aws marketplace

SANS

# Enhancing Your Security Visibility and Detection-Response Operations in AWS

Explore how to get more signal and less noise from your Amazon Web Services (AWS) environment.

# AWS Marketplace Introduction

Security teams are often tasked with separating out large streams of alerts to distinguish signals from noise. Such manual efforts can often get in the way of their efforts to prioritize critical incidents. However, by collecting key security information and automating incident response, organizations can more quickly identify critical threats and improve visibility into their AWS environment. In this whitepaper, SANS analyst and senior instructor, Dave Shackleford explores how organizations can leverage solutions to get more signal and less noise to enhance and accelerate their security operations.

Building on Shackleford's perspective, AWS Marketplace will share how you can specifically apply this process to your AWS environment. They will introduce relevant software seller solutions that can help you gain better context for events in your environment and boost your remediation efforts. Finally, AWS Marketplace solution sellers will be featured as available options for strengthening your security visibility in AWS.

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

Sumo Logic Cloud-Native Machine Data Analytics Service (Annually)

Securonix Next Generation SIEM

Sonrai Security Identity and Data Protection Platform for Multi-cloud

Demisto Enterprise AMI

A SANS Whitepaper

# How to Improve Security Visibility and Detection/Response Operations in AWS

Written by **Dave Shackleford**

January 2020

*Sponsored by:*

**AWS Marketplace**

## The Need for Cloud Security Monitoring

Security teams have increasingly realized a need to focus on monitoring tools and tactics for cloud environments. We've seen many types of cloud security incidents in the past several years, ranging from external intrusion attempts to internal misconfiguration and accidental exposure. Fortunately, cloud service providers (CSPs) have worked hard to create better cloud-native controls and services, as well as to enable third-party solutions to integrate with the cloud fabric for improved visibility and control. Security teams need to work diligently to update security monitoring and response practices to better reflect cloud-based tools and use cases.

In general, security teams need to focus on two major types of event monitoring in the cloud:

- **Event-driven monitoring—**The most common types of monitoring security teams have traditionally focused on are event-based. Events can be monitored from a wide variety of sources, including operating system logs, application logs, network device and platform logs, and security systems (intrusion detection and prevention, data protection tools, anti-malware platforms and many more). In the cloud, all of these sources are still important, and security teams can—and should—collect them all. However, the cloud control plane can also generate and track events occurring across an organization's infrastructure, so security teams can use a new category of events to monitor for unusual or suspicious activity.

For example, a security operations center (SOC) could monitor events for an EC2 instance spawned from a nonapproved machine image or a user attempting to deactivate multifactor authentication (MFA).

- **Behavior-driven monitoring—**The other major type of security monitoring needed in many environments is driven by events that occur over time and indicate a pattern or trend in behaviors. Many use cases coincide with this model of monitoring, including cases of insider abuse, credential hijacking and illicit use of cloud resources. To best monitor for behaviors, security teams need access to and insight from larger datasets over longer periods of time to see whether unusual or malicious activities are occurring. 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.

Cloud security monitoring and response increasingly focus on automation. While not all cloud security processes should be completely automated, there are many innovative automation capabilities built into the cloud control plane that can significantly improve many security monitoring and operations practices.

Collectively, logging and event monitoring, as well as automation strategies and tools, can enable security teams to build a continuous monitoring strategy in the cloud. This consists of two core strategies:

- Baseline monitoring and logging for workloads and the cloud control plane
- Scanning within the cloud for behaviors, conditions and vulnerabilities

## Enabling Cloud-Native Event Logs and Event Management

To establish baseline monitoring, security teams should gather and process the following:

- Cloud control plane logs (such as AWS CloudTrail[1] logs)
- Workload OS/application logs
- Network flow logs for virtual private clouds (VPCs)

Security teams should also leverage automation for improved operational capabilities with services like AWS Lambda and AWS Config.

[1] This paper mentions solution names to provide real-life examples of how cloud security tools can be used. The use of these examples is not an endorsement of any solution.

## Cloud Control Plane Logs

The first, and perhaps most obvious, step security analysts need to take is to collect logs from all relevant CSP environments. At the same time, analysts need to ensure that all the logs are going to a common location. An example of a cloud control plane logging service is AWS CloudTrail, which records any API calls made to Amazon Web Services (AWS). The service captures an extensive amount of data that security professionals will want to see, including the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters and the response elements returned by AWS. AWS CloudTrail logging captures all requests made from the standard AWS Management Console, command-line tools, any AWS Software Development Kits (SDKs) and other AWS services.

AWS CloudTrail solves one of the most challenging issues many security teams face when migrating IT resources into AWS: the capture and maintenance of cloud service event data that can feed log management and SIEM platforms. AWS CloudTrail uses Amazon S3 buckets for storage of the log data, allowing security teams to leverage the same APIs to access data quickly and easily for correlation and aggregation internally. Log data can also be automatically deleted after a certain period of time, or archived to internal storage or additional Amazon services like Amazon S3 Glacier for longer-term retention. Aggregation of log data across accounts and regions is possible, as is automated alerting and notification when certain events are registered. AWS CloudTrail log file integrity can also be enabled to hash all logs upon delivery and then monitor them afterward as well.

Most major CSPs allow logs to be downloaded from their environment (e.g., leading SaaS providers) or stored in a dedicated storage node (e.g., a dedicated S3 bucket). There are also a number of third-party security event aggregation and analysis platforms available for the cloud, including Sumo Logic[2] and others. These services may offer teams a simpler way to aggregate logs from multiple cloud services, and they often integrate more readily with these services through provider APIs.

## Workload Security Events

The second type of logs that teams need to collect are those associated with different server and container workloads. You should collect logs from your instance OS, just as you would in your own data center. This means syslog, Windows events and all the other logs you'd normally try to collect for security and operational reasons. The basic mechanics of generating logs and sending them somewhere might be the same, in general, depending on the deployment model you have. Really, you should monitor these logs just like logs from your in-house systems. However, because of volume and cost, sending them to an in-cloud log collector and/or event management platform likely makes sense. This process is distinct from logging within the CSP environment,

[2] Sumo Logic is a registered trademark of Sumo Logic Inc.

where you focus on API calls and access to the admin console for your cloud environment. It's important to make the distinction between cloud *system* monitoring and cloud *environment* monitoring. To ensure security, you must log and monitor systems just as you always have.

To enable consistent workload monitoring and logging, many organizations need to create and enable a central cloud log repository to store logs generated within workloads. There are many ways to accomplish this, but AWS has a unique agent, Amazon CloudWatch, that can be installed into Amazon EC2 workloads. This agent forwards syslog and other standard events to a dedicated Amazon CloudWatch logging group. From there, these logs can be parsed and analyzed, or streamed to a different event management and monitoring solution through streaming services like Amazon Kinesis Data Firehose.

> *It's important to make the distinction between cloud* system *monitoring and cloud* environment *monitoring. You must log and monitor systems just as you always have.*

For most organizations, the data export costs associated with large volumes of workload logs can prove somewhat prohibitive to simply sending all logs back to on-premises data collectors and SIEM tools. While this may work with a small volume of cloud services and workloads, large organizations will eventually want to enable cloud-native log collection and analysis tools instead.

## Network Flow Logs

Another critical type of data that should be collected and monitored in cloud environments is network flow data. For all major clouds, this can be enabled at the virtual private cloud (VPC) level, and these flow logs can then be sent to a dedicated storage node for analysis. With AWS VPC Flow Monitoring, network and security teams can add network behavioral monitoring to their overall capability set, and these logs have a wealth of data that can prove useful in detecting strange patterns of access and behavior in the AWS environment.

Most network traffic is recorded in AWS, except for:

- Traffic between EC2 instances and Amazon DNS services
- Amazon Windows license activation traffic for Windows EC2 instances
- Multiple IP addresses traffic (only primary address is logged)
- Instance metadata traffic to and from **`169.254.169.254`**
- DHCP traffic

Analysts can use this data to detect unusual patterns of communication between instances and workloads in the VPC environment, as well as specific malicious or suspicious activities originating outside the cloud and targeting assets (for example, SSH brute-force attempts). Keep in mind that enabling this type of logging can produce a staggering quantity of event data, and you will need to leverage some sort of toolkit (SIEM, security analytics, etc.) to build behavioral baselines for monitoring purposes.

# Improving Visibility in the Cloud

To improve security visibility in the cloud, security operations teams will want to develop a continuous monitoring strategy that uses a combination of cloud-native services and third-party options. This strategy provides the most comprehensive range of coverage for both proactively assessing the environment and detecting unusual events or anomalous behavior rapidly. Within AWS, for example, a continuous monitoring framework might include such services as:

- **Amazon Inspector—**This service performs vulnerability assessments of your cloud instances. An agent is required to perform scans, and most operating systems are supported (at least most Linux and Windows OSes). Amazon Inspector provides a number of rules templates, including CVE (for listing missing patches and other typical vulnerabilities that a vulnerability scanner would report on), CIS Benchmarks (for industry-standard configuration and control practices), general security best practices and so on. Scans can run between 15 minutes and 24 hours. Longer scans are more thorough and provide better baselines. Longer scans can really help to evaluate state over time and may help you to detect the state of systems in a rapidly changing DevOps environment. Amazon Simple Notification Service (SNS) notifications can be queued to alert you or feed to scripts and automation engines like AWS Lambda.

*A continuous monitoring strategy that uses a combination of cloud-native services and third-party options provides the most complete range of coverage for both proactively assessing the environment and detecting unusual events or anomalous behavior rapidly.*

- **AWS Config—**This configuration monitoring toolkit for your AWS systems can define your baseline image, monitor systems continually and alert whenever a system's configuration changes. AWS Config is natively integrated into AWS, and it can easily be set up to help keep your system state secure. Another key feature of AWS Config is its inventory capability. One advantage of the cloud is that nothing can hide, because all assets are 1) software-defined and 2) linked inextricably to the CSP's backplane. For this reason, the discovery and inventory elements of change and configuration management should be easier than ever! In the case of AWS Config, it doesn't get much easier—the service just finds everything and then lets you query AWS to see what you have. Recent additions to the AWS Config service allow for automated remediation and alerting as well.
- **Amazon CloudWatch—**This service allows you to monitor data and events and create alarms based on events in your AWS environment. Amazon CloudWatch, which integrates with almost all AWS services, can collect and track metrics, monitor log files, initiate alarms and automatically respond to changes in your AWS environment. For this reason, it's one of the most flexible monitoring tools you can use.

- **AWS Security Hub—**This service offers basic continuous monitoring for AWS accounts, looking at CIS Benchmarks configuration checks and more. Additionally, a number of third-party security tools can integrate into AWS Security Hub to create a centralized dashboard of events and security monitoring and operations.
- **Amazon GuardDuty—**This service analyzes a vast volume of log and intelligence data (both internal to AWS and from third parties) to deliver threat intelligence about customer account behavior. Results from Amazon GuardDuty can be integrated into Amazon CloudWatch and other event-triggering systems in AWS, or sent to the SOC or other locations for analysis with different tools.
- **Amazon Detective—**This service collects and aggregates logs across AWS resources and performs deep analysis on them to detect behavior anomalies and other events for faster and more efficient root-cause analysis and investigations. This feature is still in preview as of early 2020.

Many organizations may want to integrate all cloud-based events—both workload events and cloud control plane events—into an existing centralized detection and response capacity (usually focused on integrating SIEM and other large-scale correlation platforms for cloud monitoring). There are cloud-integrated API connectors for all major SIEMs today, such as Sumo Logic, Securonix, Sonrai Security and more. While this option is certainly a possibility, the costs to aggregate and export data (even over dedicated network connections like AWS Direct Connect) may be significant. For this reason, many organizations are now considering or implementing cloud-native SIEM tools.

## What to Look For: Enabling the SOC

Once cloud logs are being collected and aggregated, analysts need to sift through all the various events and start prioritizing them. There are several keys to this process, including:

- **Adding context—**If logs can be "tagged" as originating from a specific ISP or CSP, that can help provide context on the use cases of the service. For example, logs from identity management services like AWS Identity and Access Management (IAM) have a specific user context, whereas events from Amazon EC2 may need additional details about workloads to provide the proper context for evaluation.
- **Defining priorities—**Security analysts focused on the cloud must first decide what events and behaviors are most critical to monitor. Common starting points include any login activity to cloud management consoles; any changes or attempted changes to important cloud objects and data; any creation, deletion or modification of credentials or cryptographic keys; and attempts to modify or delete audit logs.

- **Tuning alerts—**Tuning is incredibly important for cloud logging and event management. You want to suppress redundant alerts, both those that are entirely operational in nature and those not directly related to security. To build appropriate behavioral baselines of events in the environment, you also likely need to allow several weeks or even months of data to accumulate. Make tuning a regular part of your weekly monitoring processes.
- **Housekeeping of accounts and credentials—**Leftover user credentials, cloud accounts and data can lead to potential risks in the cloud. Work closely with human resources teams to disable credentials to cloud accounts quickly, and monitor for all attempts to log in with disabled or deleted credentials for at least several weeks after a user has left the organization. It's a good practice to monitor user account activity of employees who have given notice to ensure that they don't try to take or sabotage critical data. For example, look for sudden increases in data exports, transfer or overall account use.

Another area of focus for cloud events should be the originating point of cloud activity. Security teams should consider a login from a new country or location where the organization doesn't do business or have users to be a very high priority alert. Many cloud logs include enough detail to note where the login came from.

## Identification and Prioritization of Potential Events

Where to start? Security operations teams might feel somewhat overwhelmed when starting to sift through cloud logs and events. Fortunately, many types of events and information can help identify potential incidents in the cloud, including:

- **Incident notifications from your CSP—**This depends on your CSP model and deployment type, as well as contractual SLAs and terms.
- **Billing alarms—**These are key! If you have a reasonable idea of a monthly billing range, you can break this down to define "checkpoints" of what your bill should be at any given time. If these thresholds are crossed, a billing alarm could alert you and investigate what is causing the additional cost.
- **IAM activity (logins in particular)—**Monitor your user activity within the cloud. In particular, monitor admins carefully, because these user credentials are prime targets for attackers. Any nonfederated user access should also be a high priority.
- **Cloud environment logs (e.g., AWS CloudTrail)—**General API logs can tell you when instances are created or changed, when storage attributes change and so on. Focus on the types of events that could be problematic to the environment. These event types include access or changes to critical assets, modification of identity policies, deletion or changes to cryptographic keys, and so on.

As a general rule, security operations teams should prioritize the following types of events (listed by order of priority/severity):

- **Priority 1**
  - Launching a workload that is not from an approved template
  - Launching any containers from unapproved images in a repository
  - Launching any assets in unapproved regions
  - Modifying any IAM roles or policies
  - Modifying or disabling cloud control plane logging or other security controls
  - Logins to the web console (unauthorized)
- **Priority 2**
  - Unusual user behaviors (trying to access unauthorized resources, etc.)
  - Adding/updating new workload images
  - Adding/updating new container images
  - Logins to the web console (authorized)
  - Updating/changing serverless configuration
- **Priority 3**
  - Changes to security groups or network access control lists (ACLs)
  - Updating/changing serverless function code

## Top Cloud Monitoring Use Cases and Workflows

A cloud monitoring workflow should ideally look like one shown in Figure 1.

Logging begins with a central logging engine like AWS CloudTrail and/or a log collection agent from a SIEM solution extracting log data from a data store (primarily for workload logs if applicable). All logs, irrespective of source, need to be monitored for suspicious activity in the context of what environment the assets operate within, with detection filters set up to send alerts or perform more automated response actions. Any security operations team should spend time with all cloud environment logs to better understand the behavior of the workloads and services operating there.

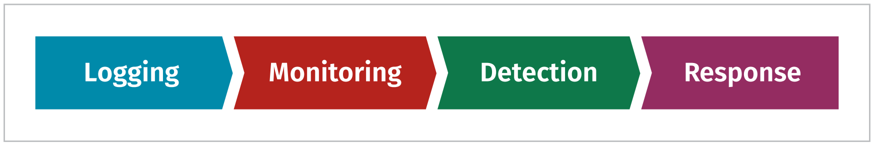


*Figure 1. Cloud Monitoring Workflow*

For example, AWS CloudTrail captures an enormous range of event data, and tools like Amazon CloudWatch enable you to search for many different events. Table 1 on the next page lists some examples of starting points.

Additionally, there are a number of serverless events in AWS Lambda that could prove to be interesting starting points. For example, if someone deletes a function (**`DeleteFunction`**), this might be important. The same could apply for **`RemovePermission`**.

**Table 1. Starting Points for Event Searches**

| AWS CloudTrail Event | Reason for Investigation |
|---|---|
| **`ConsoleLogin`** | A user initiates console login activity. |
| **`StopLogging`** | A user tries to stop AWS CloudTrail. |
| **`CreateNetworkAclEntry`** | Someone creates a network ACL, which could expose attack surfaces or vectors. |
| **`CreateRoute`** | Someone creates a new route for data path control, which could expose attack surfaces or vectors. |
| **`AuthorizeSecurityGroupEgress`**<br>**`AuthorizeSecurityGroupIngress`**<br>**`RevokeSecurityGroupEgress`**<br>**`RevokeSecurityGroupIngress`** | Monitor all changes to security groups. |
| **`ApplySecurityGroupsToLoadBalancer`**<br>**`SetSecurityGroups`** | Security group changes that tie to elastic load balancers are interesting, often in scaling operations. This may indicate unusual traffic surges in the environment. |
| **`AuthorizeDBSecurityGroupIngress`**<br>**`CreateDBSecurityGroup`**<br>**`DeleteDBSecurityGroup`**<br>**`RevokeDBSecurityGroupIngress`** | Amazon RDS instances have a different nomenclature for security groups, but are the same thing conceptually. Security teams should monitor such instances. |

Table 2 lists the most critical AWS Lambda events to monitor immediately for security.

**Table 2. Events for Immediate Monitoring**

| AWS Lambda Event | Reason for Monitoring |
|---|---|
| **`DeleteEventSourceMapping`** | Someone could delete the data source that triggers an AWS Lambda function, making it "blind." |
| **`DeleteFunction`** | A function could be deleted purposefully or accidentally, leading to security issues. |
| **`RemovePermission`** | This could lead to a lockout scenario or lack of access when needed (think IAM service account or role access to AWS Lambda). |
| **`UpdateEventSourceMapping`** | Data could be pulled from a different source, leading to incorrect function results. |
| **`UpdateFunctionCode`** | The function could be broken or tampered with to prevent security-specific functionality from executing (for example, by adding comments). |
| **`UpdateFunctionConfiguration`** | The configuration of the function could be changed to limit its resources, causing poor or flawed execution. |

Security teams also need to be proactive in securing the cloud environment. Security operations and engineering teams should work with cloud operations and engineering teams to implement more effective controls around:

- **IAM and privileges (and credential security)—**This can be one of the most difficult areas to solidify in cloud security, because there are many types of privileges and roles that can be defined. AWS has a service called AWS IAM Access Analyzer, which is free and integrated into the AWS IAM platform. This service can help with assessing any AWS native or custom IAM policies to determine where excessive or unintended privilege allocation may be present based on AWS best practices and assigned users/groups.

- **Resources and resource utilization—**Cloud control plane logs from services like AWS CloudTrail can (and should) be heavily leveraged to monitor new, modified and deleted assets in the environment, as well as access to assets and service interaction in the cloud environment. These logs need to be integrated with a SIEM and/or cloud-native cloud monitoring solution like Amazon CloudWatch to build the appropriate triggers for alerting, as well as monitoring and reporting metrics as warranted. Some behavioral trending over time can also be assessed and reported through analytics tools like AWS Security Hub and Amazon GuardDuty, as well.
- **Activity in specific regions—**One of the best quick wins for security teams is to purposefully disable all geographic regions not in use; a follow-up to this is enabling explicit monitoring for cloud control plane logs (like AWS CloudTrail) to look for any activity in regions marked as "not in use" or "disabled." A common tactic intruders use for malicious activities like cryptocurrency mining is to create unauthorized assets and workloads in unused regions to "buy time" before detection. Teams should consider any alert for activity in an unauthorized or unused region a high priority.

Regardless of the tools chosen, SOC teams need to adapt their workflows and monitoring processes to include as much log and event data from the cloud as possible. This invariably requires significant effort to better learn and understand the patterns of events and service interaction in the cloud environments chosen. Spending some time each month or quarter developing "game day" or tabletop exercises to flesh out cloud monitoring and response use cases is an excellent way to engage the SOC team in cloud initiatives and improve the team's skills and processes at the same time.

## SOAR and the Role of Automation

Increasingly, more enterprise incident response teams are actively looking for opportunities to automate processes that often take up too much of their highly skilled analysts' time, as well as those processes that require lots of repetition (and may provide little value in investigations). Common activities that many teams consider for automation include the following:

- **Identifying and correlating alerts—**Many analysts spend inordinate amounts of time wading through repetitive alerts and alarms from many log and event sources, and spend time piecing together correlation strategies for similar events. While this is valuable for later stages of investigations, it can also be highly repetitive and is therefore a good candidate for some degree of automation.
- **Identifying and suppressing false positives—**This work can be tedious on a good day, and overwhelming on a bad one. Identifying false positives can often be streamlined or automated using modern event management and incident response automation tools.

- **Initial investigation and threat hunting—**Analysts need to quickly find evidence of compromise or unusual activity, and often need to do so at scale.
- **Opening and updating incident tickets/cases—**Due to improved integration with ticketing systems, event management and monitoring tools used by response teams can often generate tickets to the right team members and update these as evidence comes in.
- **Producing reports and metrics—**Once evidence has been collected and cases are underway or resolved, generating reports and metrics can take a lot of analysts' time.

Examples of security response automation include:

- Automated DNS lookups of domain names never seen before
- Automated searches for detected indicators of compromise
- Automated forensic imaging of disk and memory from a suspect system, driven by alerts triggered in network- and host-based anti-malware platforms and tools
- Network access controls automatically blocking outbound command and control (C2) channels from a suspected system

A fair number of vendors and tools can help integrate automation activities and unify disparate tools and platforms in use for detection and response. These include Swimlane, Demisto, IBM Resilient Incident Response Platform[3] and more, most of which leverage APIs with other platforms and tools to allow them to share data and create streamlined response workflows. Factors to consider when evaluating these automation tools include maturity of the vendor, integration partners, alignment with SIEM and event management, and ease of use and implementation.

Incident response (IR) in the cloud may rely on scripting, automation and continuous monitoring more heavily than in-house IR currently does. Many of the detection and response tools emerging for the cloud are heavily geared toward automation capabilities. To effectively implement automated IR in the cloud, IR teams need to build automated "triggers" for event types that run all the time (such as Amazon CloudWatch filters), especially as the environment gets more dynamic. Deciding what triggers to implement and what actions to take is really the most time-consuming aspect of building a semi-automated or automated response framework in the cloud. Do you focus on user actions? Specific events generated by instances or storage objects? Failure events? Spending time learning about cloud environment behaviors and working to better understand "normal" patterns of use is invaluable here.

> *Factors to consider when evaluating security response automation tools include maturity of the vendor, integration partners, alignment with SIEM and event management, and ease of use and implementation.*

[3] Swimlane is a trademark of Swimlane LLC; Demisto is a trademark of Demisto Inc.; IBM and IBM Resilient Incident Response Platform are registered trademarks of International Business Machines Corp.

The following list provides a breakdown of the security automation model to consider for cloud deployments—it's really broken into three major components:

- **Phase 1: Learn—**In this phase, you monitor for events occurring in the environment. With AWS, this would likely come from AWS CloudTrail logs, Amazon VPC Flow Logs, Amazon CloudWatch Logs, etc.
- **Phase 2: Trigger—**Based on some pattern matching, using Amazon CloudWatch alerts or even a SIEM like Sumo Logic, you then trigger some sort of follow-up action.
- **Phase 3: React/Respond—**The final phase is the actual action triggered during the automation. This could be an AWS Lambda function that performs an action, a vulnerability scan or an alert sent via SNS or other method.

The use cases for phases 2 and 3, where certain events trigger responses, vary widely. These might include tagging assets that are behaving suspiciously, disabling access keys or user/service credentials, changing a security group to one that is a "quarantine" zone without internet access, or simply alerting a group of SOC analysts. Security teams need to spend some time developing these automation use cases and then look into the tooling needed to accomplish these goals through cloud-native and third-party services.

## Conclusion

The cloud has a lot to offer in the way of security monitoring and visibility. Security teams have the ability to capably monitor for both event-driven and behavior-driven activity, and they now have a single environment they can query for all the cloud control plane visibility they could want. Security teams need to adapt monitoring and preventive/detection tools in some cases, although they might have more options due to cloud-native and third-party controls and services that are rapidly expanding. Teams can implement and monitor the entire spectrum of control areas, too, ranging from network controls like firewalls and intrusion detection services to endpoint protection and monitoring agents to vulnerability scanning continuously. With large-scale analytics processing and numerous options to enable, collect, store and transmit log and event data from their cloud assets and environment, teams can more readily analyze everything happening in this part of the hybrid cloud network 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).

That said, there's still a lot of work for SOC teams to do in reviewing events and building detection and response use cases. Building effective correlation cases for cloud monitoring can also be readily accomplished with the tools and services available today, but it will take time and a better understanding for SOC teams to adapt to different event sources and types.

One area of significant promise is automation—teams have all the event details they need, as well as tools and services to store and process them. With SOAR solutions and cloud-native processing and automation engines, security operations teams should see definitive improvements in their detection and response capabilities, because the cloud is a unified fabric with innumerable APIs to employ (for querying information and for performing detection, response and mitigation). As infrastructure becomes progressively more software-defined, this will be more and more important to security professionals everywhere.

## 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

# Strengthen your AWS security with AWS services and third-party solutions.

Security operations teams looking to advance their visibility and detection-response in AWS must develop a continuous monitoring strategy that includes cloud-native services and third-party solutions. Proactively assessing your AWS environment for vulnerabilities and rapidly detecting unusual events or activity are key components of this strategy.

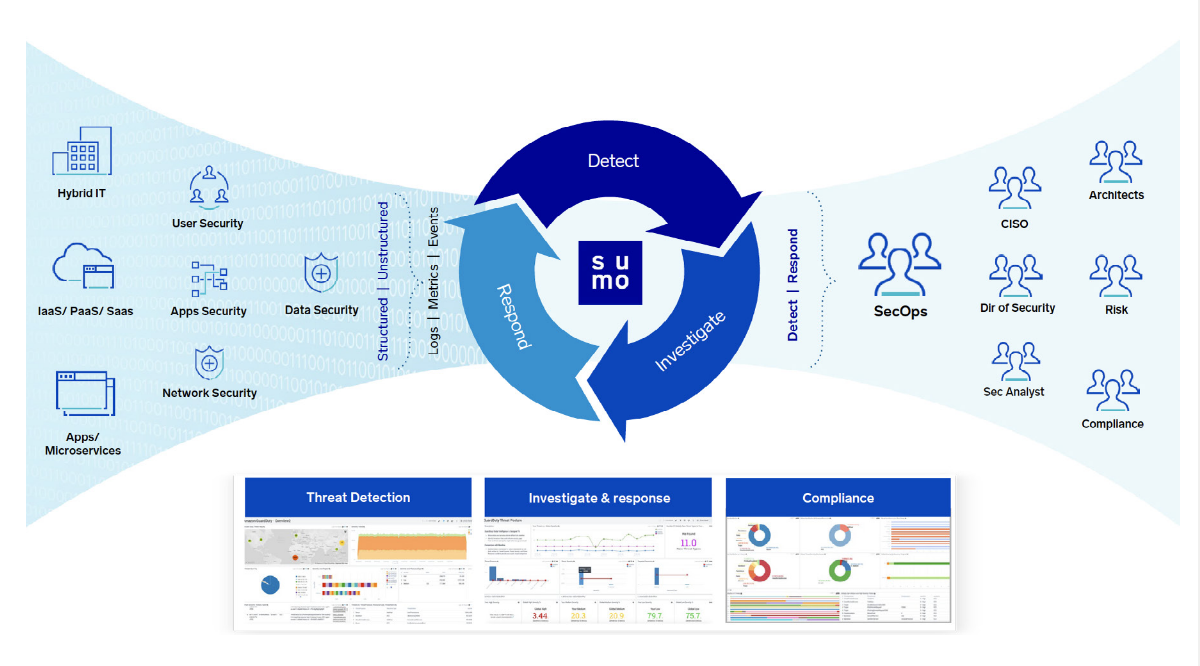
Amazon Security Hub can help aggregate, organize, and prioritize your security alerts to enable your continuous monitoring strategy. In addition, Amazon Detective collects and aggregates logs across AWS resources and performs deep analysis to detect behavior anomalies and other events for faster and more efficient root cause analysis and investigations.

The integration of security information and event management (SIEM) and security orchestration automation and response (SOAR) technologies can also help enhance detection and response. Due to the high costs of aggregating and exporting data, organizations are implementing cloud-native SIEM tools to increase visibility into their environment. For example, Sumo Logic's Cloud-Native Machine Data Analytics Service is a SIEM solution that can generate continuous machine learning and statistical baselines from Amazon GuardDuty's threat detection service. Customers can then use those baselines to benchmark, prioritize, and optimize security configuration and detection across their AWS environment.

### How AWS customers are leveraging Sumo Logic to enhance their security operations

Sumo Logic is a secure cloud-native analytics platform that can help improve security visibility and accelerate detection and response across your AWS environment. Some of the ways that customers are leveraging Sumo Logic to enhance their security posture include:

- **Improve visibility across AWS:** Sumo Logic can process more than 100 petabytes of data and handle over 20 million queries daily. It is an elastic solution that scales irrespective of data volume or number of users. It can also handle a large variety of formats, whether structured, unstructured, or semi-structured. This allows for broad visibility across your entire AWS environment.



- **Actionable insights through better context:** Many AWS customers use Sumo Logic to distill thousands of log lines into easy to understand patterns. With just a few clicks, you can compare and reduce those logs into just 3-4 cluster patterns through their LogReduce and LogCompare functions. This can bring actionable insights by creating more signal and less noise.

- **Accelerate detection and response:** Sumo Logic supports cross-functional collaboration by correlating data from multiple data sources, showing data in the context of time-series metrics. This provides a single source of truth for monitoring and troubleshooting in order to accelerate detection and response.

Securonix and Sonrai Security are other SIEM solutions available in AWS Marketplace. Securonix combines log management, user and entity behavior analytics (UEBA), and security incident response into a single operations platform. The Sonrai Public Cloud Security Platform finds and removes previously invisible cloud identity risk by finding excessive privilege, privilege escalation risk, and separation of duty risk. Demisto offers a SOAR platform that allows security teams to automate manual tasks, not only freeing up analysts to focus on more meaningful activities but also reducing mean time to response (MTTR).

## 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, solutions 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 threat detection and incident response solutions in AWS Marketplace

Security teams are using AWS native services and seller 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 solutions can help you get started:

sumo logic

**Sumo Logic Cloud-Native Machine Data Analytics Service (Annually)**
Continuous intelligence across your entire application lifecycle and stack

SECURONIX

**Securonix Next Generation SIEM**
SIEM, UEBA, and security data lake capabilities

DEMISTO

**Demisto Enterprise AMI**
Security automation and response platform

sonraí SECURITY

**Identity and Data Protection Platform for Multi-cloud**
Finds and removes previously invisible cloud identity risk