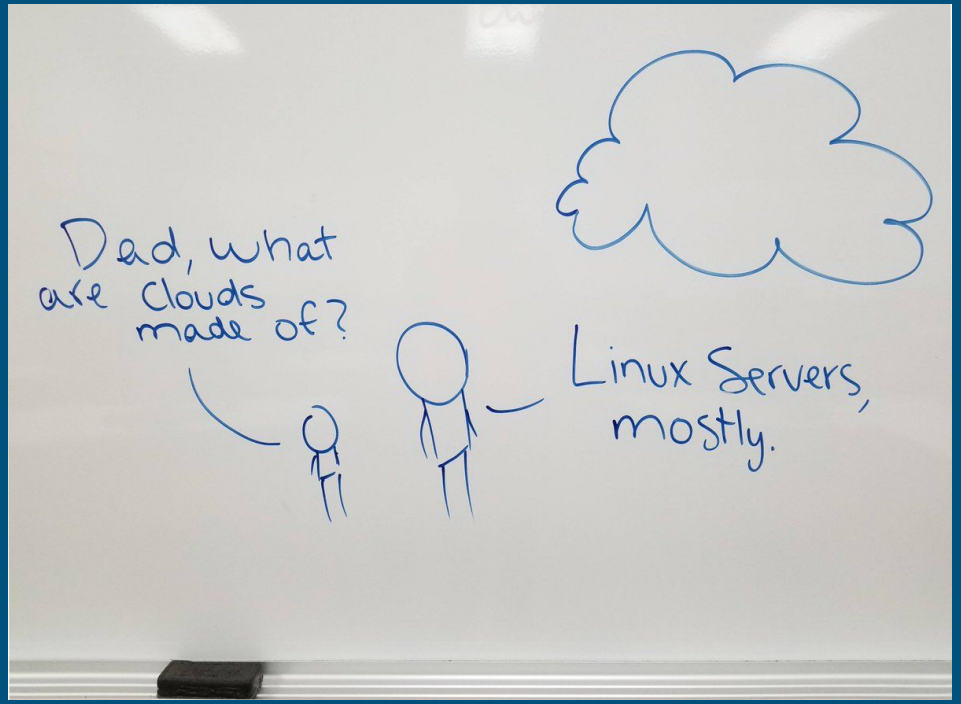
Cloud Security Workshop

amazon web services

What is AWS?

- Don’t feel like getting too in depth with it
- CLOUD PROVIDER
- Essentially borrowing Compute Resources and utilizing them virtually
- IAAS, SAAS, PAAS



Let’s just jump to Security

- Shared Responsibility Model
- IAM
- Inspector
- WAF (Hands Off)
- GuardDuty

FOLLOW ALONG

https://tinyurl.com/CDO-CloudSecurity

Shared Responsibility Model

Amazon is responsible for Security OF the Cloud

You are responsible for Security IN the Cloud

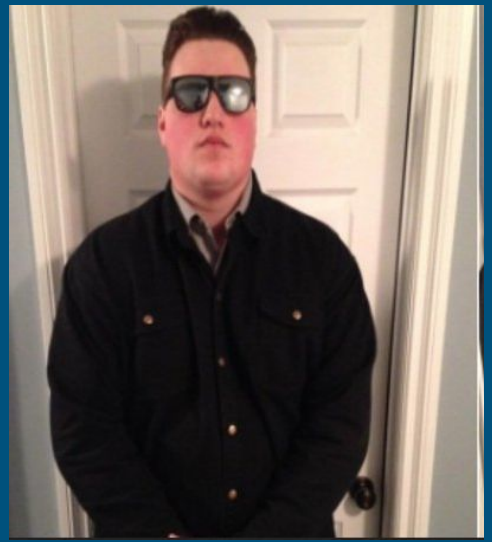
Capital One was hacked big time, blaming the breach on a "firewall misconfiguration."

But Amazon says it is not responsible.

"AWS was not compromised in any way and functioned as designed," the company said in a statement. "The perpetrator gained access through a misconfiguration of the web application and not the underlying cloud-based infrastructure. As Capital One explained clearly in its disclosure, this type of vulnerability is not specific to the cloud."

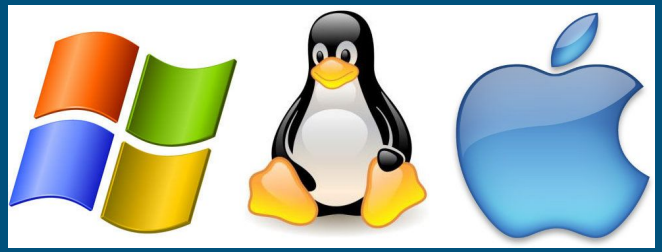
https://application.security/

IAM



AWS's Words: "AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources"

My Words: How people log on, What people are allowed to access, How I see what people are doing



Build Users

- Create an access ID for Cloud Account (**Be Unique**)

-Create a user name “**Jack**”

- Set a password for him

Assigning Permissions

- Give Jack Full Access to Cloud Trail ONLY

Test User Access

-Login as Jack

-Test permissions on services

Roles (Roles vs Users)

An IAM user has permanent long-term credentials and is used to directly interact with AWS services. An IAM role does not have any credentials and cannot make direct requests to AWS services. IAM roles are meant to be assumed by authorized entities, such as IAM users, applications, or an AWS service such as EC2.

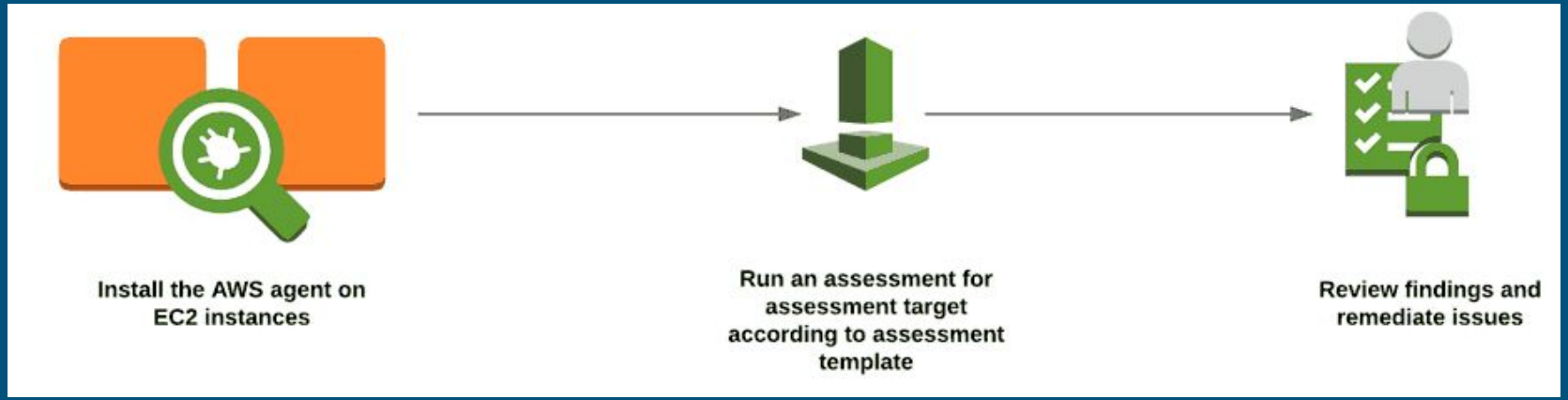
- Create role for EC2 named Inspector and give it full SSM Access (Systems Manager)
- That will allow Commands to be executed remotely from the Cloud on EC2 Machines.

Inspector

AWS's Words: "Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS."

My Words: It's a vulnerability scanner...a compliance scanner...a standards scanner...

Inspector


Install the AWS agent on EC2 instances
Run an assessment for assessment target according to assessment template
Review findings and remediate issues

Build Instances

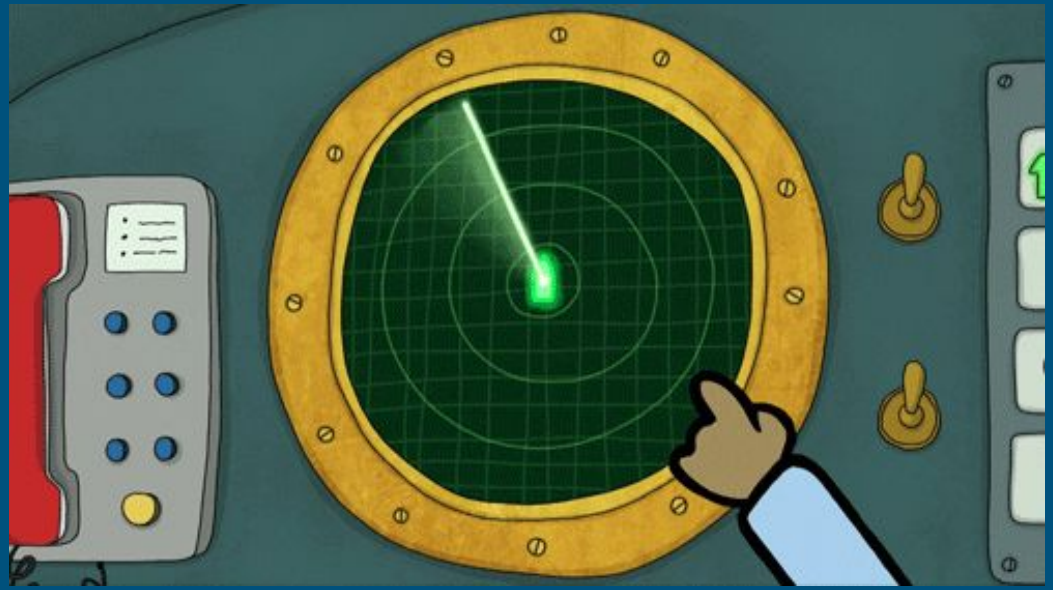
- Spin up an Amazon Instance (EC2 Virtual Computer)
- Allow HTTPS in Security Group
- Connect “Inspector” role to Instance

Begin Scan

-Pick Targets

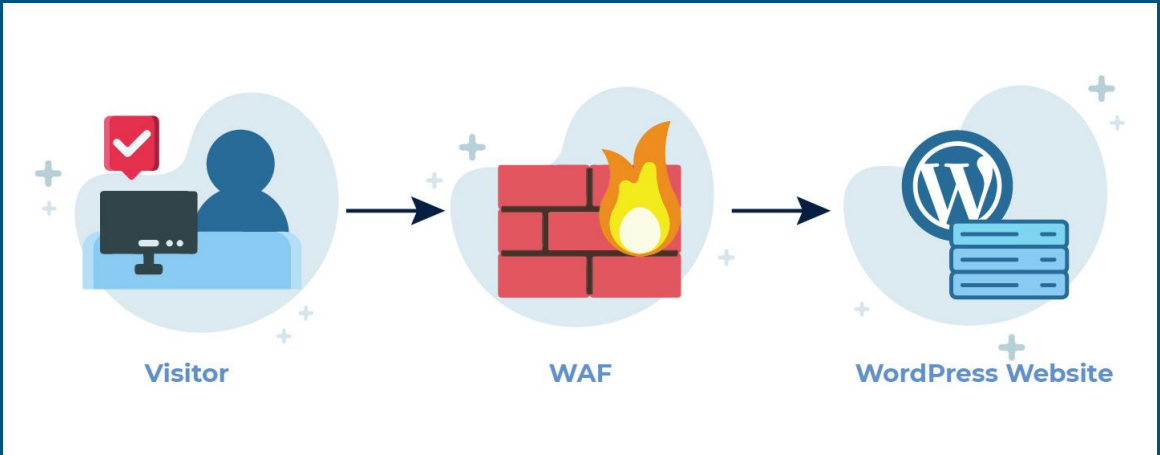
-Specify Template

-Begin Scan



WAF (Web Application Firewall)

AWS's Words: "AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives you control over which traffic to allow or block to your web applications by defining customizable web security rules."



My Words: Web Firewall that applies a set of rules to an HTTP conversation, Operates on the Application Layer, Prevents attacks such as SQL Injection and Cross Site Scripting.

WAF (Web Application Firewall)

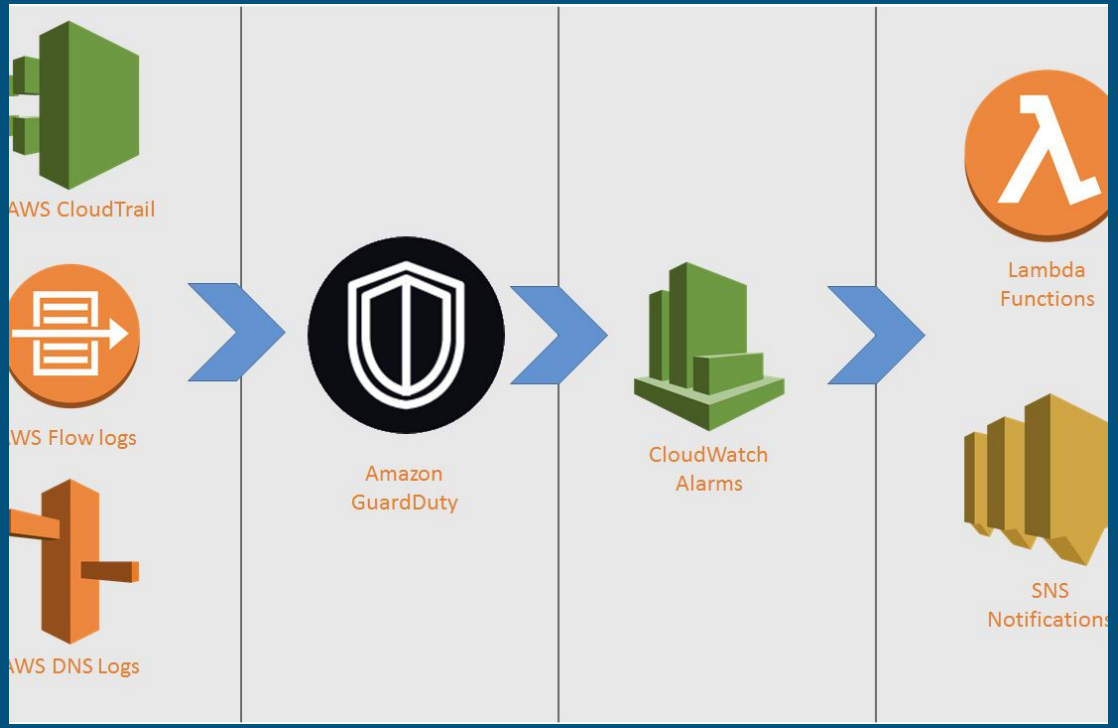
Inspector Results

-See what was returned from the scan

GuardDuty!

AWS'S Words: "Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads"

My Words: It's an Intrusion Detection System for your AWS Environment.

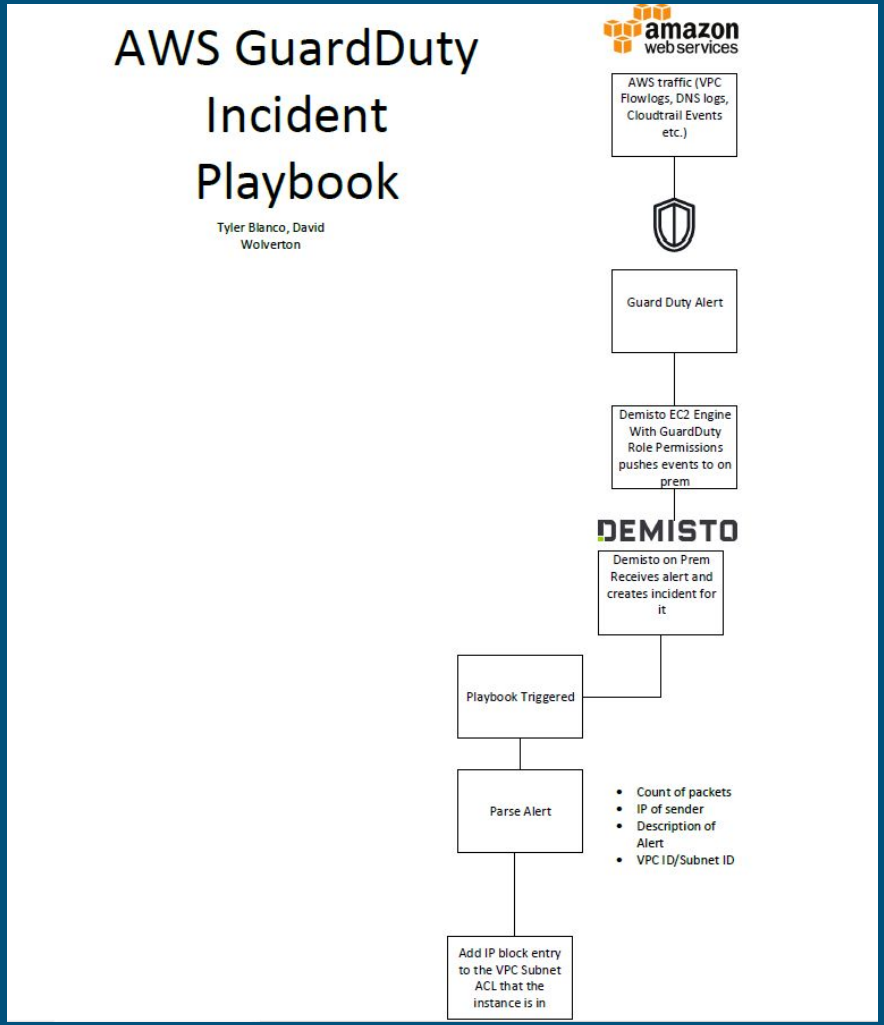


GuardDuty

-Generate Sample Reports

-Look Around!

-My Project



Thank you for coming! (End of Workshop)

Questions?

-Terminate Instances and turn off GuardDuty

News:

Add us on Social Media!

Twitter: **@ualbanyCDO**

Instagram: **ualbany_cdo**

Website: **uacyber.org**

Myinvolvement: **Cyber Defense Org**

We have a discord!