Author: Balamurugan

Version: 1.0

**AWS -GuardDuty**

Amazon GuardDuty protects our Aws accounts and resources against Threat attacks.

It is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and helps to fix it.

It uses Machine Learning concept to automatically detects the Threats.

It supports AWS CloudWatch Events to push the notifications and trigger the lambda function for automatic remediation

It guards:

* S3
* Container workloads
* Instance workloads
* Accounts and Users

**UseCases:**

S3: Guard unusual data access in S3, API calls from malicious IP addresses.

EC2: Detects if unknown user trying to access EC2 console via SSH

Accounts: Continuously monitors the accounts and reports quickly if any unknown user trying to access AWS console.

Companies uses GuardDuty:

* CROSSBRIDGE
* APPSFLYER
* SWISSPOST

**AFM -AWS Firewall Manager**

**Similar company : Akamai 3rd party also provides same service**

It is a security management service.

It allows you to configure and manage a Firewall rules centrally for your various accounts and applications.

Single service to build firewall rules, create security policies to your entire infrastructure.

With this AFM- we can create a WAF [Web Application Firewall] rules for Application Load Balancers, API Gateways, and Amazon CloudFront distributions.

AWS Shield is advanced protections for your ALB, ELB Classic Load Balancers, Elastic IP Addresses and CloudFront distributions.

**WebApplication Threats:**

* Application Vulnerabilities
* HTTP floods
* Bots and Scrappers

**Challenges faced by customers**:

* Large no. of resources and accounts – Hard to manage security policies
* Large org creates new application all the time – Hard to ensure that new application is secured from day 1
* No central single place to monitor and apply if any threat is coming to application/organization
* For eg. Multiple scrappers loading our site with 1000s of HTTP requests from different Ips. We should identify the IP range and blacklist those Ips

AWS Firewall Manager helps to write WAF rules to achieve and overcome the above challenges.

AWS WAF applies on application layer/ HTTP layer of our website.

AWS WAF provides:

* Web traffic filters with custom rules
* Managed rules to block the malicious requests
* Active monitoring and tuning the rules

**AFM Key Benefits:**

FW policies applies across all the AWS accounts

Easily block the malicious requests from across the world automatically.

Hierarchical rule enforcement

Receive notifications from SNS for non-compliance events

Components associated with AWS Firewall Manager:

* TrendMicro
* F5
* iMPERVA
* Trustwave

**WorkFlow of AFM automation using GuardDuty**

**GuardDuty**

Lambda Func

CloudWatch

AWS WAF

FW Manager

ACC 1

ACC 2

Pre-Requisites for AFM:

1. Enable AWS organizations full Features.
2. Enable AWS config records in all accounts
3. Make an account as Firewall manager Admin

Steps:

* Security Admin : Create RuleGroup (or) Subscribe to managed RuleGroup from AWS.
* Specify the policy scope: applies to all ALBs or CloudFront or based on Tags of AWS resources
* Create necessary WAF Rules and config for monitoring.

1. Subscribe **RuleGroup** from marketplace: **Cost based**

You can choose F5 rules for WAF or AlertLogic rules

1. Apply RuleGroup across all the accounts:

Goto AWS console 🡪 Firewall Manager 🡪 FW manager policies 🡪 Create policy

Choose existing Rulegroup🡪 choose region 🡪 Name: DemoPolicy

Choose Rulegroup 🡪 AlertLogic or F5

1. Define Policy scope:

Choose ALB where you want to apply this rule. Apply this policy to existing and new resources and save

Now AFM shows all the accounts which are all non-complaint- Reason may be WebACL is not setup for this account

1. set webACL : Goto WebACLs 🡪 Rules 🡪 you can see a new WebACL created with all the ALBs associated with it. Else create new WebACL and add it
2. Now AFM is going to go through all the accounts WebACLs and make it complaint