Cloud Security Monitoring on AWS

Sherif Talaat

Continuous Security Monitoring on AWS

GIAC (GMON) Gold Certification

Author: Sherif Talaat, sherif.talaat@hotmail.com
Advisor: Hamed Khiabani, Ph.D.
Accepted: January 31st, 2021

Abstract

Cloud services adoption is growing massively year over year. In most cases, moving to the cloud decision is driven by cost optimization goals. Organizations usually start the cloud journey with the lift-and-shift approach, migrating the datacenter as-is, including the security services and controls, even the physical appliances, to the equivalent virtual appliances from the respective vendor. In some cases, the security controls used on-premises are not as effective with cloud services. Moreover, in some other cases, it can be expensive as well. This paper illustrates Amazon Web Services (AWS) security services a security professional can use to aid the cloud service's continuous security monitoring operations.

1. Introduction

Cloud Computing is becoming a de facto for consumers and enterprise segments. The industry analysts' reports, such as Gartner and IDC, show a rapid increase in cloud computing adoption by organizations year over year. According to IDG 2020 Cloud Computing Study, *"81% of organizations have at least one application or a portion of their computing infrastructure in the cloud. 92% of organization's IT environment is at least somewhat in the cloud"* (IDG, 2020).

Organizations are often moving to the cloud to achieve cost savings, but it is not the only reason. Cloud computing offers reliability, scalability, and flexibility that a traditional on-premises cannot reach. The driver for cloud migration is different for each organization based on its business priorities. One of the advantages is the flexibility to provision and de-provision resources in minutes while paying for the utilization period. The fast pace of cloud computing innovation leads to more frequent service updates, such as introducing new features or fixing a bug.

The flexibility of cloud computing that we see as an advantage can be a disadvantage to the organization and a burden on its information security team. A misperception of cloud security is putting assumptions based on the service provider's marketing messaging without any validation and due diligence.

For instance, a specific cloud service provider that is HIPAA compliant does not make the organization's application HIPAA certified by default. None of the cloud service providers is HIPAA certified -since none of them provide a medical service- but they are meeting HIPAA compliance requirements. That means the underlying infrastructure complies with the HIPAA requirements, yet the organization still must put the right measure on its application as well; this what cloud service providers usually refer to as the "Shared Responsibility Model."

The organizations and cloud service providers' responsibility varies based on the type of services, whether it is IaaS, PaaS, or SaaS. The rule of thumb is the more control the organization has, the more responsibilities to deal with, and vice versa. The following diagram demonstrates the shared responsibility model of AWS (AWS, 2020).

Sherif Talaat, sherif.talaat@hotmail.com

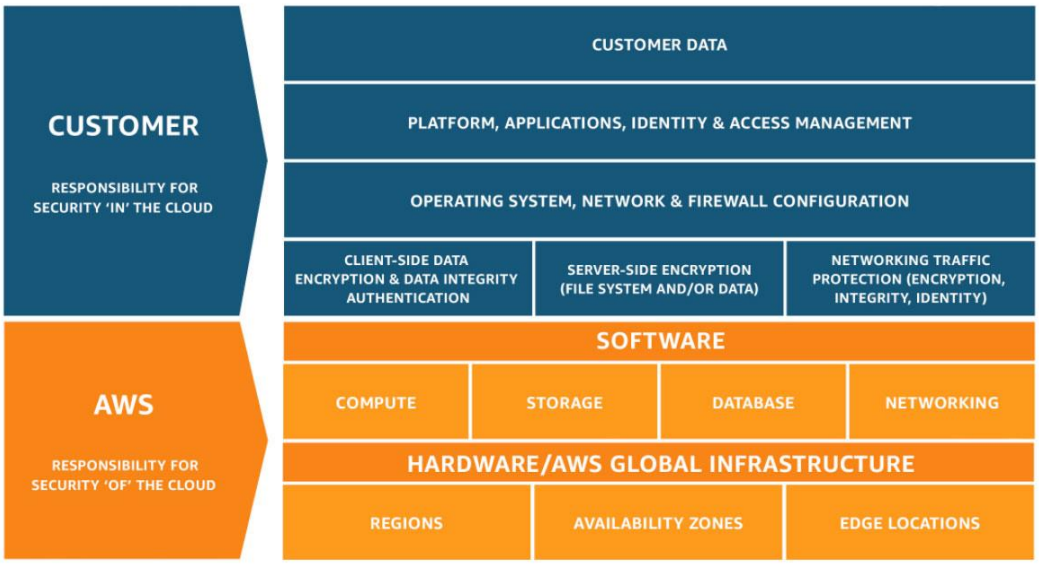


Figure 1: AWS Shared Responsibility Model

This paper discusses the various cloud-native security controls available in Amazon Web Services (AWS) to help security engineers implement technical controls for continuous security monitoring. The focus will be on the core services that should be in any enterprise network. It does not focus on step-by-step guidance but on what to enable, how it can help, and finding the right information to help the security professionals achieve their goals.

2. AWS Global Infrastructure

For an organization to start using AWS cloud, it must have at least one AWS account. The AWS account is where to provision and use AWS services across the different AWS regions. A region in the definition of AWS is a geographical area where AWS has physical datacenters (AWS, Regions and Availability Zones, 2020). Each region has multiple **Availability Zones (AZ),** which are multiple isolated datacenters within each region. This architecture provides the maximum availability for the services within the same geographical area, accordingly help organizations to have a higher uptime.

A single organization can have multiple AWS accounts for different projects, departments, or even different environments (Production, Staging, Development). Those

AWS accounts can be stand-alone and separately managed or organized under one master account as in **AWS Organizations**. **AWS Organizations** can be used and enforced to govern, control, and monitor the AWS environment as it expands (AWS, AWS Organizations, 2020).

3. Amazon Virtual Private Cloud (VPC)

Amazon VPC is the cornerstone of any AWS environment. VPC is a virtual data center on the cloud; it enables organizations to build a virtual network to launch different infrastructure resources. Amazon VPC usually represents one of the AWS regions; there can be multiple VPCs in one region.

The VPC usually has multiple subnets, distributed across multiple availability zones (AZ) within the same region to provide high availability. As a best practice, an organization would place various servers such as front-end web servers in multiple AZs to achieve high-availability. Each subnet has a route table to route the traffic between the subnet and other networking components in the VPC, such as Internet Gateway, VPN Gateway, and NAT Gateway.

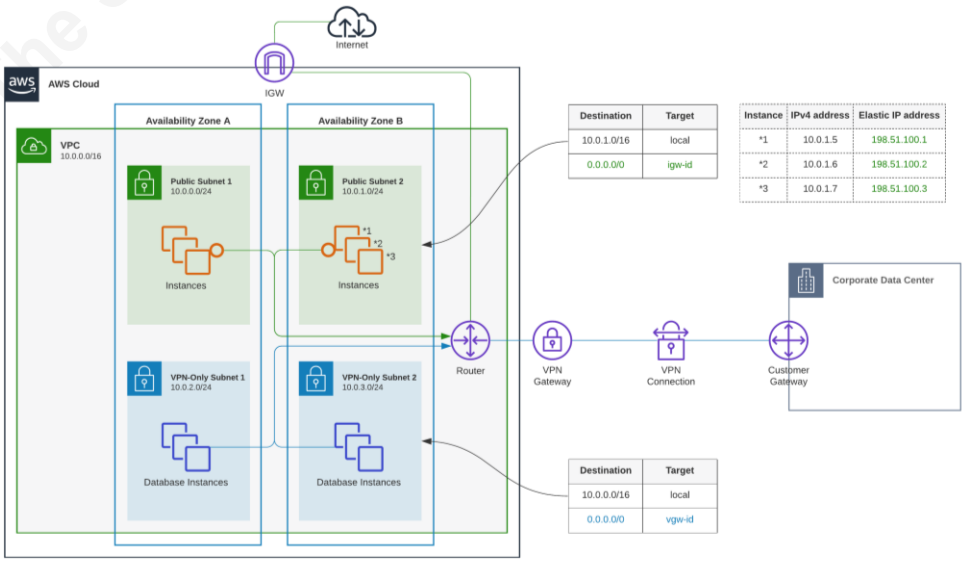


Figure 2: AWS VPC with hybrid connectivity over VPN

Sherif Talaat, sherif.talaat@hotmail.com

3.1. Amazon VPC networking components

In addition to subnets, Amazon VPC contains other components.

3.1.1. Security groups (SG)

A security group is a firewall that controls the inbound and outbound traffic on the EC2 instance level. In security groups, only allow rules are configurable but not deny rules since the traffic is denied by design unless there is an explicit allow rule. Security groups are stateful, no need to allow traffic flow in both directions (AWS, Security groups for your VPC, 2020). An important note to keep in mind is that the security group has "**allow all outbound**" traffic to **0.0.0.0/0** by default, so that rule should be revised to be more restrictive if needed.

3.1.2. Network Access Control List (NACL)

NACLs are like security group in a sense it controls the traffic. However, it works on the subnet level, not the EC2 instance level like security groups. NACLs are stateless, which means it should explicitly allow ports in both directions. It can also configure both allow and deny rules. The default NACL policy allows inbound to and outbound traffic from **0.0.0.0/0**, so considering revising it as well.

3.1.3. Internet gateways

The Internet gateway enables the communication between a VPC and the internet in both ways. It allows EC2 instances to connect to the internet and allow access to the EC2 instances from the internet is assigned a public IP address. The main differentiator between a public subnet and a private subnet is that the first has an internet gateway (AWS, Internet gateways, 2020). Another type of internet gateways is called Egress-only internet gateways, allowing outbound communication over IPv6 only (AWS, Egress-only internet gateways, 2020).

3.1.4. NAT gateways

NAT gateway enables instances in private subnets to connect to the internet and other AWS services. While Internet gateways allow outbound IPv6 traffic only, NAT gateways allow outbound internet traffic over IPv4.

Unlike the internet gateway, it does not allow access to the instances from the internet. NAT gateways allow the internet without any granular control, so a common practice is replacing the NAT gateway with a firewall/proxy to control the internet traffic.

3.1.5. Route tables

By default, the traffic inside VPC stays in the VPC unless there are explicit routes to allow traffic to leave it. Route tables allow configuring a set of routing rules to define how traffic will travel outside the boundaries of the VPC (AWS, Route tables, 2020). For instance, routing the traffic to the internet via NAT gateway or between Amazon VPC and on-premises network via VPN gateway.

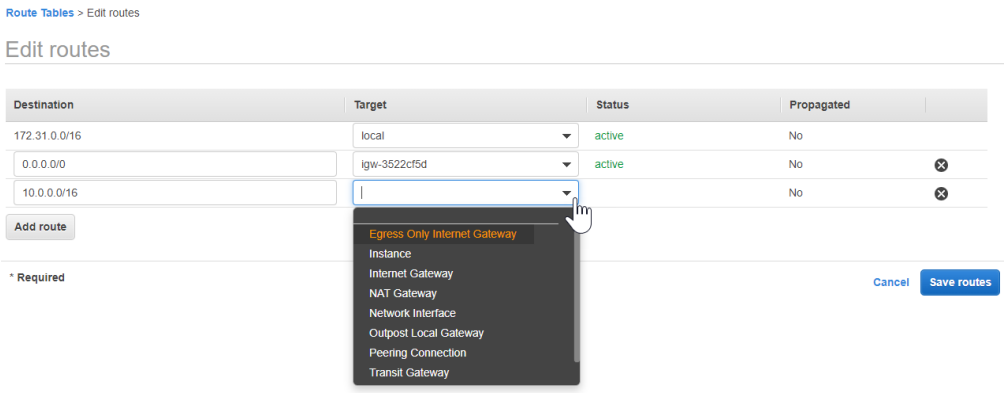


Figure 3: VPC Route Table

3.1.6. VPN, direct connect, and VPC endpoint

While some organizations are cloud-native (aka, born on the cloud) and have their entire infrastructure hosted there, most organizations still use a hybrid approach. In hybrid-cloud, organizations distribute the different applications and infrastructure components between the cloud and on-premises facility. Amazon VPC provides multiple options for organizations to extend the on-premises facilities to the cloud.

The most common option, de facto, is a virtual private network (VPN) over the public internet. The VPN could be site-to-site between the on-premises datacenter and Amazon VPC, or client-to-site, which is beneficial in scenarios like users working from home. Another connectivity option is AWS Direct Connect, which provides a private dedicated network connection between the on-premises datacenter and AWS without traversing the internet. Additionally, Direct Connect offers a better latency compared to VPN.

Sherif Talaat, sherif.talaat@hotmail.com

Similar connectivity models are available even for services on AWS. For example, the EC2 instances running inside Amazon VPC can communicate with other AWS services hosted outside the VPC either over a public internet connection or via **VPC Endpoint** (AWS, VPC endpoints, 2020), which provides a private connection between your VPC and AWS services.

3.2. VPC Flow Logs

VPC Flow Logs captures the IP traffic information going to and from the network interfaces inside a VPC. The flow logs are generated for a specific network interface, specific subnet, or entire VPC. Flow logs settings have the flexibility to choose the type of traffic to capture, rejected, accepted, or all (AWS, VPC Flow Logs, 2020).

Flow Logs are not limited to interfaces created for the EC2 instances; it includes network interfaces for other services, such as Elastic Load Balancers, Amazon RDS, and NAT Gateway. Flow logs publish to Amazon CloudWatch as log streams, where each log stream represents a specific network interface. Additionally, sending logs to Amazon S3 as a log file object. The modern SIEM and USM solutions have connectors to AWS to read VPC Flow Logs format from Amazon S3 directly; storing logs on Amazon S3 is cost-efficient, especially if required to retain for an extended period.

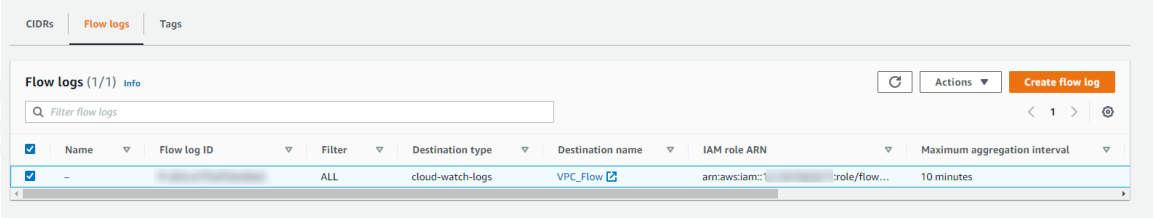


Figure 4: VPC Flow Logs

The VPC Flow Logs is available in two formats: default and custom. The default format includes the basic information as shown below

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

```
2 121397083071 eni-099a6010655c96644 172.31.35.79 162.248.241.94 46920
123 17 1 76 1600329577 1600329632 ACCEPT OK
```

The VPC Flow Logs can record more information; however, the extra fields get defined in a custom format (AWS, VPC Flow Logs - Custom format, 2020). Then, logs get aggregated with an interval of 1 minute or 10 minutes (AWS, VPC Flow Logs, 2020). While VPC Flow Logs is a tool for traffic capturing, it cannot serve scenarios like traffic inspection since it is not instantaneous. However, it is still useful for scenarios like troubleshooting traffic flows, security groups & NACLs rules, and even for security solutions that can find anomalies in traffic logs like Amazon GuardDuty or SIEM solution.

3.3. VPC Traffic Mirroring

In essence, VPC Flow Logs and Traffic Mirroring are capturing the same traffic information. However, the main differentiator is that VPC traffic mirroring can capture traffic in a near real-time fashion and send a copy of that traffic to out-of-band security appliances (AWS, Traffic Mirroring and VPC Flow Logs, 2020). For instance, Network Intrusion Detection System (NIDS) sensors such as Zeek, Suricata, and others (AWS, Working with open-source tools for Traffic Mirroring, 2020).

The following configurations are the configurations to enable traffic mirroring on resources in Amazon VPC (AWS, Traffic Mirroring concepts, 2020):

- **Target:** A target defines the security solution's virtual appliance's elastic network interface to send the mirrored traffic.
- **Filter:** A filter defines the traffic to capture and send to the target in a traffic mirror session. For example, create a filter to monitor all the rejected TCP traffic within a specific CIDR block.
- **Session:** A session defines the mirrored traffic source, the target of that mirrored traffic, and the traffic content based on the mirror filters. A source is an elastic network interface of the server to capture its traffic.

3.4. VPC Reachability Analyzer

The reachability analyzer is a newly added feature to Amazon VPC. As the name implies, it analyzes the network communication path to and from the resources (i.e., EC2 instance) within the VPC and checks whether they are reachable or not. If the destination resource is reachable from a specific source, the reachability analyzer will show every

hop in the path between the source and destination. If the destination is unreachable, it shows which configuration is blocking the communication. (AWS, What is VPC Reachability Analyzer?, 2020)

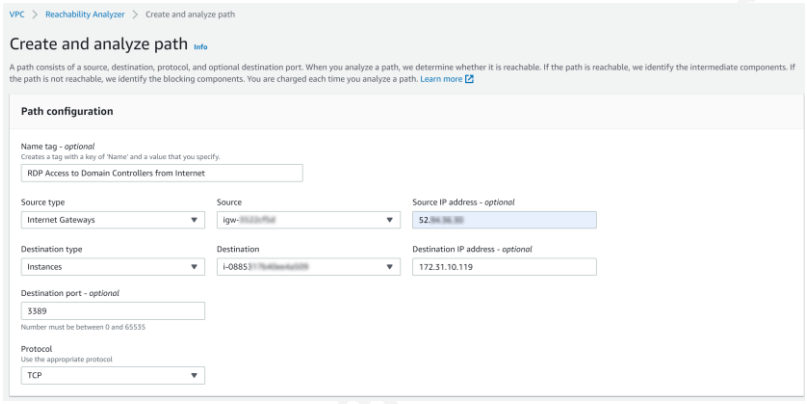


Figure 5: VPC Reachability Analyzer - Create an analyzer

The reachability analyzer is not like ping and traceroute; it does not send packets from the source to the destination. Instead, it builds a model for the network configuration, then evaluates that configuration. For example, for a user to access a specific EC2 instance over the internet via RDP. The traffic goes through the internet gateway, and then the NACLs followed by security groups until it reaches the EC2 instance.

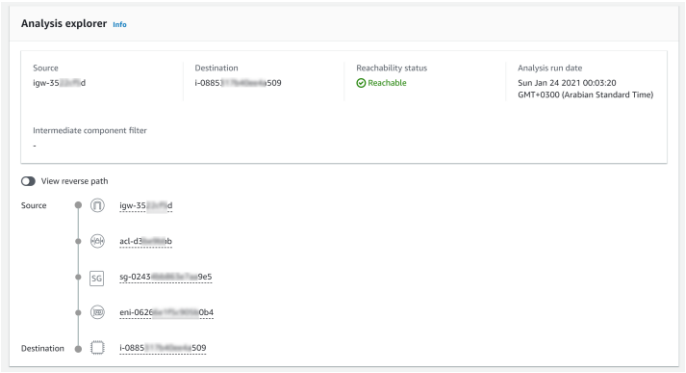


Figure 6: VPC Reachability Analyzer - Results

4. Network Security

There are multiple ways to deploy security controls on AWS. A security engineer can choose from AWS native services such as AWS Network Firewall and AWS WAF or choose a 3rd party solution from AWS Marketplace.

Sherif Talaat, sherif.talaat@hotmail.com

4.1. Network Firewall

In November 2020, AWS announced AWS Network Firewall, a managed firewall service that provides network protection for Amazon VPCs (AWS, AWS Network Firewall, 2020). "AWS Network Firewall: More Than Just Layer 4" (Nicholson, 2020). AWS Network Firewall is a stateful firewall with packet inspection, inbound & outbound web filtering, and intrusion prevention capabilities.

AWS Network Firewall has a signature-based detection engine that inspects the traffic flow and matches it against a list of known threat signatures and anomalies. In addition to a flexible rules engine that allows a fine-grained firewall policy definition. The rules engine allows importing rules written in open-source rule formats such as Suricata IPS rules. AWS Network Firewall integrates with third-party security solutions. This integration support scenarios like managed threat intelligence feed (i.e., domain-based IOCs) or sending traffic logs to log analytics solution to find anomalies and suspicious traffic (AWS, AWS Network Firewall partners, 2020).

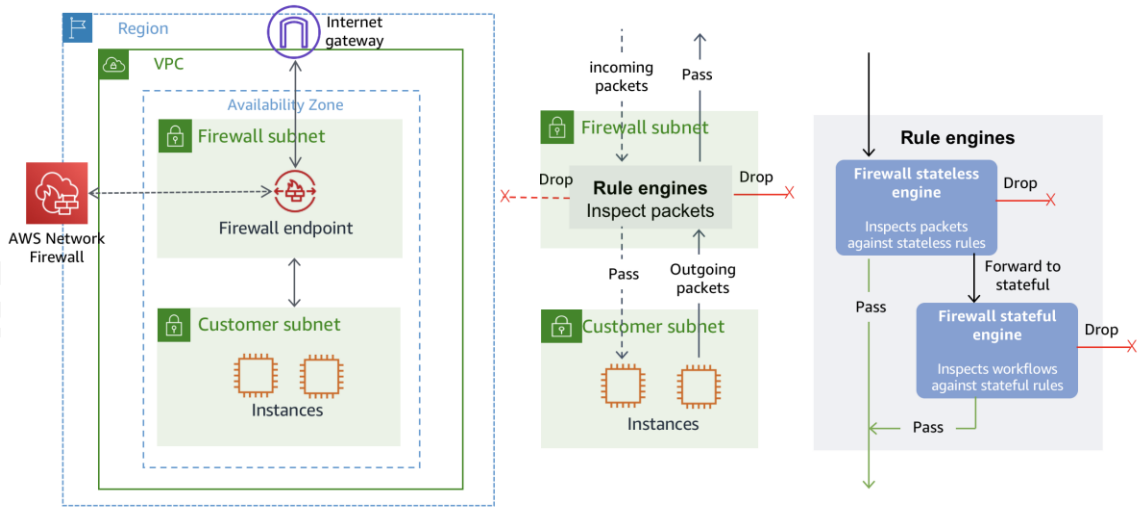


Figure 7: AWS Network Firewall – Rules Engine (AWS, AWS Network Firewall, 2020)

4.2. Web Application Firewall (WAF)

AWS WAF provides layer-7 protection to web applications against common web exploits such as SQL injection, cross-site scripting (XSS), HTTP floods, blocking bad actors' IP addresses, blocking IP addresses submitting bad requests, and many more. AWS WAF works with Amazon CloudFront (Amazon CDN), Application Load-Balancer, and Amazon API Gateway.

Sherif Talaat, sherif.talaat@hotmail.com

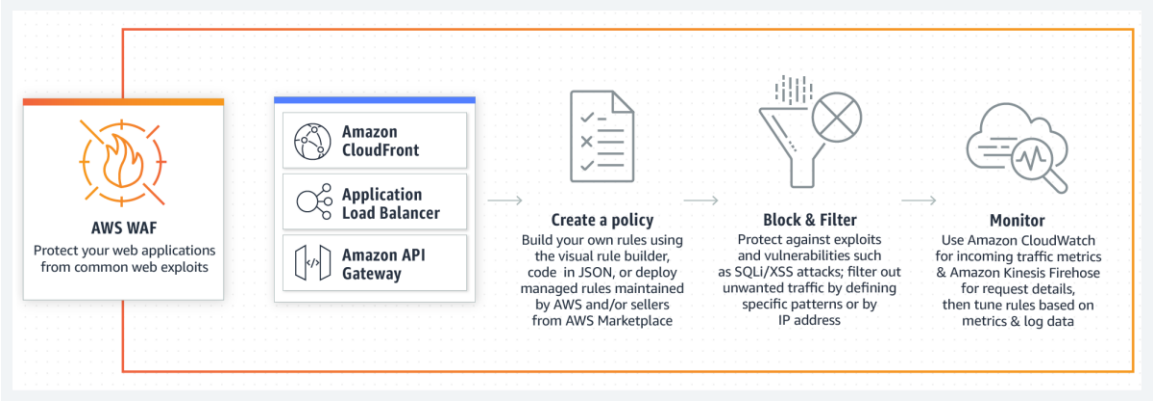


Figure 8: AWS WAF - How it works

A security engineer can craft WAF rules from scratch or choose from AWS Managed Rules. WAF Managed rules are pre-configured managed rules that protect against the common application vulnerabilities and bad traffic we mentioned earlier. Similarly, A security engineer chooses AWS WAF Managed Rules from third-party vendors like F5, Fortinet, Imperva, and others (AWS, Managed rules for AWS Web Application Firewall, 2020).

The AWS Solutions library offers a pre-configured security automation solution that simplifies the deployment using CloudFormation template (AWS, AWS WAF Security Automations, 2020). The solution is a good starting point to deploy AWS WAF with rules to protect against common attacks. Also, it provides some security automation capabilities, such as detecting bad bots and blocking them.

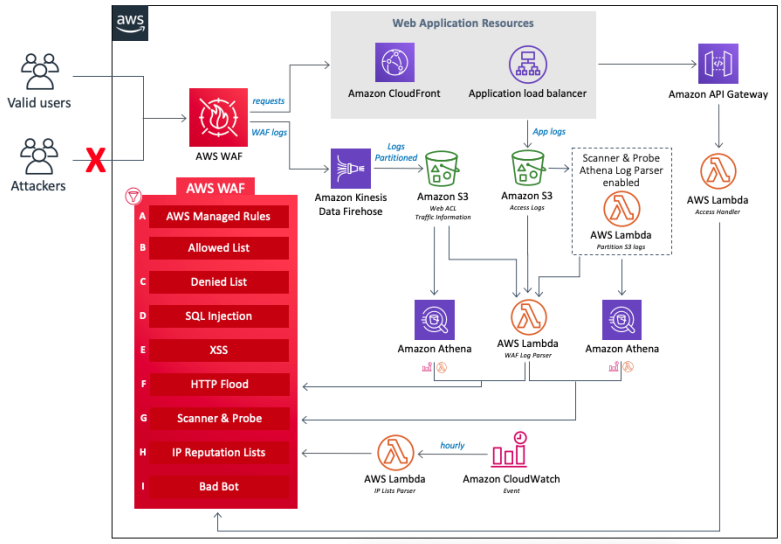


Figure 9: AWS WAF Security Automations Architecture (AWS Solutions, 2020)

Sherif Talaat, sherif.talaat@hotmail.com

4.3. DDoS Protection

In 2020, AWS defended its infrastructure against the largest DDoS attack in internet history with a volume of 2.3 Tbps; the attack was mitigated by AWS Shield (Porter, 2020).

AWS Shield is a managed service that protects against Distributed Denial of Service (DDoS) attacks targeting layer-3 and layer-4, such as SYN/UDP floods and reflection attacks. AWS Shield is available for organizations in two editions; **Standard,** which is by default enabled for all AWS customers, and **Advanced,** which provides enhanced protection against sophisticated and more extensive attacks with near real-time notifications of DDoS incidents (AWS, AWS Shield Features, 2020).

Figure 10: Global activity detected by AWS Shield

An advantage of AWS Shield Advanced is the 24x7 access to the AWS DDoS Response Team (DRT), who can proactively engage directly with the organization to help manage incidents, identify the root cause, and apply the mitigation, including crafting a custom-tailored rule.

Another advantage of AWS Shield Advanced is the cost protection against usage spikes. Scalability is a proven benefit of the cloud; the auto-scaling feature of AWS allows organizations to add/remove resources in response to traffic spikes. If a DDoS attack led to triggering auto-scaling to provision resources to absorb that traffic, the DDoS service team could waive those extra charges.

4.4. AWS Firewall Manager

So far, the security services discussed, such as security groups, network firewall, and WAF, have rules to configure and deployed. As the cloud workloads grow, this rules' management is getting complicated and leaves room for mistakes.

AWS Firewall Manager allows the security engineer to manage and configure different security rules and policies from a unified console. Also, it integrates with AWS Organizations to extend that central management capability across numerous AWS accounts under the same AWS Organization (AWS, AWS Firewall Manager, 2020).

Furthermore, AWS Firewall Manager can apply a security baseline for security groups, audit and enforce (remediate) security groups, and even clean up unused and redundant security groups.

5. Endpoint and Services Security

On the cloud, endpoints go beyond end-user computers. It still can be an end-user computer like Amazon WorkSpaces (Desktop-as-a-Service). It could be an EC2 instance or a database endpoint used to read from and write to that database. The security and monitoring of the endpoints -irrespective of their type- remains an essential operation.

5.1. Service monitoring and logging

Amazon CloudWatch is a real-time monitoring and log collection service for different AWS services, applications, and infrastructure resources. With Amazon CloudWatch, organizations can collect performance metrics (i.e., CPU utilization, memory utilization, network in/out, disk IOPS) and system & application logs.

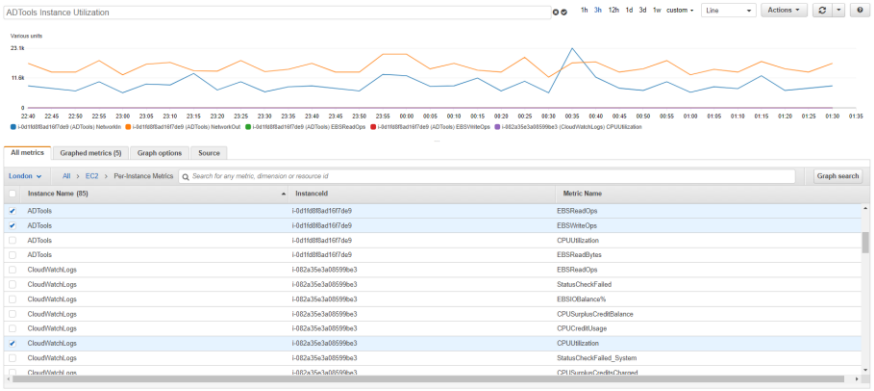


Figure 11: CloudWatch Metrics for EC2 Instances

Sherif Talaat, sherif.talaat@hotmail.com

Amazon CloudWatch extends support to hybrid environments with Amazon CloudWatch agents. It is available on supported operating systems versions of Windows and different Linux distributions (AWS, CloudWatch Agent, 2020). The OS-level logging capability is advantageous for the security engineers; if the CloudWatch agent is available on the system, there is no need to install any additional agent for the SIEM/USM solution to collect those logs. Most modern security monitoring tools have connectors to AWS and can read from Amazon CloudWatch Log Groups.

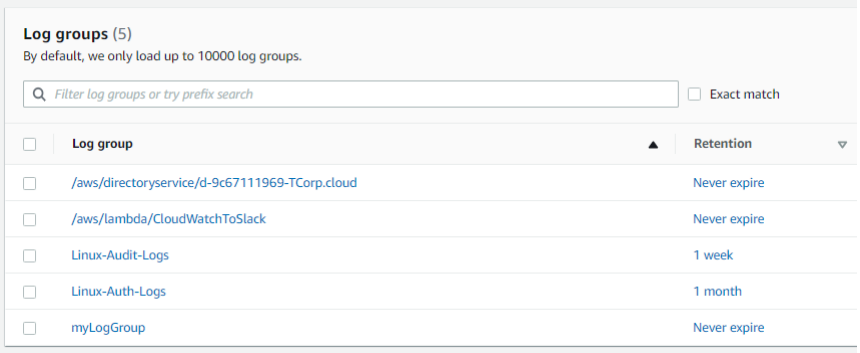


Figure 12: CloudWatch - Log Groups

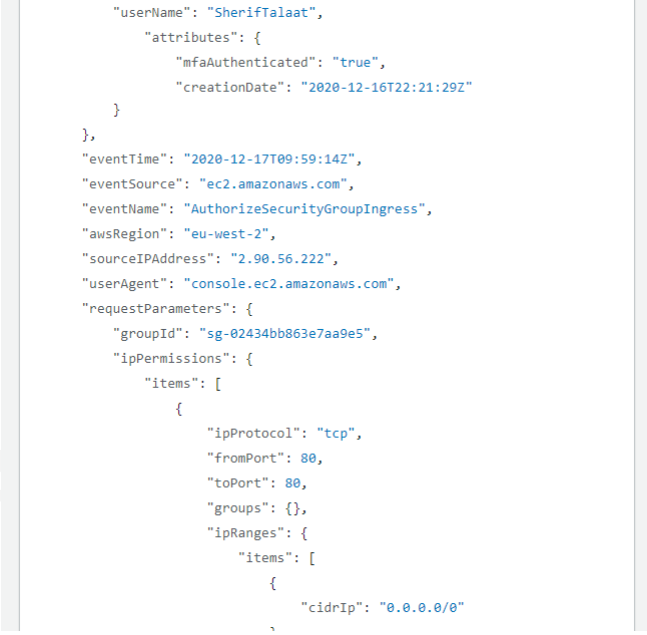
The CloudWatch log group's default retention setting is "never expire"; in that case, the logs remain indefinitely. There are different retention period options between a day and ten years (AWS, What Is Amazon CloudWatch Logs?, 2020). CloudWatch Alarms notify the system administrator of certain events. It also integrates with Lambda via Amazon EventBridge (formerly, CloudWatch Events) to respond to a specific API call.

5.2. Auditing for governance, risk, and compliance

Continuous monitoring for AWS account and resources is as important as monitoring applications, databases, and servers running on AWS. AWS account is the control plane that has full control of all the resources on AWS.

AWS CloudTrail is an auditing service that records all the account activities and events history. In AWS, everything is an API, so every action taken through the AWS management console, command-line tools, and AWS SDKs is triggering an API call, and AWS CloudTrail records it. Moreover, the AWS CloudTrail Insights feature helps identify unusual activities in AWS accounts, such as unusual API calls or spikes in specific API calls.

The trail for every log event provides comprehensive information, including but not limited to credentials used for the event, source IP address, event source, event name, event time, user agent, and many others. All this information can help in finding anomalies, tracking changes, and prove non-repudiation. The following sample is part of CloudTrail records showing a user made a change for a security group's inbound rules to allow TCP port 80.



```
        "userName": "SherifTalaat",
            "attributes": {
                "mfaAuthenticated": "true",
                "creationDate": "2020-12-16T22:21:29Z"
            }
    },
    "eventTime": "2020-12-17T09:59:14Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "AuthorizeSecurityGroupIngress",
    "awsRegion": "eu-west-2",
    "sourceIPAddress": "2.90.56.222",
    "userAgent": "console.ec2.amazonaws.com",
    "requestParameters": {
        "groupId": "sg-02434bb863e7aa9e5",
        "ipPermissions": {
            "items": [
                {
                    "ipProtocol": "tcp",
                    "fromPort": 80,
                    "toPort": 80,
                    "groups": {},
                    "ipRanges": {
                        "items": [
                            {
                                "cidrIp": "0.0.0.0/0"
```


Figure 13: CloudTrail log sample

Like most AWS services, AWS CloudTrail publishes logs to Amazon CloudWatch and Amazon S3. Due to the criticality of the audit logs, the organization should consider enabling the following AWS CloudTrail features:

- Enable CloudTrail for all regions and not the only one it operates on. It is crucial to capture any activity that happens under the AWS account irrespective of which region. It makes it easy to catch bad actors trying to under the radar.
- Enable log file integrity validation to detect any changes and modification of CloudTrail logs.
- AWS CloudTrail might contain confidential data such as usernames, access keys, tokens, or any other sensitive information. So it is essential to enable the log encryption feature to protect the logs against unauthorized access.

Sherif Talaat, sherif.talaat@hotmail.com

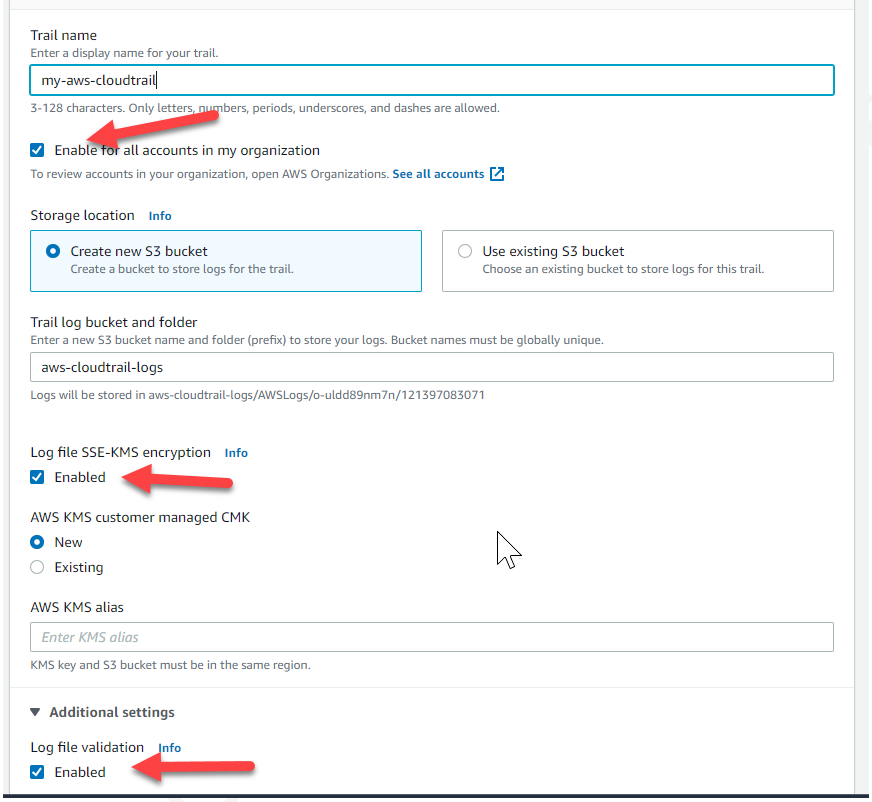


Figure 14: CloudTrail - New trail creation wizard

5.3. Privilege account monitoring

In 2014, InfoWorld magazine published the article "Murder in the Amazon cloud.", the author of the article explains how Code Spaces, a GitHub-like service, disappeared overnight. It was not because their servers got hacked or that database got wiped, but because the hacker gained access to the control plane of their AWS account and locked the legit owners out (Venezia, 204).

In AWS, There are two Identity & Access Management (IAM) features the security engineers should be aware of: Credentials report and Access Analyzer.

5.3.1. Credential report

The credential report generates a status report for all the users under a specific AWS account. It provides information such as (AWS, Getting credential reports for your AWS account, 2020):

- User creation time
- Password last use time

- Password last change time
- password rotation
- MFA status
- Any access keys linked to that user account
    - The date of the previous use and for which region and which service
    - The access key rotation date.

This information can help understand the credentials' current state, find red flags, and take corrective action like removing zombie accounts, force multi-factor authentication, and rotate access keys.

5.3.2. Access analyzer

Access Analyzer monitors and analyzes resource-based policies such as IAM roles, AWS KMS key policies, and Amazon S3 bucket policy. Then, it generates findings if a policy is granting external entity access to that resources. For example, an Amazon S3 bucket allows public access, or IAM roles giving AWS user in other AWS account access to local resources. These findings can help the security administrator spot misconfiguration and maybe persistent access to the control plane (AWS, How Access Analyzer works, 2020).

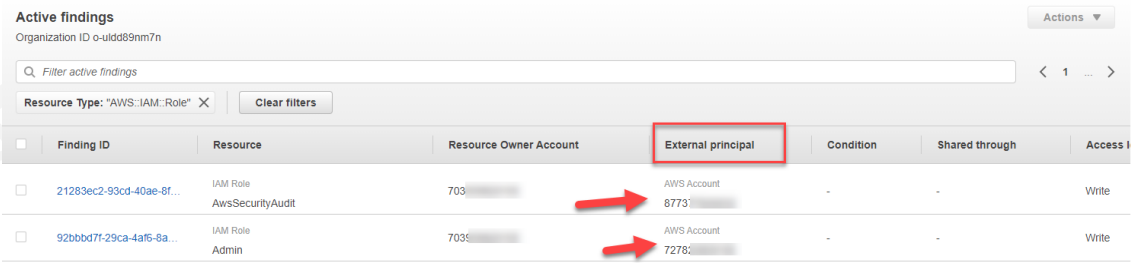


Figure 15: Access Analyzer showing external principals have access to the local AWS account

5.4. Systems Management

In information security, "you cannot secure what you cannot see" (Pescatore, 2018), and in the cloud, the list of "what you cannot see" can overgrow and get out of control if the proper controls are not in place. Simply because with a few clicks, a developer can provision hundreds of resources in a few minutes.

AWS Systems Manager (SSM) provides a set of services (modules) to serve the different purposes of system management, monitoring, and automation. Out of the entire list of SSM modules, security engineer can focus on (or at least start with):

5.4.1. AWS System Manager Inventory

It collects information from all the EC2 instances around the instance details information such as hardware specifications, operating systems, software installed, Windows updates, Windows services & roles, Windows registry, network configurations, monitor file integrity, and more.

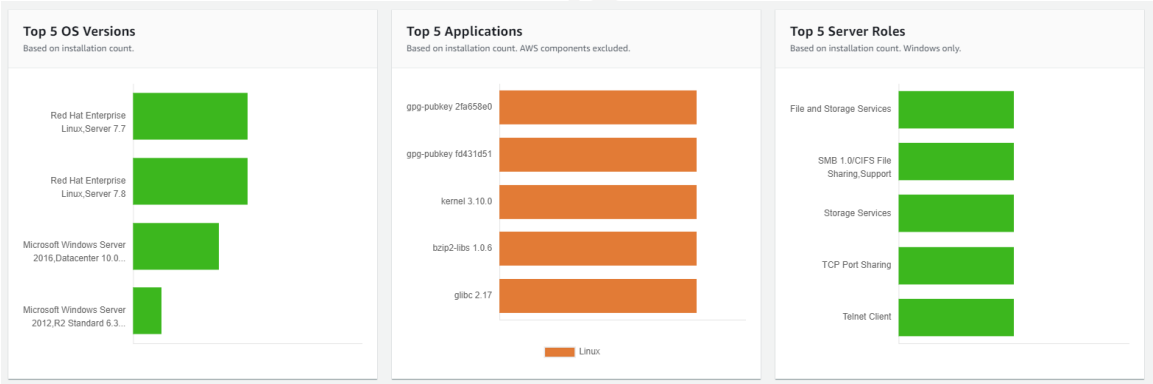


Figure 16: Systems Manager Inventory dashboard

5.4.2. AWS System Manager Distributor

It provides system administrators with the ability to create, package, store, and distribute software packages. SSM distributor can configure a CRON schedule every hour or every day to deploy a specific package. Putting it in a security-related context, a security engineer can configure SSM distributor to run at the end of every business day to install Sysmon or GRR client on the newly provisioned EC2 instances. Furthermore, report its status to the compliance dashboard.

5.4.3. AWS System Manager Patch Manager

The Patch manager scans the servers for the missing operating systems updates (Windows, Linux, and macOS) and application patches. The Patch Manager supports both EC2 instances and on-premises servers as well. A security engineer can define a patch baseline, such as approving all security patches for Windows with critical severity.

It can also report missing patches or outdated systems to the compliance dashboard to easily track the patching process.

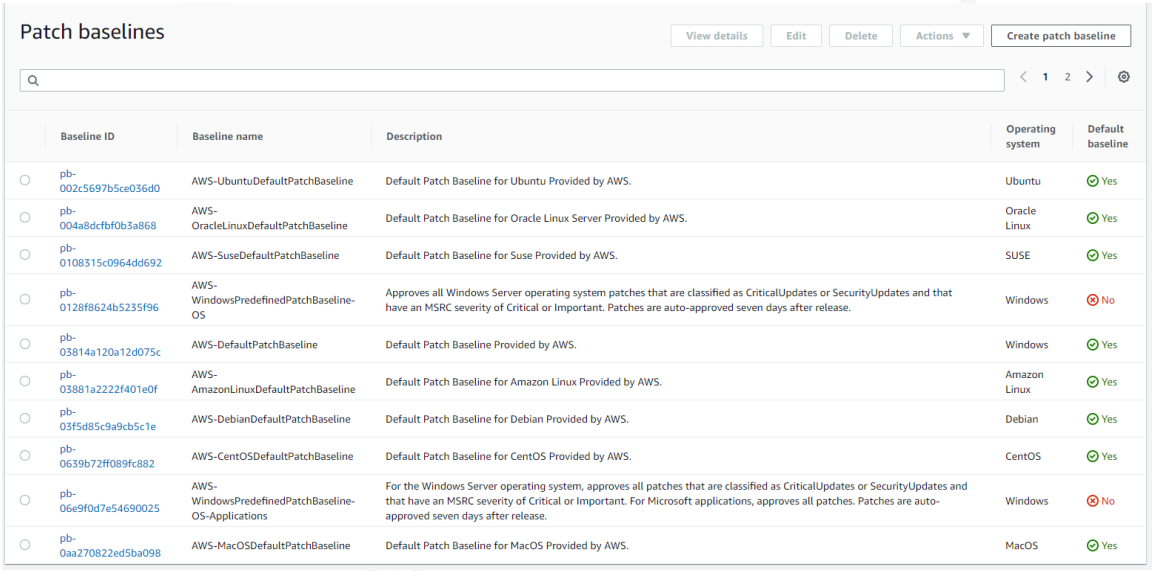


Figure 17: Systems Manager Patch Manager patch baselines

5.4.4. AWS System Manager Run Command

Run Command allows system administrators and security engineers to manage the servers without interactive sessions, such as SSH. With Run Command, the engineer can choose from a list of pre-built command documents (playbooks), such as installing an application or creating a user. It can also merely running a stand-alone ad-hoc command using command documents **AWS-RunShellScript** for Linux and **AWS-RunPowerShellScript** for both Windows and Linux.

5.4.5. AWS System Sessions Manager

The Sessions Manager is a secure alternative to bastion hosts. It enables a browser-based interactive shell (for Linux) and CLI (for Windows) without a need for a bastion host or allowing inbound firewall ports such as SSH 22. Enabling session manager gives an advantage for the security engineer. First, AWS IAM policies control user access and enforce access conditions, such as MFA and connection from specific source IP addresses. Second, CloudTrail records the activities. Third, it reduces the attack surface of the EC2 instances.

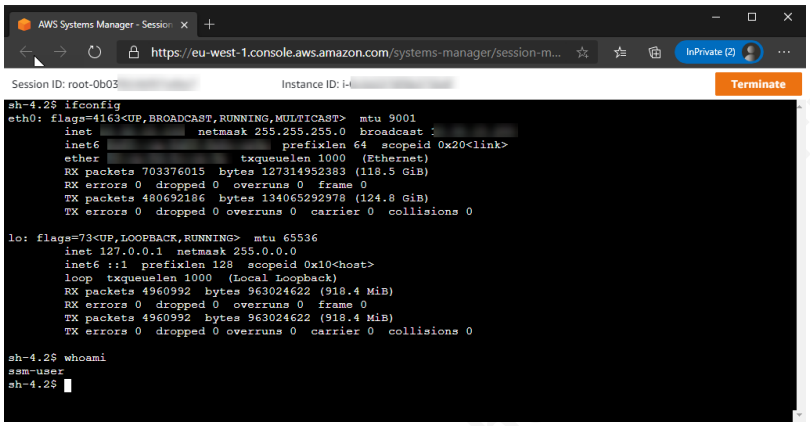


Figure 18: Systems Manager Session Manager

5.4.6. AWS System Automation

Automation is like Run Command in executing commands on a server without a need for interactive logging; however, SSM Automation takes it to the next level, from running a single step command/script to a multi-steps' automation playbook. It helps automate repetitive multi-step tasks such as evidence collection in the incident response process. For instance, a security engineer can use SSM Automation to create a playbook to; isolate the EC2 instance, take a snapshot, store it in a specific Amazon S3 bucket, and then terminate the instance.

5.5. Secure Baseline Configuration

A secure baseline configuration means having a balanced starting point for the system with its required components to operate and proper security controls. In building a secure baseline configuration, the security engineer usually builds a golden image containing the operating system with the latest updates, patches, core applications, and other typical administrative tasks. The system administrator can then take it from there to install any add-ons required according to each user profile or business group.

In AWS, there are multiple options to build a secure baseline configuration, and it depends on where an organization wants to go. For instance, if the target for a secure baseline configuration is a hardened version of the operating system, then a prehardened OS-image on the AWS marketplace is a good starting point. A security engineer can save time and select from hundreds of hardened images on AWS Marketplace, including images by Center of Internet Security (CIS) for different operating systems pre-configured according to the CIS benchmark (AWS, CIS AMIs, 2020).

Sherif Talaat, sherif.talaat@hotmail.com

A secure baseline for other organizations may require customization like changing a particular security configuration to meet an application's needs or installing software like an EDR agent. In that scenario, EC2 Image Builder would be of great benefit. Usually, building and maintaining golden images is a cumbersome process. The engineer in charge will have to boot it up periodically to install new patches, software updates, fix the configurations, and so on.

EC2 Image Builder simplifies that process. Instead of building a static image that requires manual maintenance, it creates a pipeline (workflow) to customize all steps of building a golden image. For instance, it can make a pipeline that runs weekly to produce an image. The pipeline will start from selecting a base operating system image; this could be Amazon EC2 AMI or on-premises VM formats (VHDX, VMDK, and OVF). The pipeline can always choose the latest available OS version. Then, define a different component installed on the image, such as Amazon CloudWatch agent and the latest Windows updates. After that, the EC2 Image Builder can run some validations such as successful reboot test, network connectivity, performing CIS security assessment (AWS, EC2 Image Builder, 2020).

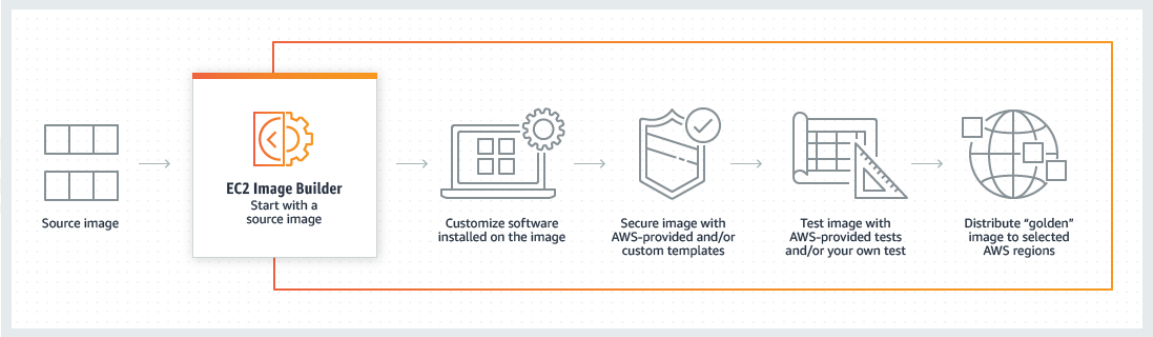


Figure 19: EC2 image builder - how it works (AWS, EC2 Image Builder, 2020)

Furthermore, it defines AWS infrastructure configuration elements like IAM roles, EC2 instance type, VPC, subnet, security group, and key pairs. Finally, the pipeline will store the image on S3 after the completion of the process.

6. Continuous Monitoring & Automation

6.1. Automated security assessment

Conducting a scheduled vulnerability assessment is a cornerstone of a continuous monitoring strategy. It is even one of the checklist items for compliance certifications such as PCI DSS, requiring constant vulnerability assessment and remediation.

Amazon Inspector is a security assessment service that helps find vulnerabilities and security misconfigurations through a set of pre-defined configurations known as assessment template. Each assessment template contains rules packages that define how Amazon Inspector should evaluate the assessment target – EC2 instance (AWS, Amazon Inspector rules, 2020). Based on the assessment template the security engineer chooses, some assessments are agentless and do not require an Inspector agent on the target. Till the moment of writing this paper, Amazon Inspector has the four rules packages.

6.1.1. Network reachability

The rules in this package analyze the network configurations to find security flaws and misconfigurations that could lead to EC2 instances getting exposed. It automates monitoring and assessing the different AWS networking components such as VPC, subnets, security groups, NACLs, route tables, load balancers, and internet gateways.

Unlike other rules packages, the Network Reachability rule package is agentless, making it an excellent non-intrusive network scanner. That said, if the Amazon Inspector agent exists on the target, it provides more information. For example, without the agent, Amazon Inspector would tell that a specific EC2 instance is reachable from the entire internet range (0.0.0.0/0) on port 22. However, if the agent in place, the finding would tell which process is listening on that port.

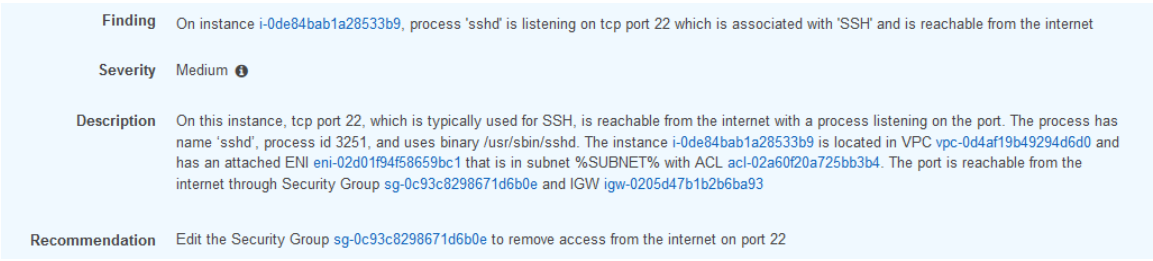


Figure 20: Amazon Inspector - finding sample

6.1.2. Common vulnerability and exposures (CVEs)

As the name indicates, this rules package scans the target EC2 instances to verify if they are subject to a known CVEs, the source of the CVEs is MITER organization (https://cve.mitre.org)

6.1.3. Center for Internet Security (CIS) benchmarks

This rules package assesses the target EC2 instances according to the CIS security benchmarks. It has different benchmarks for the various version of Windows Server and Linux distributions.

6.1.4. Security best practice

The number of rules in this package is minimal compared to other rules, yet it targets medium and high severity issues. It checks for critical system security configuration for Linux, such as root login over SSH, whether ASLR & DEP are enabled or not, and permissions of the system directories.

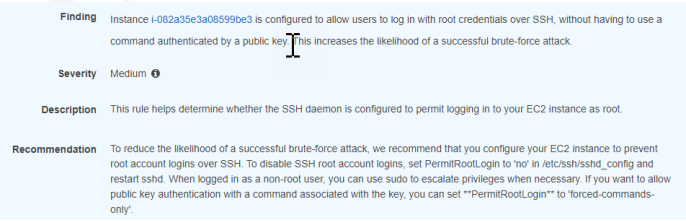


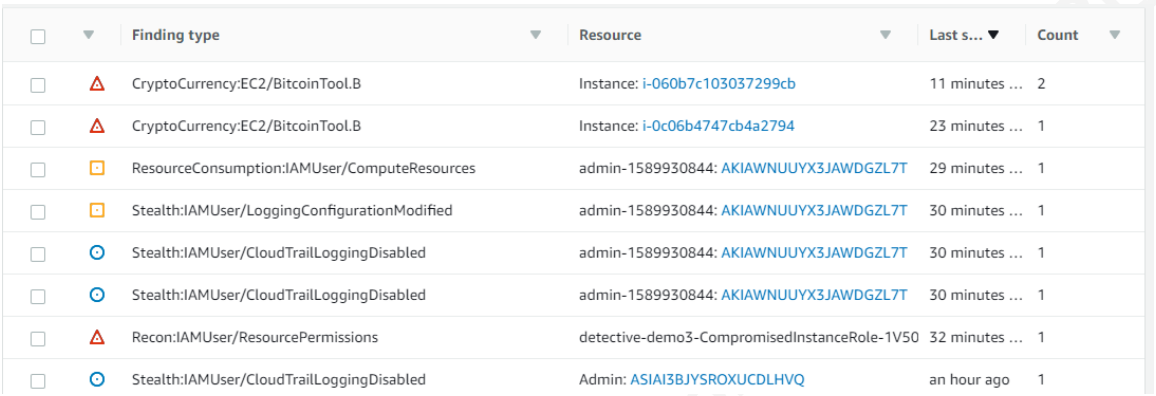
Figure 21: Amazon Inspector - Security Best Practice finding

6.2. Threat detection & investigation

6.2.1. Amazon GuardDuty

Vulnerability assessments can reveal a missing update or security patch, but it cannot tell if a vulnerability got exploited or if the network traffic looks suspicious. It is the job of threat intelligence and threat detection tools that read from different data sources, aggregate information, and look for anomalies to find a threat, which is precisely what Amazon GuardDuty does. GuardDuty is an agentless threat intelligence service. It continuously collects and aggregates events from different data sources, such as AWS CloudTrail, Amazon VPC Flow Logs, and DNS logs. In addition to threat intelligence feeds from AWS and third-party vendors (i.e., CrowdStrike, and Proofpoint) coupled with machine learning to identify malicious activities and unauthorized behaviors (AWS, Amazon GuardDuty, 2020).

Sherif Talaat, sherif.talaat@hotmail.com



Finding type	Resource	Last s...	Count
CryptoCurrency:EC2/BitcoinTool.B	Instance: i-060b7c103037299cb	11 minutes ...	2
CryptoCurrency:EC2/BitcoinTool.B	Instance: i-0c06b4747cb4a2794	23 minutes ...	1
ResourceConsumption:IAMUser/ComputeResources	admin-1589930844: AKIAWNUUYX3JAWDGZL7T	29 minutes ...	1
Stealth:IAMUser/LoggingConfigurationModified	admin-1589930844: AKIAWNUUYX3JAWDGZL7T	30 minutes ...	1
Stealth:IAMUser/CloudTrailLoggingDisabled	admin-1589930844: AKIAWNUUYX3JAWDGZL7T	30 minutes ...	1
Stealth:IAMUser/CloudTrailLoggingDisabled	admin-1589930844: AKIAWNUUYX3JAWDGZL7T	30 minutes ...	1
Recon:IAMUser/ResourcePermissions	detective-demo3-CompromisedInstanceRole-1V50	32 minutes ...	1
Stealth:IAMUser/CloudTrailLoggingDisabled	Admin: ASIAI3BJYSROXUCDLHVQ	an hour ago	1

Figure 22: Amazon GuardDuty Console - Findings sample

GuardDuty can detect various types of threats such as reconnaissance activities, port sweep, brute force, C2 activities, crypto-currency mining, DNS data exfiltration, and other (AWS, GuardDuty finding format, 2020).

6.2.2. Amazon Detective

Once Amazon GuardDuty detects a threat, the security engineer should start the investigation process. Here comes Amazon Detective into the picture to help with triage security findings, incident investigation, and threat hunting.

Like Amazon GuardDuty, Amazon Detective reads events from multiple sources, including GuardDuty itself, to visualize all details and put a context for a specific identified threat and activity related to the finding to identify the root cause.

For instance, if an account is compromised, Amazon Detective can help the security engineer answer questions like; when that happened? what are the findings associated with that account? What are the successful activities completed by the account after the compromise? What activities tried to achieve but failed to do?

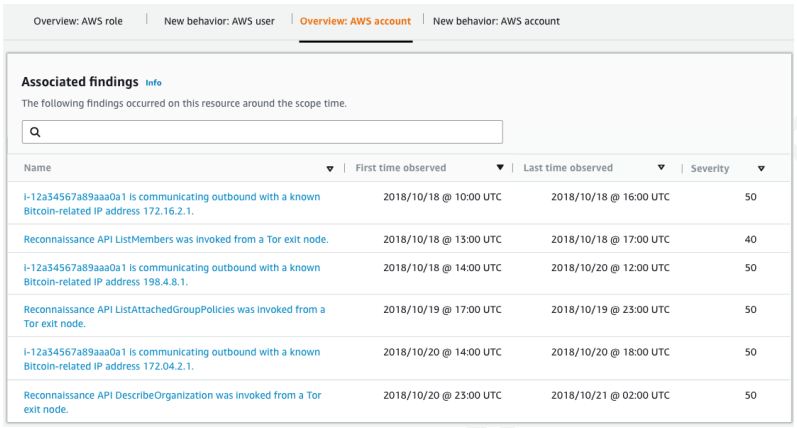


Figure 23: Amazon Detective

6.3. Continuous Compliance Checks

Compliance is usually looking after what is running on servers like operating systems, applications, and databases. When running on the cloud, the compliance should include the AWS account itself as a control plane for the entire infrastructure. As an example, CIS has a security benchmark for AWS, similar to what it has for the different operating systems (CIS, 2020). For instance, system engineers should configure and enforce password policies via AWS IAM, similar to what Active Directory does to Windows user accounts. Another example is enabling audit logs on AWS accounts similar to the operating system and applications, and the list goes on.

6.3.1. AWS Config

AWS Config is a service that allows continuous monitoring and evaluation of AWS resources'. It ensures the configuration's compliance according to an industry-standard such as the CIS security benchmark or a customized corporate security standard.

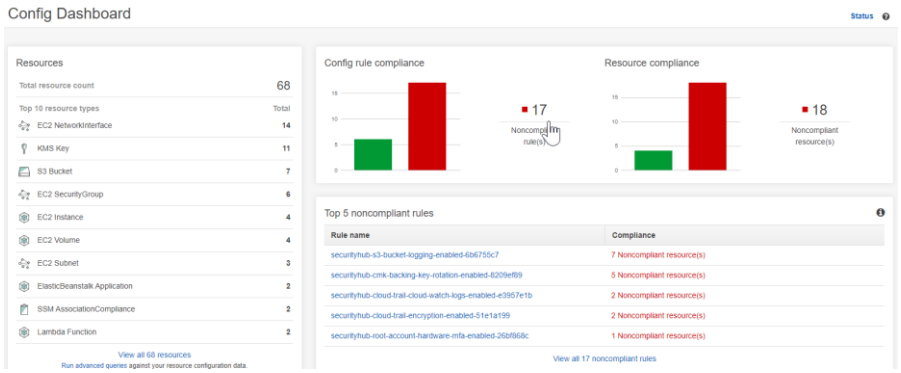


Figure 24: AWS Config dashboard

Additionally, AWS Config records the configurations' changes so it can be easy to spot the deviation from the baseline – what exactly has changed and when - which helps aid the troubleshooting and recovery phase. Moreover, AWS Config can automatically remediate the non-compliant resources and put them back into compliance. For example, a compliance policy requires that CloudTrail must be enabled. Suppose it gets disabled for any reason or a new AWS account in the organization created without enabling CloudTrail. In that case, Config will automatically put the account in a non-compliant state, send an alert to the concerned team (i.e., SOC), or trigger a Lambda function to remediate the issue automatically.

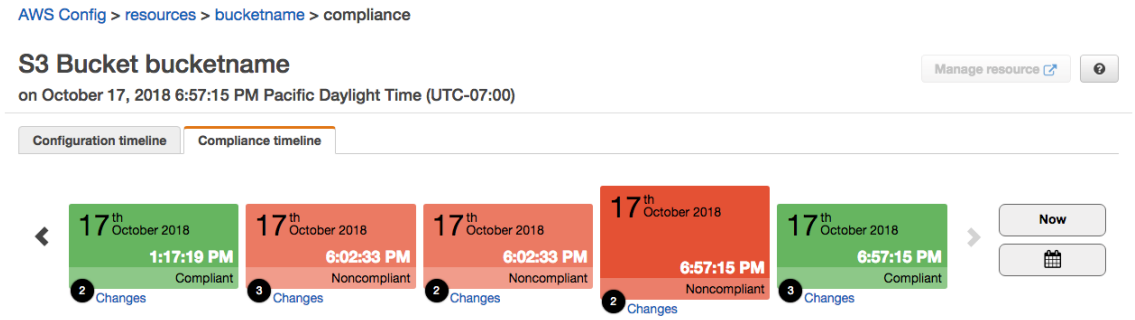


Figure 25: AWS Config - Compliance timeline

Security engineers can create different Config rules for various compliance checks. Nevertheless, it does not sound practical when implementing a compliance check for industry standards like PCI DSS, NIST CSF, HIPAA. For this purpose, Conformance Packs come in handy.

Conformance Packs in AWS Config are like Rules Packages in Amazon Inspector. A conformance pack is a single package that contains a set of compliance evaluation rules and remediation actions. There are many of them available for different industry standards, compliance certifications, and security best practices. For example, there is a conformance pack for "**Operational Best Practice for NIST CSF**" which contains multiple Config rules, each related to one or more NIST CSF controls (AWS, Conformance Packs, 2020).

6.3.2. AWS Audit Manager

While AWS Config helps make sure technical controls are in place to meet the compliance requirement, AWS Audit Manager helps find the evidence on the existence

of those controls. Auditors and compliance officers need to prove that an application or service meets a specific compliance requirement and controls are in place, which is a time consuming – and usually manual – efforts.

AWS Audit Manager can continuously monitor the AWS resources, assess them according to specific compliance requirements, collect the required evidence on the adequate controls, and then export the results in an audit-friendly report (AWS, AWS Audit Manager, 2020).

6.4. Centralized Monitoring

No one tool fits all needs, especially when it comes to security. Most of the security tools have a separate console to configure it and navigate through their findings. Moving back and forth between consoles is inconvenient and slows down the efforts of the security engineers.

AWS Security Hub ingests findings and alerts from AWS services such as Firewall Manager, IAM Access Analyzer, GuardDuty, Inspector, and third-party tools like Alert Logic SIEMless FireEye Helix, Rapid7, and many others. It provides a single consolidate view of all the security findings across different services and AWS accounts within the organization (AWS, AWS Security Hub, 2020).

Figure 26: AWS Security Hub - How it works (AWS, AWS Security Hub, 2020)

It visualizes the findings using dashboards and insights, so it is easier for the security engineer to find resources with the most critical results or instances that do not meet security best practices. Also, it can set to take action based on pre-defined playbooks.

Furthermore, because it contains data from different security services, it can evaluate the entire environment's security posture against specific standards such as AWS Security Best Practice and CIS AWS Foundations Benchmark.

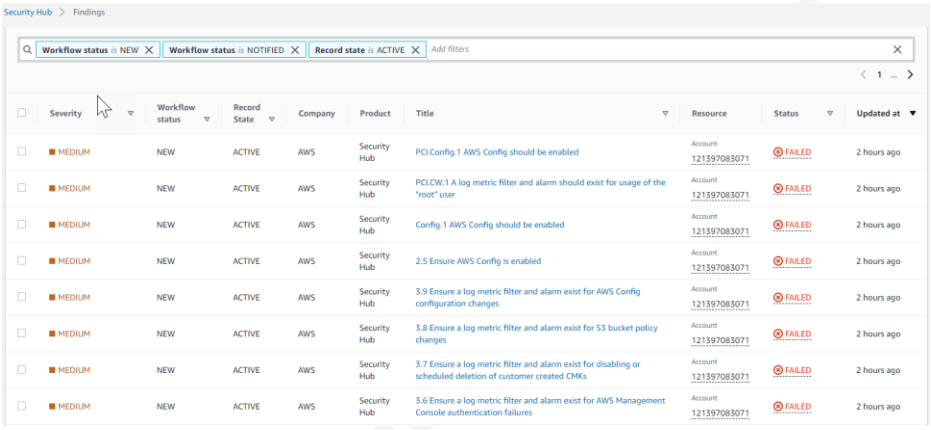


Figure 27: Security Hub - Findings sample

AWS solutions library offers an automated response and remediation solution with a pre-defined remediation playbook (AWS, AWS Security Hub Automated Response and Remediation, 2020). This solution can serve as a starting point for getting started with AWS Security Hub.

Another approach to centralize and visualize the thousands of events the different services generate is ELK (Elasticsearch, Logstash, and Kibana) stack. It is prevalent among the information security community. A famous example of ELK implementation is Security Onion and SANS SOF-ELK VMs, and the only difference is that AWS ELK is a Software-as-a-Service (SaaS), not a VM. The following screenshot demonstrates the AWS WAF dashboard example built with ELK (AWS, AWS WAF Dashboard, 2020).

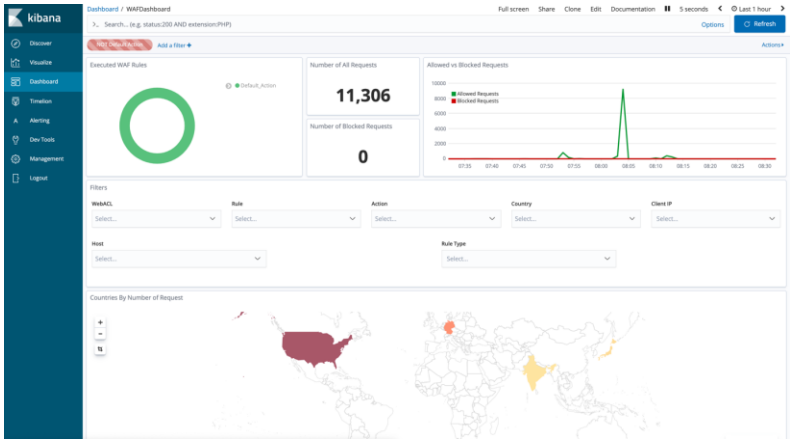


Figure 28: AWS WAF Dashboard

Sherif Talaat, sherif.talaat@hotmail.com

The AWS solutions library has a Centralized Logging solution that is worth checking. It collects, analyzes, and visualizes the logs from Amazon CloudWatch in a single dashboard powered by Kibana.

6.5. Scripting and Automation

Most of the AWS security services discussed in this paper have built-in automation to some extent to continuously running assessment & security checks, collecting information, and consolidating results. These services can take action, but very few (and in specific cases) have pre-configured actions. The point is that the action varies from case to case and from one organization to another. So the action is left to the person in charge to decide, and here comes the advantage of having some scripting skill.

With services like Systems Manager Run Command and Systems Manager Automation, a security engineer can run a script or trigger a workflow to complete a specific task, but this is not fully automated since it has human interaction.

In AWS, the full automation approach is finding the event, sending an alarm or notification, and then triggering a remediation action (AWS, security response automation on AWS, 2019).

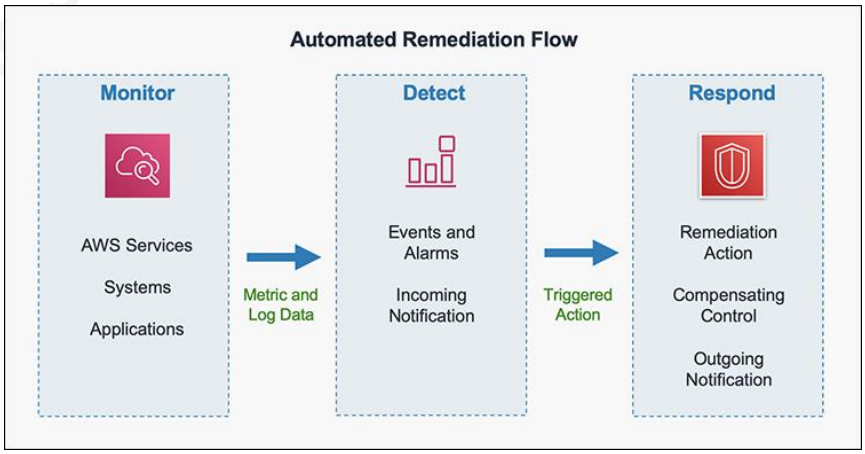


Figure 29: Automated Remediation Flow (AWS, security response automation on AWS, 2019)

AWS CloudTrail and Amazon EventBridge (formerly, CloudWatch Events) play a significant role in that process. Almost every AWS services integrate with CloudWatch to trigger a CloudWatch Event, which can invoke an action based on an event pattern or a specific schedule. Even if the service does not integrate with CloudWatch, its events still are captured by CloudTrail, which integrates with CloudWatch.

The action could be a built-in pre-defined action like when a server stops responding, CloudWatch Events can invoke the EC2 *RebootInstances* API to reboot the EC2 instance. Also, the action can be custom as well. For instance, based on Amazon Inspector finding, CloudWatch Event can invoke Systems Manager Run Command, Systems Manager Automation runbook, or even a Lambda function.

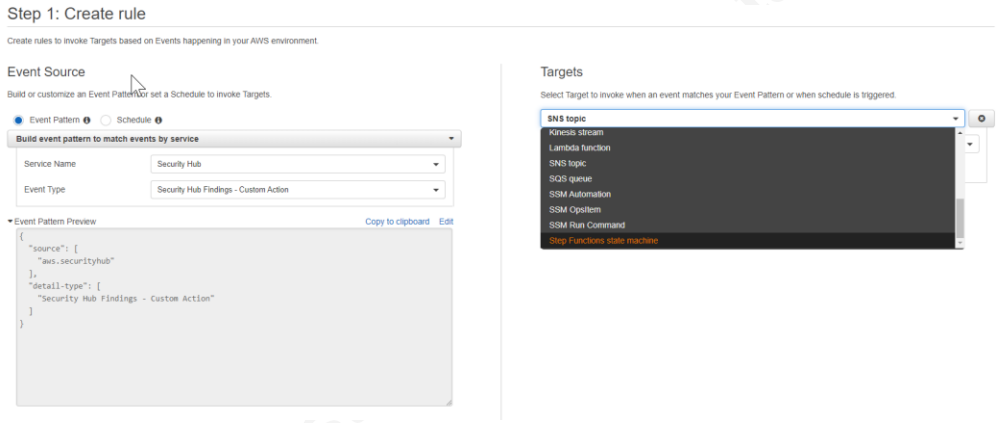


Figure 30: CloudWatch Events - Create an event rule

The preceding figure shows a window for creating the CloudWatch event rule for AWS Security Hub events. Like any AWS resource, the rule has an Amazon resource name (ARN), a unique identified. Later, within the Security Hub console itself, the ARN for the event rule is linked to a custom action. The security engineer can quickly respond to findings with a few clicks without leaving the security hub console.

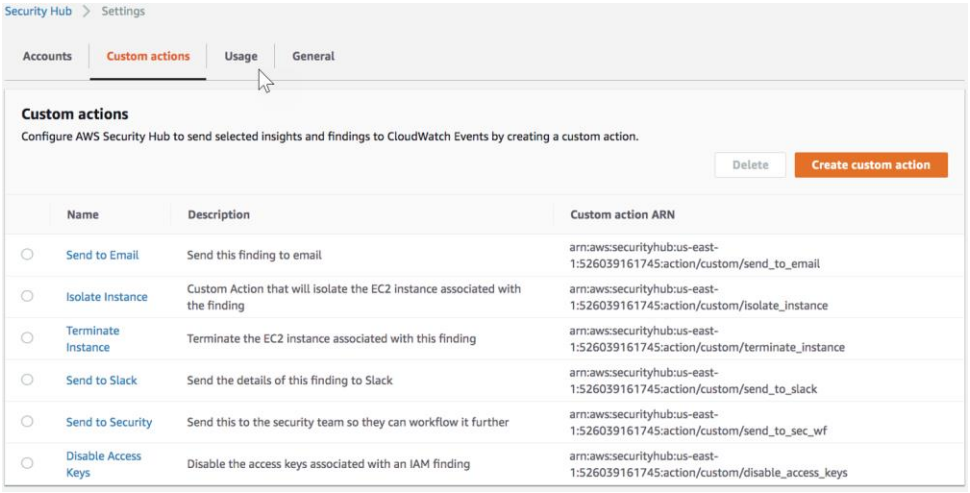


Figure 31: Security Hub - Custom actions

7. Conclusion

Cloud pace of innovation is swift compared to on-premises technologies. For instance, AWS offers more than 175 services; each comes with lots of features. This wide range of services is hard to cope with, especially for third-party solutions providers. It requires a third-party vendor to update a solution to understand and deal with a new service/feature, which takes some time. Here comes the advantage of using a native security service that is built-in the platform.

When AWS releases a new service, it provides proper security controls and integration with the other services on the platform. The service would at least integrate with AWS IAM for permissions and access controls, integrate with CloudWatch for monitoring and alerting, and integrate with CloudTrail for auditing. That native integration ensures that the security engineers have the tools to security, monitor, and protect any AWS workload without dependency on third-party tools in most cases. On the contrary, third-party solutions rely on native services such as CloudTrail to monitor and track the platform's activities.

There has been an undeclared agreement that native services -especially free ones – are not efficient, and it is better to use a solution from a specialized third-party vendor. This paper spot the lights on different AWS native managed security services and how they would fit into the security landscape. By implementing those services, organizations can; 1) have better visibility and security posture of the workloads on the cloud. 2) reduce operations complexity. 3) optimize the cost by eliminating unnecessary duplicate third-party controls.

References

AWS. (2019, November 26). *security response automation on AWS*. Retrieved from AWS Security Blog: https://aws.amazon.com/blogs/security/how-get-started-security-response-automation-aws/

AWS. (2020). *Amazon GuardDuty*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://aws.amazon.com/guardduty/features/

AWS. (2020). *Amazon Inspector rules packages and rules*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://docs.aws.amazon.com/inspector/latest/userguide/inspector_rule-packages.html

AWS. (2020). *AWS Audit Manager*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://aws.amazon.com/audit-manager/

AWS. (2020). *AWS Firewall Manager*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://docs.aws.amazon.com/waf/latest/developerguide/fms-chapter.html

AWS. (2020). *AWS Network Firewall*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://aws.amazon.com/blogs/aws/aws-network-firewall-new-managed-firewall-service-in-vpc/

AWS. (2020). *AWS Network Firewall partners*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://aws.amazon.com/network-firewall/partners/

AWS. (2020). *AWS Organizations*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://aws.amazon.com/organizations/

AWS. (2020). *AWS Security Hub*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://aws.amazon.com/security-hub/

AWS. (2020). *AWS Security Hub Automated Response and Remediation*. Retrieved from AWS Solutions: https://aws.amazon.com/solutions/implementations/aws-security-hub-automated-response-and-remediation/

AWS. (2020). *AWS Shield Features*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://aws.amazon.com/shield/features/

AWS. (2020). *AWS WAF Dashboard*. Retrieved from AWS Security Blog: https://aws.amazon.com/blogs/security/deploy-dashboard-for-aws-waf-minimal-effort/

AWS. (2020). *AWS WAF Security Automations*. Retrieved from AWS Solutions: https://aws.amazon.com/solutions/implementations/aws-waf-security-automations/

AWS. (2020). *CIS AMIs*. Retrieved from AWS Marketplace: https://aws.amazon.com/marketplace/search/results?x=0&y=0&searchTerms=cis

AWS. (2020). *CloudWatch Agent*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Install-CloudWatch-Agent.html

AWS. (2020). *Conformance Packs*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://docs.aws.amazon.com/config/latest/developerguide/conformance-packs.html

AWS. (2020). *EC2 Image Builder*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://aws.amazon.com/image-builder/

AWS. (2020). *Egress-only internet gateways*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html

AWS. (2020). *Getting credential reports for your AWS account*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html

AWS. (2020). *GuardDuty finding format*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-format.html

AWS. (2020). *How Access Analyzer works*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services:

https://docs.aws.amazon.com/IAM/latest/UserGuide/access-analyzer-concepts.html

AWS. (2020). *Internet gateways*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html

AWS. (2020). *Logical Separation on AWS*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://d1.awsstatic.com/whitepapers/compliance/AWS_Logical_Separation_Handbook.pdf

AWS. (2020). *Managed rules for AWS Web Application Firewall*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://aws.amazon.com/marketplace/solutions/security/waf-managed-rules

AWS. (2020). *Network ACLs*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

AWS. (2020). *Regions and Availability Zones*. Retrieved from Regions and Availability Zones

AWS. (2020). *Route tables*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html

AWS. (2020). *Security groups for your VPC*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html#VPCSecurityGroups

AWS. (2020). *Shared Responsibility Model*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://aws.amazon.com/compliance/shared-responsibility-model/

AWS. (2020). *Traffic Mirroring and VPC Flow Logs*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://docs.aws.amazon.com/vpc/latest/mirroring/flow-log.html

AWS. (2020). *Traffic Mirroring concepts*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://docs.aws.amazon.com/vpc/latest/mirroring/what-is-traffic-mirroring.html

AWS. (2020). *Validating CloudTrail Log File Integrity*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html

AWS. (2020). *VPC endpoints*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html

AWS. (2020). *VPC Flow Logs*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html

AWS. (2020). *VPC Flow Logs - Custom format*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html#flow-logs-fields

AWS. (2020). *What Is Amazon CloudWatch Logs?* Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html

AWS. (2020). *What is VPC Reachability Analyzer?* Retrieved from https://docs.aws.amazon.com/vpc/latest/reachability/what-is-reachability-analyzer.html

AWS. (2020). *Working with open-source tools for Traffic Mirroring*. Retrieved from Amazon Web Services (AWS) - Cloud Computing Services: https://docs.aws.amazon.com/vpc/latest/mirroring/tm-example-open-source.html

CIS. (2020). *Securing Amazon Web Services*. Retrieved from CIS Benchmarks: https://www.cisecurity.org/benchmark/amazon_web_services/

IDG. (2020, 08 06). *2020 Cloud Computing Study*. Retrieved from IDG: https://www.idg.com/tools-for-marketers/2020-cloud-computing-study/

Nicholson, R. (2020, November 20). *AWS Network Firewall: More Than Just Layer 4*. Retrieved from SANS Institute: https://www.sans.org/blog/aws-network-firewall-more-than-just-layer-4/

Pescatore, J. (2018, April 25). *You Can't Secure What You Can't See*. Retrieved from SANS Webcasts: https://www.sans.org/webcasts/cant-secure-cant-importance-visibility-cloud-107600

Porter, J. (2020, June 18). *Amazon says it mitigated the largest DDoS attack ever recorded*. Retrieved from The Verge: https://www.theverge.com/2020/6/18/21295337/amazon-aws-biggest-ddos-attack-ever-2-3-tbps-shield-github-netscout-arbor

Venezia, P. (204, June 23). *Murder in the Amazon cloud*. Retrieved from InfoWorld: https://www.infoworld.com/article/2608076/murder-in-the-amazon-cloud.html