aws marketplace

SANS

Building a Security Visibility Strategy for the AWS Cloud

How to broaden security visibility with AWS services and software solutions in AWS Marketplace.

AWS Marketplace Introduction

In the following whitepaper SANS instructor, Dave Shackleford, will explain how visibility in the cloud differs from more traditional security visibility. He will suggest how organizations can move toward establishing a cloud visibility strategy, using practical examples to illustrate the process. You will learn how to gain insight into the events and behaviors that move into and through your cloud environment—across networking, systems, storage, and applications. This will enable you to determine who did what, and when, in key visibility security scenarios.

Building on Dave's perspective, AWS Marketplace will then describe how security teams can leverage AWS Security Hub and complementary solutions in AWS Marketplace, a digital catalog of software products designed to run on AWS, to support their security visibility strategy. This includes an introduction to Splunk and their security solutions that can enhance visibility.

The featured Splunk solutions for this use case can be accessed in AWS Marketplace:

Splunk Cloud
Splunk Enterprise
Splunk Phantom

SANS

A SANS Whitepaper

How to Build a Security Visibility Strategy in the Cloud

Written by **Dave Shackleford**

March 2019

Sponsored by:

AWS Marketplace

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 CloudTrail[1] 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).

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

- **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 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.

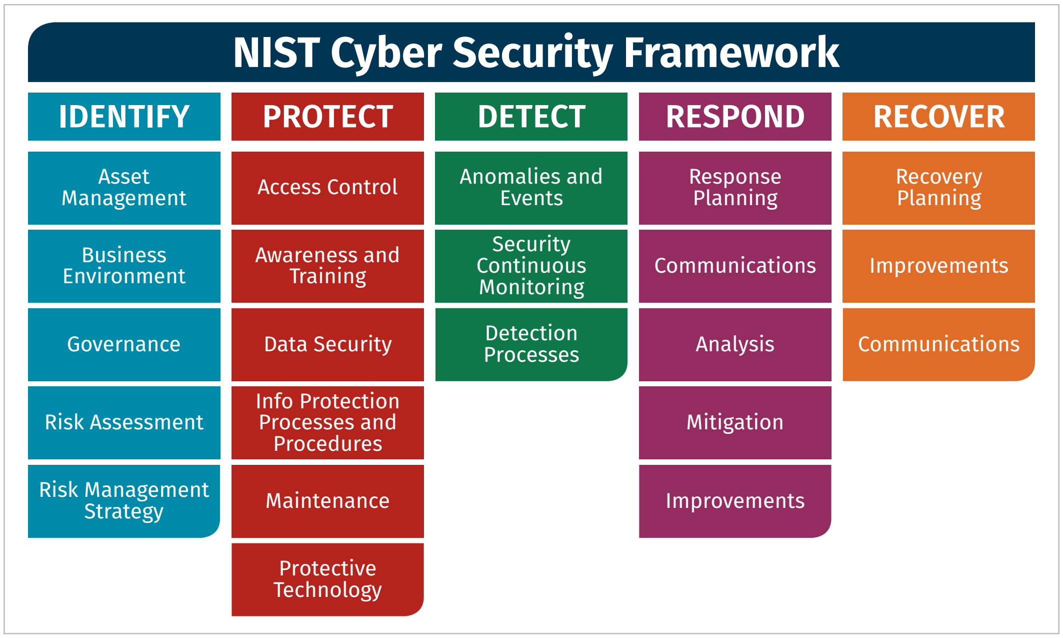
Security Visibility Today

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 Controls[2] 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 on the next page.

[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.

[2] www.cisecurity.org/controls

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:



NIST Cyber Security Framework

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Figure 1. The NIST Cyber Security Framework[3]

- **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.
- **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. Developing true application visibility often relies on feeding events into event management and SIEM platforms, which have also been well adapted into cloud environments, often via API integration.
- **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.

[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

- **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!

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.

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."

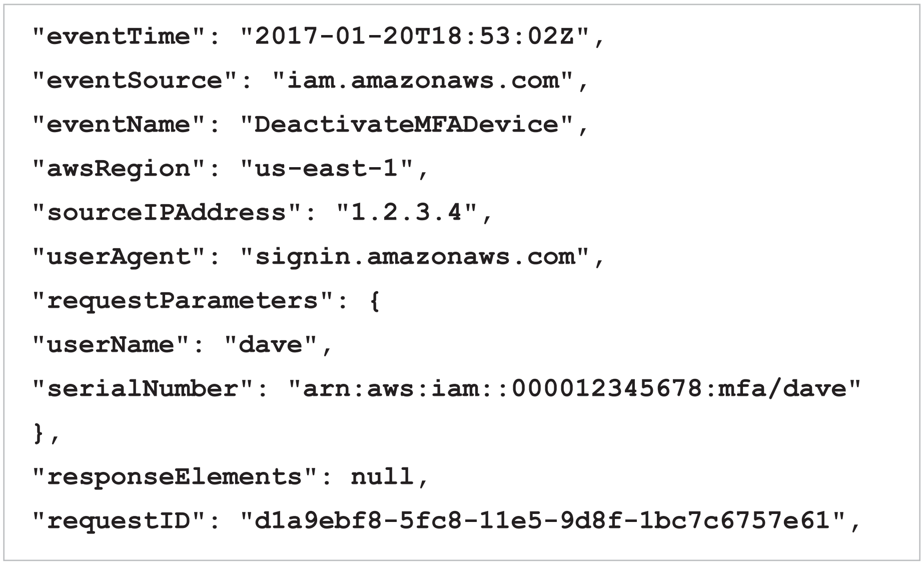
Today, this statement is blatantly false, because major infrastructure-as-a-service (IaaS) providers have enabled extensive logging of all activity within the environment, essentially recording every API call made in any way.

"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.

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.



```
"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

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 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:

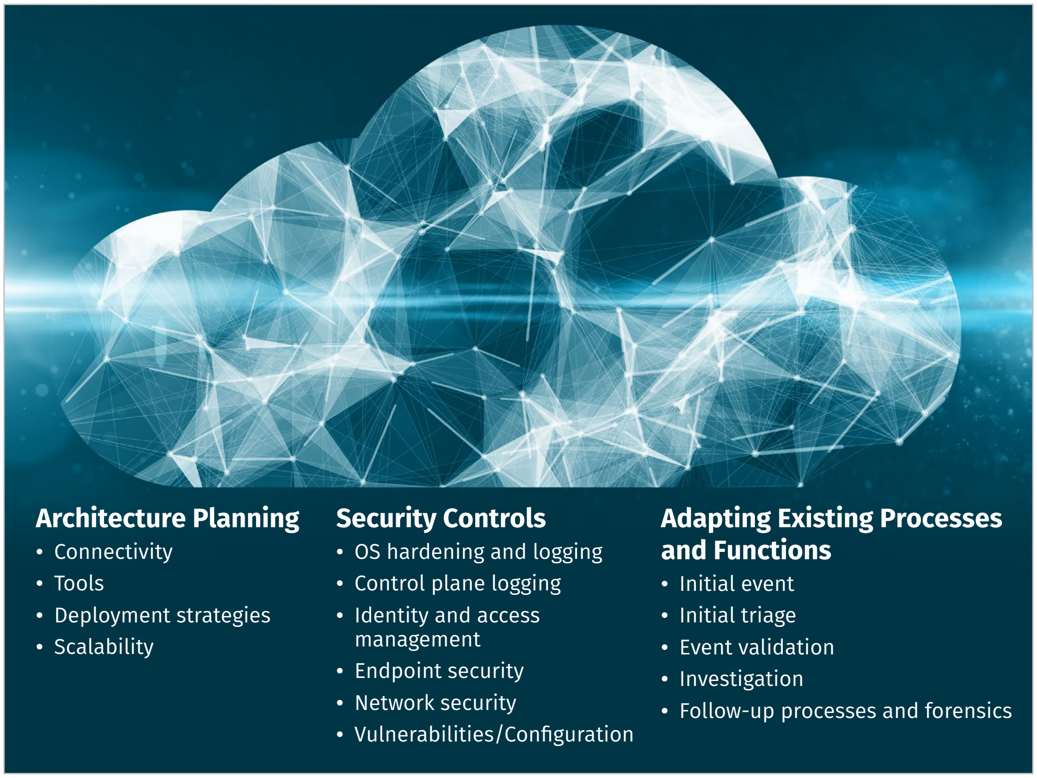
1. Be sure to investigate third-party options from vendors and service providers that can enhance and augment your monitoring and visibility strategy.
2. Before considering the latest cloud-native tools and capabilities from cloud providers, consider the critical factors that may dictate when you should 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.

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
- Connectivity
- Tools
- Deployment strategies
- Scalability

Security Controls
- OS hardening and logging
- Control plane logging
- Identity and access management
- Endpoint security
- Network security
- Vulnerabilities/Configuration

Adapting Existing Processes and Functions
- Initial event
- Initial triage
- Event validation
- Investigation
- Follow-up processes and forensics

Figure 3. Planning Steps for a Cloud-Aware SOC

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).

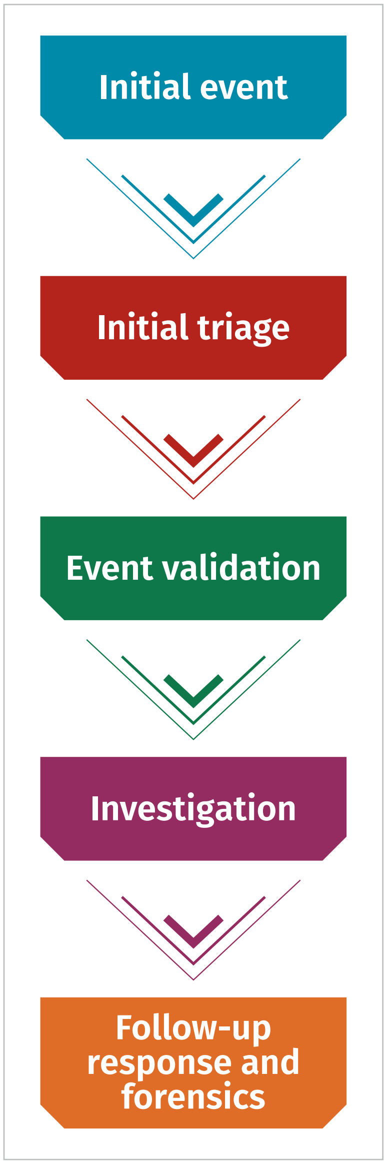


Figure 4. Process for Adapting Processes and Functions

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.

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:

aws marketplace

aws marketplace

How to better align to your security visibility strategy in AWS

As new assets and resources are created or changed in an Amazon Web Services (AWS) environment, the APIs and software used to perform these actions can also provide a detailed audit trail of events for analysis. Many AWS services have the ability to log events, as well as metrics, to inform behavioral insights across a breadth of log data, which can be used by security teams to establish or strengthen their security visibility strategy.

However, since these services can collectively produce terabytes of log data, it's crucial to know how to determine what is relevant for deeper analysis and, if needed, action. AWS Security Hub can help security teams achieve this by aggregating, organizing, and prioritizing security alerts or findings from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, and Amazon Macie, as well as from software seller solutions.

Establish and enhance your security visibility with AWS Security Hub and software seller integrations

AWS Security Hub brings together a breadth of logs, security alerts, and other data from multiple AWS accounts, parsing and normalizing data from disparate formats. This enables security teams to continuously monitor their environment using automated compliance checks based on the AWS best practices and industry standards their organizations follow. From there, security teams can easily take action by triggering ticketing, chat, email, or auto-remediation via integration with Amazon CloudWatch events and AWS Lambda.

For organizations moving new workloads to AWS, AWS Security Hub addresses four key challenges:

1. Ensuring that AWS infrastructure meets internal and external compliance requirements
2. Parsing out and normalizing different data formats from dozens of security tools for easier analysis, significantly reducing the hours required for investigation
3. Prioritizing the large volume of alerts being triggered (which can range from tens to thousands per day depending on which tools an organization is using) to focus and simplify response
4. Gaining a single-pane-of-glass view across security and compliance tools and all AWS accounts

AWS Security Hub's ability to automatically aggregate findings from software seller solutions offers security teams many options for how they prioritize security operations, and what tools they use to do it. Today, there are 24 software seller integrations for AWS Security Hub spanning categories such as firewalls, endpoint security, vulnerability management, continuous compliance monitoring, security orchestration automation and response (SOAR), managed security service providers (MSSP), security information and event management (SIEM), and more. These vendor solutions collectively address both event and behavioral detection.

Splunk Cloud is a popular AWS Marketplace security solution that supports security and operational visibility across AWS environments, including applications, infrastructure, and AWS services such as AWS CloudTrail, AWS Config, and Amazon VPC Flow Logs. Splunk Cloud enables security teams to rapidly troubleshoot applications, ensure security and compliance, and monitor business-critical services.

Splunk Enterprise and Splunk Phantom integrations with AWS Security Hub are designed to help security teams further accelerate detection, investigation, and response to potential threats within their AWS security environments. Splunk integration enables serverless automation to gather findings from AWS Security Hub sending them to a HTTP Event Collector in the Splunk platform. With the Splunk Phantom App for AWS Security Hub, findings can be sent to Phantom for automated context enrichment with additional threat intelligence information or to perform automated response actions. By adding broader context to findings, security teams can be enabled to make informed decisions and take action quickly.

AWS customers can easily access the Splunk Phantom AMI via a listing in the AWS Marketplace and use Splunk Phantom SOAR features in AWS environments. This offering includes the free Splunk Phantom Community Edition, so customers can evaluate the product's capabilities. Phantom's flexible app model supports 225+ apps and 1,200+ APIs, enabling you to connect and coordinate complex workflows across your team and tools.

Splunk offers container visibility support as well. Containerized applications are one of the most popular tools for organizations migrating workloads to the cloud. Security teams that use, or want to use, Splunk can take advantage of this via AWS Marketplace. You can quickly deploy Splunk Docker Image n services such as Amazon ECS, Amazon Elastic Container Services for Kubernetes (Amazon EKS), and AWS Fargate by using deployment templates such as task definitions, Helm charts, and AWS CloudFormation templates provided by Splunk.

Why use AWS Marketplace?

AWS Marketplace simplifies software licensing and procurement by offering thousands of software listings from popular categories like Security, Networking, Storage, Business Intelligence, Machine Learning, Database, and DevOps. Organizations can leverage offerings from independent security software vendors in AWS Marketplace to secure applications, data, storage, networking, and more on AWS, and enable operational intelligence across their entire environment.

Customers can use 1-Click deployment to quickly launch pre-configured software and choose software solutions in both Amazon Machine Image (AMI) formats and SaaS subscriptions, with software entitlement options such as hourly, monthly, annual, and multi-year.

AWS Marketplace is supported by a global team of security practitioners, solution architects, product specialists, and other experts to help security teams connect with the software and resources needed to prioritize security operations in AWS.

How to get started with security solutions in AWS Marketplace

Security teams are using AWS native services and ISV solutions in AWS Marketplace to help build automated, innovative, and secure solutions to address relevant use cases and further harden their cloud security posture. The following steps can help you get started:

Browse free trials of the solutions mentioned above by clicking on the logos below

splunk>cloud™

Security and operational visibility across your AWS environment - including applications

splunk>enterprise

Collect and index any machine-generated data from virtually any source or location in real time

splunk> phantom

Security infrastructure orchestration, playbook automation and case management