging

Ensure that all cloud provider control plane logging (such as AWS CloudTrail) is enabled and that these logs are being centrally collected and streamed to an on-premises or in-cloud SIEM through API integration. Any third-party services performing independent control plane logging and monitoring should be generating events and logs that can ideally be extracted via API and centralized within a SIEM or analytics platform. In addition, enable cloud-native behavioral analytics tools to monitor account behavior and activity specifically.

Identity and Access Management (IAM)

All directory service logs should be centrally collected, as should other logs such as central policy coordination through tools like identity and access management tools offered by cloud providers. Because most IAM users and groups tend to be service accounts and unique DevOps, testing and administration accounts, be sure to carefully monitor all activity pertaining to these users and roles. Any addition, deletion or changes of IAM policies should be noted carefully and prioritized, too.

Endpoint Security

Ideally, SOC teams will have installed and enabled endpoint detection and response (EDR) agents from a trusted third party or leading open source project, including tools that perform host IDS functions. Send all these events to a monitoring console that can integrate with SIEM and analytics tools.

Network Security

A SOC team should enable next-generation firewall (NGFW) platforms that offer intrusion prevention and detection, along with traditional network protocol and service/port control. Also, enable and send cloud DNS logs and network flow records to a central monitoring platform that can feed data to SIEM and analytics tools.

Vulnerabilities/Configuration

Set up a best-of-breed third-party network and application vulnerability scanner to feed vulnerability reporting data back to a SIEM or analytics platform, and use a cloud-native scanning tool (if available) to enable more continuous monitoring (if available). Any continuous monitoring tools that the cloud provider offers should also be enabled to scan for specific conditions. For example, are all running workloads being started from approved images?

Threat Detection

With the proper visibility in place through logging and monitoring, along with large-scale analytics and data processing tools and capabilities, cloud consumers can now track and monitor both control plane activity (covered earlier) and threats from both internal and external sources over time. With a more complete picture of behavior, organizations can detect malicious, suspicious, and accidental/unintended actions and events.

Adapting Existing Processes and Functions

Finally, a SOC needs to adapt some of its existing processes and functions to properly improve visibility into their deployment of hybrid architectures. Take the following example of a traditional SOC walkthrough (see Figure 4).

Initial Event

Based on collection and large-scale analytics processing of flow logs within their SIEM, SOC staff is alerted to a workload in a cloud subnet scanning or trying to communicate with other subnet members. These are recorded as **REJECT** messages from a number of ports where the subnet attempted communication. Simultaneously, a serverless function that autotags instances exhibiting these scanning behaviors is triggered, adding the tag **Suspicious** to the instance with a value of **Yes**.

Within the same time frame as this initial alert, additional correlating evidence appears implicating strange behavior patterns on the part of an IAM account used in application interactions with this same system. The account was invoked from a remote command-line installation versus internal-only invocation.

Initial Triage

The SOC team uses a central analytics processing tool to look up additional correlating information. This could include:

- Additional IAM activity for this same service account in the last 24 hours.
- EDR agent alerts (if any) for the past 24 hours.
- Logs from third-party control plane scanning and monitoring tools—has the environment shown any unusual or less secure configuration details recently that could lead to this?
- Logs and events from NGFW platforms performing firewall and IPS functions—have any unusual traffic patterns been seen going outbound from this system, or inbound to it?

Event Validation

Using a dedicated account with specific programmatic access privileges into the production environment, the SOC team runs a query to find out the instance configuration details based on the image it was deployed from, as well as how long the instance has been running and its remote IP address (if it has a public interface). Another SOC account query looks for any and all systems with the **Suspicious** tag every 30 seconds to see if new systems are appearing in the same subnet.

Investigation

Based on the behaviors seen, the SOC team runs a vulnerability scan on the workload to see if any obvious misconfigurations are present, or whether known vulnerabilities are found that could be exploited. At this point, the team can declare a formal investigation, open a ticket and initiate follow-up response and forensics processes.

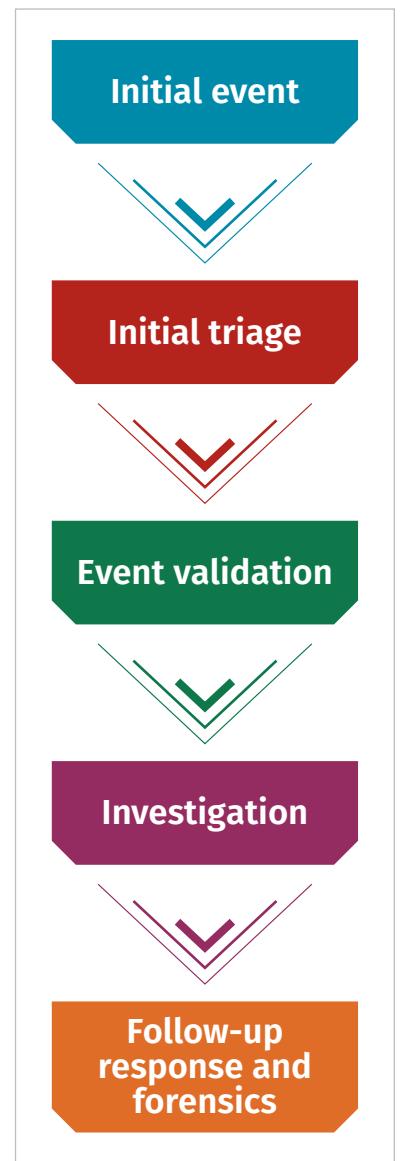


Figure 4. Process for Adapting Processes and Functions

Summary

The cloud has a lot to offer in the way of security monitoring and visibility. Organizations have the ability to capably monitor for both event-driven and behavior-driven activity, and now they have a single environment they can query for all the cloud control plane visibility they could ask for. Some adaptation of monitoring and preventive/detective tools may be required. However, organizations have more options because of the variety of cloud-native and third-party controls and services available. It is possible to implement and monitor the entire spectrum of control areas, ranging from network controls, including firewalls and intrusion detection services, to endpoint protection and monitoring agents, to continuous vulnerability scanning. Given large-scale analytics processing and numerous options to enable, collect, store and transmit log and event data from cloud assets and environments, organizations can more readily analyze everything happening in segments of their hybrid cloud networks and correlate this data with internal event information generated from existing security tools (some of which may be covering both internal and public cloud space).

However, organizations need to coordinate security operations more closely with cloud engineering and architecture teams, as well as DevOps and others. SOC teams can easily build effective correlation cases for cloud monitoring, but they need to understand and adapt to different event sources and types, which often takes time.

The SOC team can, in turn, build adapted processes to monitor cloud-based events and information, analyze and evaluate systems and the environment to better correlate and validate what's happening, and then initiate additional cloud-specific triage and response as needed. All of this is built from a solid base of extensive cloud security visibility, which is a real possibility today.

About the Author

Dave Shackleford, a SANS analyst, senior instructor, course author, GIAC technical director and member of the board of directors for the SANS Technology Institute, is the founder and principal consultant with Voodoo Security. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. A VMware vExpert, Dave has extensive experience designing and configuring secure virtualized infrastructures. He previously worked as chief security officer for Configuresoft and CTO for the Center for Internet Security. Dave currently helps lead the Atlanta chapter of the Cloud Security Alliance.

Sponsor

SANS would like to thank this paper's sponsor:



RETURN TO THE
TABLE OF CONTENTS

JumpStart Guide for SIEM in AWS

Written by **J. Michael Butler**

August 2019

Sponsored by:

AWS Marketplace
in conjunction with
Optiv

Webcast

You can access the associated webcast at:
<https://pages.awscloud.com/JumpStart-SIEM>

Introduction

Gone are the days of focused technicians in a darkened lab with a table full of terminals located somewhere deep below the data center. Thankfully, simple logging and manual reviews by a roomful of techs have morphed into more automated processes. With SIEM systems, logs are now normalized and collected in a central location for analysis. As SIEMs have matured, more automatic alerting, and even reactions to events, have moved us into the security orchestration and automated response (SOAR) world—or as it's also known in some circles, SIEM on steroids. Currently, according to Gartner, "Analytics are a core capability of all SIEM solutions."¹ Analytics and response are what SOAR is all about.

At its most basic level, the SIEM is defined by NIST as an "[a]pplication that provides the ability to gather security data from information system components and present that data as actionable information via a single interface."² Adding SOAR integrates additional data feeds, correlation, analysis and automated functions based on identified incidents, indicators, events and threats.

In addition to SIEM log collection, some added data feeds for a SOAR system would likely include endpoint management system alerts, threat and vulnerability data from third parties (for example, STIX/TAXII feeds), and help desk and collected forensics data, all to be correlated with the SIEM data. Once that data is analyzed, remediation or other actions can automatically take place for those issues identified by the organization as reliably founded and actionable. The questionable issues can be referred to the SOC (security operations center) for further analysis as needed.

In this paper, we discuss needs, implementation options, capabilities, and various considerations for organizations seeking to implement SIEM/SOAR capabilities in Amazon Web Services (AWS). We discuss the integration of SIEM and SOAR in the cloud environment and how that compares to on-premises use. What does a cloud use case look like? What are the differences between cloud and on-premises deployments? Then we offer suggestions for planning integration of SIEM and SOAR into an AWS cloud environment in the way that is most beneficial to an organization. We hope to help organizations evaluate the options and make the best choice.

[SIEM] provides the ability to gather security data from information system components and present that data as actionable information via a single interface.

—National Institute of Standards and Technology

¹ "Critical Capabilities for Security Information and Event Management," www.gartner.com/doc/reprints?id=1-5VGLBIM&ct=181129&st=sb

² Computer Security Resource Center Glossary, <https://csrc.nist.gov/glossary/term/Security-Information-and-Event-Management-Tool>

Understanding Your Needs

First, consider what technology your organization needs to adequately collect, analyze and react to SIEM data. If your organization can already determine the actionable events or incidents in the existing environment with current tools, the temptation may be to try to adapt those tools to the cloud or vice versa. In that case, be sure to review the security offerings available in the cloud that can improve on what the on-premises solutions offer. New features offering enhancements or alternatives for an on-premises system are being added regularly to the cloud.

After a careful determination of your organization's feature and function requirements, present those requirements to your vendors and start the discussions about what you need to make it all work. Look at the new technologies that may be needed.

Be certain to review existing gaps and what it would take to eliminate them. Be wary of the "gotchas" that will require (possibly significant) resource investments, such as additional subscription fees, personnel and training, and ongoing costs such as annual software maintenance fees. Also consider growth to scale and requirements to enable that growth, and, conversely, the ability to shrink to scale. Cloud environments make it easier to scale up and shrink down resources in response to users' needs. This is especially useful for organizations that experience seasonal change.

The organization should have a long-range plan to budget for implementation, ongoing operations, and hardware and software maintenance. No one needs one more software package to sit on the shelf without providing value. As the SIEM/SOAR project moves forward, revisit requirements regularly to make sure the organization's incident response needs are being met. Figure 1 illustrates the process.

In the SANS 2019 Cloud Security Survey, 75% of the respondents reported using as many as 10 cloud providers for all operations, and 3% of the respondents said they use more than 100 providers!³ If your organization has multiple cloud providers, consider the need for SIEM/SOAR tools to be capable of accumulating and analyzing data from all of the cloud environments in use. This functionality is particularly needed if the organization has communication or network channels set up between multiple environments, causing incidents in one environment to have an undesirable impact on another.

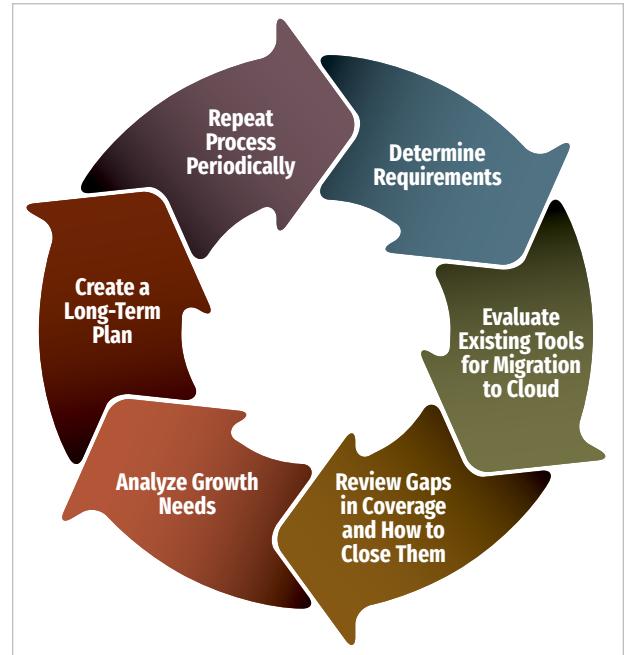


Figure 1. Process for Understanding Your Needs

³ "SANS 2019 Cloud Security Survey," www.sans.org/reading-room/whitepapers/cloud/paper/38940 (registration required)

Implementation Options in AWS

If your organization is thinking of leveraging current on-premises technologies for SIEM and SOAR as you move to the AWS cloud, be sure to take note of the new cloud-native solutions that were not previously available. As of this writing, AWS Security Hub,⁴ which provides compliance data, security alerts and security findings, is now generally available. Many desirable SIEM features are now native options in the AWS cloud. It is also important to note that third-party providers, including AWS partners Splunk and Sumologic, have already integrated with AWS Security Hub.

Cloud-Optimized

Consider the cost delta between using the cloud solutions versus the on-premises tools, as well as the costs for the significant storage requirements of SIEM/SOAR data in the cloud versus on premises. Also look at the license fees to be paid for the solution your organization needs versus any on-demand licensing available through AWS for access to its solution partners. At the very least, the cloud-native options can enhance other tools the organization uses, whether the SIEM data is stored in the cloud or on premises.

One advantage of working with off-premises options is the clearer pricing models when compared to running everything on premises. Many cost factors in the data center have to be included if the organization is to get a true picture of the total cost of ownership (TCO). For example, how much is being paid for CPU cycles, mass storage, power requirements, HVAC requirements, facility space, hardware, software, licensing, maintenance, upkeep, personnel and other hidden costs in on-premises environments? On the other hand, the pricing models will be much clearer from cloud providers, and TCO is more easily determined in the cloud.

Managed Services

Managed services are also an option, of course. If the organization does not have in-house expertise or resources, consider a third-party firm that can manage the SIEM/SOAR solution(s) of choice. It ultimately boils down to the requirements of the organization, the most efficient way(s) to meet those requirements and available budget. It may even be practical to start with managed services with a view to transitioning to an internal team over time. That way the organization can see a more immediate return on its investment in SIEM and SOAR while building out its systems and acquiring the needed resources and training to bring its program up to speed. Starting with managed services will mean more up-front cost but also much faster implementation and maturity.

⁴ This paper mentions product names to provide real-life examples. The use of these examples is not an endorsement of any product.

Consulting Partner Private Offers

Customers can also engage through Consulting Partner Private Offers (CPPO) to work directly with trusted advisors to select and configure SIEM/SOAR solutions from AWS Marketplace. As organizations build out their cloud and cloud security strategy and plan, they may want to consider working with partners to accelerate their efforts or fill any gaps in knowledge or resources that are identified. All consulting partners may extend AWS Marketplace third-party solutions directly to customers through CPPO.⁵ Not every organization will be able to find resources with deep cloud experience. Even experienced cloud technologists may have experience only in specific industries or with specific cloud vendors. A requirements document could be helpful when approaching prospective consultants.

Needs and Capabilities: The Business Case for SIEM and SOAR in the Cloud

Among the features that cloud architecture offers for SIEM and SOAR that an on-premises system cannot is visibility across multiple environments in different availability zones or regions. Such visibility could be even more important for global organizations. Consider also that the redundancy of the cloud practically guarantees reliable uptime, which is not available to an organization internally without great expense and multiple data centers.

Then factor in the ability of the cloud provider to offer pricing based on dynamic workloads and short life cycles, where entire environments can be spun up and shut down in a matter of minutes—again, not something a typical data center can provide to an organization. Even leveraging on-premises virtual hosts doesn't offer as much flexibility, especially compared to serverless implementations in the cloud.

Needs and Capabilities

Organizations require a lot of their SIEM/SOAR systems.



The need: Aggregating log events and security information from multiple systems, collecting data about threats and automatically responding to low-level security events without human intervention

⁵ AWS Marketplace Channel Programs, <https://aws.amazon.com/marketplace/partners/channel-programs>

Capabilities

- Security threat and incident detection
- Bidirectional feeds with Amazon Security Hub
- Increased efficiencies
- Analytics and alerting
- Detailed drill-down compliance reporting
- Increased efficiencies for physical and digital security operations
- Event and threat intelligence correlation

For incident response functions, SOAR supplements SIEM and helps to:

- Define
- Prioritize
- Standardize
- Automate⁶

General Cloud SIEM and SOAR Considerations

Regardless of the SIEM/SOAR technology or cloud vendor selected, some general business, technical and operational considerations are associated with implementing security in the cloud. The following sections highlight many of these considerations.

Business Considerations

	Consideration	Details
	Policies and standards	<p>Organizations will need to evaluate cloud capabilities to determine what changes are needed to ensure that compliance with policies and standards is achievable.</p> <p>Organizations should evaluate relevant retention policies for collected log data. They should determine what happens if a matter becomes litigious and a legal hold on certain data is necessary, as well as where and how data will be held in a secure state for the period of the legal hold.</p>
	Governance model	<p>Organizations need to decide whether to centralize or decentralize governance over cloud incident response and determine whether existing governance models used for traditional incident response can be extended to the cloud or if a cloud-specific model is required.</p> <p>Consider that cloud workloads can more easily span the globe and that data residency and visibility restrictions may apply in certain regions.</p>
	Reporting and metrics	<p>Providing the right metrics, key performance indicators (KPIs) and key risk indicators (KRIs) to the right stakeholders may require changes to account authorization for cloud architectures.</p> <p>Organizations will need to define reporting requirements specific to cloud workloads and evaluate features and products against these requirements.</p>
	Funding and support	<p>Funding and support for cloud SIEM and SOAR implementations may not currently be available.</p> <p>Management may not understand the shared responsibility model as it pertains to cloud usage and may assume that all needed features of SIEM and SOAR are included.</p> <p>Management will need to be educated to understand the implementation model and the related requirements as it determines the appropriate funding and support model.</p>
	Risk classification	<p>Acceptable risk vs. mitigated risk vs. transferred risk (NIST 800-30) is a consideration when determining what action(s) should or should not take place upon discovery of an incident or potential incident.</p> <p>The organization will need to determine the risk of automatically responding to SIEM alerts in an orchestrated manner as opposed to sending certain alerts to a manual queue or ignoring certain alerts altogether.</p>

⁶ Tech Target, <https://searchsecurity.techtarget.com/definition/SOAR>

Technical Considerations

	Consideration	Details
	SIEM capabilities	<p>As organizations update policies and standards to address cloud workloads, they should also identify the technologies needed to comply with these new requirements.</p> <p>Some organizations may choose to be very prescriptive about which technologies should be used, while others may define the required capabilities and allow individual cloud operations teams to select their own technologies.</p>
	Supported technology	<p>Some technologies may not be supported for all cloud services or for all platforms running on cloud services.</p> <p>Organizations need to decide whether they will allow unsupported technologies, and if so, under what conditions.</p>
	Agent-based technologies	<p>No matter how lightweight, agent-based technologies decrease performance. In the cloud, they increase costs.</p> <p>Organizations may have a restriction on the number of agents that can be installed on each cloud resource. Determine how many security agents are already in place to decide whether a limit increase will be necessary. Any specific overhead allowance for agents should be evaluated during any proof of concept. Consider agentless technology options to preserve resources.</p>
	Near-real-time logging and response	<p>Logging is, or is near, real time. Organizations must determine their communication speeds and requirements.</p> <p>Organizations need to decide whether (near) real-time detection and response is required based on their cloud architecture. Consider data to be logged and storage requirements and location(s).</p>
	Secure communication	As log data is collected by the SIEM and forwarded to SOAR, all communications must be secure, verifiable, immutable and forensically sound.

Operational Considerations

	Consideration	Details
	Operational responsibility and model	<p>Operation of cloud resources is substantially different from the operation of traditional infrastructure, and that may affect who is responsible for implementing and configuring SIEM and SOAR capabilities.</p> <p>Organizations need to decide how best to implement and configure SIEM and SOAR technology, and which group(s) will be responsible for these tasks. Multiple teams may be involved, such as the identity management group, AWS architecture and administration group(s) and SIEM/SOAR admins. Determine whether operations should be centralized or decentralized, on premises or in the cloud.</p>
	Monitoring and response	<p>While implementation and configuration of SIEM and SOAR capabilities may be assigned to an existing cloud operations team, monitoring may be the responsibility of others, and response may be assigned separately.</p> <p>Organizations need to determine who will be responsible for monitoring and responding to endpoint security events. Will it be a centralized group, or does it make sense to separate out certain response functions to existing silos?</p>
	Processes and procedures	<p>Organizations may have specific processes and procedures for dealing with security events related to their traditional on-premises infrastructure. It is likely, however, that these processes and procedures will be different in the cloud.</p> <p>Organizations need to create new operational processes and procedures for SIEM and automated incident response in the cloud.</p>

AWS Implementation Considerations

The general considerations discussed so far can help organizations lay the groundwork as well as secure funding and support for SIEM/SOAR functionality in the cloud. Now let's take a more detailed look at some specific considerations an organization will need to evaluate before implementing these solutions in AWS.

SIEM continues to mature, especially with the addition of analytics that allow for orchestration and automation (SOAR). Along with events and logs needed for SIEM and SOAR functionality normally being fed into Amazon-native tools, threat intelligence is also introduced to the AWS environment. Amazon GuardDuty provides additional monitoring and alerts for known threats. Such native AWS services help provide data for analytics. This analysis then leads to the needed detection of threats based on anomalous behavior known to be common to certain malicious activities.

In the considerations we have already enumerated, an organization can begin to determine budget and resource needs for implementing or enhancing SIEM and SOAR technologies. Let's take a look at considerations specifically related to SIEM and SOAR in the AWS environment.

	Consideration	Details
	Cloud context support	<p>Due to the dynamic nature of the cloud, a resource that existed a few hours ago may not exist right now. Because SOAR technologies perform analysis of data or binaries external to the resource itself, there is a chance that when SOAR analysis is completed, the resource may no longer exist.</p> <p>Evaluate:</p> <ul style="list-style-type: none">• The flexibility for extension of log collections to include context• The additional cloud context (tags or image IDs, for example) that is captured, retained and used by SIEM and SOAR technology to allow correlation of findings and behavior with resources• The special concerns associated with studying resources that have potentially replaced the original resource from which data was gathered• The ability to ensure immutable accuracy with date/time stamps from all sources <p>SIEM technologies typically send data and binaries to separate SOAR systems or to the vendor's cloud infrastructure to perform analysis. Depending on the cloud regions in use, the transfer of data and binaries to different systems could affect technology performance as well as cost.</p>

Consideration	Details
	<p>Bandwidth and latency</p> <p>SIEM technologies typically send data and binaries to separate SOAR systems or to the vendor's cloud infrastructure to perform analysis. Depending on the cloud regions in use, the transfer of data and binaries to different systems could affect technology performance as well as cost.</p> <p>Evaluate:</p> <ul style="list-style-type: none"> • The architecture of the tools under consideration • The amount of data that will be transferred and where the data is being transferred from and to • Potential impacts on cost and performance due to bandwidth • Performance impact of latency between cloud regions and other relevant resources
	<p>Logging sources—general</p> <p>Centralized logging may include events from any or all of the following sources (these logging source lists should not be considered all-inclusive, given that requirements for events to log will vary in different organizations):</p> <ul style="list-style-type: none"> • Host level • Operations • Security • Application • Firewall • DHCP • DNS <p>Evaluate:</p> <ul style="list-style-type: none"> • Which of the systems will be logged, and which events from those systems. This evaluation helps determine the space requirements for logs. • Storage; set up expandable elastic storage in case of a significant incident that fires off a large number of events. • Interfacing options with Amazon CloudWatch • Long-term storage; leverage Amazon S3 Glacier for long-term storage or overflow storage of logs, especially when review of particular logs may seldom be necessary.
	<p>Logging sources—AWS</p> <p>AWS CloudTrail offers logging of AWS-specific logging as well as logging common to any environment.</p> <ul style="list-style-type: none"> • AWS CloudTrail <ul style="list-style-type: none"> – Security logs – Audit logs – VPC flow logs – API calls <p>Evaluate:</p> <ul style="list-style-type: none"> • Regulatory requirements • Retention requirements • Space requirements • Audit requirements • Amazon S3 Glacier for long-term storage or overflow
	<p>Logging sources—endpoints</p> <p>Endpoint tools and systems can feed logs to factor into the SIEM and SOAR, tying events together from servers and workstations with data collected from the host environment, network device, and other sources to provide a robust super-timeline related to incidents. Such timelines can paint a clear picture of the incident from birth to death and help with containment and eradication as well as lessons learned to avoid recurrence in the future.</p> <ul style="list-style-type: none"> • Help desk tools • Asset management systems • Malware • Proxy data <p>Evaluate:</p> <ul style="list-style-type: none"> • Which events will be logged • The ability to manage date/time accuracy with the Network Time Protocol for the environment

	Consideration	Details
	Logging sources—security	<p>Sophisticated security tools, especially those responsible for managing credentials, offer log entries to track such activities in detail. In addition, the origins of threat and vulnerability data, whether open source or commercial, should be factored into the SIEM for review and analysis.</p> <ul style="list-style-type: none"> • Identity management tools • Credential secure storage • Vulnerability data • Threat data <p>Evaluate:</p> <ul style="list-style-type: none"> • Granularity of logging • Reputation of threat and vulnerability data feeds • Multifactor requirements for access to such powerful tools
	Incident response	<p>Incident response (IR) will use the collected logs in the SIEM to determine when an event should be elevated to incident status. Once an incident is established, the IR team must determine an appropriate response. With the addition of SOAR, well-defined incidents can be contained automatically. The remaining incidents must be reviewed manually by some assigned security operations team for working through an established model, such as NIST SP 800-61. (See Figure 2.)</p> <ul style="list-style-type: none"> • Automatic response • Manual response and intervention <p>Evaluate:</p> <ul style="list-style-type: none"> • How much manual response is needed? • What is the skill level needed to handle the manual response issues? • What alerts are based on events that are reliable indicators of incidents upon which action can immediately and automatically take place? • Can those incidents be separated from incidents that require further analysis before action can take place?
	Reporting	<p>Reporting is one of the more important aspects of any SIEM/SOAR implementation. Reports will be used by technicians to help determine how to quickly identify and contain an incident as well as for determining the best strategy for eradication of the incident. Reports also document lessons learned to help eliminate or minimize recurrence. Reporting will have different audiences, all of which need the data communicated in the way most relevant for them. Those working in the areas of management, legal and compliance, for example, tend to have less technical backgrounds, so the approach and the language need to be different than a report intended for a database administrator or a web application programmer.</p> <ul style="list-style-type: none"> • Analytics • Dashboards • Management • Compliance • Legal <p>Evaluate:</p> <ul style="list-style-type: none"> • What are the requirements from management, legal, compliance, security, operations and other teams for necessary reports to assist with evaluation of each area's gaps and to help them complete their tasks? • What report mechanisms and documentation will help pinpoint needed actions? • Are there reports that help with “lessons learned” meetings to reduce repeat occurrences?

Moving SIEM and SOAR to AWS requires the granular evaluation of impact on what needs to be logged. If the information, including context, is not complete enough to be actionable, it is of no use. Speed is also important. Ingestion of events, analysis of events, and alerting or automatic reactions to alerts all need to happen as close to real time as possible. Having all the pertinent data in one location with more-than-adequate CPU cycles,

memory, storage space and bandwidth provides an advantage for response speed and resiliency. The other speed factor has to do with sourcing of the logged information. The sourcing will vary between organizations depending on how they utilize on-premises systems versus cloud systems and the connectivity between the two. AWS offers communication “pipes” through AWS Direct Connect that allow up to 10GB connectivity for getting the data from the organization to the cloud and back. Next, determine the sources providing log feeds to the SIEM. Finally, after analysis, determine what responses can be automated and what kind of alerting and reporting are necessary.



Figure 2. Continuous Integration Process⁷

Making the Choice

To summarize, the key considerations for implementing SIEM and SOAR in AWS include:

- Resources
- Cloud context
- Efficiency
- Ease of use
- Integration requirements
- Availability of built-in tools
- Time to alert and reaction

Have a Plan

Pull together resources from the appropriate teams; management, architecture, operations and information security are all important to the discussion. Determine the desired results from a SIEM system in the environment, then specify the requirements that will provide those results. Separate the “must haves” from the “nice to haves” and share that with the relevant vendors. Don’t forget to discuss the requirements with every

⁷ NIST, Computer Security Incident Handling Guide, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

relevant cloud vendor, such as any off-premises vendors used for HR, legal, change management, security threat and vulnerability management, or any other outsourced functions, in addition to the major cloud providers, such as AWS.

You must make decisions about what events from which systems must be included in the logs collected for analysis. How granular will the collections need to be in order to meet legal, regulatory, contractual and policy requirements? Don't forget to determine what events do not need to be collected, because every additional event collected will have an effect on data storage and a resulting cost.

Lastly, put together a team of subject-matter experts to decide what collection of events is a reliable positive indicator to trigger automatic response. Determine what the response(s) should be and put together a plan to refine and update those as needed on an ongoing basis.

Consider Partners

An organization should consider using CPPO partners who can accelerate integration of SIEM and SOAR into or with the cloud. As already mentioned, using a third-party vendor to manage the implementation provides the benefit of a quicker ROI and helps bring the organization up to speed operationally. Budgeting for adequate training is also crucial. SIEM/SOAR team members can gain some experience while working alongside partners. Consider the plethora of training videos and courses available from SANS and AWS and their partners that can lead to certification of the technical staff who will manage the cloud implementations. Make sure the partners you choose have a strong background in cloud use and/or consulting.

Don't overlook your cloud provider as a potential partner in achieving success as an infrastructure provider consultant. Speak to your chosen cloud provider to understand which SIEM providers work closely with them. Ask which have achieved security competency and thus are recommended by AWS for cloud environments, for example.

Conduct a Proof-of-Concept Test and Evaluate Options for Desired Features

Your choices must provide the results you expect, or get as close as is reasonably possible. The best way to see how close a vendor comes is to perform a proof-of-concept test. Fortunately, when working with the cloud, services and environments can be spun up temporarily for just such testing. Determine the services you need from the AWS Security Hub, for example, and test the capabilities online. Research which services and systems are available for free testing from AWS and take advantage of those options. Your organization needs to know what to expect from the options it chooses and determine whether those results will add value.

Conclusion

Back to our underground lab full of techies staring at multiple screens: With an adequately funded and implemented analytical SIEM system, supplemented by orchestration and automation (SOAR), security personnel will be spending less time hunting for evil and more time remediating the issues that cause the alerts. In an ideal world, many lower-level incidents will be handled automatically, freeing up personnel to address the more challenging issues that often present greater risk.

With SIEM and SOAR in the AWS cloud, the data center resource needs are handled by AWS. The hardware and everything needed to keep it running are no longer a concern for the organization, freeing up personnel and financial resources for other needs.

To get there, many decisions must be made. See Figure 3 for questions to address.

This paper provides talking points and direction for an organization that wants to move down a decision path. Hopefully, these choices will lead to a quicker implementation of the tools that fit best and provide the best return on investment.

Through this evaluation process, look at the features and functionality available from AWS. Many aspects of SIEM collection, analysis and SOAR implementation are already baked into the AWS environment. Careful consideration should be given to the cost delta between leveraging the features and functionality (including AWS partner options) in AWS, as compared to the local data center and its resources.

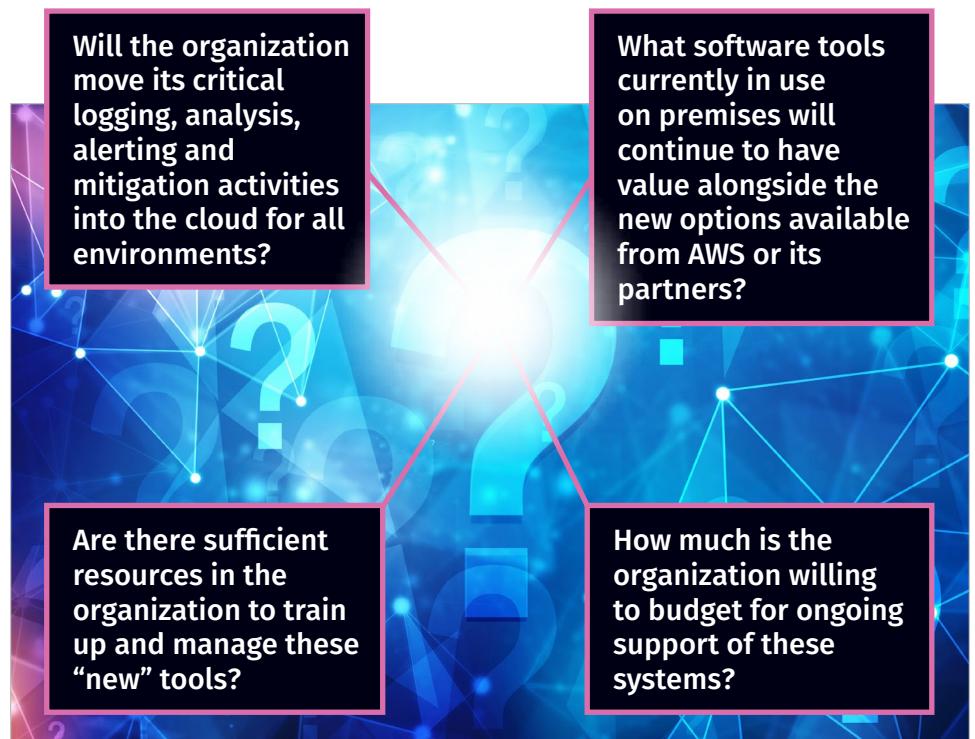


Figure 3. Questions for Cloud vs. On-Premises

About the Author

J. Michael Butler is a SANS analyst who has also written SANS security training courseware and audited certification test questions; presents thought-provoking webcasts; and writes position papers, articles and blogs. He is an information security consultant with a leading provider of technical services for the mortgage industry, where he is involved in migration of assets to the cloud. Mike's responsibilities have included computer forensics, incident response, enterprise security incident management planning, internal auditing of information systems and infrastructure, information security policies, service delivery and distributed systems support. He holds the GCFA, GCIH, CISA, GSEC and EnCE certifications.

Sponsor

SANS would like to thank this paper's sponsor:



in conjunction with



About Optiv

Optiv is a market-leading provider of end-to-end cybersecurity solutions. Optiv helps clients plan, build and run successful cybersecurity programs that achieve business objectives through our depth and breadth of cybersecurity offerings, extensive capabilities and proven expertise in cybersecurity strategy, managed security services, incident response, risk and compliance, security consulting, training and support, integration and architecture services, and security technology. Optiv maintains premium partnerships with more than 350 of the leading security technology manufacturers.

RETURN TO THE
TABLE OF CONTENTS



How to Build a Threat Detection Strategy in AWS

Written by **David Szili**

August 2019

Sponsored by:

AWS Marketplace

Webcast

You can access the associated webcast at:
<https://pages.awscloud.com/threat-detection.html>

Introduction

One major concern security teams have is losing visibility and detection capabilities when their organization moves to a cloud. While this might have been true in the early days of cloud services, these days providers are announcing new threat detection features and offerings almost every month. These new services open up the possibility of adjusting traditional network- and host-based monitoring to support intrusion detection in the cloud.

In this paper, we focus on the key steps illustrated in Figure 1 to detect threats in Amazon Web Services (AWS) and gradually build a security monitoring strategy.

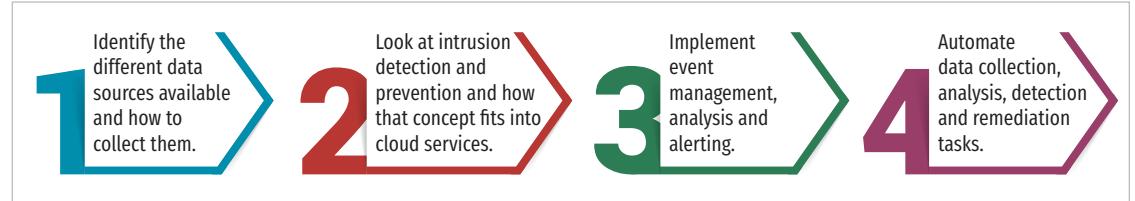


Figure 1. Steps to Build a Security Monitoring Strategy

Threat detection and continuous security monitoring in cloud environments have to integrate security monitoring of instances and images (system monitoring), just as they do on premises. For cloud services, however, it is also crucial to include the monitoring of the cloud network infrastructure and cloud management plane (cloud monitoring).

In terms of system monitoring, organizations must collect system logs and vulnerability scan results. They must also check the integrity and compliance of instances against policies and security baselines. The collection of operating system logs can be challenging because they require centralized collection for analysis and correlation. Given the volume of this data and the associated cost of sending it back to an on-premises solution, using an in-cloud log collector or event management platform can be a much more viable option.

As for the AWS Cloud environment, security teams must monitor admin access, changes made to the environment, API calls, storage and database access, and any access to sensitive and critical components. In the following sections, we explore data sources and services that help with event management and analysis.

The focal point of the threat detection strategy is to collect data from systems, networks and the cloud environment in a central platform for analysis and alerting. AWS Security Hub¹ is a service that automates the collection process and organizes and prioritizes security alerts into a single, comprehensive view. The data sources, services and solutions described in this paper all feed into this monitoring solution to provide visibility and detect threats.

¹ Because this paper is an exploration of threat detection in AWS, it is important to talk about the tools available. The use of these examples is not an endorsement of any product or service.

Data Collection

The first step in creating a security monitoring strategy is to identify the available data sources and determine how to collect data from them. Key data sources include endpoint detection and response (EDR) tools, flow logs, data from intrusion detection and prevention tools, and alerts from Amazon GuardDuty (discussed in the “Event Management and Analysis” section) and other AWS tools. When considering data collection for security monitoring, the winning strategy is to focus on the data sources with the highest value and the best cost–benefit ratio—and to do so efficiently. AWS Security Hub simplifies data collection from a variety of sources and collects alerts into a single, comprehensive view, as described in the “Event Management and Analysis” section.

In the case of AWS, these are Amazon VPC Flow Logs and AWS CloudTrail logs. Amazon VPC Flow Logs provide visibility into VPC and instances network traffic. Flow records are small and have a fixed size, making them highly scalable, with longer retention times, even for large organizations. AWS CloudTrail provides the logs for monitoring the AWS Cloud environment itself. We examine these two data sources next.

Focus on the data sources with the highest value and the best cost–benefit ratio—and do so efficiently.

Flow Logs

Flow records, such as NetFlow or IPFIX, are a statistical summary of the traffic observed. Common attributes allow grouping of packets into a flow record. These attributes are the source and destination IP addresses, the source and destination ports, and the network protocol (usually TCP, UDP or ICMP). As a result of this summary nature of the flow records, they do not contain information about the application layer. Therefore, visibility is limited to Layer 4 and below. Flow logs still offer means to:

- Scope a compromise and identify communication with known attacker addresses.
- Identify large flow spikes that might suggest data exfiltration.
- Identify large counts of frequent, small traffic bursts that may be command and control traffic.
- Detect strange patterns of access and behavior.

Because a significant portion of today’s network traffic is encrypted and application data is unavailable for analysts, the lack of Layer 7 information in flow records is of little concern. Flow analysis techniques work exactly the same for both encrypted and unencrypted communications. This makes flow analysis a great method for threat hunting without the need for SSL/TLS interception and full-packet capture.

The Amazon VPC Flow Logs feature enables security analysts to capture information about the IP traffic going to and from network interfaces in the VPC. Flow logs can be sent to Amazon CloudWatch or Amazon S3 buckets. A new log stream is created for each monitored network interface.

Amazon VPC Flow Logs records are space-separated strings. Similar to other flow records, such as NetFlow or IPFIX, they contain the network interface name, source and destination IP addresses and ports, number of packets, number of bytes, and the start and end times of the traffic flow. One significant difference is that the flow record contains information on whether the security groups or network access controls lists (NACLs) permitted or rejected the traffic. The list of fields are as follows:

```
<version> <account-id> <interface-id> <srcaddr> <dstaddr> <srcport> <dstport> <protocol> <packets>
<bytes> <start> <end> <action> <log-status>
```

The following flow record example is for NTP traffic (destination port 123, UDP protocol) that was allowed:

```
2 123456789010 eni-abc123deabc123def 172.31.32.81 172.31.16.139 59808 123 17 1 76 1563100613
1563100667 ACCEPT OK
```

This flow record example is for RDP traffic (destination port 3389, TCP protocol), which was rejected:

```
2 123456789010 eni-abc123deabc123def 172.31.9.69 172.31.32.81 44844 3389 6 20 4249 1563100613
1563100667 REJECT OK
```

Because VPC Flow Logs can produce a large quantity of event data, you will likely need a tool, such as a log aggregator and analytics platform or a SIEM solution, for monitoring and analysis (see the next section). For example, Amazon CloudWatch has a simple interface to search in log group events, but also has Amazon CloudWatch Logs Insights, which provides a powerful, purpose-built query language that can be used to search and analyze your logs. It is ideal for threat hunting and allows security analysts to use the techniques mentioned previously.

Amazon CloudWatch Log Insights has prebuilt sample queries for VPC flow logs, making it easy to get familiar with the query language and perform the analysis. These sample queries include cases like:

- Average, minimum and maximum byte transfers by source and destination IP addresses
- Top 10 byte transfers by source and destination IP addresses
- Top 20 source IP addresses with the highest number of rejected requests

Security analysts must be aware that Amazon VPC Flow Logs exclude certain IP traffic such as Amazon DNS activity, DHCP or license activation. This is usually desired to avoid the duplication of information, for example, in the case of VPC mirrored traffic. In other cases, additional AWS solutions can fill in these gaps. For example, Amazon GuardDuty also monitors DNS traffic.

Amazon VPC Flow Logs is an essential tool to leverage and should be collected in every VPC that has important assets.

API and Account Activity Logs

Cloud security also requires detailed visibility into user and resource activity. Actions that take place through the AWS Management Console, command-line tools or API services are just as important for preserving the integrity of cloud environments as they are for monitoring network activity and hunting for threats. This kind of event history helps in troubleshooting, change tracking and security analysis. The events should contain detailed information, including but not limited to:

- Time of the API call
- Identity of the API caller
- Source IP address of the API caller
- Request and response parameters

One of the first major additions to Amazon's security services was AWS CloudTrail, an AWS logging service that provides a history of any AWS API calls across accounts and Regions. AWS CloudTrail is enabled on your AWS account when you create it. From the AWS CloudTrail console, you can view, filter and download the most recent 90 days of events in CSV or JSON formats. You can also see the resources referenced by an event and pivot to AWS Config to view the resource timeline.

You can configure AWS CloudTrail trails to log management events and data events. Management events provide insight into management operations that are performed on resources in your AWS account. Examples include configuring security policies, registering devices and setting up logging. You can choose to log read-only, write-only, all, or no management events. Data events provide insight into the resource operations performed on or within a resource—for example, Amazon S3 object-level API activity or AWS Lambda function execution activity. To determine whether an AWS CloudTrail log file was modified, deleted or unchanged after it was delivered, you can enable log file validation.

AWS CloudTrail typically delivers log files within 15 minutes of account activity, and it publishes log files multiple times an hour, about every five minutes. The events are in JSON format, which makes them humanly readable and easy to parse programmatically.

The log entry in Figure 2 on the next page shows that a root user

(`“userIdentity”: { “type”: “Root”}`) successfully signed into the AWS Management Console (`“eventName”: “ConsoleLogin”`) using multifactor authentication (`“MFAUsed”: “Yes”`):

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "Root",
    "principalId": "123456789010",
    "arn": "arn:aws:iam::123456789010:root",
    "accountId": "123456789010",
    "accessKeyId": ""
  },
  "eventTime": "2019-07-01T10:48:13Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "ConsoleLogin",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "1.2.3.4",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0",
  "requestParameters": null,
  "responseElements": {
    "ConsoleLogin": "Success"
  },
  "additionalEventData": {
    "LoginTo": "https://console.aws.amazon.com/console/home?state=hashArgs%23&isauthcode=true",
    "MobileVersion": "No",
    "MFAUsed": "Yes"
  },
  "eventID": "3fcfb582-bc34-4c39-b021-10a394ab61cb",
  "eventType": "AwsConsoleSignIn",
  "recipientAccountId": "123456789010"
}
```

The event history feature allows you to perform simple queries and filter events in many ways, except for wildcard searches. You can use Amazon Athena for more in-depth analysis using standard SQL to interactively query the AWS CloudTrail log files delivered to the Amazon S3 bucket for that trail.

Figure 2. AWS CloudTrail Event Example

For an ongoing record of activity and events in AWS accounts, you have to create a trail and send events to an Amazon S3 bucket or Amazon CloudWatch Logs. Log data can be automatically deleted, or it can be archived to long-term storage, for example, in Amazon S3 Glacier.

AWS CloudTrail provides exceptionally detailed visibility for AWS account activity, which is a key aspect of security and operational monitoring best practices.

Intrusion Detection and Prevention Systems

The second step in creating a security monitoring strategy is to determine how IDS/IPS fit into that strategy. Such systems have the same objectives in the cloud as on premises, such as alerting based on signature matching, behavioral anomalies and protocol mismatch. However, these solutions differ from the ones we have on premises, and because they must be adapted to the cloud environment, they might look less familiar at first. In a cloud environment such as AWS, you have control over your virtual machine instances and to your VPCs at some level, but not the physical network or the hypervisor platform (which includes components like virtual switches). The cloud service provider controls these lower layers; therefore, monitoring tools have to leverage the features provided by the upper layers.

Network IDS/IPS

On-premises network IDS/IPS (NIDS/NIPS) differs somewhat from cloud deployments. However, AWS offers additional features that enable network security monitoring. Hardware network taps or mirror ports (also known as SPAN ports) from hardware and virtual switches are not feasible because of the lack of Layer 2 access, but similar alternatives are available using agents or traffic mirroring. Security appliances that can be deployed in-line for monitoring or blocking can also be implemented in AWS.

One option is to send back all the traffic to on-premises sensors via a dedicated connection like AWS Direct Connect or through a VPN. This allows you to see traffic coming in to and out of the VPC, although on-premises sensors cannot see instance-to-instance traffic. Nonetheless, this model can be combined with the methods mentioned below for better coverage.

The other option is a do-it-yourself approach: using NAT instances or multihomed instances with multiple elastic network interfaces (ENIs) that can act as gateways and inspect traffic passing through them. This option results in more complex network design, extra configuration steps like the installation of NIDS/NIPS software or Linux traffic bridging, and additional resources to manage the platform, because there is usually no official support. Different instance types have a maximum number of network interfaces, and smaller instances typically only allow two.

A great alternative to the preceding approach is to use AWS Partner Network (APN) solutions from AWS Marketplace, which has major vendors like F5 Networks, Palo Alto Networks, Sophos and Check Point Software Technologies. Most NIDS/NIPS features could be handled by unified threat management (UTM) and next-generation firewall (NGFW) appliances from firewall vendors. These virtual appliances are also deployed in-line as gateway devices (requires customized routing, VPC peering) in order to observe and manage traffic traversing the cloud environment, and they can have multiple ENIs to tap into multiple subnets.

Traffic Mirroring

Traffic mirroring in the cloud used to be challenging, requiring the installation and management of third-party agents on Amazon EC2 instances to capture and mirror EC2 instance traffic. One such platform is Gigamon's GigaVUE CloudSuite for AWS, which acquires, optimizes and distributes selected traffic to security and monitoring tools by performing traffic acquisition using G-vTAP agents.

Amazon VPC Traffic Mirroring addresses these challenges and enables customers to natively replicate their network traffic without having to install and run packet-forwarding agents on Amazon EC2 instances. Amazon VPC Traffic Mirroring captures packets at the ENI level, which cannot be tampered with from the user space, thus offering better security. It also supports traffic filtering and packet truncation, allowing selective monitoring of network traffic. AWS Marketplace already has monitoring

solutions integrated with Amazon VPC Traffic Mirroring, such as ExtraHop Reveal(x) Cloud.

The main elements of VPC traffic mirroring are:

- **Mirror source**—An AWS network resource (ENI) in a VPC
- **Mirror target**—An ENI or network load balancer that is the destination for the mirrored traffic
- **Mirror filter**—A set of rules that defines the traffic that is copied in a traffic mirror session
- **Mirror session**—An entity that describes traffic mirroring from a source to a target using filters

The mirror target can be in the same AWS account as the mirror source or in a cross-account AWS environment, capturing traffic from VPCs spread across many AWS accounts and then routing it to a central VPC for inspection. The filter can specify protocol, source and destination port ranges, and classless inter-domain routing (CIDR) blocks for the source and destination. Rules are numbered and processed in order within the scope of a particular mirror session. Sessions are also numbered and evaluated in order. The first match (accept or reject) determines the fate of the packet, because a given packet is sent to at most one target.

Be aware that VPC traffic mirroring is unlike a traditional network tap or mirror port. Mirrored traffic is encapsulated with a VXLAN header and then routed by using the VPC route table. VXLAN traffic (UDP port 4789) must be allowed from the traffic mirror source in the security groups that are associated with the traffic mirror target. Applications that receive the mirrored traffic should be able to parse these VXLAN-encapsulated packets.

Amazon VPC Traffic Mirroring is a game-changer that opens up the possibility of bringing traditional network security monitoring solutions into the AWS environment.

Host-Based IDS/IPS

On the other side of IDS/IPS are host-based IDS/IPS (HIDS/HIPS) and anti-malware solutions. The good news is that these tools can be installed on cloud virtual machines in the same way as on premises. Note, however, that most traditional HIDS/HIPS agents require more resources, which usually comes with a performance impact on the instances.

Host security monitoring also tends to be more complex to manage. Sensors/agents must be deployed so that they can report back to a management server for analysis. Security teams must take care of event management and log collection and consider network bandwidth to decide whether they want to send the events back to on-premises systems, another virtual machine instance in AWS or maybe to another (SaaS) cloud service. Every time a new instance gets brought up or terminated, the security team must make sure the sensor/agent has to be deployed or decommissioned properly.

Fortunately, there are more cloud-focused, integrated HIDS/HIPS and anti-malware marketplace offerings, such as Trend Micro Deep Security, CloudPassage and Dome9 (now part of Check Point), that can be distributed at the hypervisor layer. Next-generation antivirus (NGAV) and EDR tools like Carbon Black or CrowdStrike have also moved to a SaaS model to support cloud deployments.

Event Management and Analysis

After identifying the most important data sources, collecting data from them and deploying security sensors, we need the means to manage the data collected. Event management and monitoring in a cloud environment consist of activities like scanning for vulnerabilities, event monitoring, alerting, correlation and analysis.

Many security analysts are aware of Amazon CloudWatch, a monitoring and management service available within AWS. Amazon CloudWatch is a highly flexible, general-purpose tool that is not only meant for security, but also to get a unified view of operational health by monitor applications, resource utilization or systemwide performance changes.

Amazon CloudWatch basically functions as a repository for logs and metrics. AWS services put metrics into the repository, and statistics can be calculated based on those metrics. This statistical data can then be displayed graphically with visualizations (graphs) and dashboards. There are many default metrics available, and custom metrics can be defined too.

Amazon CloudWatch can take logs from Amazon EC2 instances (CPU, memory, network usage, etc.) every five minutes (basic monitoring) or every minute (detailed monitoring), and it has agents that can be installed on instances to send their operating system logs. Amazon CloudWatch Logs can also be used to store and analyze logs from AWS CloudTrail and Amazon VPC Flow Logs. These log entries can be filtered into metrics to define alarms.

The most significant benefit of Amazon CloudWatch is that it is very well integrated with almost every other AWS service, including AWS Security Hub. You can create alarms and periodic events and send them to other tools (for example, AWS Lambda or Amazon Simple Notification Service [Amazon SNS]), and make automatic changes to the resources you are monitoring when a threshold is reached.

AWS Security Hub consumes data from services like AWS Config, Amazon GuardDuty, Amazon Inspector and Amazon Macie, and from supported APN Partner Solutions. AWS Security Hub reduces the effort of collecting all this information. It provides a single, comprehensive view that aggregates, organizes and prioritizes security alerts using a consistent findings format. These findings are displayed on dashboards with actionable graphs and tables.

Putting It All Together

AWS offers various services and access to security, identity and compliance tools from AWS partners. These include firewalls, network or endpoint IDS/IPS applications, and vulnerability and compliance scanners. Because they can easily generate thousands of security events and alerts every day, all in different formats and stored across different platforms, a unified interface is needed for management. Figure 3 illustrates what that unified interface should include.

Amazon GuardDuty is an AWS threat detection service that continuously monitors for malicious activity



and unauthorized behavior. The analysis is based on threat intelligence feeds (such as lists of malicious IPs, domains, URLs from Amazon GuardDuty partners) and machine learning to identify unexpected, potentially unauthorized and malicious activity.

Amazon GuardDuty combines, analyzes and processes the following data sources:

- **AWS CloudTrail event logs**—Monitors all access and behavior of AWS accounts and infrastructure
- **Amazon VPC Flow Logs and DNS logs**—Identifies malicious, unauthorized or unexpected behavior in AWS accounts and infrastructure

It is important to note that Amazon GuardDuty was not designed to manage logs or make them accessible in your account. It is built for AWS workloads and AWS data, and is not intended to support data from on-premises or other services. For example, in the case of DNS logs, Amazon GuardDuty can access and process DNS logs through the internal AWS DNS resolvers, but not from third-party DNS resolvers. After it receives the logs, it extracts various fields from these logs for profiling and anomaly detection, and then discards the logs. It is important to collect and store your flow and API logs, as discussed in the “Data Collection” section, in order to retain them for investigations.

The produced security findings (potential security issues) can be viewed in the console, retrieved via an HTTPS API. Alternatively, Amazon GuardDuty can create Amazon CloudWatch Events that can be sent to a SIEM platform, or automated remediation actions can be performed by using AWS Lambda.

Security findings are assigned a severity level of high, medium, or low. These findings are detailed and include information about the affected resource as well as attacker IP address, ASN and IP address geolocation. Amazon GuardDuty has various finding types that cover the entire attacker life cycle, such as reconnaissance, unauthorized access, privilege escalation and persistence.

By importing these findings into AWS Security Hub, you can filter and archive results and create a collection of findings, called “insights,” that are grouped. Insights help to identify common security issues that may require remediation action. AWS Security Hub includes several managed insights by default, but you can create custom insights too. These findings are displayed on dashboards with actionable graphs and tables.

Figure 3. Unified Interface for Management of Events and Alerts

AWS Security Hub also generates its own findings by running automated, continuous configuration and compliance checks based on industry standards and best practices from the Center for Internet Security (CIS) AWS Foundations Benchmark, which is enabled by default. These checks provide a compliance score and identify specific accounts or resources that require attention.

To take advantage of the benefits AWS Security Hub provides, you have to enable and configure the settings of these data sources through their respective consoles or APIs. AWS Security Hub also integrates with AWS CloudTrail, which captures API calls for AWS Security Hub as events.

Organizations may need to use additional third-party tools to integrate with existing tools, to meet compliance requirements or simply to leverage additional features. AWS partners have several cloud-focused event management platforms available. Sumo Logic is a cloud-native data analytics platform, not only for security, but also for operations and business usage. Sumo Logic offers SIEM functionality and machine learning analytics to create baselines and perform anomaly-based detection. Splunk Technology also has several tools for cloud event management, such as Splunk Cloud for security and operational visibility. Open source analytics and monitoring hosted offerings like Amazon Elasticsearch Service on Elastic Cloud and Grafana are also available in AWS Marketplace. Alternatively, Amazon Elasticsearch Service offers Elasticsearch, managed Kibana and integrations with Logstash and other AWS Services.

Automation

The final step in the threat detection strategy is to bring in tools to automate response and remediation after the detection of a threat or vulnerability. This model has three major components:

- **Collecting and monitoring for events** occurring in the environment using AWS CloudTrail logs, Amazon VPC Flow Logs and Amazon VPC Traffic Mirroring. Automated assessment services such as Amazon Inspector, CloudPassage Halo or AWS Config can collect security audit results.
- **Triggering alerts** based on specific patterns and anomalies by relying on Amazon CloudWatch alarms, Amazon GuardDuty findings or alerts from third-party SIEMs. Amazon SNS can be used together with Amazon CloudWatch to send messages when an alarm threshold is reached.
- **Taking action** and starting an automated reaction with tools like AWS Lambda. AWS services such as Amazon CloudWatch or Amazon GuardDuty can automatically trigger AWS Lambda code to perform actions. AWS Systems Manager also has the capability to run automation workflows with triggers using AWS Systems Manager State Manager. Security teams can also take advantage of security orchestration, automation and response (SOAR) platforms like Splunk Phantom or Palo Alto Demisto.

Now, in the next section, we bring together all the steps in building a threat detection strategy.

Security Monitoring Best Practices in AWS

A security team that takes into consideration the recommendations of the previous sections and makes the time investment to fit together the different detection components is able to use cloud-native services and define automated detection and remediation workflows. By reducing the amount of manual labor in the team, the team has more time to focus on other areas of information security.

AWS Security Monitoring Best Practices

Some of the most important security monitoring recommendations for the team include:

- Turn on AWS CloudTrail logging in every Region and integrate it with Amazon CloudWatch Logs. Ensure that log file validation is enabled and that logs are encrypted using AWS Key Management Service (KMS).
- Turn on Amazon VPC Flow Logs for every VPC, or at least for the ones with critical assets.
- Leverage Amazon S3 bucket versioning for secure retention and use Object Lock to block object version deletion. Create Write-Once-Read-Many Archive Storage with Amazon S3 Glacier for long-term storage.
- Aggregate AWS CloudTrail log files from multiple accounts to a single bucket. It is a good security practice to set up a separate account and replicate logs to that account, so logs cannot be deleted for a particular account.
- Monitor events and set up Amazon CloudWatch alarms for:
 - User and identity and access management (IAM) activity, especially login events and admin user activity
 - Resource creation events
 - Failed access to resources
 - Policy and configuration changes
 - VPC configuration changes related to security groups, NACs, network gateways, route tables, etc.
 - Billing alarms
 - API calls such as storage attribute changes, unauthorized calls and AWS Lambda events
 - Activity in unusual Regions and at unusual time frames

By reducing the amount of manual labor in the team, the team has more time to focus on other areas of information security.

The CIS has benchmarks on AWS monitoring and logging, offering basic but sound recommendations that anyone can implement and use as a starting point:

- The **CIS Amazon Web Services Foundations** document provides guidance for configuring security options for a subset of AWS.
- **CIS Amazon Web Services Three-tier Web** provides guidance for establishing a secure operational posture for a three-tier web architecture deployed to the AWS environment.

The Process

This process has to start with data collection. The security team must set up AWS API and user activity logging with AWS CloudTrail. These logs are the team's sources for the metrics and triggers it identifies for the Amazon CloudWatch alarms. This already makes the team capable of responding automatically to events such as resource changes, for example, when someone tries to disable AWS CloudTrail logging or log in with an AWS account root user at unexpected times from an unexpected location. These can be simple rules to indicate the events of interest and the automated actions to take when an event matches a rule. The actions that can be triggered include but are not limited to:

- Invoking an AWS Lambda function
- Invoking Amazon EC2 Run Command
- Notifying an Amazon SNS topic

To monitor network traffic and packet flows in its VPCs, the team will rely on Amazon VPC Flow Logs and configure Amazon VPC Traffic Mirroring to send traffic from instances to network security sensors. Depending on the skill set of the security team members, the team might choose to use open source tools for its NIDS/NIPS and HIDS/HIPS needs, or deploy APN partner AMIs like NGFW/UTM appliances across their VPCs.

If the security team wants to go one step further, it can enable AWS-built services like AWS Trusted Advisor, AWS Config, Amazon Inspector and Amazon GuardDuty. These are designed to exchange data and interact with other core AWS services, to identify potential security findings and raise alarms.

AWS Security Hub or an APN partner event management service could allow the team to enable, configure and connect APN partner tools and review findings in one central location. AWS Security Hub can also automatically send all findings to Amazon CloudWatch Events. After an Amazon CloudWatch Event is sent or a finding notification is posted to an SNS topic, an AWS Lambda function can be triggered, and services like AWS Systems Manager can be used from within the AWS Lambda function to perform automatic remediation on the instance.

Conclusion

By relying on the most common data sources, organizations can build a powerful threat detection strategy and gradually improve their monitoring capabilities. The focus should be on the data types that can provide the highest value and not only cover network and system monitoring but also have the information needed for cloud environment monitoring. Advancements in monitoring, such as Amazon VPC Traffic Mirroring, can be the means of adapting traditional security monitoring techniques to the cloud.

Collecting the data is just one half of the equation. Without analysis and event management, data collection does not provide any value. Analysts can detect suspicious or malicious events during a manual threat hunting process or alerts could be triggered based on predefined conditions, rules or machine learning. Combining the different cloud-native services and features available can also help in detecting threats.

The ultimate goal is to take advantage of automation tools that can serve as a force multiplier and assist security teams immensely in incident response and vulnerability remediation by automating the most common tasks.

About the Author

David Szili is a SANS instructor for [SANS FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response](#). A managing partner and CTO at a Luxembourg-based consulting company, he has more than eight years of professional experience in penetration testing, red teaming, vulnerability assessment, vulnerability management, security monitoring, security architecture design, incident response, digital forensics and software development. David holds several IT security certifications, including the GSEC, GCFE, GCED, GCIA, GCIH, GMON, GNFA, GYPC, GMOB, OSCP, OSWP and CEH. He is also a member of the BSides Luxembourg conference organizing team.

Sponsor

SANS would like to thank this paper's sponsor:



RETURN TO THE
TABLE OF CONTENTS

Next Steps

By applying the guidelines in the preceding whitepapers, you have been able to:

- Justify the need for SIEM and SOAR products to reduce time to detect and time to respond
- Understand the different types of relevant security data and the analysis capabilities required to turn that data into meaningful security alerts
- Document the key considerations that drive the overall monitoring and response architecture and drive SIEM product and service selection
- Deploy an integrated threat detection and response architecture

Using these guidelines, the key next steps are to perform a gap assessment of both the completeness of your visibility and your team's real ability to capture, normalize, reduce and analyze the collected data. Not all gaps require new or more security products. There are often gaps in visibility and analysis processes that can be closed programmatically or by taking advantage of capabilities of existing security tools or capabilities of the cloud infrastructure. Additional staff may not be required either. Automation tools backed by training to "upskill" existing personnel can often close that gap.

With purely on-premises-based security controls, the relative ease of monitoring and collecting security-relevant data has often been impacted by the cost and complexity of managing and analyzing the flood of data. The elasticity of cloud-based processing provides the tools and capabilities for overcoming those barriers and turning that flood of data into meaningful chunks of information to support rapid detection and mitigation of threats. The key to taking advantage of those cloud-based capabilities is a skilled staff augmented by force multipliers such as SIEM and SOAR products.

[RETURN TO THE
TABLE OF CONTENTS](#)