CISCO

You make **possible**

Securing Clouds: Untraditional Defenses

I am in your cloud, hacking

Moses Frost, Multi-Domain Architect Security
@mosesrenegade twitters

BRKSEC-2605

Barcelona | January 27-31, 2020

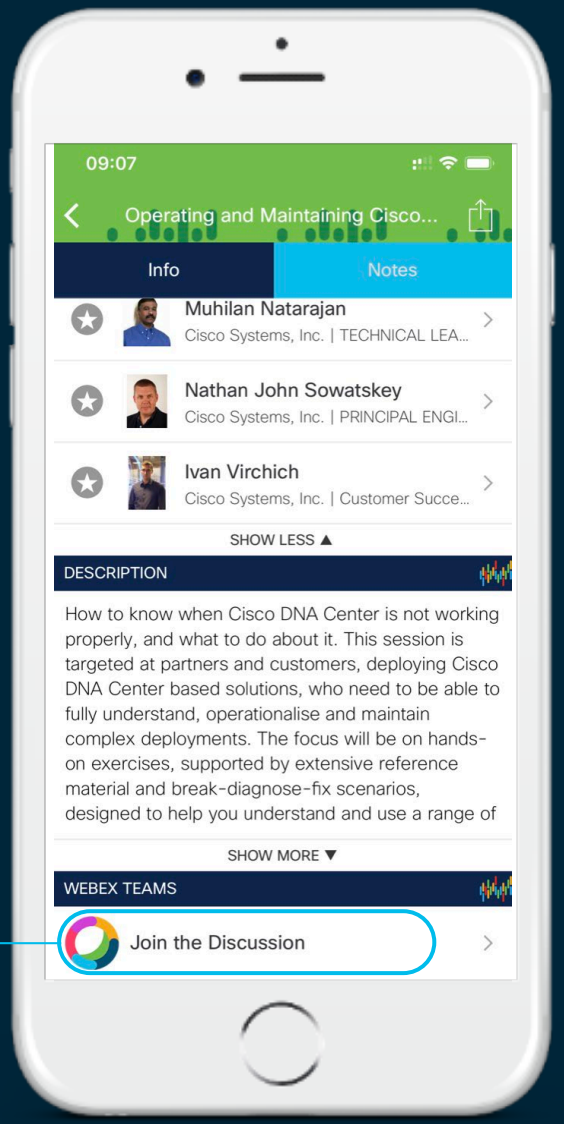
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



cat whoami.json

```
{ “Moses Frost @mosesrenegade on social media”,
   “@ Cisco since 2012, One of the Cyber Threat Defense / CDC
Architects”,
   “Red Teamer, Hacker, Tinkerer, Forensics, Security since the 90’s”,
   “SANS Author / Instructor”,
    “Fun Facts!” [
      “BBS’s in the ‘90s ( Obv/2 )”,
       “Linux Kernel 1.3 (Dev Tree, Because why not)”,
      “Never wants to troubleshoot ISDN again <- no”
  ] }
```

Obligatory

Cuban Descent

From Miami

Agenda

- Traditional Defenses - A Crash Course
- Cloud Crash Course
- hacky hack hack : The Cloud
- Defenses in the Cloud
- Conclusion

Some restrictions

Time: We cannot cover

... All the cloud infrastructures (Azure, GCP, Digital Ocean, Alibaba Cloud, Etc, etc)

... Kubernetes and Services Meshes (Only briefly)

... Microservices and Cloud Native Applications

We would need a week or so ☺

Instead check these out!

Either today, tomorrow, or On-Demand!

*{ "**BRKSEC-2186**": "A MultiCloud Segmentation Journey through Big Data with Tetration",*

*"**BRKSEC-2602**": "Cloud Managed Security Architecture and Design",*

*"**BRKSEC-2382**": "Application Centric and User-Centric Security with Duo",*

*"**BRKSEC-1839**": "Introduction to Application Security and DevSecOps"*

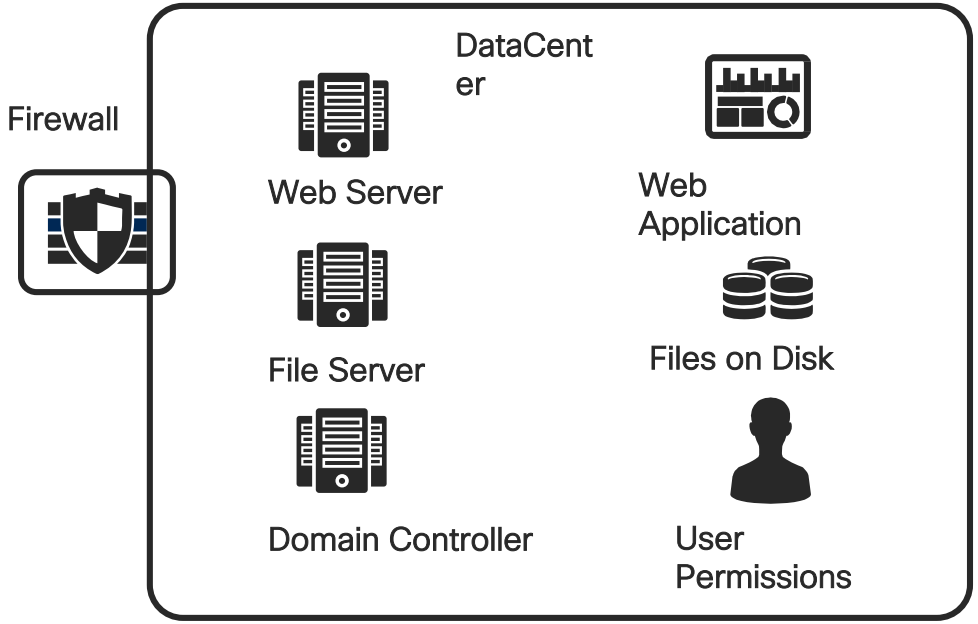
}

Traditional Defenses – Crash Course

What are ‘traditional’ defenses?

Several options

- Network Defenses
  - I need to block ports with a Firewall, Inspect Packets with an IPS, protect users with segmentation
- Server / Systems Defenses
  - ACL on Filesystems
  - User Permissions
  - RBAC
- Application / Database Defenses
  - Secure Coding
  - WAF

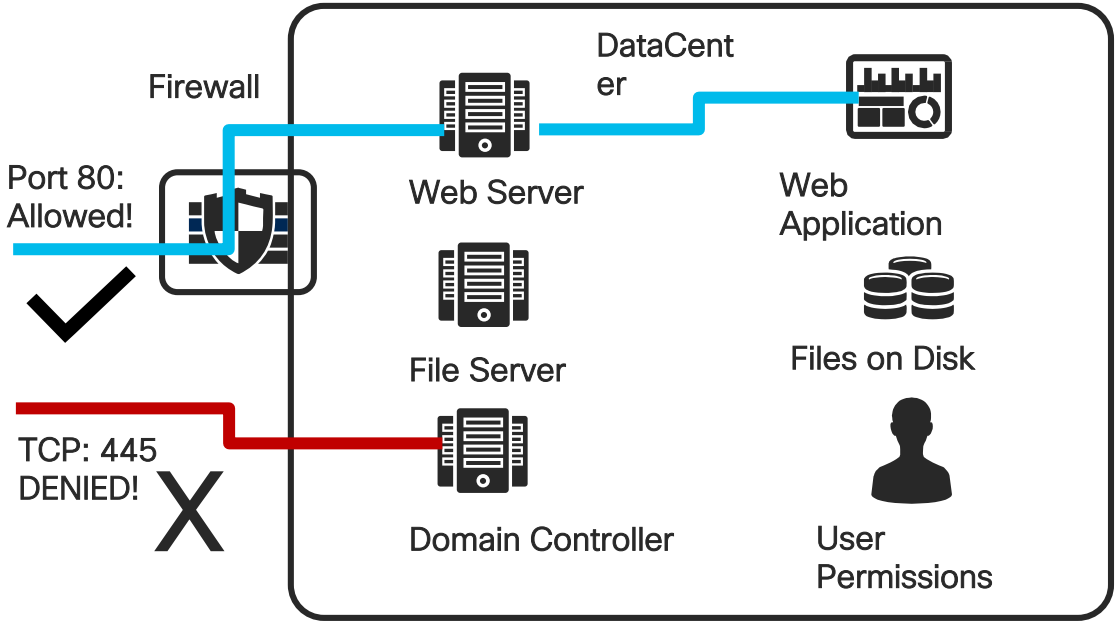


Traditional Defenses – Crash Course

What are ‘traditional’ defenses?

Several options

- **Network Defenses**
  - I need to block ports with a Firewall, Inspect Packets with an IPS, protect users with segmentation
- Server / Systems Defenses
  - ACL on Filesystems
  - User Permissions
  - RBAC
- Application / Database Defenses
  - Secure Coding
  - WAF

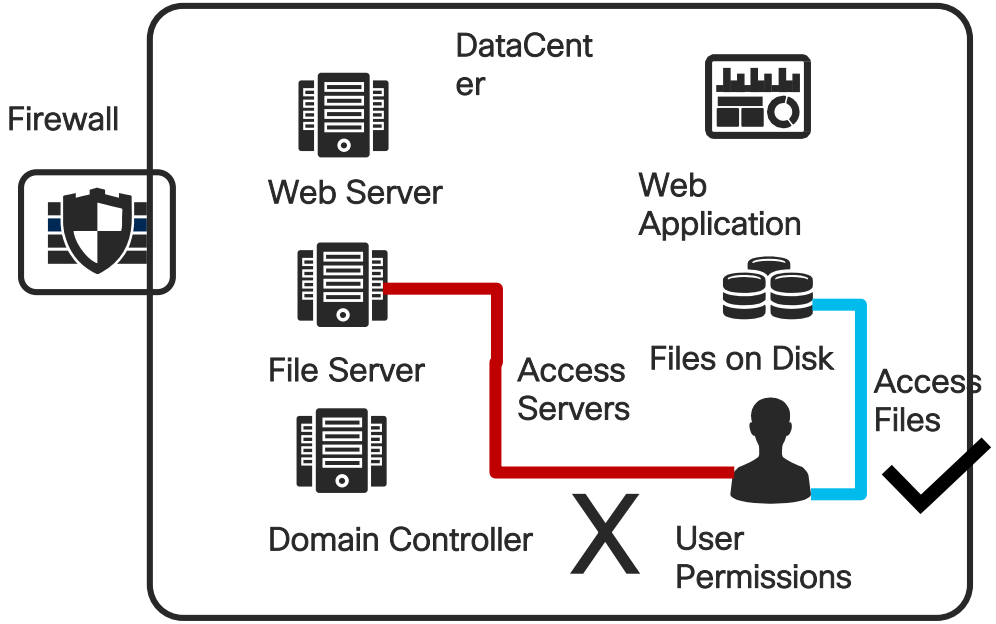


Traditional Defenses – Crash Course

What are ‘traditional’ defenses?

Several options

- Network Defenses
  - I need to block ports with a Firewall, Inspect Packets with an IPS, protect users with segmentation
- Server / Systems Defenses
  - ACL on Filesystems
  - User Permissions
  - RBAC
- Application / Database Defenses
  - Secure Coding
  - WAF

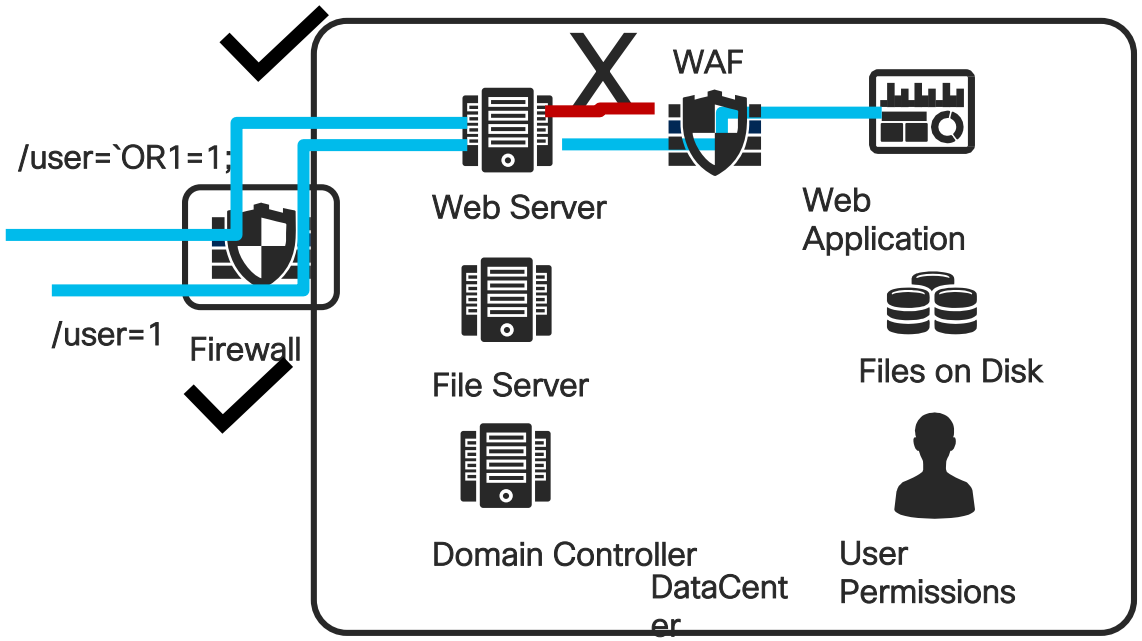


Traditional Defenses – Crash Course

What are ‘traditional’ defenses?

Several options

- **Network Defenses**
  - I need to block ports with a Firewall, Inspect Packets with an IPS, protect users with segmentation
- Server / Systems Defenses
  - ACL on Filesystems
  - User Permissions
  - RBAC
- Application / Database Defenses
  - Secure Coding
  - WAF



Cloud Crash Course

Cloud Architectures a Crash Course

All cloud architectures are the same *but different*

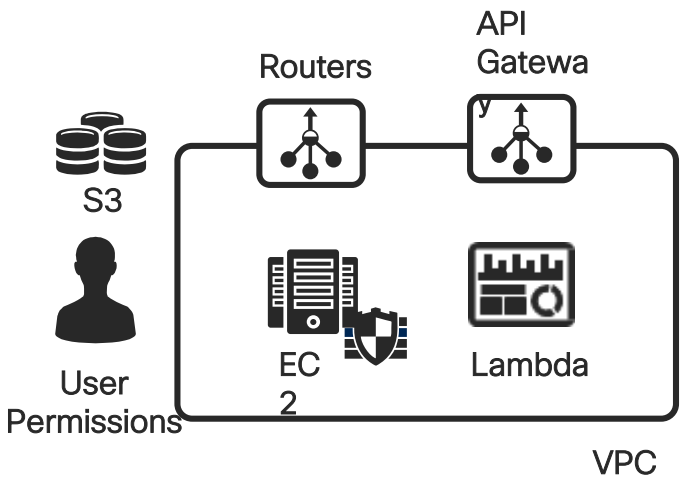
Function	Amazon AWS	Microsoft Azure	Google Cloud
Virtual Machines	EC2, Lightsail	Virtual Machine	Compute
Virtual Private "Networks"	VPC	VPC	VPC
Function as a Service	Lambda	Functions	Functions
Object Store	S3	Blob Storage	Objects
Databases	RDS	Azure SQL	Cloud SQL
Permissions	IAM	AzureAD / Azure Permissions	Google IAM

Cloud Architecture Components

We will focus on a *few* of the cloud services

- Amazon claims it has about 175 services, Azure over 600

We will cover the ones that are ***common***



The mature Cloud Service Providers will have the following services typically available:

AWS S3 or a Object Storage Environment that is not behind a Virtual Public Cloud

Compute or Virtual Machines

Some type of Serverless Environment

There is a permission model on all cloud providers, they all differ

Compute and Networking

Typically Cloud Native Applications cannot rely on the underlying hardware or networking

Considerations that make Cloud Environments Unique:

- Compute can disappear
- Networking and VPCs can suddenly disappear
- Storage can disappear

You *design* your application around this

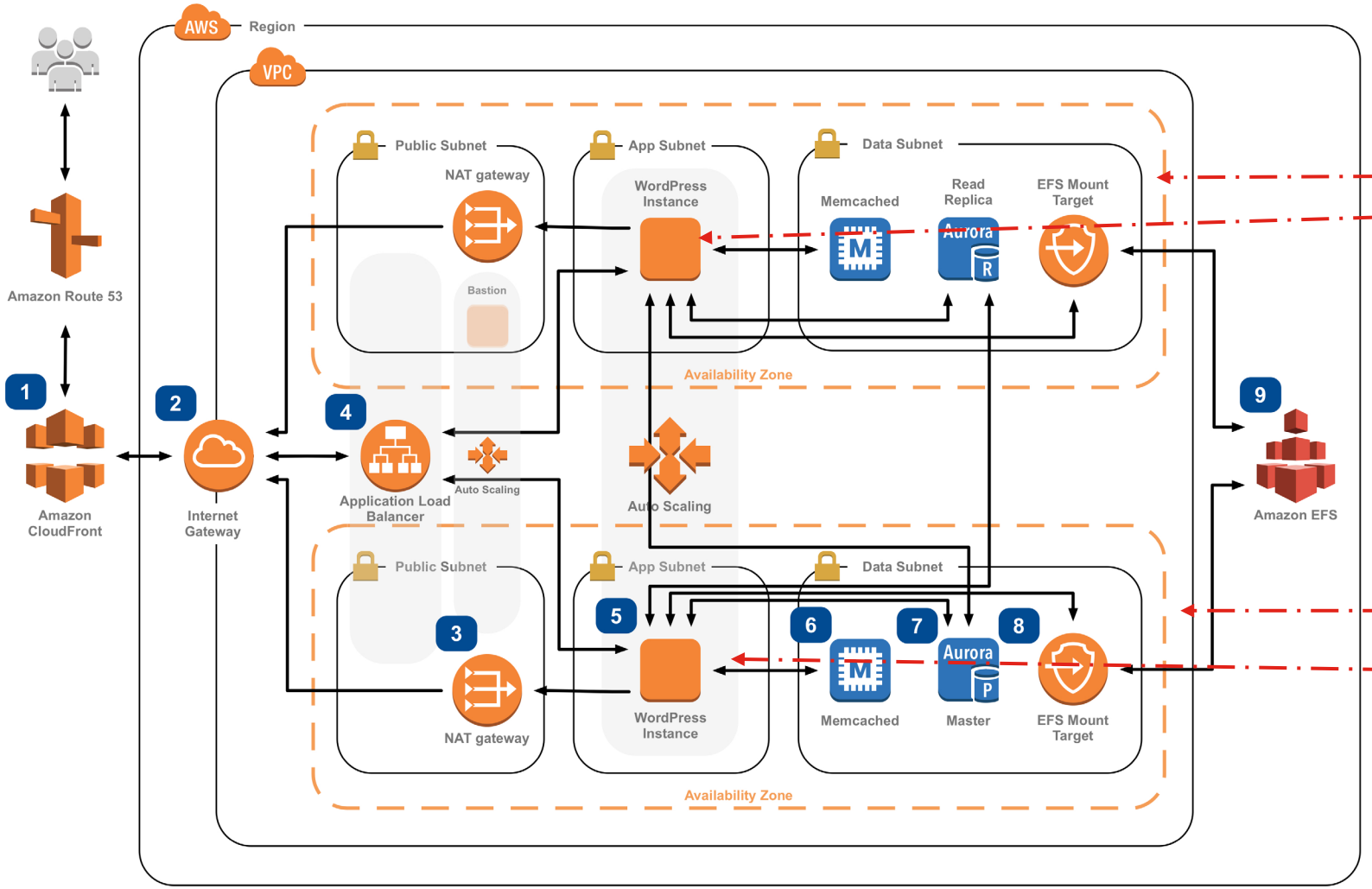
Multiple Availability Zones for

- Compute
- For Databases or Datastorage Nodes
- For AWS S3 buckets (multi-region)

You can interact dynamically with most of these providers

- Scalable Services
- Terraform / Ansible / Cloudformation

Example Architecture for Wordpress*



Network "A" Side
Computer in "A"

Network "A" Side
Computer in "A"

* This image is from AWS at: https://github.com/aws-samples/aws-refarch-wordpress

Hacky hack hack: the cloud

Australian boy who hacked into Apple network admired the group, court told

Company says no data compromised by 16-year-old although court hears he stored information' in a folder called 'hacky hack hack'

"If I had an hour to solve a problem, I'd spend *55 minutes* thinking about the problem and *five minutes* thinking about solutions."

-- Albert Einstein

Hacking the cloud?

We will be using ‘CloudGoat’ by Rhino Security to demonstrate the attacks in the talk

- *https://rhinosecuritylabs.com/aws/cloudgoat-vulnerable-design-aws-environment/*

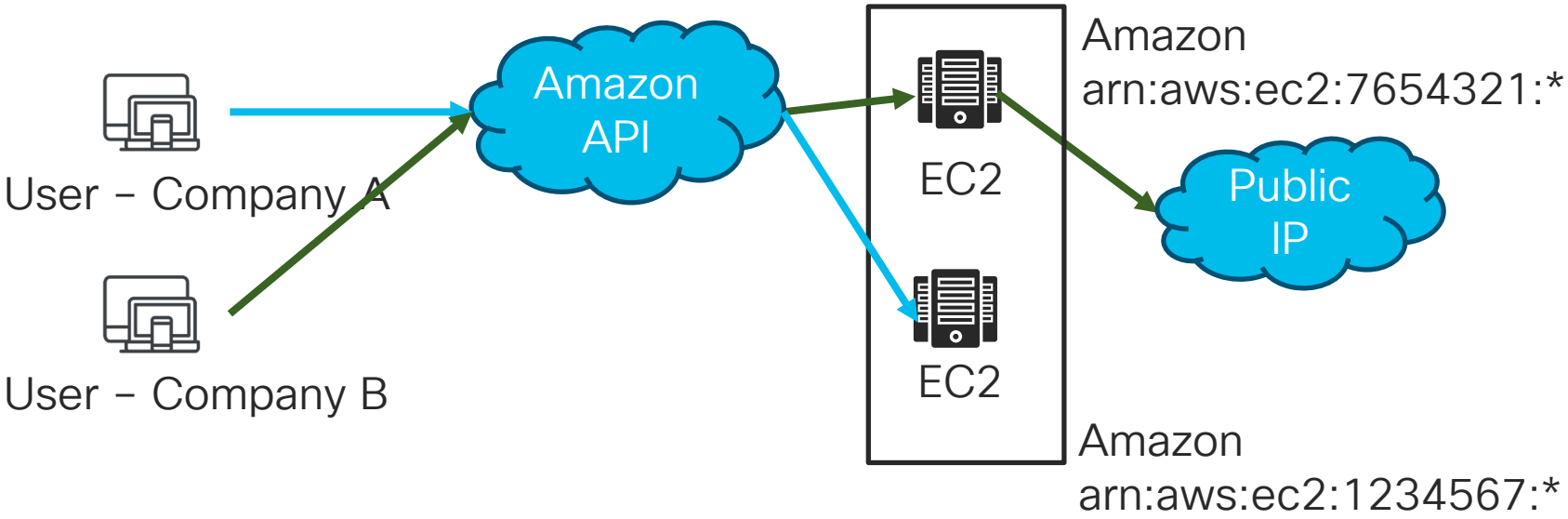
We will be using two scenarios:

- cloud_breach_s3
- ec2_ssrf

A word on Cloud Architecture

Cloud Service Providers have very specific items that we need to be aware of:

They usually provide an API SDK or just a pain API to control your assets

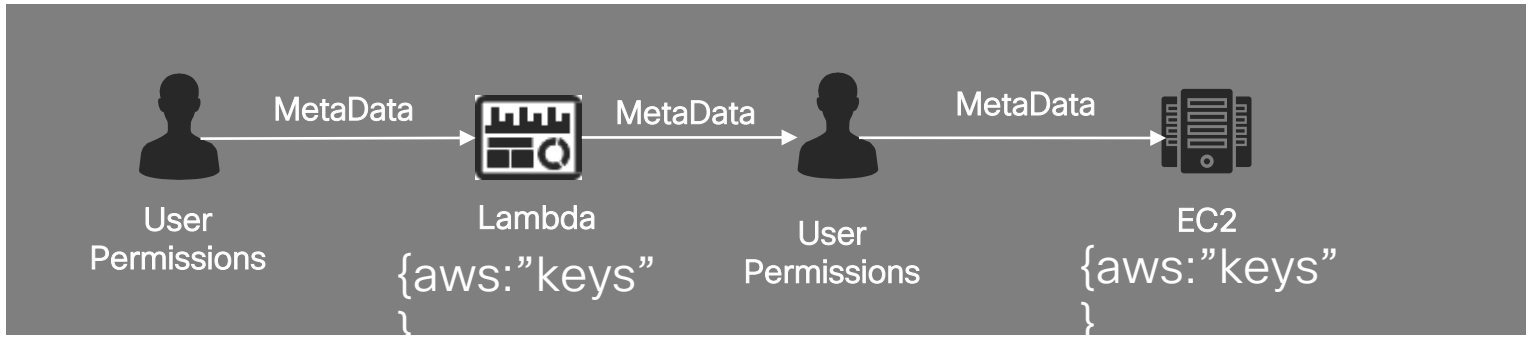


*How is that the cloud knows whose asset belongs to who? (*ARN=Amazon Resource Name)*

Cloud Breach S3

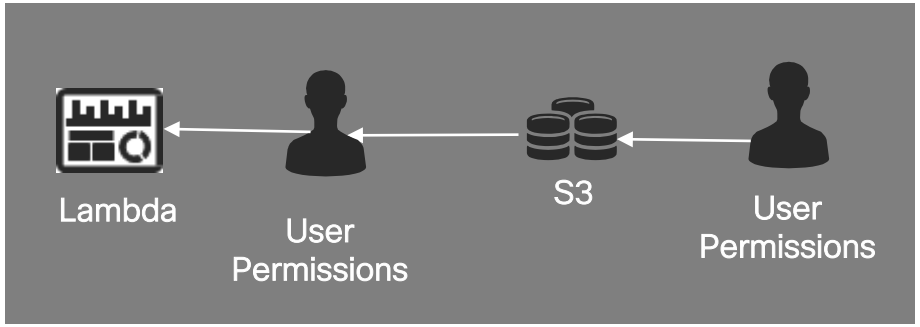
DEMO

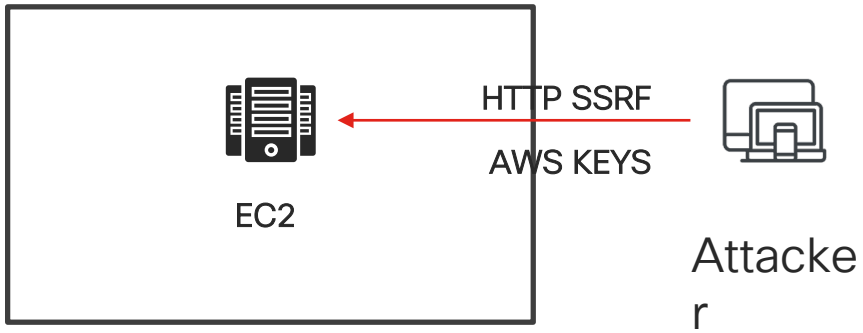
EC2_SSRF



AWS Control Plane

External Data Access





DEMO

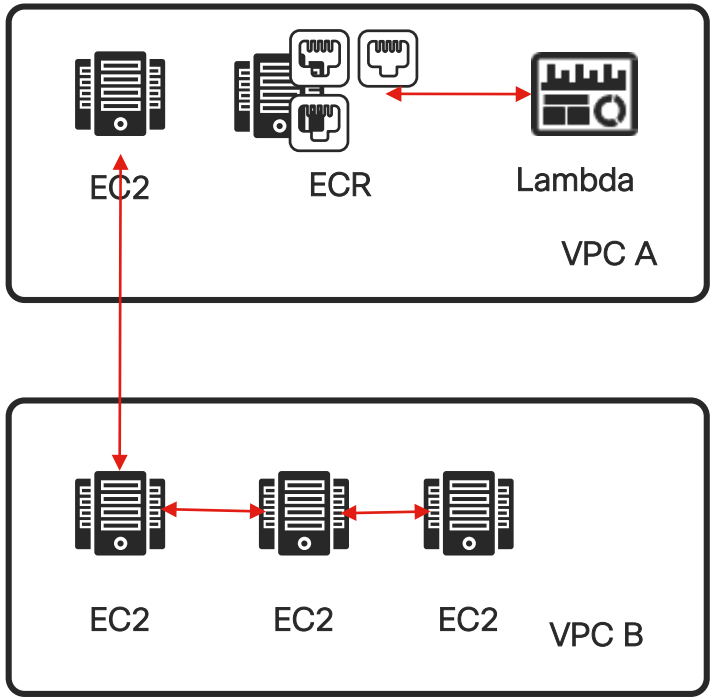
AWS Metadata - Lambda


```
{
   "Functions": [
----
         "FunctionName": "cg-lambda-cgidehlz443e30",
         "FunctionArn": "arn:aws:lambda:us-east-1:054164944767:function:cg-lambda-cgidehlz443e30",
         "Environment": {
            "Variables": {
               "EC2_ACCESS_KEY_ID": "AKIAQXXXXXREDATACTEDXXXX",
               "EC2_SECRET_KEY_ID": "W5X4yXXXXXXREDACTEDXXXXXXXXXXXXXXXXXXXX"
            }
```

Other attack considerations

Not all attacks will be based on the permissions of the hosts, and as such we have an opportunity to also insert *other technologies*

- If the hosts beacon, or talk, between themselves
- If they execute services between VPC's
- If they talk from a function like ECR (containers) to other functions over a network connection (like lambda)



What do we notice in each one of these attacks?

They do not solely rely on NETWORK or ENDPOINT connections, some of them rely on the CSP like AWS having *control* over these resources and resource groups

They *can talk* over their network interface to other systems, just bear in mind that there are typically two interfaces on these systems (if not more).

- ipv4 private
- ipv6 private
- ipv4 public (attached to the service)
- ipv6 public (attached to the service)
- NAT Gateway with IPv4 (or IPv6)

Some CSP's require you to PAY extra for private networking, like in DigitalOcean. In DigitalOcean, public is the default.

DEFEND

What do we notice in each one of these attacks?

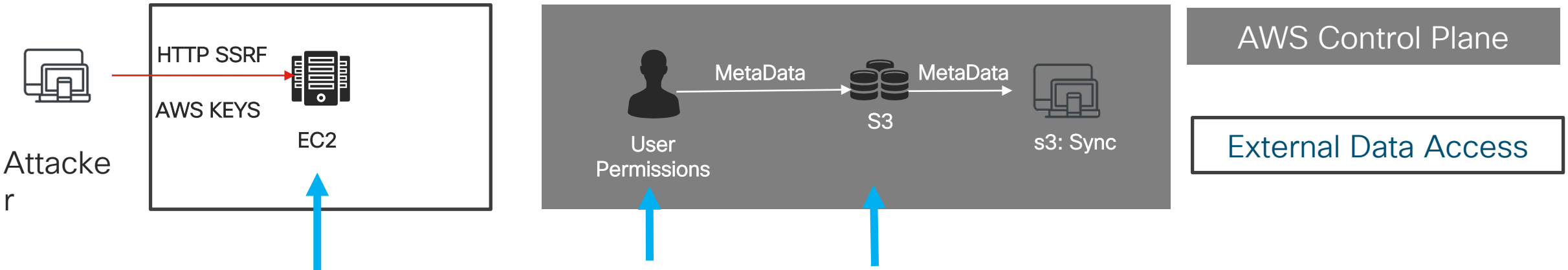
Attacks cannot always be fully prevented

There will *always* be a way in

- How can you *make it **painful***
- How can you ***SEE IT***
- How can you ***address it***

We will break down each attack and talk about **prevention in depth**

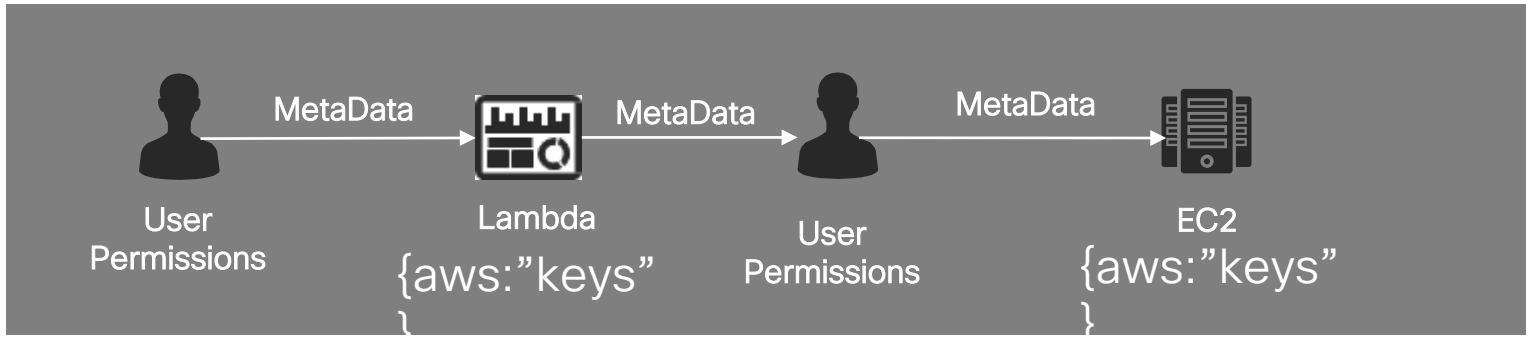
CloudGoat: Cloud Breach S3



Prevention: IAM, IAM, IAM
Detection: AWS CloudWatch Logs, Cisco StealthWatch Cloud

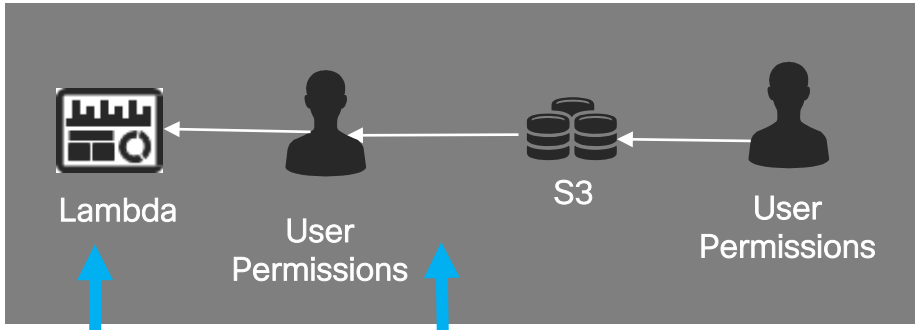
Prevention: AWS features a Cloud WAF (GuardDuty), but there are *others, **and there are good reasons to chose others!***
Detection: Cisco Stealthwatch Cloud, Cisco Tetration

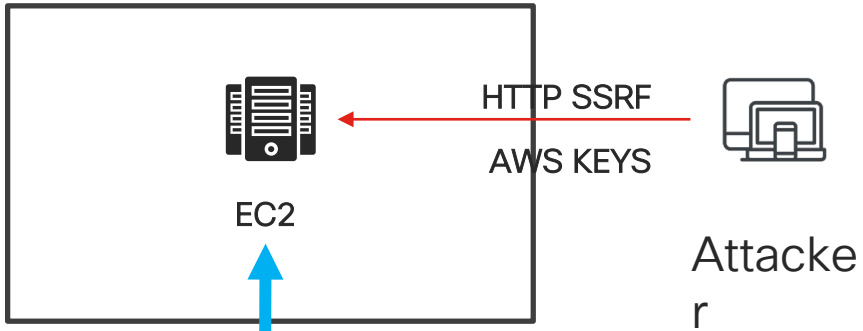
Cloudgoat: EC2_SSRF



AWS Control Plane

External Data Access





Prevention: IAM, IAM, IAM
Detection: AWS CloudWatch Logs, Cisco StealthWatch Cloud

Prevention: AWS features a CloudWAF (GuardDuty), but there are *others, and there are good reasons to chose others!*
Detection: Cisco Stealthwatch Cloud, Cisco Tetration

AWS IAM

AWS IAM is an RBAC System.

Google has their own permissions model, similar to AWS

Azure has their own as well, not similar to AWS

Each one of these is *DIFFERENT*

On the right is example of the JSON array that controls access to resources in AWS

- **s3:*** means all permissions which is too many
- **Resource**:"*" means **ALL** S3 Buckets, also too many!

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS IAM Restrictions

Make sure that resources that require access to other resources have constraints

Constraints can be:

- Actions: Read, or Write, or List, but others
  - S3 READ has almost 40 distinct controls)
- Resources: What Amazon ARN's can you access, so for S3 which buckets
- Constraints: You can TAG attributes, i.e Name:TagKeys, Value=Project-Ravenclaw

```
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject"
            ],
            "Resource":
"arn:aws:s3:::arn:aws:s3:::cg-bucket-
for-class/*",
            "Condition": {

"ForAnyValue:StringEquals": {
                    "aws:TagKeys":
"Project-Ravenclaw"
```

Using Logging

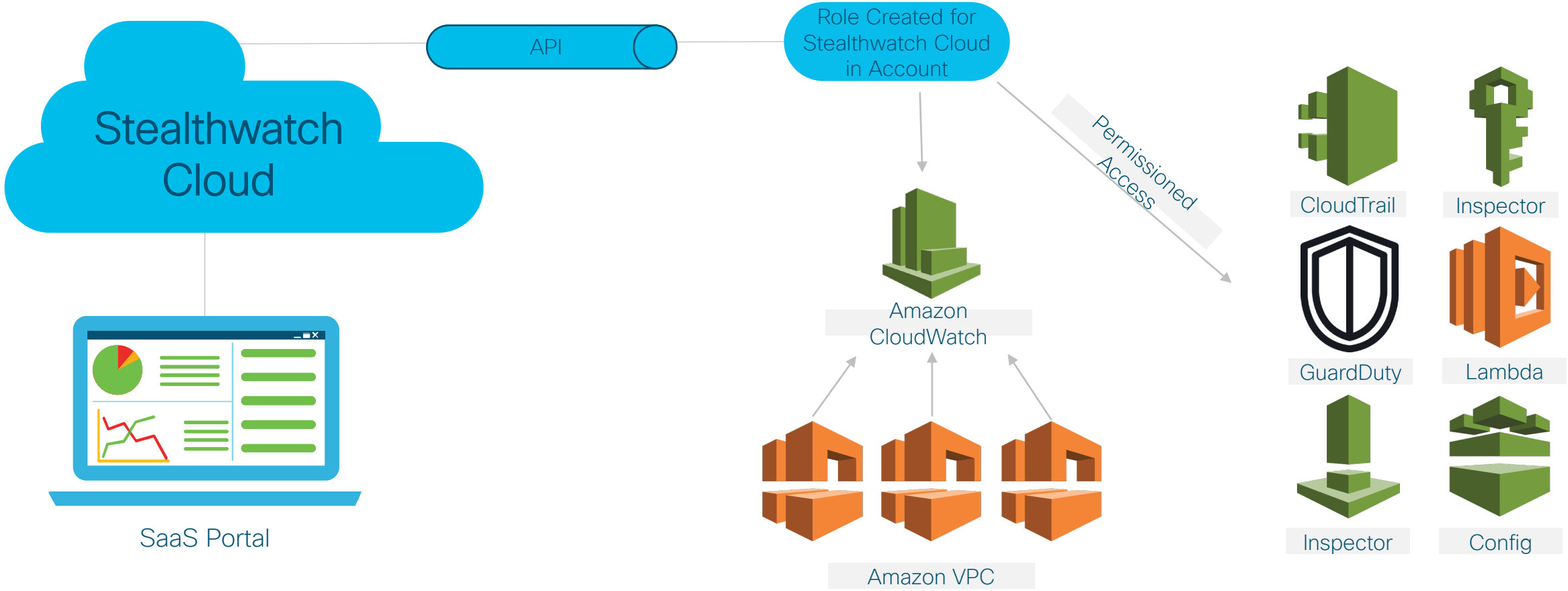
AWS CloudTrail Logging is useful for API Tracking

10, 05:58:54 PM	root	ConsoleLogin
10, 10:43:12 AM	root	ConsoleLogin
07, 07:39:09 PM	cg-lambda-cgidehlz443e30	CreateLogStream
07, 07:38:54 PM	cg-lambda-cgidehlz443e30	CreateLogStream

It does not log all API requests, but it can let you know of login events, and potentially key usage.

Some keys ***bypass*** API's such as root keys, alert on the usage of these keys

Stealthwatch Cloud
*in aws



AWS CloudTrail alone does not work

Sometimes it's difficult to understand WHAT is important in the CloudTrail environment:

Cisco SWC (Stealth watch Cloud)

"Models Cloud Assets"

"Looks at VPC Flow"

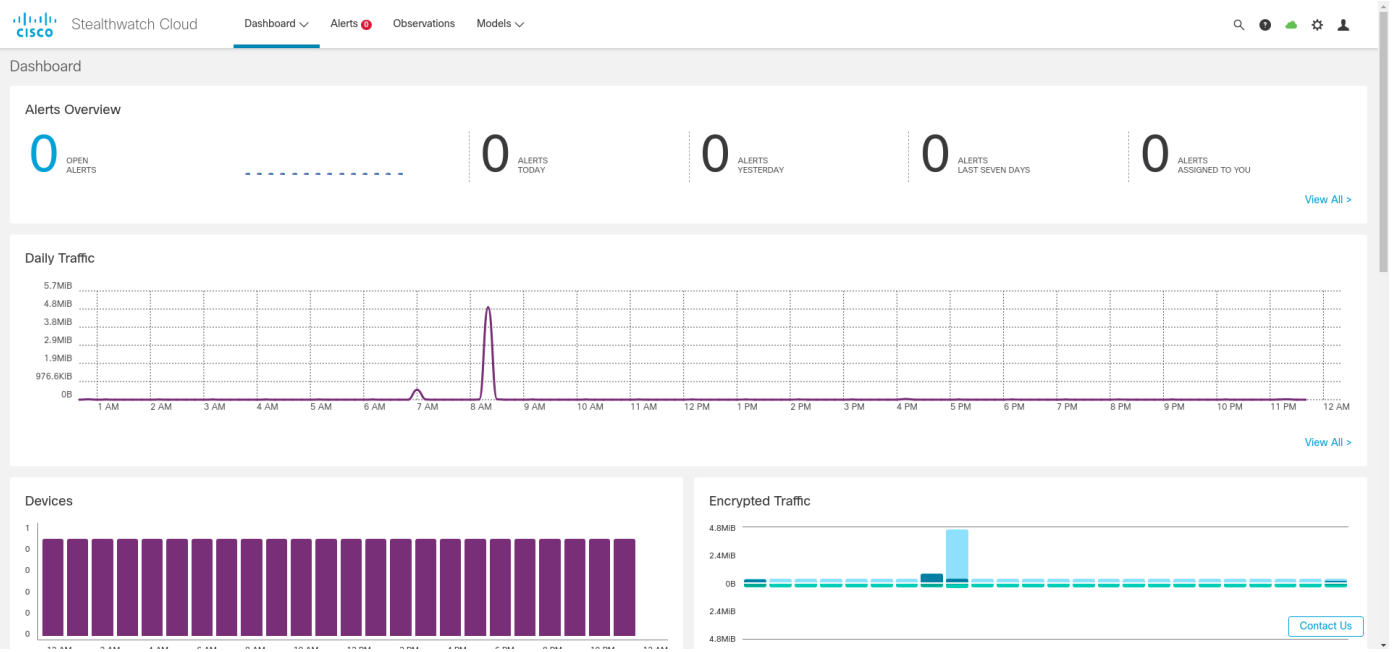
"Makes Observations on Events"

Specifically Services in the cloud

AWS CloudTrail

AWS GuardDuty

More...



Stealthwatch Cloud AWS Configuration

Configure the IAM Permissions for SWC

Enable VPC Flow Logging on a Source

Configure the SWC Portal

This will take a few minutes to register for SWC

IAM Role for the S3 Source,

This creates the IAM role to allow SWC to access your account, SWC Provides this

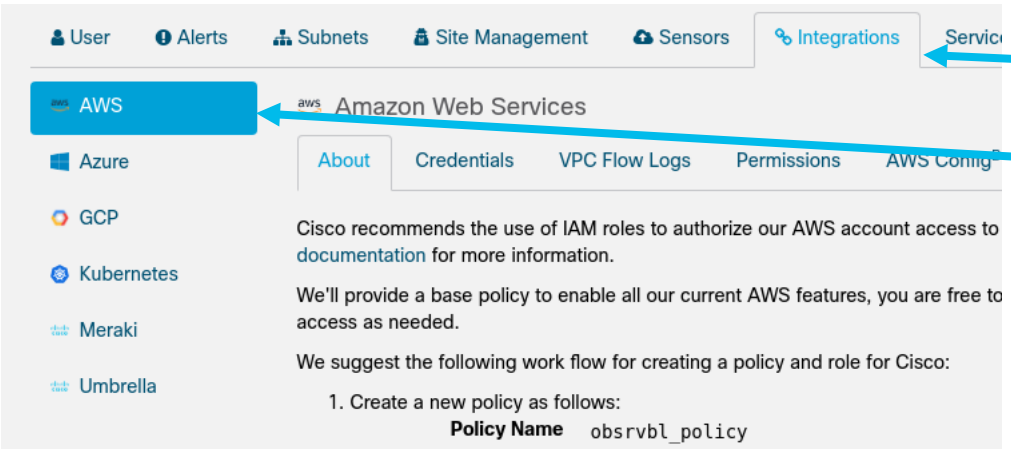
```
resource "aws_iam_role" "obsrvble_role" {
  name = "observable_role"

  assume_role_policy = <<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": “this-is-custom"
        }
      }
    }
  ]
}
EOF
}
```

Create an IAM Role

This is the ARN for *YOUR observable account*
The externalld is YOUR SWC environment

Example of finding your ARN for the previous slide



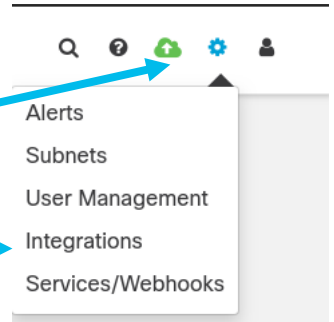
3

4

5

1

2



2. Create a new role.
   - Select the *Another AWS account* type
   - For the Account ID, enter 7[redacted]
   - Select *Require external ID* and enter cis[redacted]
   - Attach the permissions policy created above (obsrvbl_policy)
   - Set a role name (e.g., obsrvbl_role)
3. Tell Cisco the Role ARN for the new role, it will look like "arn:aws:iam::<account_id>:role/<role_name>" (e.g., "arn:aws:iam::7[redacted]:role/obsrvbl_role")

This gives Cisco Stealthwatch Cloud temporary access to a small set of Amazon APIs under your account.

IAM role for the Bucket

This is to write to the bucket the flow logs

```
resource "aws_iam_role_policy" "obsrvbl_policy_s3" {
  name = "obsrvbl_policy_s3"
  role = "${aws_iam_role.obsrvble_role.id}"

  policy = <<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::your-bucket-here"
      ]
    },
```

```
 {
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::your-bucket-here/*"
      ]
    }
  ]
}
EOF
}
```

IAM Role for the SWC

This is the policy that is attached the SWC ROLE (Which is an external system, see previous)

```
resource "aws_iam_role_policy" "obsrvbl_policy" {
  name = "obsrvbl_policy"
  role = "${aws_iam_role.obsrvble_role.id}"

  policy = <<EOF
{
"Version": "2012-10-17",
"Statement": [
    {
        "Action": [
            "autoscaling:Describe*",
            "cloudtrail:LookupEvents",
            "cloudwatch:Get*",
            "cloudwatch:List*",
            "ec2:Describe*",
            "elasticache:Describe*",
            "elasticache:List*",
            "elasticloadbalancing:Describe*",
            "guardduty:Get*",
            "guardduty:List*",
            "iam:Get*",
            "iam:List*",
            "inspector:*",
```

```
            "rds:Describe*",
            "rds:List*",
            "redshift:Describe*",
            "workspaces:Describe*",
            "route53:List*"
        ],
        "Effect": "Allow",
        "Resource": "*"
    },
    {
        "Action": [
            "logs:Describe*",
            "logs:GetLogEvents",
            "logs:FilterLogEvents",
            "logs:PutSubscriptionFilter",
            "logs:DeleteSubscriptionFilter"
        ],
        "Effect": "Allow",
        "Resource": "*"
    }
]
}
EOF
}
```

VPC Policy Logging CLI

Example is from a Terraform HCL Script that interfaces to the Amazon CLI:

```
resource "aws_s3_bucket" "cg-flow-logs-s3" {
  bucket = "cg-flow-log-s3"
  acl    = "private"
  force_destroy = true

  tags = {
    Name        = "My bucket"
    Environment = "Dev"
  }
}

resource "aws_flow_log" "cg-flow-log" {
  iam_role_arn         = "${aws_iam_role.obsrvble_role.arn}"
  log_destination      = "${aws_s3_bucket.cg-flow-logs-s3.arn}"
  log_destination_type = "s3"
  traffic_type         = "ALL"
  vpc_id               = "${aws_vpc.cg-vpc.id}"
  log_format           = "$${version} $${account-id} $${interface-id} $${srcaddr} $${dstaddr} $${srcport} $${dstport} $${protocol} $${packets} $${bytes}
$${start} $${end} $${action} $${log-status} $${vpc-id} $${subnet-id} $${instance-id} $${tcp-flags} $${type} $${pkt-srcaddr} $${pkt-dstaddr}"

}
```

Create the Bucket

Create a Flow Log with a VPC Log Format send events to the bucket and attach an IAM role

VPC Flow Logs Configuration – After terraform run

Create VPC | Actions

Filter by tags and attributes or search by keyword

1 to 4 of 4

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set	Main Route table	Main Network ACL	Tenancy	Default VPC	Classic link
CloudGoat ...	vpc-06c90bd40b39bfc2d	available	10.10.0.0/16	-	dopt-a7788bdd	rtb-0e82a129c09e410c7	acl-0a6b6f130dda3f836	default	No	Disabled
CloudGoat ...	vpc-0e833f02253b38cd7	available	10.10.0.0/16	-	dopt-a7788bdd	rtb-0a4acc0b2f69674f1	acl-05eaa6bbff0bfc53f	default	No	Disabled
CloudGoat ...	vpc-0fb35b9cbdf05181e	available	10.10.0.0/16	-	dopt-a7788bdd	rtb-0a76dc8a7acf104db	acl-0d084e09a5fad5f97	default	No	Disabled
	vpc-67e3b51d	available	172.31.0....	-	dopt-a7788bdd	rtb-f965b887	acl-b9f840c4	default	Yes	Disabled

VPC: vpc-06c90bd40b39bfc2d

Description | CIDR Blocks | Flow Logs | Tags

You can create flow logs on your resources to capture IP traffic flow information for the network interfaces for your resources. Learn more

Create flow log | Actions

1 to 1 of 1

Flow Log ID	Filter	Destination ty	Destination name	IAM Role Arn	Creation Time	Status	Log line format
fl-0eff7776746d3d07a	ALL	s3	cg-flow-log-s3	arn:aws:iam::054164944767:role/observab...	January 7, 2020 at 8:06:09 PM UTC-5	Active	custom

SWC Demo

- API calls to do *certain* action is logged
  - Certain logged in users like root
  - Create and destroy assets
- SWC will mark many of these as ***observations***
- Any network flow that can be captured in a VPC will also be logged
- Giving us the ability to see flows and gather data and look for strange behavior where we cannot install an endpoint agent.
- ***Remember this is NOT an agent-based connection, its all VPC logging and Logs***

SWC Network Alerts

Strange SSH connection

Geographically Unusual Remote Access

i-00629f07367150377

Status	Open
ID	68
Description	This device has been accessed from a remote host in a country that doesn't normally access the local network. For example, a local server accepting an SSH connection from a foreign source would trigger this alert.
Updated	Jan 21, 2020 11:50:00 AM
Created	Jan 21, 2020 11:50:00 AM
	IPs at the time of alert: 54.221.141.15, 10.10.10.67
	Hostname at the time of alert: i-00629f07367150377
Assignee	Nobody
Tags	

After reviewing an alert, closing it will let the rest of your team know it's been resolved. In addition, closing alerts sends important feedback.

Close Alert

Supporting Observations

Remote Access Observation

Device was accessed from a remote source.

20 records per page

search

Time	Device	Remote Device	Local Port	Profile	Remote IP
1/21/20 11:50 AM	i-00629f07367150377	96.71.19.172	22 (ssh)	SSHServer	96.71.19.172

CSV Showing 1 of 1

First Previous 1 Next Last

Stealthwatch Cloud In Action

Session Traffic

active filters *start time: 2020-01-10T11:41:18-05:00; ip: 106;*

Traffic | Traffic Chart | Rejects | Connections Graph

Table of matching sessions.

20 records per page

SSRF Triggered Attack

						Bytes		Packets	
Time	IP	Connected IP	Port	Connected Port	Protocol	To	From	To	From
1/11/20 11:26 AM	10.10.10.67	96 [redacted]	80 (http)	49860	TCP	731	1,561	6	5
1/11/20 11:26 AM	10.10.10.67	96 [redacted]	80 (http)	49862	TCP	590	666	6	5
1/11/20 11:26 AM	10.10.10.67	96 [redacted]	80 (http)	49864	TCP	216	112	4	2
1/11/20 11:26 AM	10.10.10.67	96 [redacted]	80 (http)	49912	TCP	1,314	1,143	8	6
1/11/20 11:26 AM	10.10.10.67	96 [redacted]	80 (http)	49918	TCP	879	2,055	7	6
1/11/20 11:17 AM	10.10.10.67	52.94.225.93	52162	443 (https)	TCP	6,732	2,989	18	18

Observations

Observations

Recent Highlights | Types | By Device | AWS New User Action Observations

AWS New User Action Observation

CloudTrail logged an AWS user doing an action for the first time.

20 records per page

search

Time	Device	Event	Event Type
1/7/20 8:14 PM	root	ConsoleLogin	AwsConsoleSignIn
1/7/20 8:10 PM	root	AttachRolePolicy	AwsApiCall
1/7/20 8:05 PM	deploy_cisco_user	PutRolePolicy	AwsApiCall

CSV Showing 1 to 3 of 3 First Previous 1 Next Last

Observations

Recent Highlights | Types | By Device

New External Server Observation

Device started communicating with an external server.

10 records per page

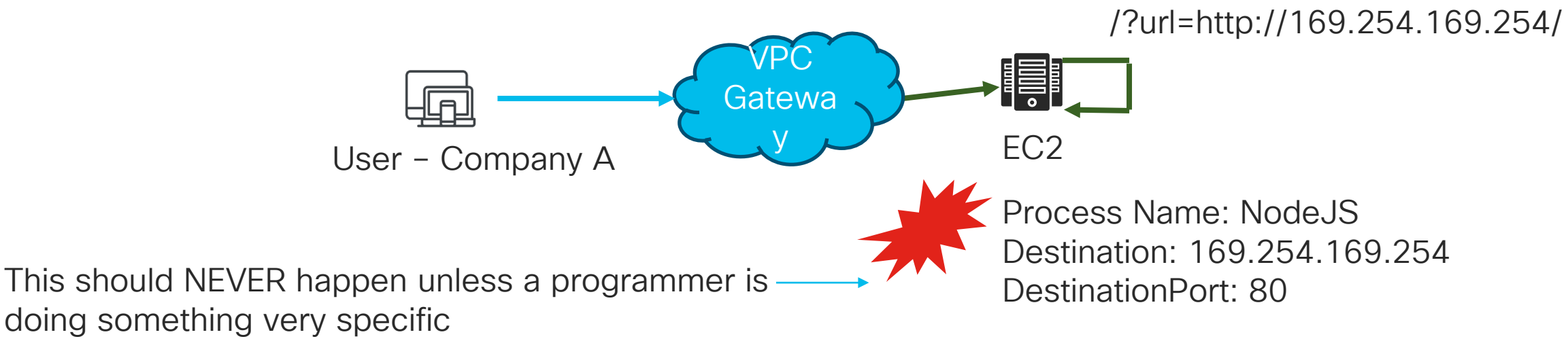
search

Time	Device	External IP	New Tag	Bytes In	Bytes Out
1/8/20 1:41 AM	i-00629f07367150377	54.192.30.36	WebServer	83,940,730	1,044,630
1/8/20 1:37 AM	i-00629f07367150377	54.152.129.43	WebServer	61,512,430	317,996
1/8/20 1:37 AM	i-00629f07367150377	91.189.91.14	WebServer	25,891,906	370,652

CSV Showing 1 to 3 of 3 First Previous 1 Next Last

Tetration analytics

- Agents can be deployed onto a EC2 Instance, or a Container Node Host for ECR/EKS and Unmanaged Kubernetes
- Agents can tell what localhost flows are and what process did the request



Example of Tetration Flow Search

Cisco Tetration FLOW SEARCH

BRKSEC-2605 Monitoring

Select time range
Jan 21 6:26am - Jan 21 12:26pm

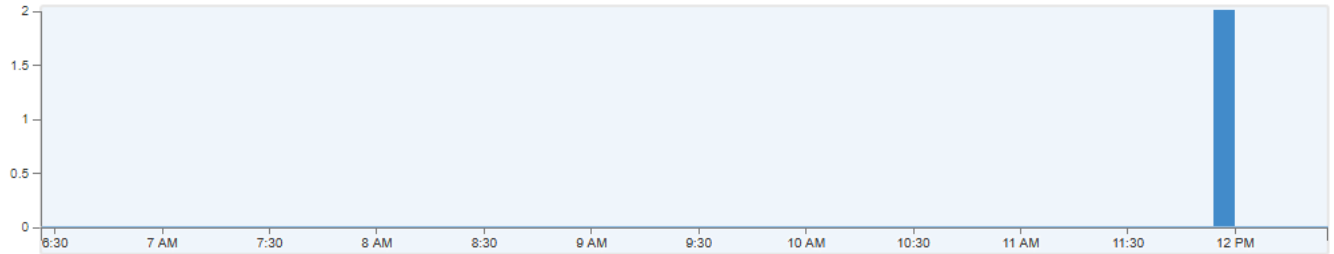
12/15 12/22 12/29 1/5 1/12 1/19

59 total observations
Showing Flow Observations

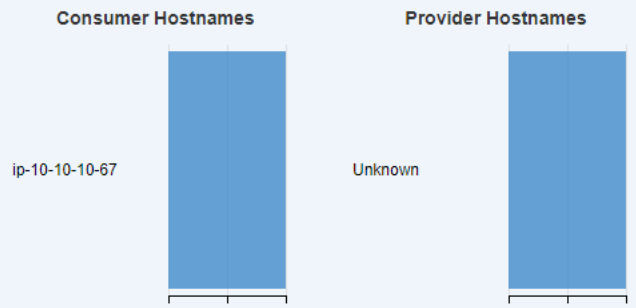
Filters Provider Address = 169.254.169.254 Filter Flows

Flow Observations

Searching for 169.254.169.254 leads us to request



Top Hostnames contributing to the selected **Flow Observations**.



Current scope is BRKSEC-2605

Current selection: **Jan 21 6:26am** to **Jan 21 12:26pm**

Found **4** Flow Observations (46ms)

Show 20 In order Sampled

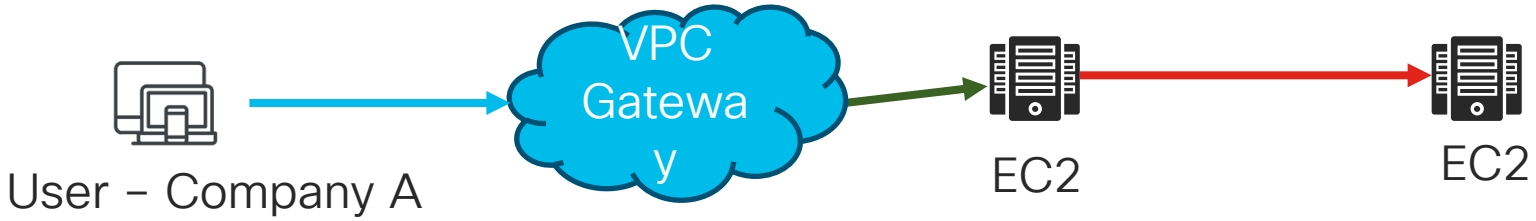
Explore Observations

Comes from 10.10.10.67 (EC2 IP), leading us to believe its not a normal request

Timestamp	Consumer Hostname	Provider Hostname	Consumer Address	Provider Address	Consumer Port	Provider Port	Protocol	Service Name	Deciding Analysis Policy Rank
Jan 21 11:55:00am	ip-10-10-10-67	Unknown	10.10.10.67	169.254.169.254	36768	80	TCP	HTTP	Unknown
Jan 21 11:55:00am	ip-10-10-10-67	Unknown	10.10.10.67	169.254.169.254	36770	80	TCP	HTTP	Unknown
Jan 21 11:57:00am	ip-10-10-10-67	Unknown	10.10.10.67	169.254.169.254	36772	80	TCP	HTTP	Unknown

Enforcement / Prevention Options

- AWS Security Groups can provide Layer 3/4 firewalling
- What do you firewall? How do you know?
- Let Tetration provide the application layer mapping and help rollout protections into AWS, onto hosts and other nodes



Process Name: node
Destination: 169.254.169.254
DestinationPort: 80

This should NEVER happen unless a programmer is doing something very specific

Options for Protection using Tetration

- Alert based on Tetration Flows
- Forensic Report can show the node process calling 169.254.169.254
- Deploy a WAF as a potential ‘stop gap’ until the software is patched
- Can deploy Tetration Enforcement very carefully as it may break other AWS functionality

MFA MFA MFA MFA MFA MFA*
*multi-factor authentication

If you don't have MFA everywhere you don't have MFA

Repeat: IF

MFA MFA MFA MFA MFA MFA*
*multi-factor authentication

If you don't have MFA everywhere you don't have MFA

Repeat: IF

YOU
DONT

MFA MFA MFA MFA MFA MFA*
*multi-factor authentication

If you don't have MFA everywhere you don't have MFA

Repeat: IF

YOU
DONT

HAVE

MFA

EVERYWHERE

MFA MFA MFA MFA MFA MFA*
*multi-factor authentication

If you don't have MFA everywhere you don't have MFA

Repeat: IF

YOU
DONT

HAVE

MFA

EVERYWHERE

YOU DON'T HAVE MFA

WHY do we say this

- API calls in this demo didn't have MFA
- **YES NOT EVERY PROGRAMATTIC KEY CAN USE MFA WE GET IT**
- AWS API calls can be protected with MFA
- Uses STS to get a temporary session token
- Session token is used in the rest of the calls


```
$ aws sts get-session-token --serial-number arn-of-the-mfa-device --token-code
code-from-token
$ aws s3 ls
```

AWS GuardDuty

Pros:

Web Application Firewall that is built into AWS a Service

Can automatically scale up and down with EC2 scale

Web application firewalls can find attacks destined to hit web sites

Cons:

GuardDuty is integrated into IAM

Attackers with enough privileges can whitelist themselves in GuardDuty

Disable GuardDuty

```
aws guardduty create-ip-set --detector-id arn:aws:123 --name im-innocent --
format txt --location https://s3bucket.amazonaws.com/mybucket/ipset.txt
```

Third Party WAFs

Pros:

Self contained and potentially closed system

Can still find web application attacks as many of these WAFs are built on Open Source WAF rules

Guard Duty uses mod_security, so does CloudFlare

Cons:

May not easily scale, depending on the WAF

Is not necessarily integrated into the EcoSystem

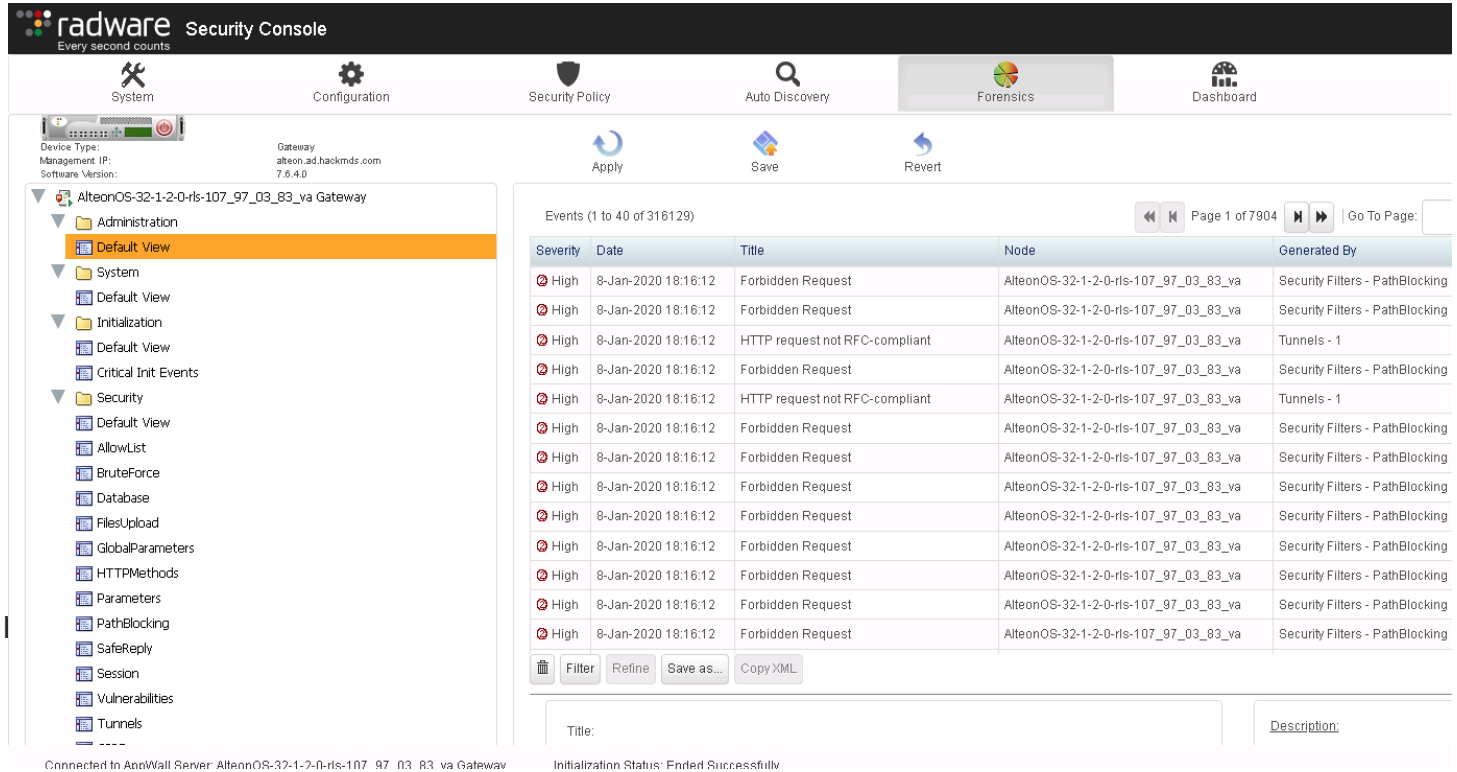
Off to the side implantations which would be challenging to push all traffic through

Think how do I put Lambda and force it *THROUGH* my Third Party WAF at Scale?

This could also be a Cloud Services WAF not in the AWS system

Radware WAF

- Positive Security Model WAF
- Delivered:
  - On Premise
  - Part of ADC
  - In a Cloud Environment like AWS
  - Kubernetes WAF
- Advantage:
  - Not part of the AWS IAM RBAC syste
  - If RBAC is compromised, this is not



Device Type: Gateway
Management IP: alteon.ad.hackmds.com
Software Version: 7.6.4.0

Events (1 to 40 of 316129)

Severity	Date	Title	Node	Generated By
High	8-Jan-2020 18:16:12	Forbidden Request	AlteonOS-32-1-2-0-rls-107_97_03_83_va	Security Filters - PathBlocking
High	8-Jan-2020 18:16:12	Forbidden Request	AlteonOS-32-1-2-0-rls-107_97_03_83_va	Security Filters - PathBlocking
High	8-Jan-2020 18:16:12	HTTP request not RFC-compliant	AlteonOS-32-1-2-0-rls-107_97_03_83_va	Tunnels - 1
High	8-Jan-2020 18:16:12	Forbidden Request	AlteonOS-32-1-2-0-rls-107_97_03_83_va	Security Filters - PathBlocking
High	8-Jan-2020 18:16:12	HTTP request not RFC-compliant	AlteonOS-32-1-2-0-rls-107_97_03_83_va	Tunnels - 1
High	8-Jan-2020 18:16:12	Forbidden Request	AlteonOS-32-1-2-0-rls-107_97_03_83_va	Security Filters - PathBlocking
High	8-Jan-2020 18:16:12	Forbidden Request	AlteonOS-32-1-2-0-rls-107_97_03_83_va	Security Filters - PathBlocking
High	8-Jan-2020 18:16:12	Forbidden Request	AlteonOS-32-1-2-0-rls-107_97_03_83_va	Security Filters - PathBlocking
High	8-Jan-2020 18:16:12	Forbidden Request	AlteonOS-32-1-2-0-rls-107_97_03_83_va	Security Filters - PathBlocking
High	8-Jan-2020 18:16:12	Forbidden Request	AlteonOS-32-1-2-0-rls-107_97_03_83_va	Security Filters - PathBlocking
High	8-Jan-2020 18:16:12	Forbidden Request	AlteonOS-32-1-2-0-rls-107_97_03_83_va	Security Filters - PathBlocking
High	8-Jan-2020 18:16:12	Forbidden Request	AlteonOS-32-1-2-0-rls-107_97_03_83_va	Security Filters - PathBlocking
High	8-Jan-2020 18:16:12	Forbidden Request	AlteonOS-32-1-2-0-rls-107_97_03_83_va	Security Filters - PathBlocking

Connected to AppWall Server: AlteonOS-32-1-2-0-rls-107_97_03_83_va Gateway

Initialization Status: Ended Successfully

Third Party WAFs

Pros:

Self contained and potentially closed system

Can still find web application attacks as many of these WAFs are built on Open Source WAF rules

Guard Duty uses mod_security, so does CloudFlare

Cons:

May not easily scale, depending on the WAF

Is not necessarily integrated into the EcoSystem

Off to the side implantations which would be challenging to push all traffic through

Think how do I put Lambda and force it *THROUGH* my Third Party WAF at Scale?

This could also be a Cloud Services WAF not in the AWS system

Key Takeaways

Identify what your problem is you cannot *solve* a problem if you don't know what your trying to fix.

Recognize that each cloud will have their own security controls that are *critical.* ***Use them.***

Architect a solution to the problem, remember this is not a typically datacenter, typically datacenter solutions may make problems **worse.**

Enhance or augment security controls with visibility and prevention tools, make this **harder** for attackers not easier

Stealthwatch Cloud – Flows for services in a VPC even agentless, Control Layer

Tetration – Flows and Control with Process Auditing for places you can have an agent, Network/Endpoint Layer

DUO – MFA [Because if you don't have MFA ***everywhere*** you don't have MFA]

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education

- Demos in the Cisco Showcase
- Walk-In Labs
- Meet the Engineer 1:1 meetings
- Related sessions

Thank you

@mosesrenegade (tweets)

CISCO

You make **possible**