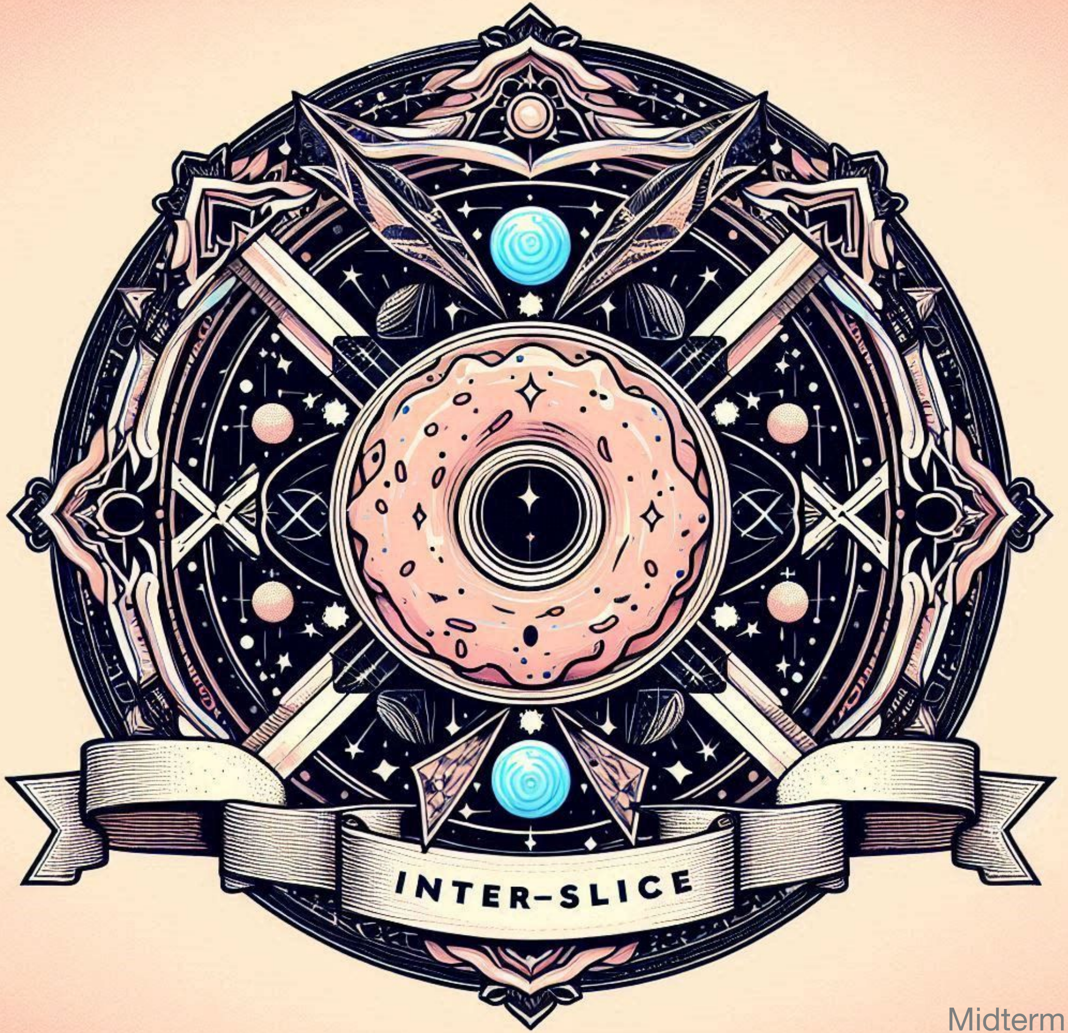


Midterm Project: Seattle-Ops-401d12

Agenda

1. Meet The Team
2. Problem Domain & Project Overview
3. Our Solutions
4. Demonstrations
5. Q&A

INTER-SLICE

InterSlice, Inc.

Steve Cherewaty

Omar Ardid

Cody Blahnik

Julian Pena

Julian Pena

- Cybersecurity Professional

- U.S. Army veteran

- Logistics expert

Omar Ardid

- Cybersecurity Professional

- Enjoy building gaming computers and playing video games

- Passionate on helping others

INTER-SLICE

Cody Blahnik

- Cybersecurity professional
- Advanced Troubleshooter
- Machine learning

Steve Cherewaty

- Cybersecurity professional

- Background in aerospace and startups

- Passion for building

INTER-SLICE

Cromulent Innovations - Problem Domain

Build Cloud Infrastructure

Implement Cloud Security

Log Aggregation/SIEM Solution

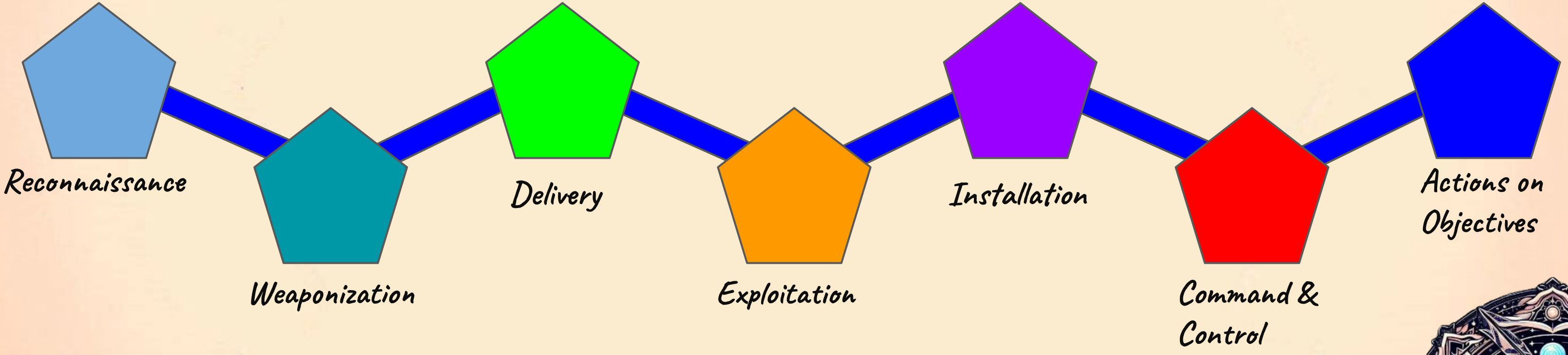
Align CIS/NIST Compliance

Demonstrate Attack-Solution

INTER-SLICE

Cyber Kill Chain

- Developed by Lockheed
- Describes the steps in cyber attacks



Reconnaissance

Weaponization

Delivery

Exploitation

Installation

Command & Control

Actions on Objectives

InterSlice Solutions

Access Control - IAM Identity Center

Exploitation

Deploy NIST & CIS-Compliant EC2's

Reconnaissance

SIEM Solution - CloudWatch

Command & Control

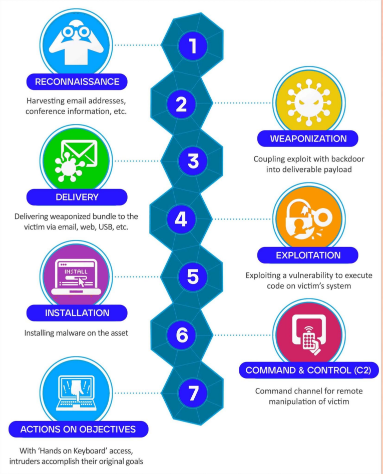
Data Protected At-Rest

Actions On Objectives

Data Protected In-Transit

Delivery

Command & Control



1 RECONNAISSANCE
Harvesting email addresses, conference information, etc.

2 WEAPONIZATION
Coupling exploit with backdoor into deliverable payload

3 DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.

4 EXPLOITATION
Exploiting a vulnerability to execute code on victim's system

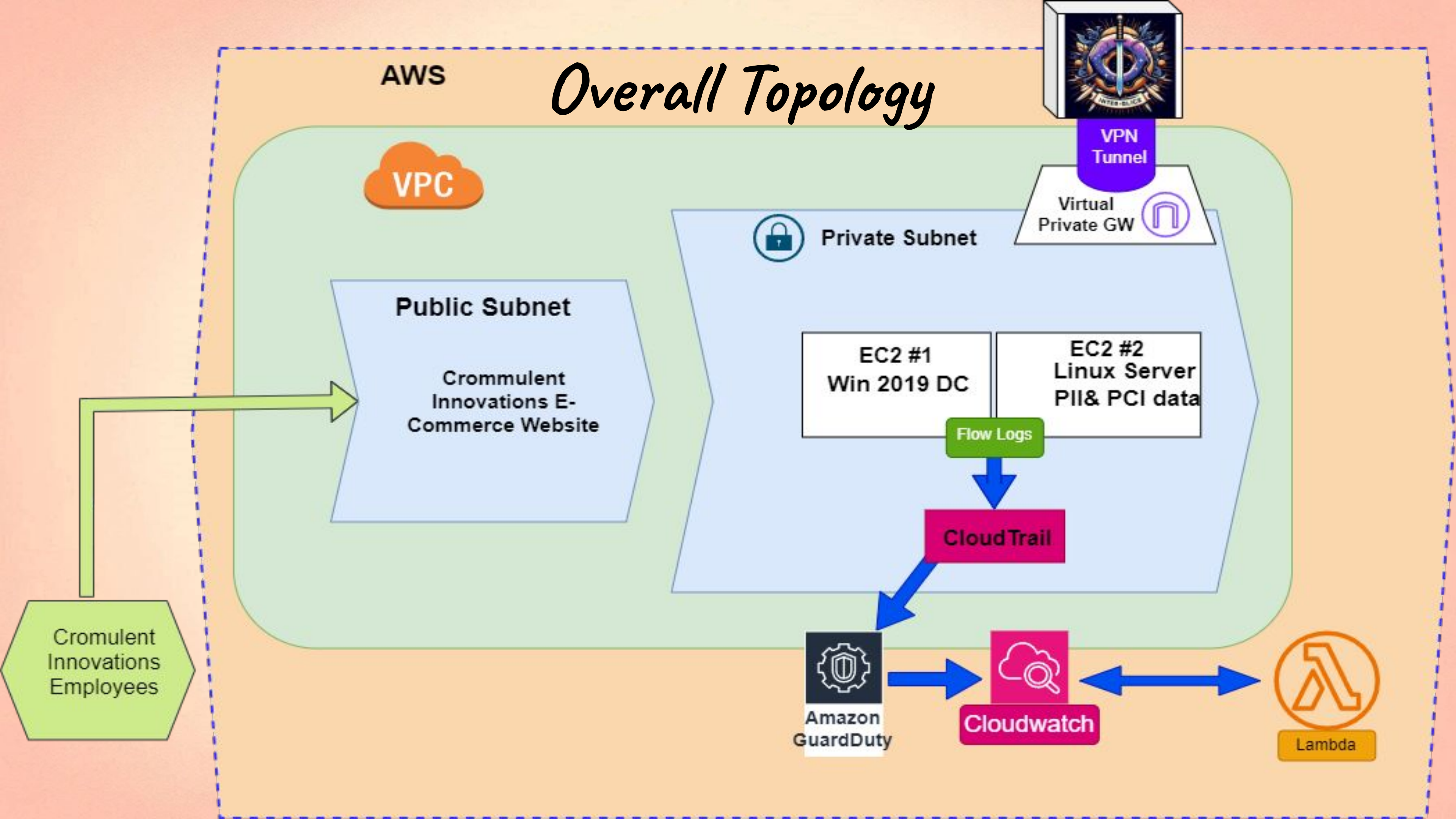
5 INSTALLATION
Installing malware on the asset

6 COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim

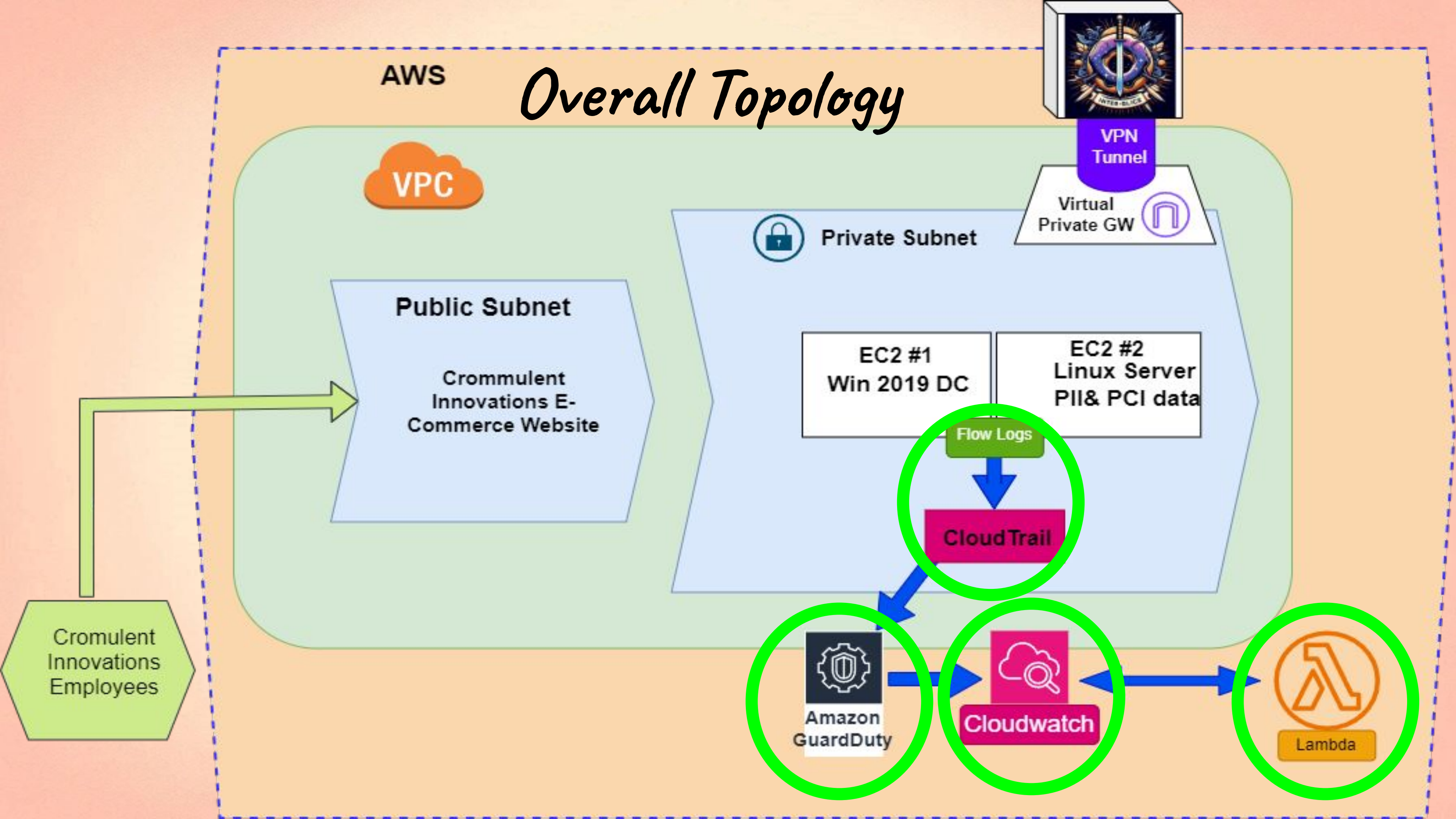
7 ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

INTER-SLICE

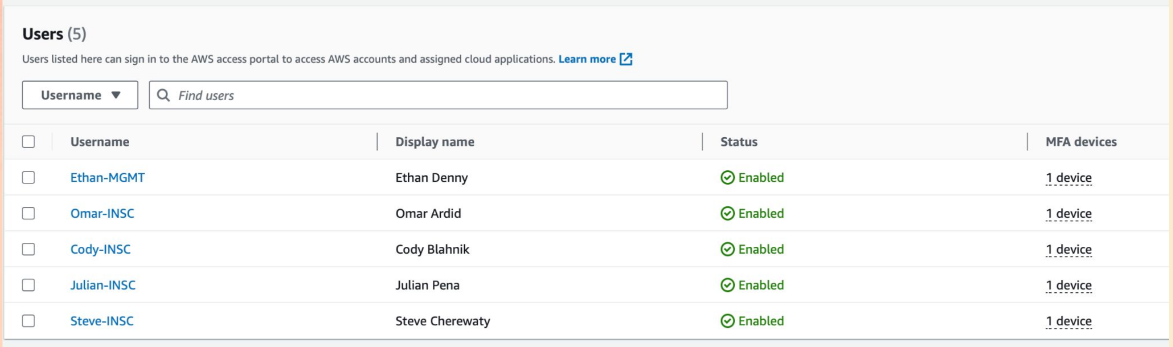
Overall Topology



Overall Topology



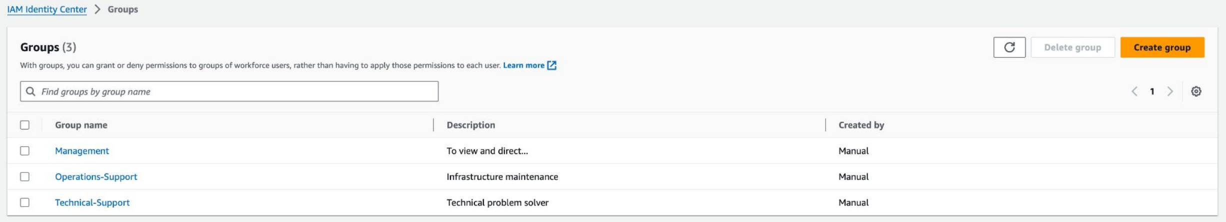
Access Control



Users (5)

Users listed here can sign in to the AWS access portal to access AWS accounts and assigned cloud applications. Learn more

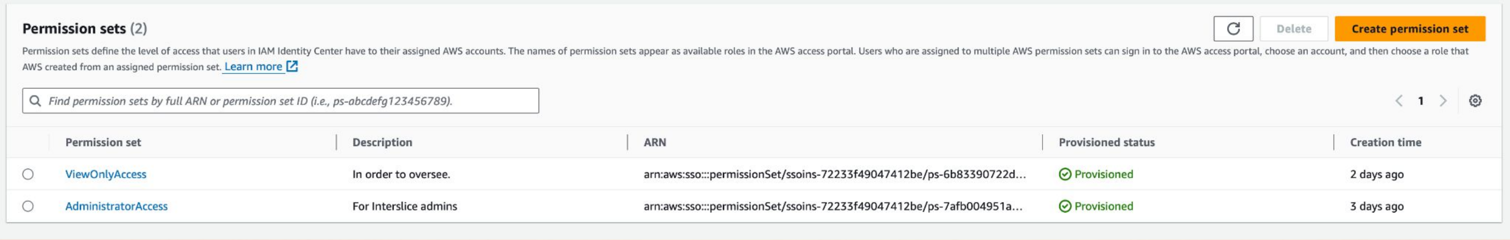
□	Username	Display name	Status	MFA devices
□	Ethan-MGMT	Ethan Denny	✓ Enabled	1 device
□	Omar-INSC	Omar Ardid	✓ Enabled	1 device
□	Cody-INSC	Cody Blahnik	✓ Enabled	1 device
□	Julian-INSC	Julian Pena	✓ Enabled	1 device
□	Steve-INSC	Steve Cherewaty	✓ Enabled	1 device



Groups (3)

With groups, you can grant or deny permissions to groups of workforce users, rather than having to apply those permissions to each user. Learn more

□	Group name	Description	Created by
□	Management	To view and direct...	Manual
□	Operations-Support	Infrastructure maintenance	Manual
□	Technical-Support	Technical problem solver	Manual


Delete
Create permission set
Find permission sets by full ARN or permission set ID (i.e., ps-abcdefg123456789).
< 1 >

Permission sets (2)

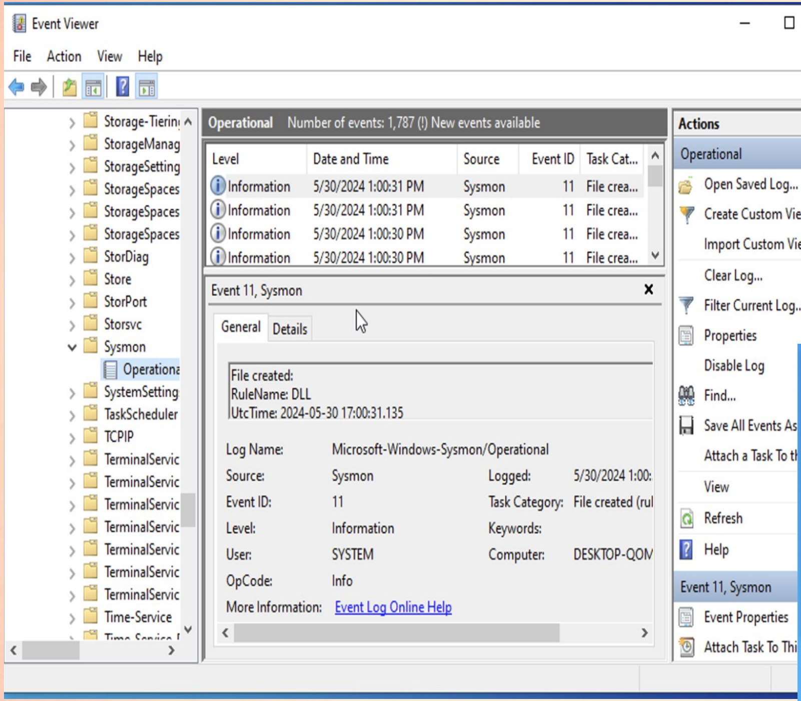
Permission sets define the level of access that users in IAM Identity Center have to their assigned AWS accounts. The names of permission sets appear as available roles in the AWS access portal. Users who are assigned to multiple AWS permission sets can sign in to the AWS access portal, choose an account, and then choose a role that AWS created from an assigned permission set. Learn more

	Permission set	Description	ARN	Provisioned status	Creation time
○	ViewOnlyAccess	In order to oversee.	arn:aws:sso:::permissionSet/ssoins-72233f49047412be/ps-6b83390722d...	✓ Provisioned	2 days ago
○	AdministratorAccess	For Interslice admins	arn:aws:sso:::permissionSet/ssoins-72233f49047412be/ps-7afb004951a...	✓ Provisioned	3 days ago

Windows Server

Deployed as EC2 instance

Uses Sysmon to (monitor and log events)



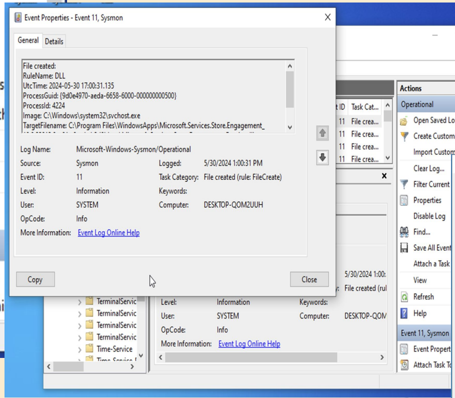
Operational Number of events: 1,787 (!) New events available

Level	Date and Time	Source	Event ID	Task Cat...
Information	5/30/2024 1:00:31 PM	Sysmon	11	File crea...
Information	5/30/2024 1:00:31 PM	Sysmon	11	File crea...
Information	5/30/2024 1:00:30 PM	Sysmon	11	File crea...
Information	5/30/2024 1:00:30 PM	Sysmon	11	File crea...

Event 11, Sysmon

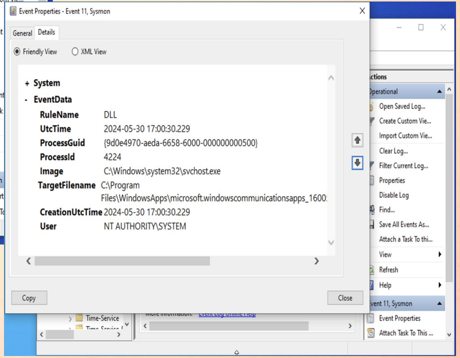
```
File created:
RuleName: DLL
UtcTime: 2024-05-30 17:00:31.135
```

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon Logged: 5/30/2024 1:00:
Event ID: 11 Task Category: File created (rul
Level: Information Keywords:
User: SYSTEM Computer: DESKTOP-QOM
OpCode: Info
More Information: Event Log Online Help



```
File created:
RuleName: DLL
UtcTime: 2024-05-30 17:00:31.135
ProcessGuid: {9d0e4970-aeda-6658-6000-000000000500}
ProcessId: 4224
Image: C:\Windows\system32\svchost.exe
TargetFilename: C:\Program Files\WindowsApps\Microsoft.Services.Store.Engagement_
```

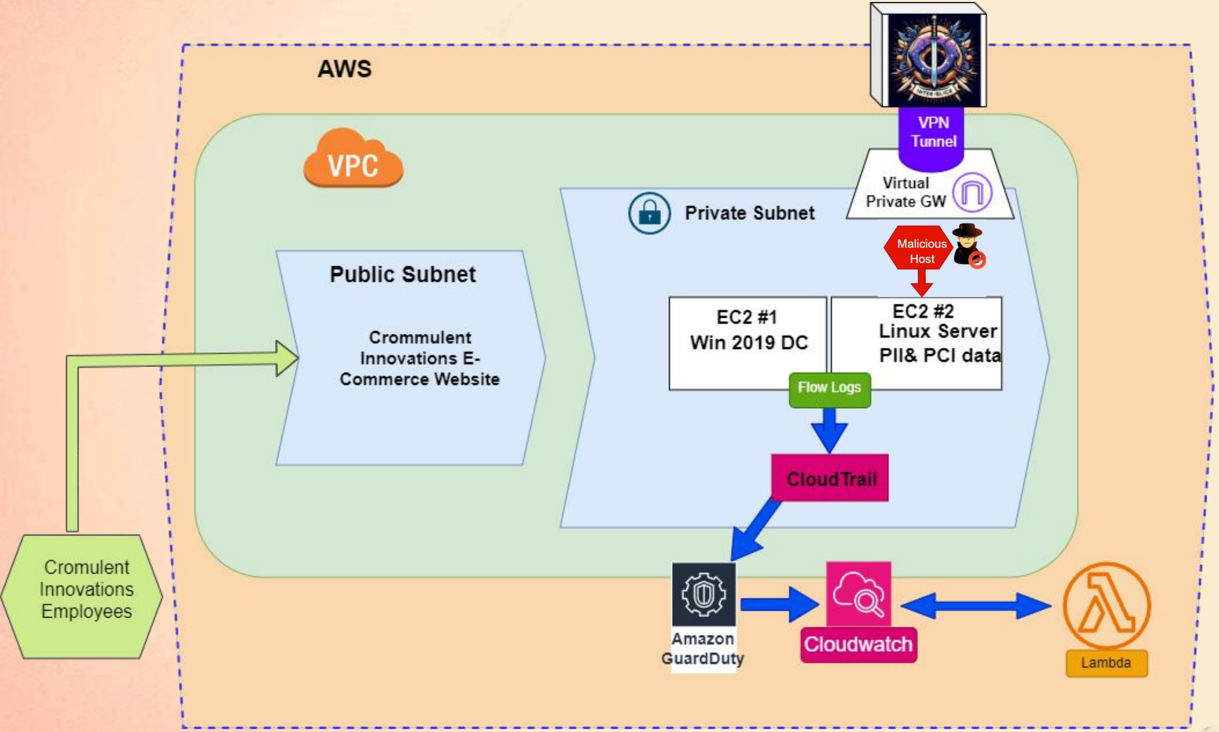
Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon Logged: 5/30/2024 1:00:31 PM
Event ID: 11 Task Category: File created (rule: FileCreate)
Level: Information Keywords:
User: SYSTEM Computer: DESKTOP-QOM2UUH
OpCode: Info
More Information: Event Log Online Help



● Friendly View ○ XML View

```
+ System
- EventData
   RuleName         DLL
   UtcTime          2024-05-30 17:00:30.229
   ProcessGuid      {9d0e4970-aeda-6658-6000-000000000500}
   ProcessId        4224
   Image            C:\Windows\system32\svchost.exe
   TargetFilename   C:\Program
                    Files\WindowsApps\microsoft.windowscommunicationsapps_1600
   CreationUtcTime  2024-05-30 17:00:30.229
   User             NT AUTHORITY\SYSTEM
```

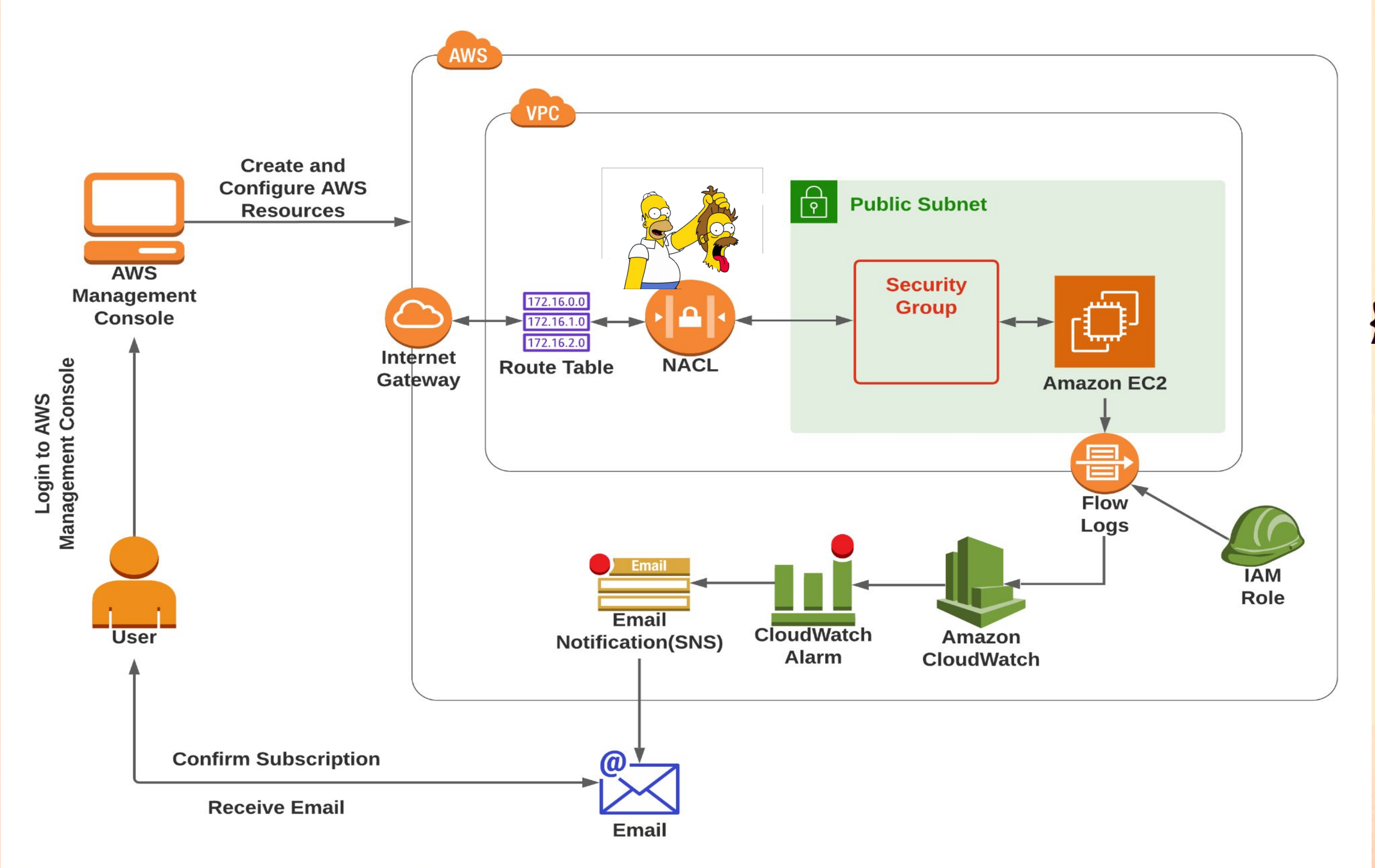
Brute Force Attempts via SSH



- Data Breach
- Automated Tools
- Unauthorized Access
- Password Guessing

Ooohh no we are under attack!!!

The strategy for the response and security measurements.



AWS

VPC

Create and Configure AWS Resources

AWS Management Console

Login to AWS Management Console

User

Internet Gateway

172.16.0.0
172.16.1.0
172.16.2.0

Route Table

NACL

Public Subnet

Security Group

Amazon EC2

Flow Logs

IAM Role

Amazon CloudWatch

CloudWatch Alarm

Email

Email Notification(SNS)

Confirm Subscription

Receive Email

Email

INTER-SLICE

Resources & Thanks. Questions?

Github

Steve Cherewaty

LinkedIn

Github

Omar Ardid

LinkedIn

Github

Cody Blahnik

LinkedIn

Github

Julian Pena

LinkedIn

Questions?