aws marketplace

SANS

Building a Threat Detection Strategy in AWS

Improve your threat detection and remediation capabilities by leveraging Amazon Web Services (AWS) services and solutions in AWS Marketplace.

AWS Marketplace Introduction

As more organizations move sensitive data to the cloud, there is a growing need to monitor and rapidly analyze the data to identify and respond to threats. In the following whitepaper, SANS analyst and senior instructor David Szili will explore security monitoring strategies and services for the cloud. You will learn key considerations around data collection, intrusion detection and prevention systems, and more to inform your threat detection strategy.

Following David's exploration, AWS Marketplace will share how this information can be applied to your AWS Cloud environment by introducing relevant AWS services that can enhance your data security. A popular threat detection software seller, Splunk, and their solutions available in AWS Marketplace will be presented as an option to enable your threat detection strategy.

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 Threat Detection Strategy in Amazon Web Services (AWS)

Written by **David Szili**

August 2019

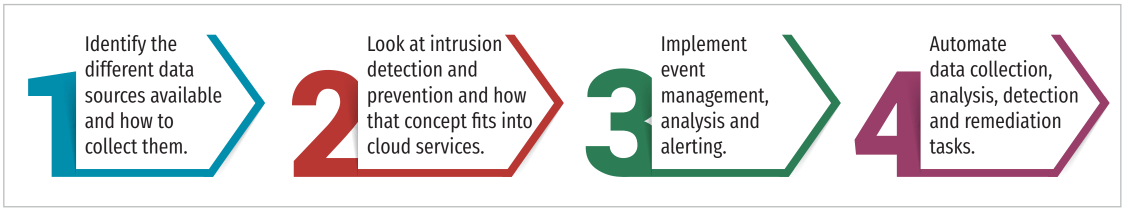
Sponsored by:

AWS Marketplace

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.



1 Identify the different data sources available and how to collect them.

2 Look at intrusion detection and prevention and how that concept fits into cloud services.

3 Implement event management, analysis and alerting.

4 Automate data collection, analysis, detection and remediation tasks.

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 Hub[1] 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.

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.

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

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.

[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.

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 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"
}
```

Figure 2. AWS CloudTrail Event Example

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.

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 the 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.

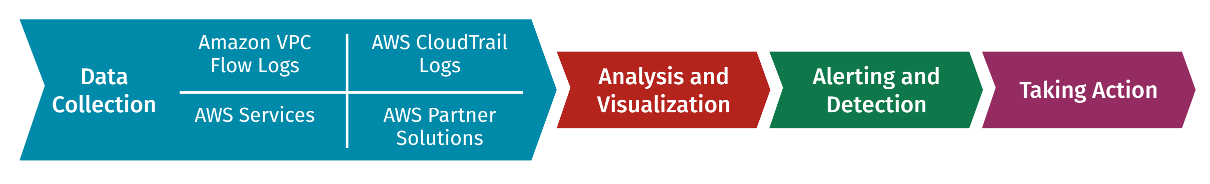


Figure 3. Unified Interface for Management of Events and Alerts

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.

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 the 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.

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

- 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

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:

aws marketplace

aws marketplace

Enabling threat detection in AWS with third-party intelligence

To protect AWS accounts and workloads, enterprises need to continually monitor for malicious activity and unauthorized behavior. AWS Marketplace offers numerous independent software vendor (ISV) threat detection solutions that integrate with foundational AWS services. For example, Splunk offers solutions that integrate with Amazon GuardDuty and AWS Security Hub.

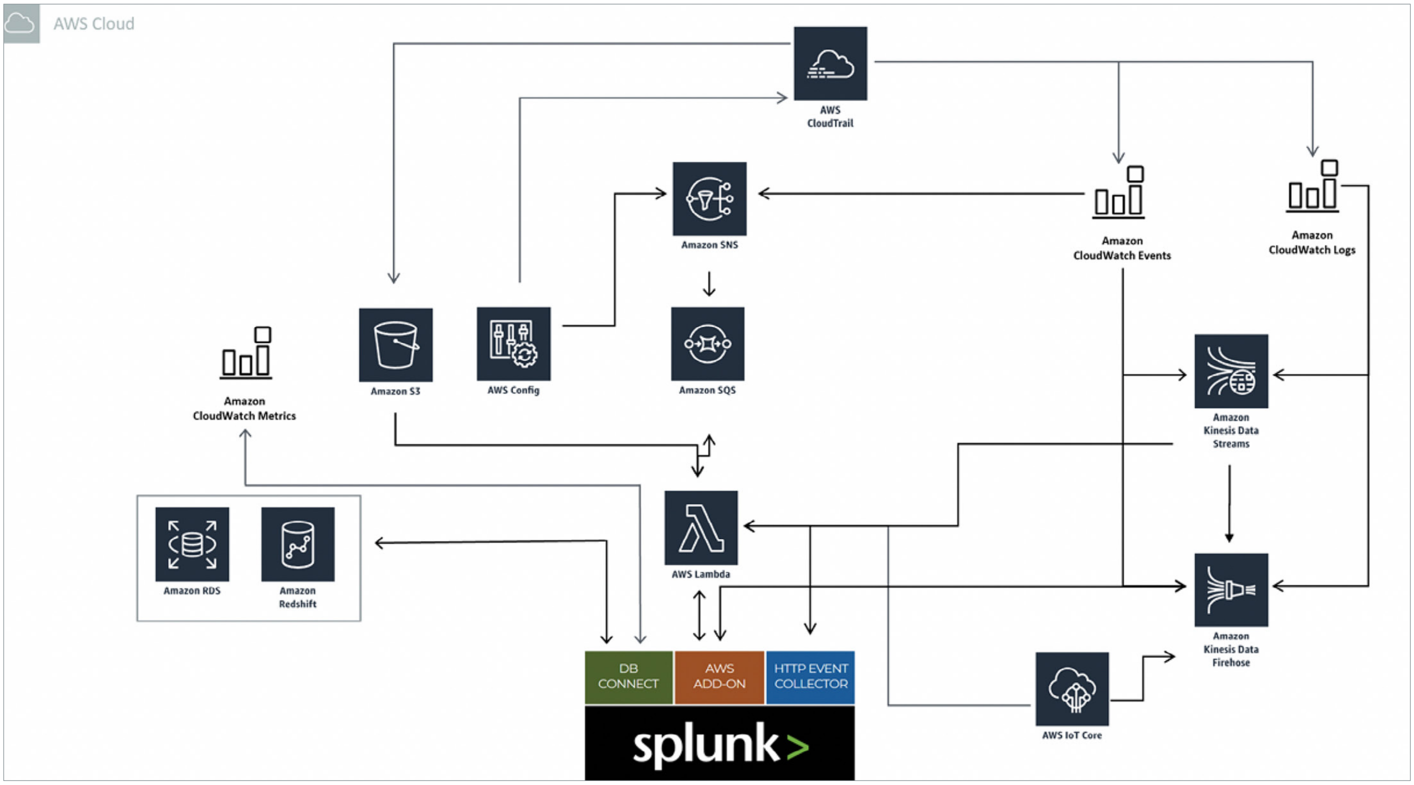
Amazon GuardDuty can tell you if anything is suspicious based on known bad activity on that sensitive data. This service analyzes tens of billions of events across multiple AWS data sources, such as AWS CloudTrail, Amazon VPC Flow Logs, and DNS logs. GuardDuty then combines managed rule-sets, threat intelligence from AWS Security and third-party intelligence partners, anomaly detection, and machine learning to intelligently detect malicious or unauthorized behavior. By then integrating with AWS CloudWatch Events, GuardDuty alerts are actionable, easy to aggregate across multiple accounts, and straightforward to push into existing event management and workflow systems. AWS Lambda can then be triggered for automated remediation or prevention.

AWS Security Hub allows you to quickly access your high-priority security alerts and compliance status across AWS accounts in one comprehensive view. Splunk, which works across cloud and on-premises deployments, can feed information into AWS Security Hub, augmenting your security visibility with additional analysis and remediation capabilities.

How AWS customers are using Splunk to enable threat detection use cases

Whether you're managing applications, infrastructure, or a security operations center in the cloud, Splunk solutions can deliver operational intelligence for a real-time understanding of what's happening across your business, and insights to help you make informed decisions.

- **Secure visibility and threat detection:** Whether you're managing applications, infrastructure, or a security operations center in the cloud, Splunk Cloud and Splunk Enterprise can deliver operational intelligence. This intelligence provides a real-time understanding of what's happening across your business and IT that can help you to make informed decisions. These solutions provide a single platform to monitor, analyze, and remediate security threats before they happen.



Splunk Cloud and Splunk Enterprise can deliver operational intelligence for a real-time understanding of what's happening across the business.

- **Secure migration:** When migrating workloads to the cloud, it's critical to monitor performance, maintain comprehensive visibility, troubleshoot and triage efficiently, and support security and compliance. This needs to happen across the entire hybrid architecture, and in a manner that collects and correlates data from every location. Splunk Enterprise can help with this; keeping the migration within schedule and budget, and to help minimize the effort required to migrate and keep TCO down, throughout the lifecycle of the project.

- **Security orchestration and automated response:** Splunk Phantom, the company's SOAR solution, combines security infrastructure orchestration, playbook automation, and case management capabilities to integrate your team, processes, and tools. It enables you to work smarter by executing a series of actions, from detonating files to quarantining devices, across your security infrastructure in seconds, versus hours or more if performed manually. You can codify your workflows into automated playbooks using the visual editor or the integrated Python development environment.

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 software 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.

Browse featured Splunk solutions mentioned above by clicking on the logos below

splunk>cloud™

splunk>enterprise

splunk>
phantom