RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **AIR-W02**

The Fog Of Cloud Security Logging

Rehman Khan

Director, Cloud & Data Security
TD Ameritrade
https://www.linkedin.com/in/rehmankhan/
@cryptorak

Matthew Lubbers

Cloud Security Architect Consultant
TD Ameritrade
https://www.linkedin.com/in/matthew-lubbers-architect/

#RSAC

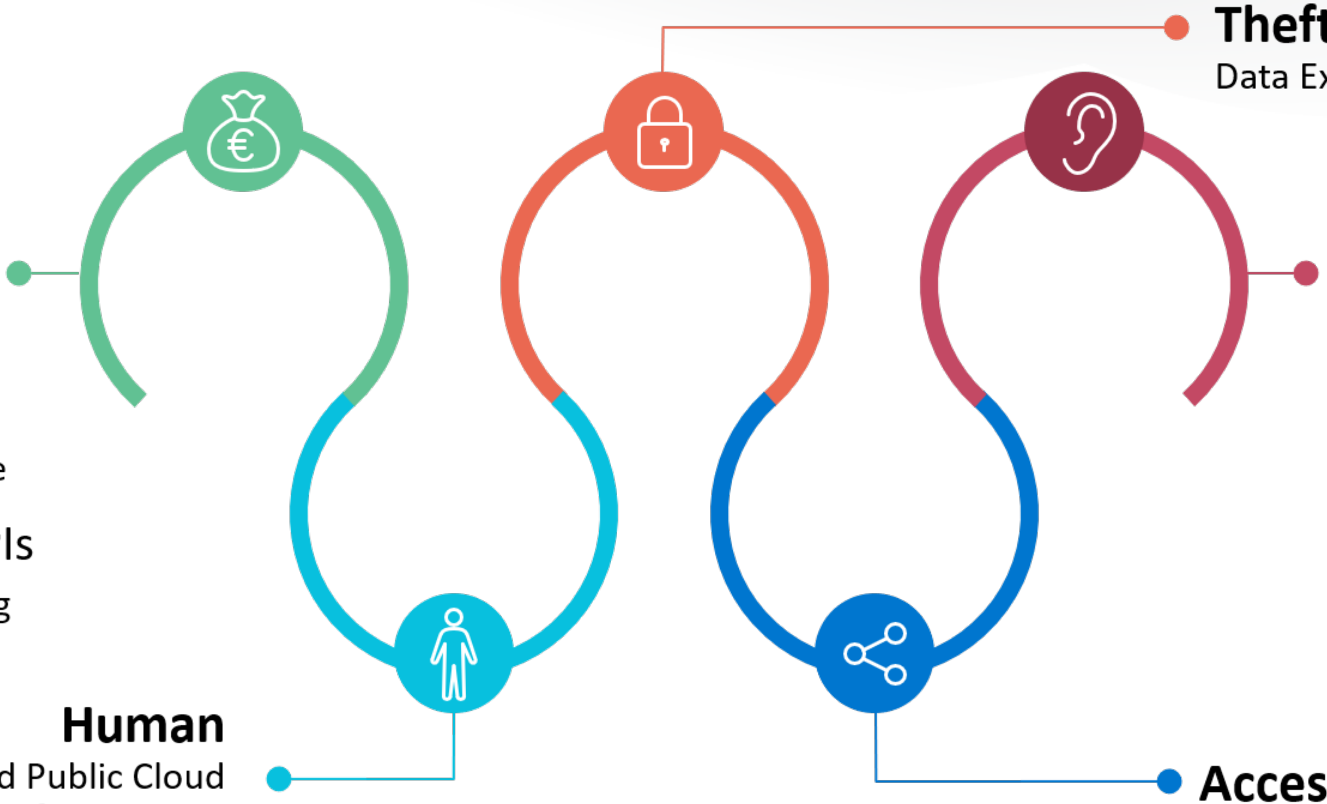
Public Cloud Security Threats

Unauthorized Access

- Account compromise

Insecure Interfaces/APIs

- External Data Sharing
- Malicious Insider



Exposure
Sensitive Data Shared Publicly

Theft
Data Exfiltration Via Unmanaged Cloud

Disruption
Hybrid Threats That Use Cloud & Web

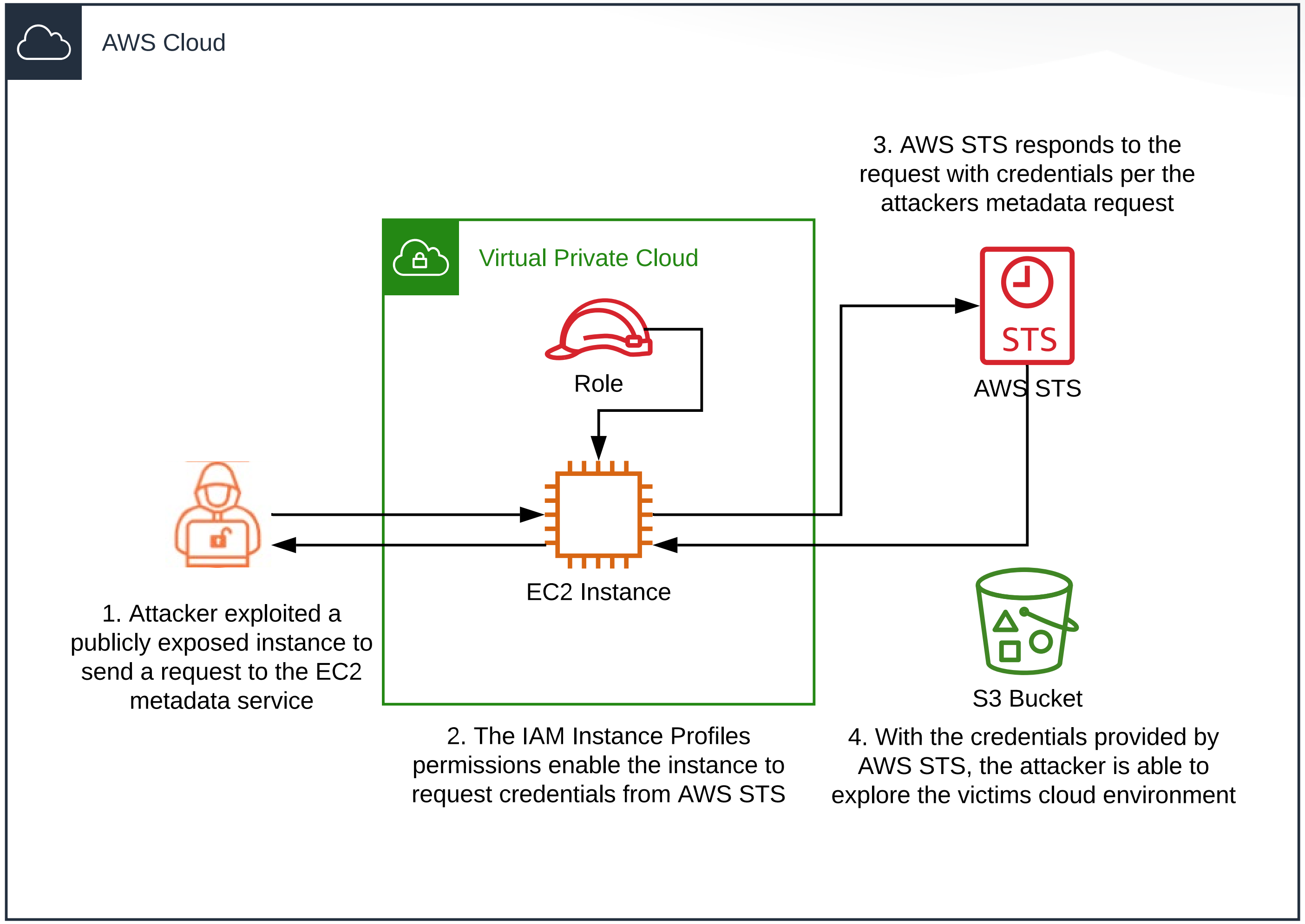
Human
Misconfigured Public Cloud Infrastructure

Access
Download To Personal Device

Misconfiguration of Cloud Platform Setup

- Malware Infections
- Data Exposure
- Vulnerability Exploitation

Opportunities To Detect Attacks, Data Exfiltration



1. Attacker exploited a publicly exposed instance to send a request to the EC2 metadata service

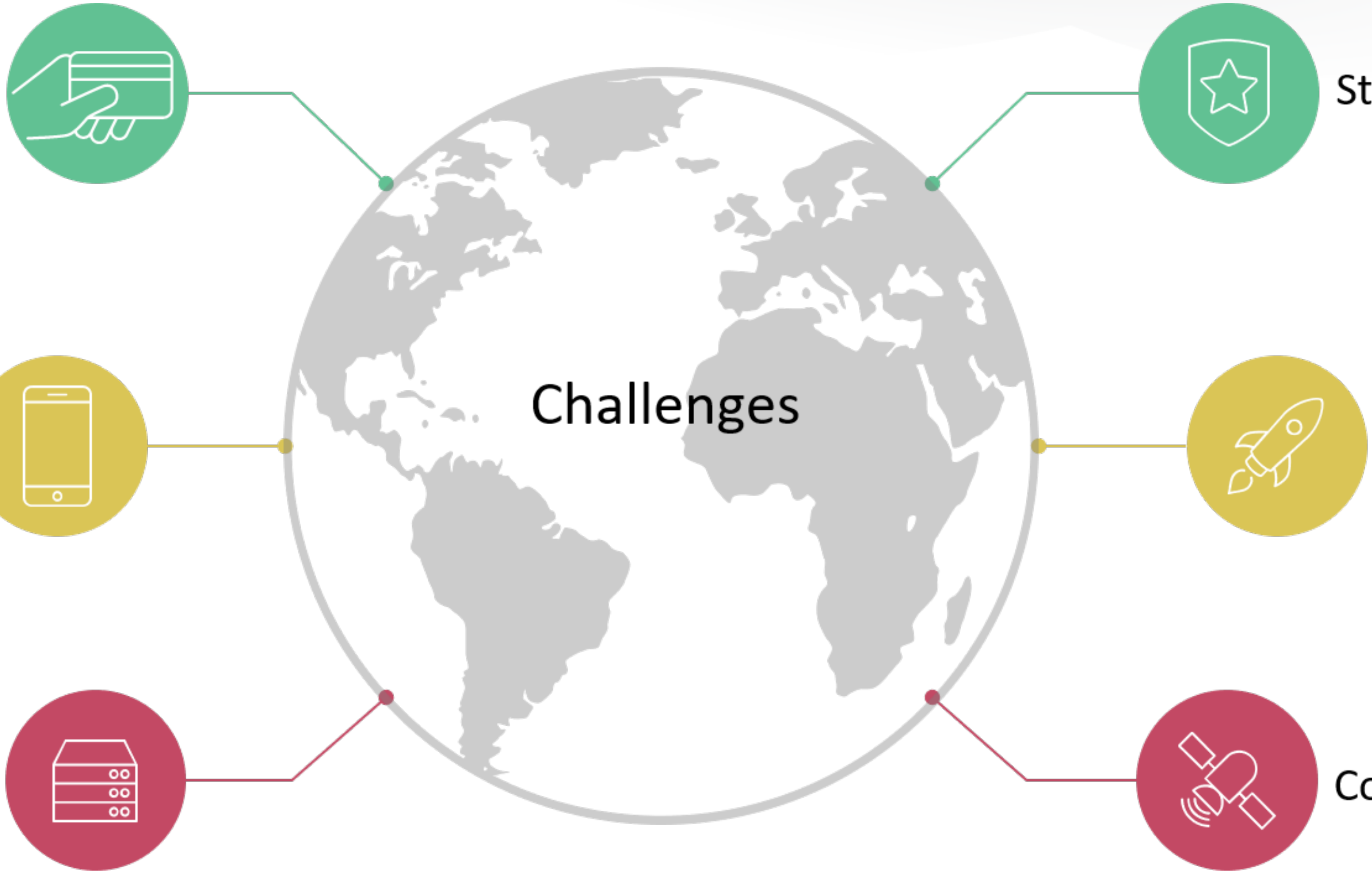
2. The IAM Instance Profiles permissions enable the instance to request credentials from AWS STS

3. AWS STS responds to the request with credentials per the attackers metadata request

4. With the credentials provided by AWS STS, the attacker is able to explore the victims cloud environment

Cloud Logs They Are Plenty….

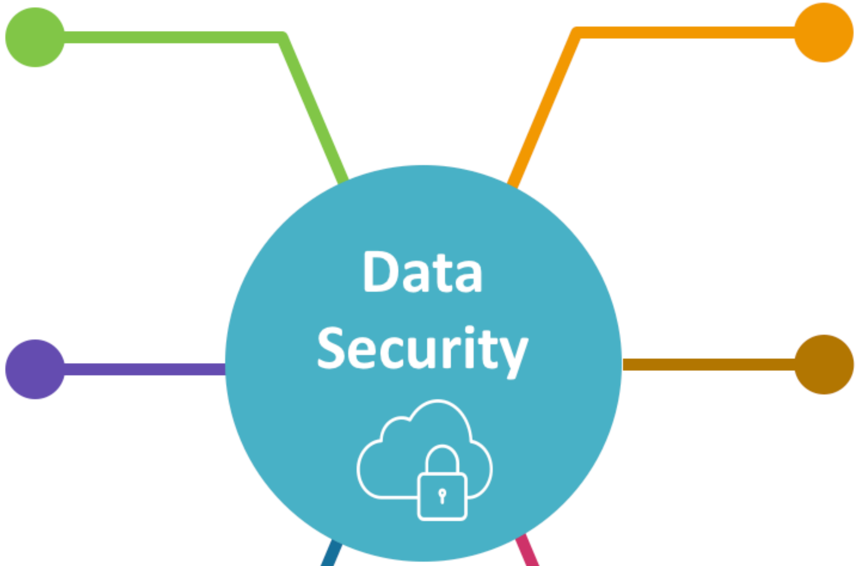
Clear The Log Fog



Challenges

- Egress Data Charges
- Direct CSP Connectivity
- On-premise Scalability
- Steep Learning Curve
- SIEMs Lack Cloud Context
- Complex Data Integration

Public Cloud Security Program



Data Security

Cloud Foundational Security

Establishing the foundational security controls for SaaS and IaaS-PaaS public cloud services (Azure, AWS and GCP)

Security Solution Deployment

Engineering and operationalizing required platform security tooling (CASB, CWPP, and CSPM)

Cloud Project Engagement

Establishing security requirements for SaaS and public cloud initiatives to ensure secure by design principles

Cloud Risk Management

Identifying, scoring and reporting risk for SaaS and public cloud initiatives

Security Automation

Deploying security controls as code through CI/CD and agile principles

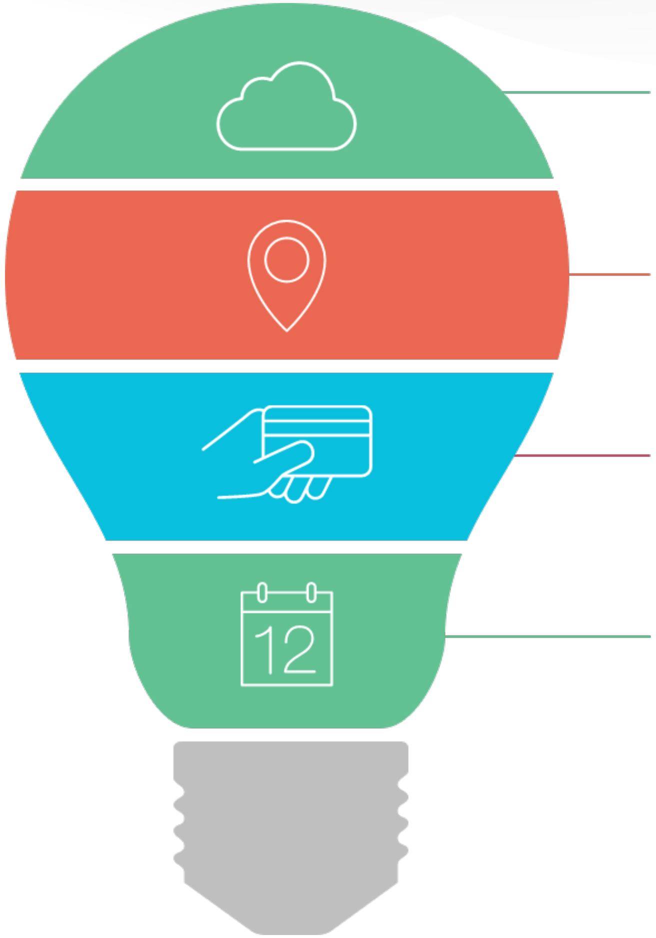
Research & Development

Investing in innovation, and continuous education on new cloud technologies and addressing emerging risk

Approach

Cloud Security Logging Strategy

- Security incident response requirements
- Business applications and layers of the architecture
- Cloud service providers capabilities around security logs
- Current on-premise security logging capabilities i.e. SIEM, Log Mgmt., etc.



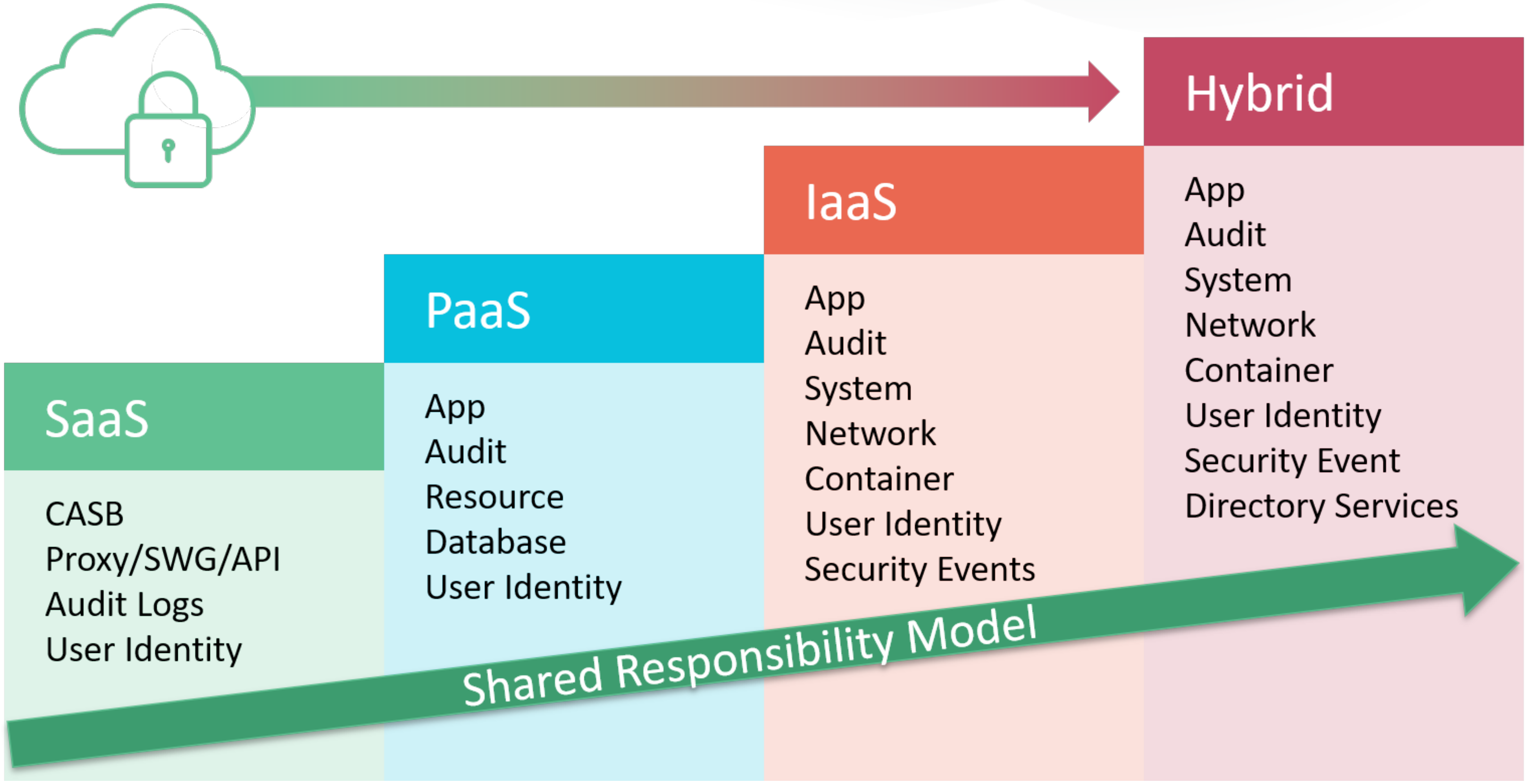
MVP approach don't try to boil the ocean

Design & Implement security logging part of security governance processes

Configuration actions based on event driven automation

Educate teams on how cloud logs are contextually different from on-premise logs

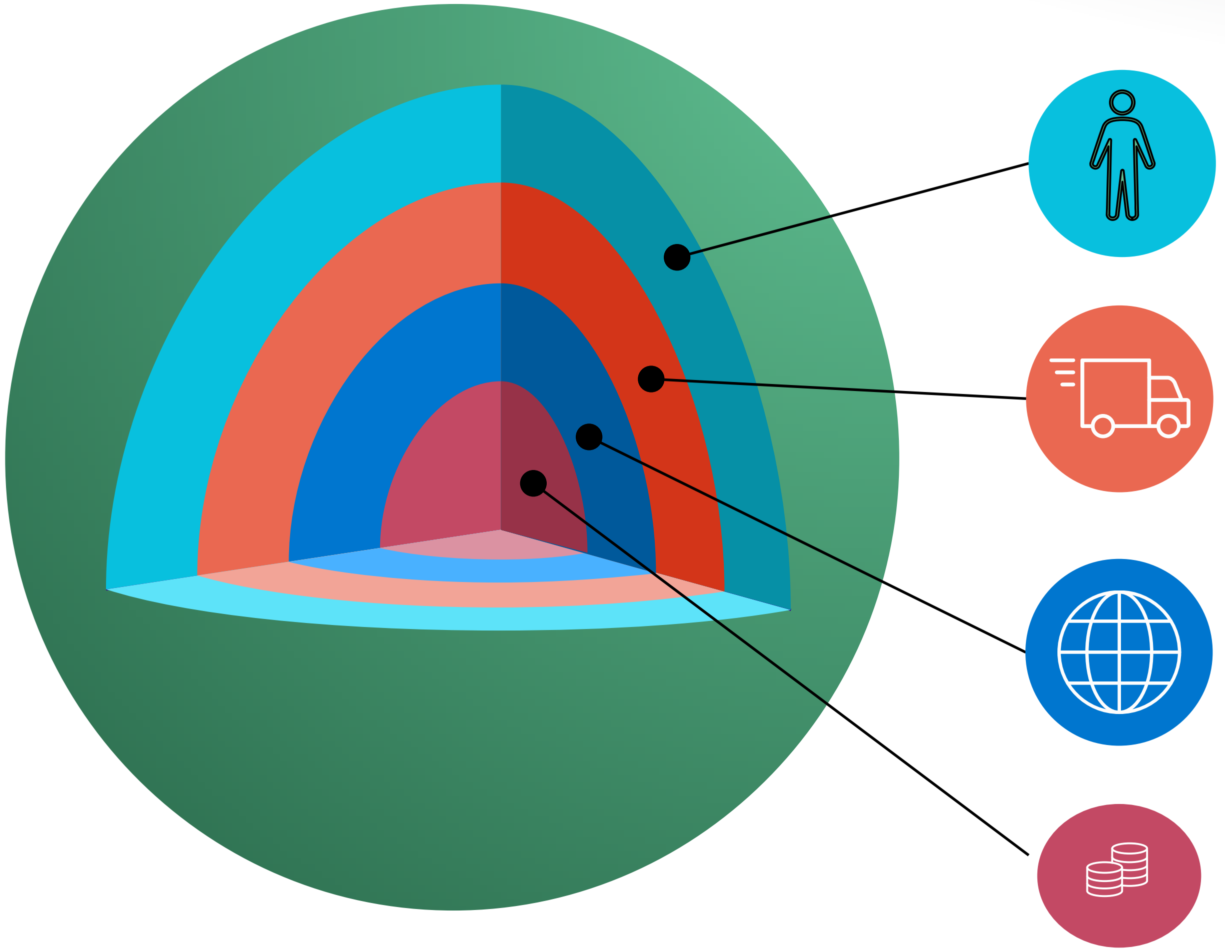
Cloud Logs by Cloud Services



SaaS	PaaS	IaaS	Hybrid
CASB	App	App	App
Proxy/SWG/API	Audit	Audit	Audit
Audit Logs	Resource	System	System
User Identity	Database	Network	Network
	User Identity	Container	Container
		User Identity	User Identity
		Security Events	Security Event
			Directory Services

Shared Responsibility Model

Monitor Critical Events & Activities



Identity Activity
Monitor Privileged Users & Unreasonable Travel Events

Resource Activity
Monitor Resource Transactions & Operations Events

Network Activity
Monitor Source & Destination Events

Data Activity
Monitor Any Data Access & Movement Events Including APIs

Context Based Monitoring

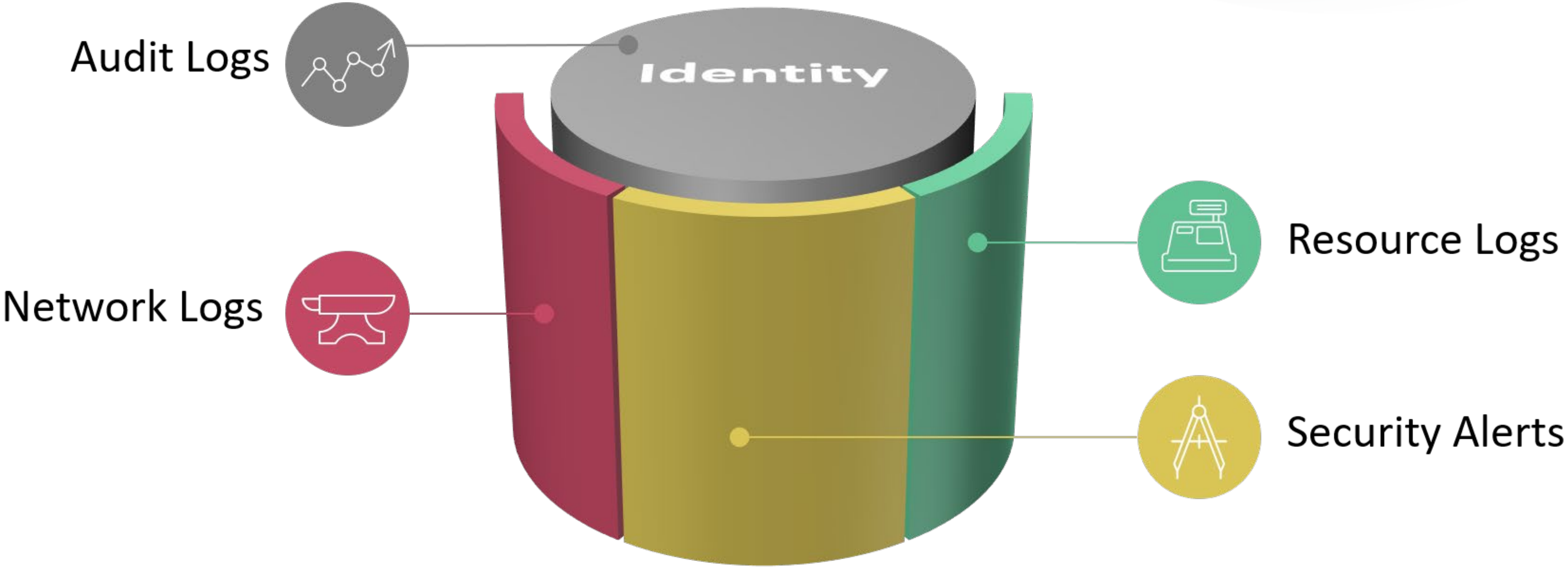
Identity

Context

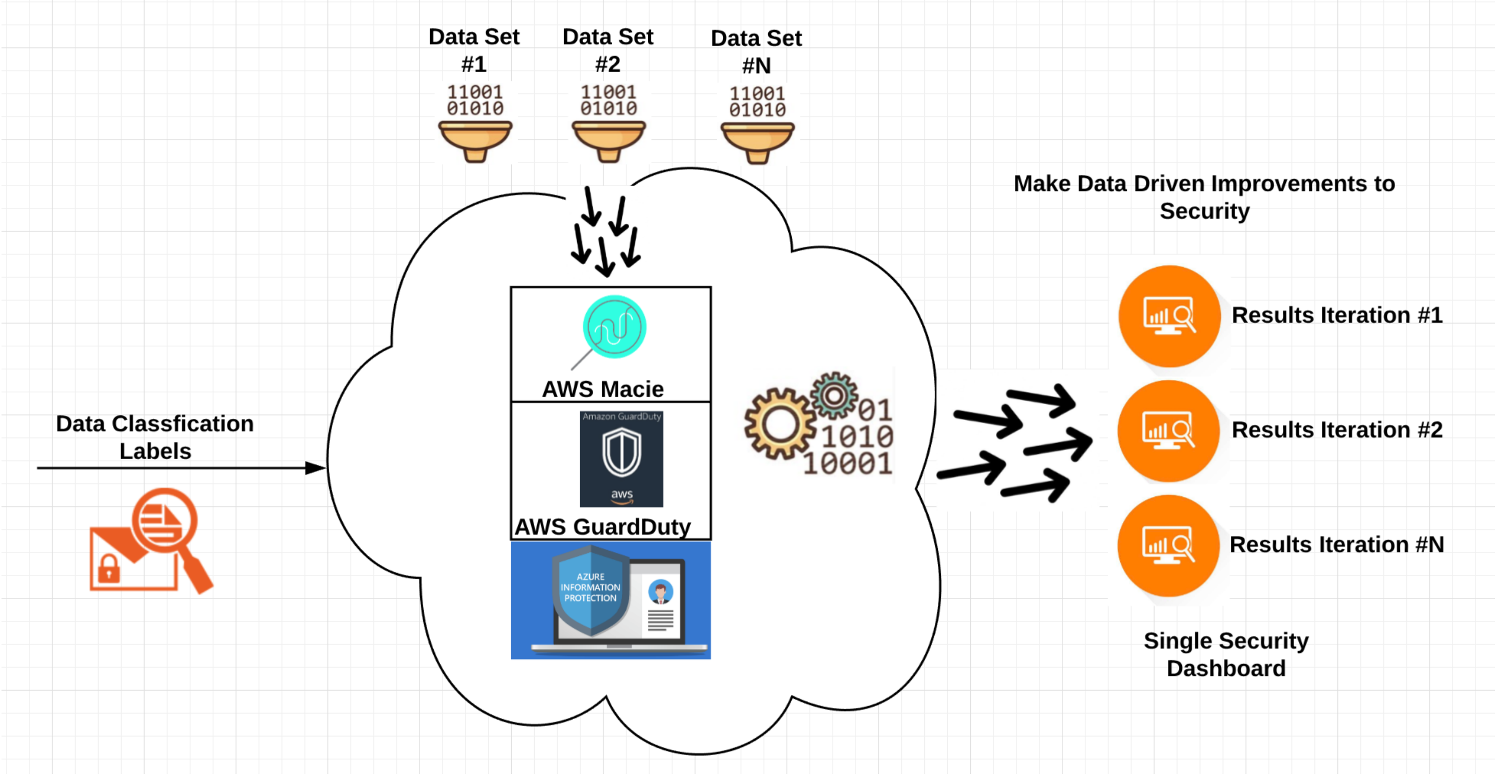
Rules Engine

Enforcement Point

Log Types, Critical Events & Attributes



Cloud Security Insights Matter



Data Set #1

Data Set #2

Data Set #N

Data Classfication Labels

AWS Macie

AWS GuardDuty

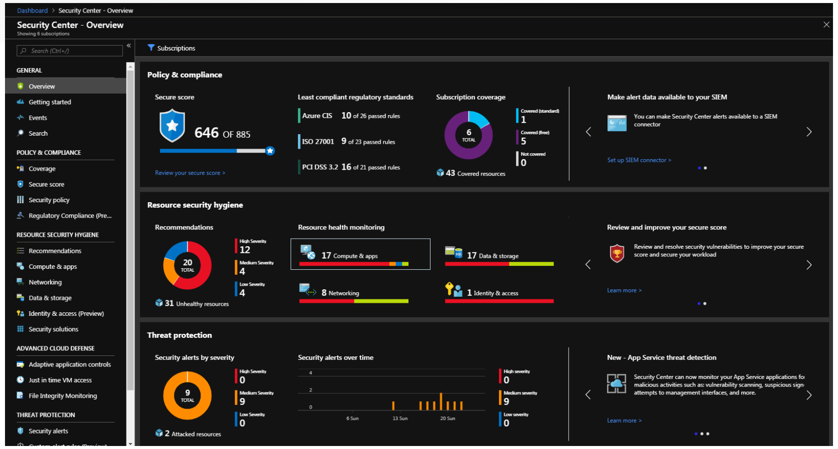
Make Data Driven Improvements to Security

Results Iteration #1

Results Iteration #2

Results Iteration #N

Single Security Dashboard



Security Center - Overview

Showing 6 subscriptions

Policy & compliance

Secure score: 646 OF 885

Review your secure score >

Least compliant regulatory standards

Azure CIS 10 of 26 passed rules

ISO 27001 9 of 23 passed rules

PCI DSS 3.2 16 of 21 passed rules

Subscription coverage: 6 TOTAL

Covered (standard) 1

Covered (free) 5

Not covered 0

43 Covered resources

Make alert data available to your SIEM

You can make Security Center alerts available to a SIEM connector

Set up SIEM connector >

Resource security hygiene

Recommendations: 20 TOTAL

High Severity 12

Medium Severity 4

Low Severity 4

31 Unhealthy resources

Resource health monitoring

17 Compute & apps

17 Data & storage

8 Networking

1 Identity & access

Review and improve your secure score

Review and resolve security vulnerabilities to improve your secure score and secure your workload

Learn more >

Threat protection

Security alerts by severity: 9 TOTAL

High Severity 0

Medium Severity 9

Low Severity 0

2 Attacked resources

Security alerts over time

High severity 0

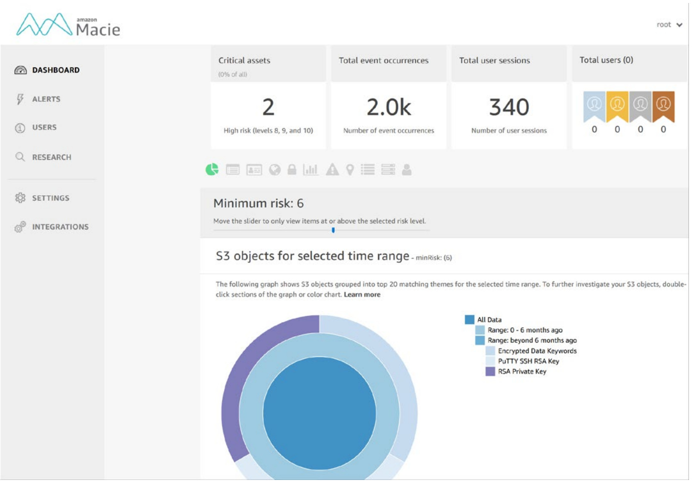
Medium severity 9

Low severity 0

New - App Service threat detection

Security Center can now monitor your App Service applications for malicious activities such as: vulnerability scanning, suspicious sign-attempts to management interfaces, and more.

Learn more >



Critical assets (0% of all): 2 High risk (levels 8, 9, and 10)

Total event occurrences: 2.0k Number of event occurrences

Total user sessions: 340 Number of user sessions

Total users (0): 0 0 0 0

Minimum risk: 6

Move the slider to only view items at or above the selected risk level.

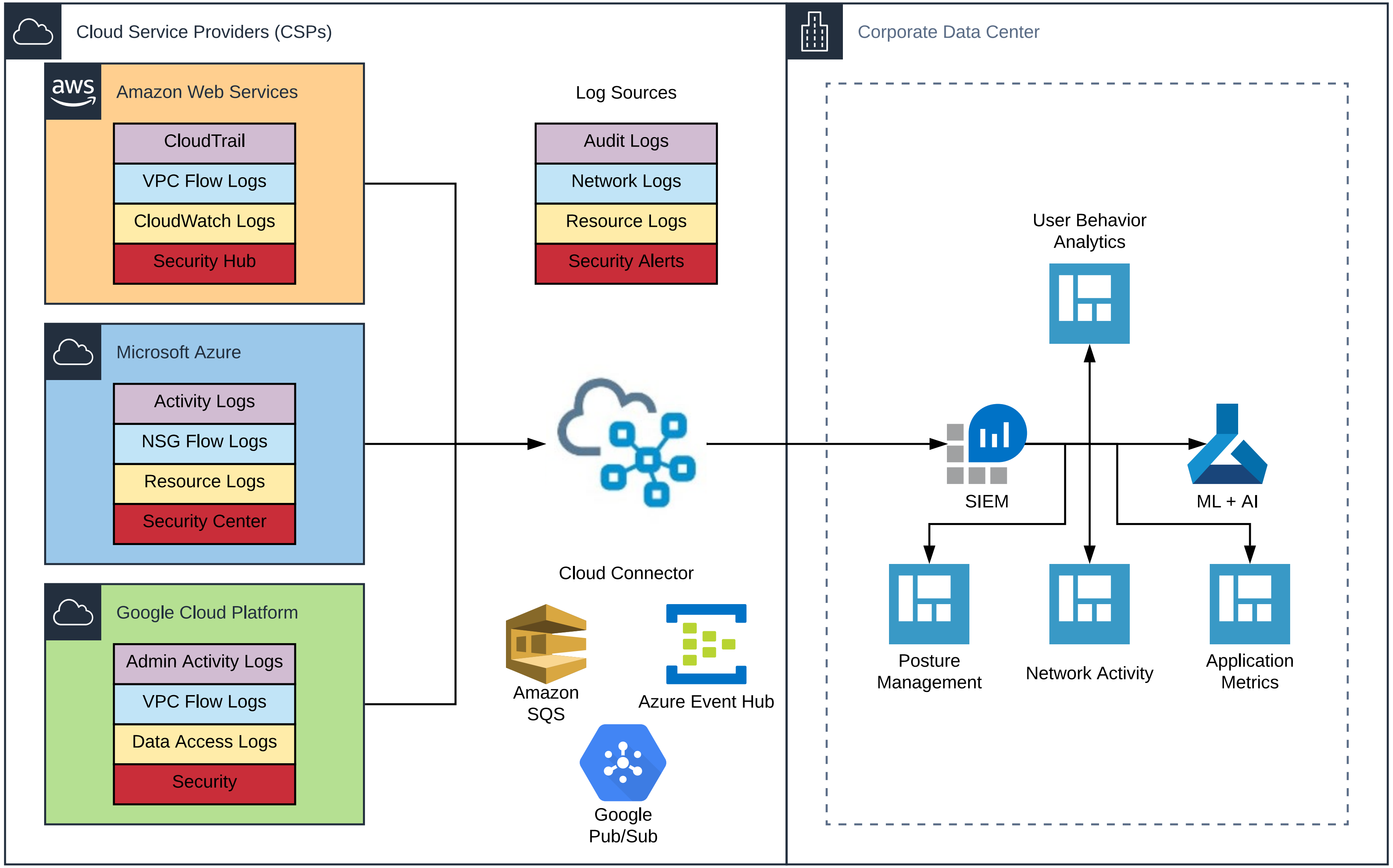
S3 objects for selected time range - minRisk: (6)

The following graph shows S3 objects grouped into top 20 matching themes for the selected time range. To further investigate your S3 objects, double-click sections of the graph or color chart. Learn more

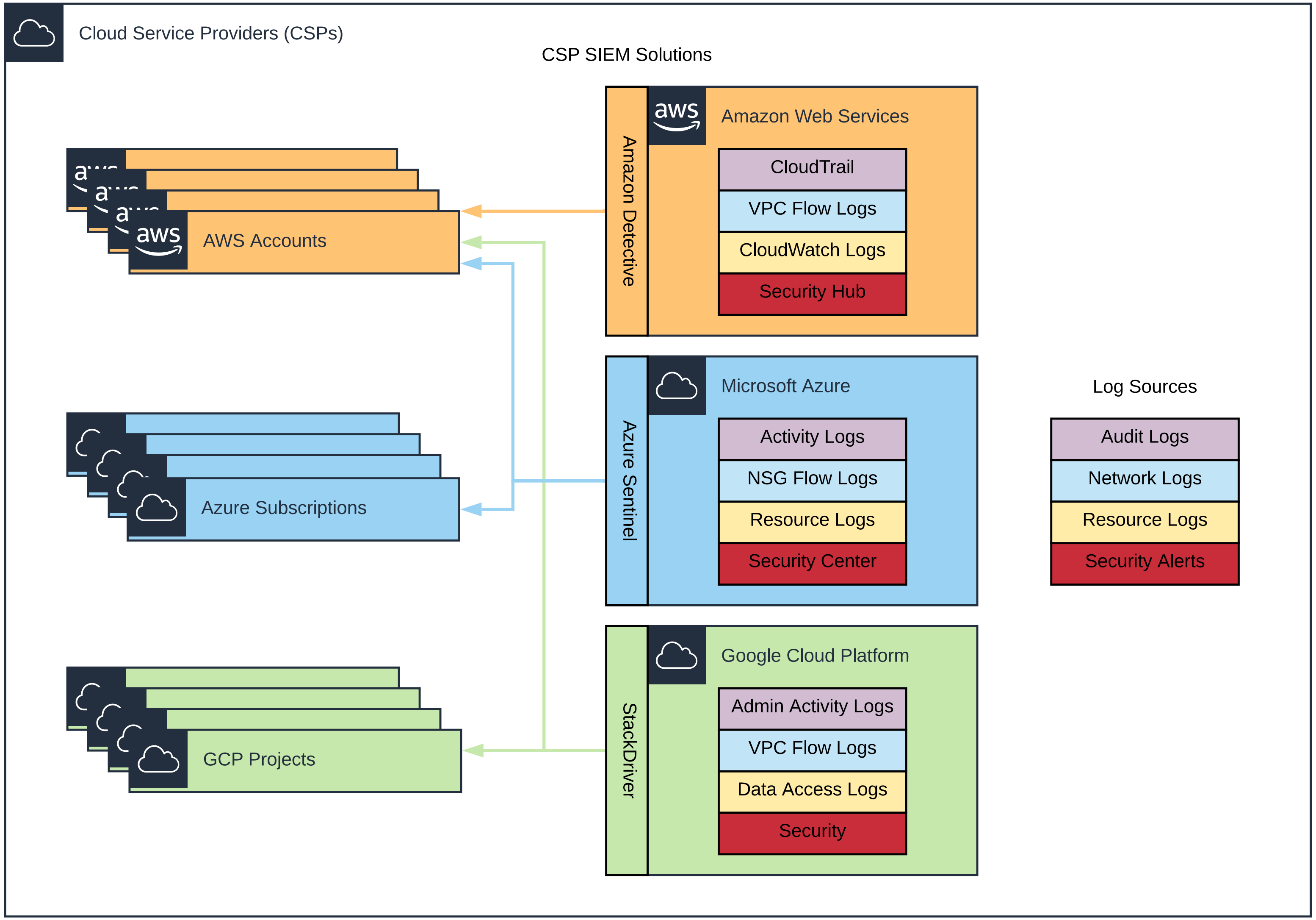
- All Data
  - Range: 0 - 6 months ago
  - Range: beyond 6 months ago
    - Encrypted Data Keywords
    - PuTTY SSH RSA Key
    - RSA Private Key

Architecture

Multi-Cloud Logging Architecture – On-Premises SIEM



Multi-Cloud Logging Architecture – CSP Cloud SIEMs



Technical Challenges & Solutions

Log Challenges & Solutions

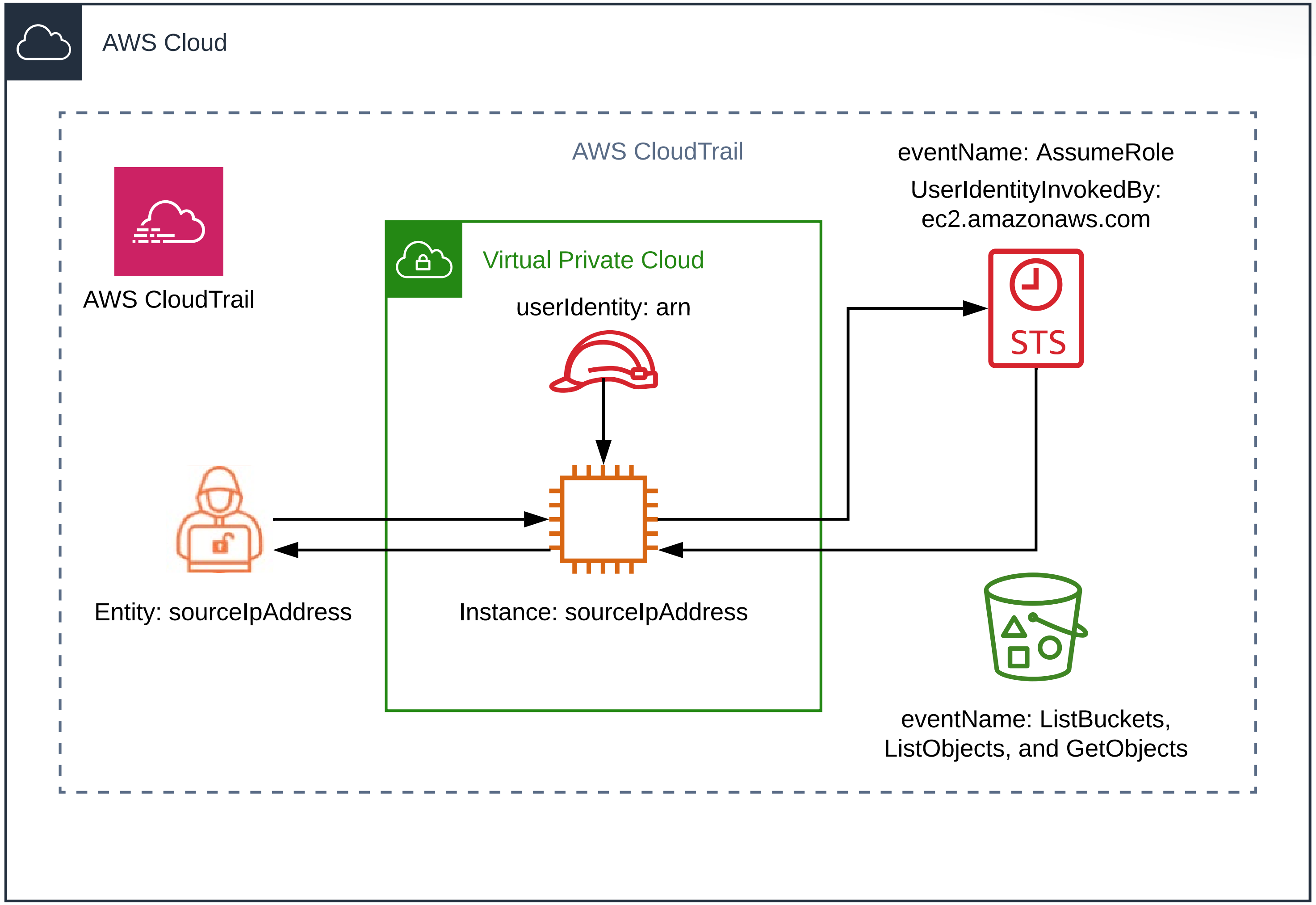
Every CSP requires different solutions to support log management
Understand each CSPs platform requirements to create effective log solution

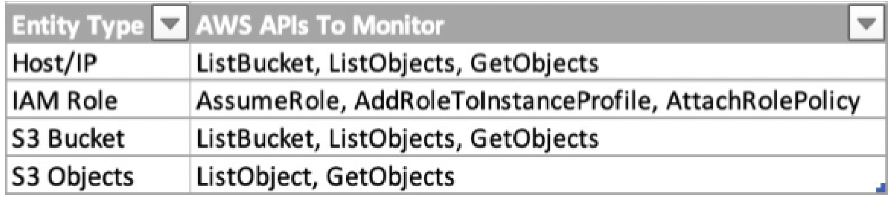
OS-level audit logs are difficult to collect without an agent
Use configuration management to deploy software agents consistently

Most CSPs do not provide built-in configuration management
Develop a golden image to reinforce organizational security standards

Network logs are difficult to read by themselves
Create network-specific dashboards: Traffic by IP, Protocol, or Host

Critical Attributes For Log Monitoring

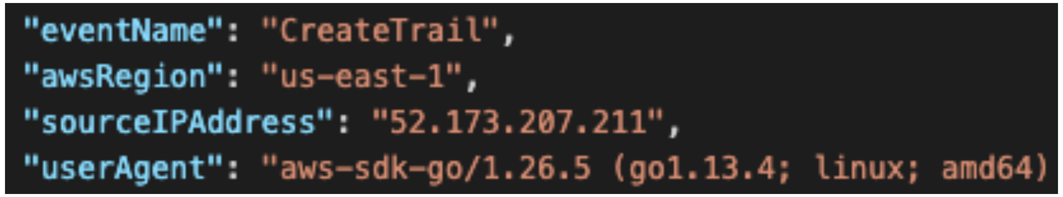




Entity Type	AWS APIs To Monitor
Host/IP	ListBucket, ListObjects, GetObjects
IAM Role	AssumeRole, AddRoleToInstanceProfile, AttachRolePolicy
S3 Bucket	ListBucket, ListObjects, GetObjects
S3 Objects	ListObject, GetObjects

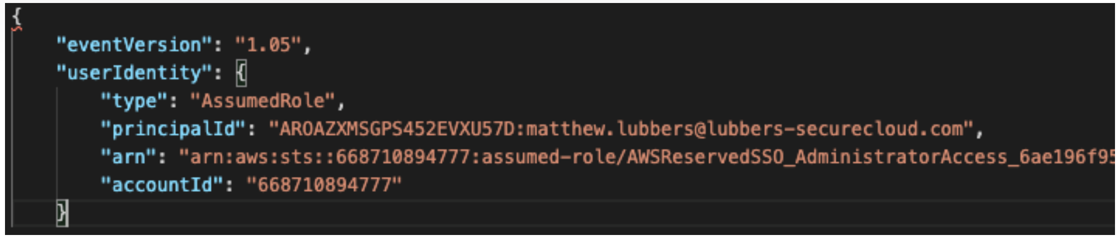
AWS Audit Log

- CloudTrail:
  - userIdentity (User/Service) – Who is doing what
  - sourceIpAddress – Where was the request generated
  - userAgent – Device information (Firefox, Win 10)
  - eventName – The API call being made



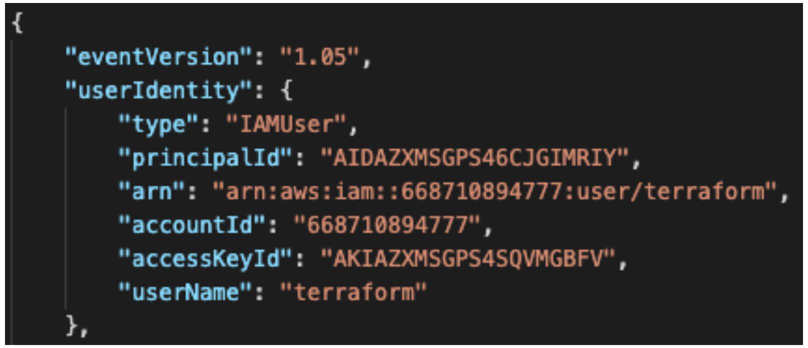
```
"eventName": "CreateTrail",
"awsRegion": "us-east-1",
"sourceIPAddress": "52.173.207.211",
"userAgent": "aws-sdk-go/1.26.5 (go1.13.4; linux; amd64)
```

Context



```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAZXMSGPS452EVXU57D:matthew.lubbers@lubbers-securecloud.com",
        "arn": "arn:aws:sts::668710894777:assumed-role/AWSReservedSSO_AdministratorAccess_6ae196f95
        "accountId": "668710894777"
    }
```

IAM Role

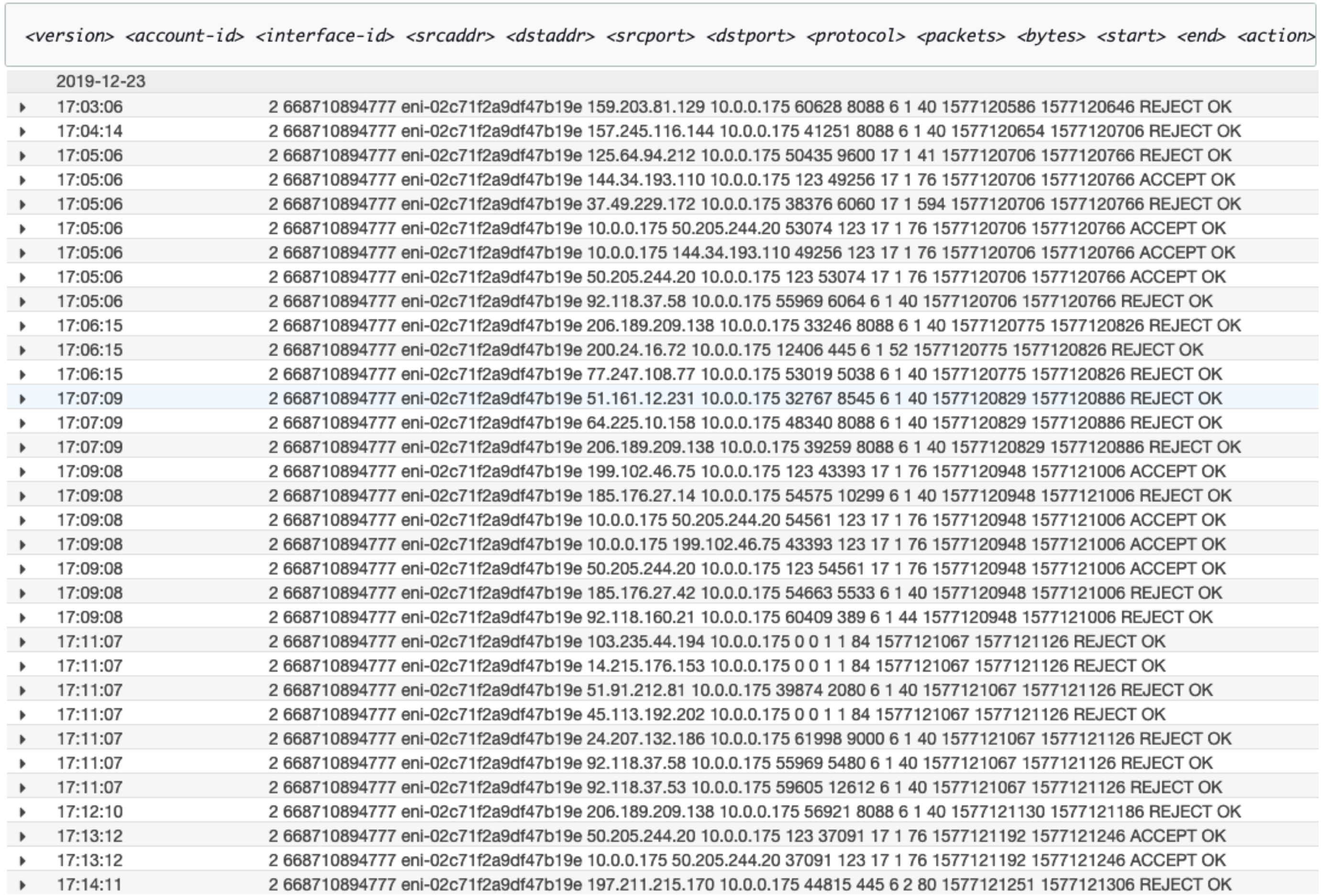


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAZXMSGPS46CJGIMRIY",
        "arn": "arn:aws:iam::668710894777:user/terraform",
        "accountId": "668710894777",
        "accessKeyId": "AKIAZXMSGPS4SQVMGBFV",
        "userName": "terraform"
    },
```

IAM User

AWS Network Log

- VPC Flow Logs
  - Source Address
  - Destination Address
  - Destination Port
  - Protocol
  - Action



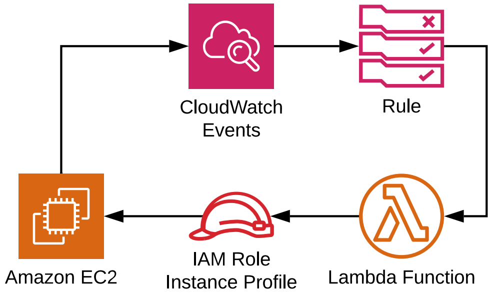
```
<version> <account-id> <interface-id> <srcaddr> <dstaddr> <srcport> <dstport> <protocol> <packets> <bytes> <start> <end> <action>

    2019-12-23
▸   17:03:06      2 668710894777 eni-02c71f2a9df47b19e 159.203.81.129 10.0.0.175 60628 8088 6 1 40 1577120586 1577120646 REJECT OK
▸   17:04:14      2 668710894777 eni-02c71f2a9df47b19e 157.245.116.144 10.0.0.175 41251 8088 6 1 40 1577120654 1577120706 REJECT OK
▸   17:05:06      2 668710894777 eni-02c71f2a9df47b19e 125.64.94.212 10.0.0.175 50435 9600 17 1 41 1577120706 1577120766 REJECT OK
▸   17:05:06      2 668710894777 eni-02c71f2a9df47b19e 144.34.193.110 10.0.0.175 123 49256 17 1 76 1577120706 1577120766 ACCEPT OK
▸   17:05:06      2 668710894777 eni-02c71f2a9df47b19e 37.49.229.172 10.0.0.175 38376 6060 17 1 594 1577120706 1577120766 REJECT OK
▸   17:05:06      2 668710894777 eni-02c71f2a9df47b19e 10.0.0.175 50.205.244.20 53074 123 17 1 76 1577120706 1577120766 ACCEPT OK
▸   17:05:06      2 668710894777 eni-02c71f2a9df47b19e 10.0.0.175 144.34.193.110 49256 123 17 1 76 1577120706 1577120766 ACCEPT OK
▸   17:05:06      2 668710894777 eni-02c71f2a9df47b19e 50.205.244.20 10.0.0.175 123 53074 17 1 76 1577120706 1577120766 ACCEPT OK
▸   17:05:06      2 668710894777 eni-02c71f2a9df47b19e 92.118.37.58 10.0.0.175 55969 6064 6 1 40 1577120706 1577120766 REJECT OK
▸   17:06:15      2 668710894777 eni-02c71f2a9df47b19e 206.189.209.138 10.0.0.175 33246 8088 6 1 40 1577120775 1577120826 REJECT OK
▸   17:06:15      2 668710894777 eni-02c71f2a9df47b19e 200.24.16.72 10.0.0.175 12406 445 6 1 52 1577120775 1577120826 REJECT OK
▸   17:06:15      2 668710894777 eni-02c71f2a9df47b19e 77.247.108.77 10.0.0.175 53019 5038 6 1 40 1577120775 1577120826 REJECT OK
▸   17:07:09      2 668710894777 eni-02c71f2a9df47b19e 51.161.12.231 10.0.0.175 32767 8545 6 1 40 1577120829 1577120886 REJECT OK
▸   17:07:09      2 668710894777 eni-02c71f2a9df47b19e 64.225.10.158 10.0.0.175 48340 8088 6 1 40 1577120829 1577120886 REJECT OK
▸   17:07:09      2 668710894777 eni-02c71f2a9df47b19e 206.189.209.138 10.0.0.175 39259 8088 6 1 40 1577120829 1577120886 REJECT OK
▸   17:09:08      2 668710894777 eni-02c71f2a9df47b19e 199.102.46.75 10.0.0.175 123 43393 17 1 76 1577120948 1577121006 ACCEPT OK
▸   17:09:08      2 668710894777 eni-02c71f2a9df47b19e 185.176.27.14 10.0.0.175 54575 10299 6 1 40 1577120948 1577121006 REJECT OK
▸   17:09:08      2 668710894777 eni-02c71f2a9df47b19e 10.0.0.175 50.205.244.20 54561 123 17 1 76 1577120948 1577121006 ACCEPT OK
▸   17:09:08      2 668710894777 eni-02c71f2a9df47b19e 10.0.0.175 199.102.46.75 43393 123 17 1 76 1577120948 1577121006 ACCEPT OK
▸   17:09:08      2 668710894777 eni-02c71f2a9df47b19e 50.205.244.20 10.0.0.175 123 54561 17 1 76 1577120948 1577121006 ACCEPT OK
▸   17:09:08      2 668710894777 eni-02c71f2a9df47b19e 185.176.27.42 10.0.0.175 54663 5533 6 1 40 1577120948 1577121006 REJECT OK
▸   17:09:08      2 668710894777 eni-02c71f2a9df47b19e 92.118.160.21 10.0.0.175 60409 389 6 1 44 1577120948 1577121006 REJECT OK
▸   17:11:07      2 668710894777 eni-02c71f2a9df47b19e 103.235.44.194 10.0.0.175 0 0 1 1 84 1577121067 1577121126 REJECT OK
▸   17:11:07      2 668710894777 eni-02c71f2a9df47b19e 14.215.176.153 10.0.0.175 0 0 1 1 84 1577121067 1577121126 REJECT OK
▸   17:11:07      2 668710894777 eni-02c71f2a9df47b19e 51.91.212.81 10.0.0.175 39874 2080 6 1 40 1577121067 1577121126 REJECT OK
▸   17:11:07      2 668710894777 eni-02c71f2a9df47b19e 45.113.192.202 10.0.0.175 0 0 1 1 84 1577121067 1577121126 REJECT OK
▸   17:11:07      2 668710894777 eni-02c71f2a9df47b19e 24.207.132.186 10.0.0.175 61998 9000 6 1 40 1577121067 1577121126 REJECT OK
▸   17:11:07      2 668710894777 eni-02c71f2a9df47b19e 92.118.37.58 10.0.0.175 55969 5480 6 1 40 1577121067 1577121126 REJECT OK
▸   17:11:07      2 668710894777 eni-02c71f2a9df47b19e 92.118.37.53 10.0.0.175 59605 12612 6 1 40 1577121067 1577121126 REJECT OK
▸   17:12:10      2 668710894777 eni-02c71f2a9df47b19e 206.189.209.138 10.0.0.175 56921 8088 6 1 40 1577121130 1577121186 REJECT OK
▸   17:13:12      2 668710894777 eni-02c71f2a9df47b19e 50.205.244.20 10.0.0.175 123 37091 17 1 76 1577121192 1577121246 ACCEPT OK
▸   17:13:12      2 668710894777 eni-02c71f2a9df47b19e 10.0.0.175 50.205.244.20 37091 123 17 1 76 1577121192 1577121246 ACCEPT OK
▸   17:14:11      2 668710894777 eni-02c71f2a9df47b19e 197.211.215.170 10.0.0.175 44815 445 6 2 80 1577121251 1577121306 REJECT OK
```

Use-case: System visibility for Compute

HashiCorp Terraform

HashiCorp Packer

Monitors CloudTrail for ec2:StartInstances, ec2:RebootInstances, or ec2:RunInstances API Call



Event Rule triggers the Lambda function

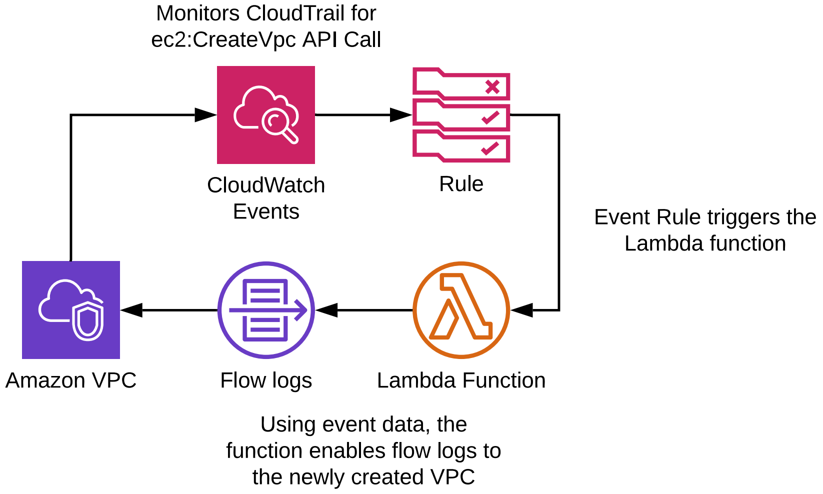
Using event data, the function attaches a role to allow syslog collection on EC2 instances

Use-case: AWS Audit Logging

HashiCorp
Terraform

Use-case: Network visibility for Security Events

HashiCorp
Terraform



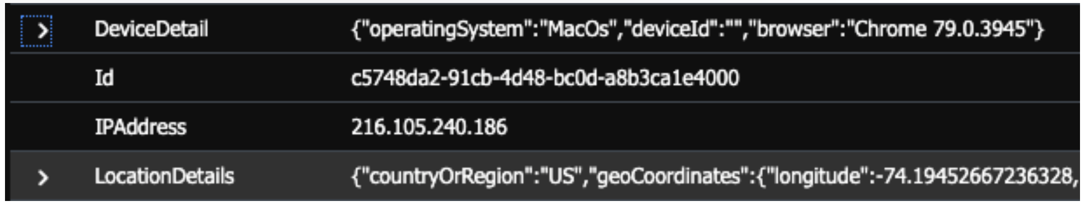
Monitors CloudTrail for ec2:CreateVpc API Call

Event Rule triggers the Lambda function

Using event data, the function enables flow logs to the newly created VPC

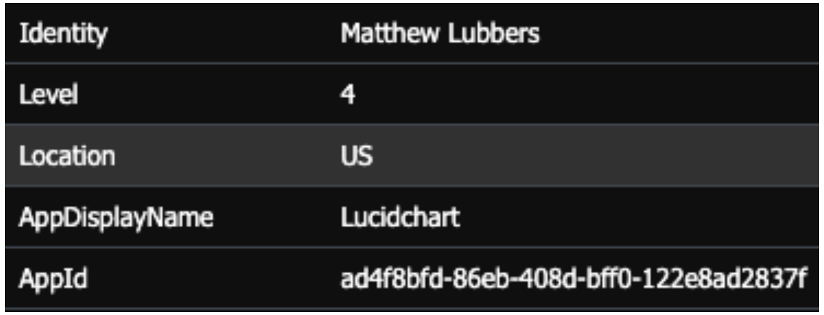
Azure Active Directory Logs

- Sign-in Logs:
  - Principal (User) – Who has logged in
  - IP Address - Where they have logged in from
  - Client – Device information
- Audit Logs
  - Initiated By (Actor) – Who is doing what in Azure AD
  - Service – The directory service being used
  - Activity – The API call made to the service



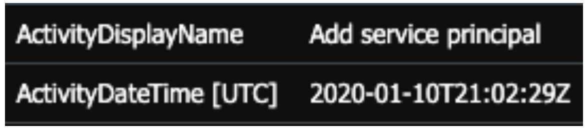
>	DeviceDetail	{"operatingSystem":"MacOs","deviceId":"","browser":"Chrome 79.0.3945"}
	Id	c5748da2-91cb-4d48-bc0d-a8b3ca1e4000
	IPAddress	216.105.240.186
>	LocationDetails	{"countryOrRegion":"US","geoCoordinates":{"longitude":-74.19452667236328,

Context



Identity	Matthew Lubbers
Level	4
Location	US
AppDisplayName	Lucidchart
AppId	ad4f8bfd-86eb-408d-bff0-122e8ad2837f

Principal

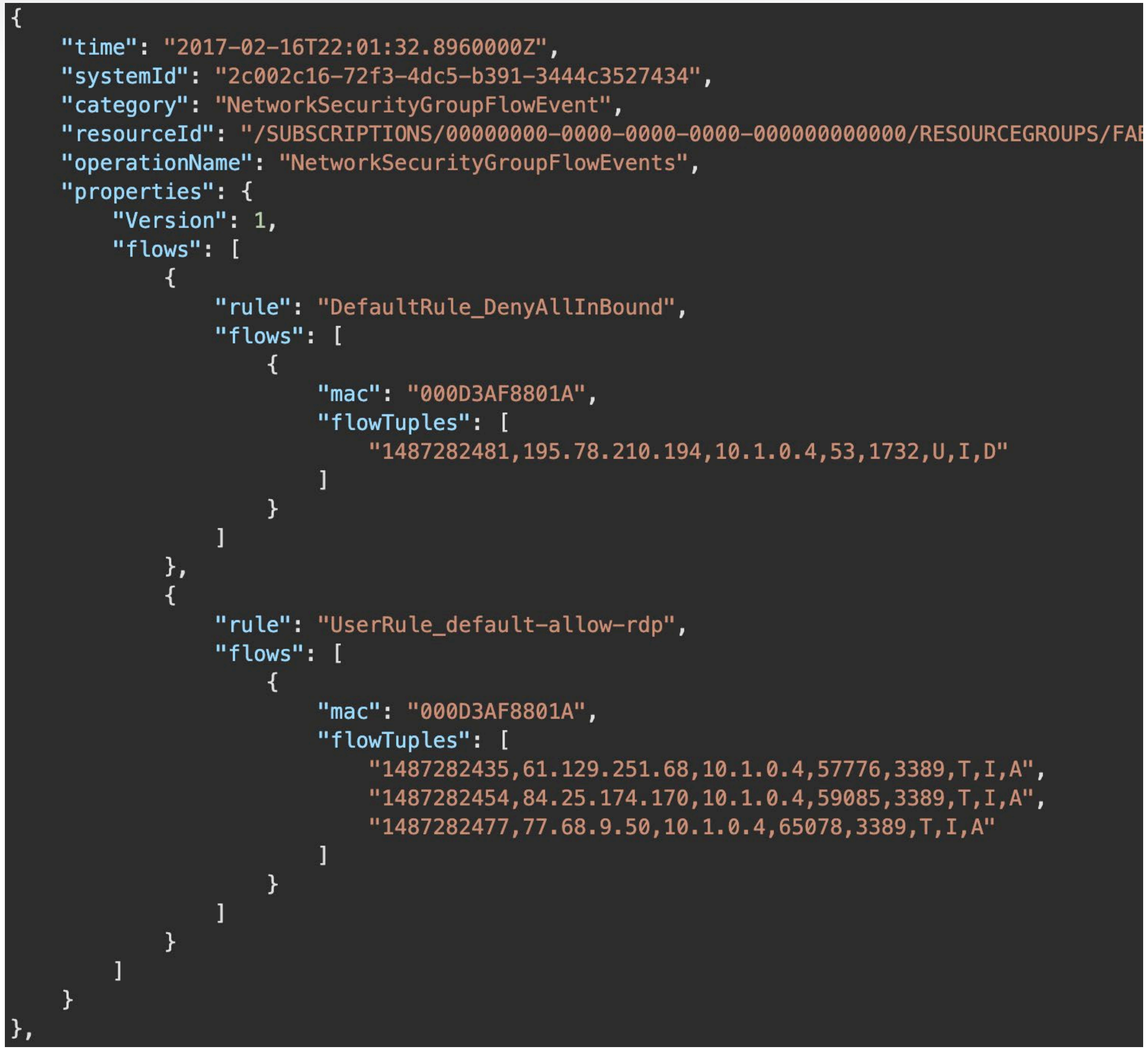


ActivityDisplayName	Add service principal
ActivityDateTime [UTC]	2020-01-10T21:02:29Z

Activity

Azure Network Logs

- NSG Flow Logs
  - Source Address
  - Destination Address
  - Destination Port
  - Protocol
  - Traffic Decision



```
{
    "time": "2017-02-16T22:01:32.8960000Z",
    "systemId": "2c002c16-72f3-4dc5-b391-3444c3527434",
    "category": "NetworkSecurityGroupFlowEvent",
    "resourceId": "/SUBSCRIPTIONS/00000000-0000-0000-0000-000000000000/RESOURCEGROUPS/FAE
    "operationName": "NetworkSecurityGroupFlowEvents",
    "properties": {
        "Version": 1,
        "flows": [
            {
                "rule": "DefaultRule_DenyAllInBound",
                "flows": [
                    {
                        "mac": "000D3AF8801A",
                        "flowTuples": [
                            "1487282481,195.78.210.194,10.1.0.4,53,1732,U,I,D"
                        ]
                    }
                ]
            },
            {
                "rule": "UserRule_default-allow-rdp",
                "flows": [
                    {
                        "mac": "000D3AF8801A",
                        "flowTuples": [
                            "1487282435,61.129.251.68,10.1.0.4,57776,3389,T,I,A",
                            "1487282454,84.25.174.170,10.1.0.4,59085,3389,T,I,A",
                            "1487282477,77.68.9.50,10.1.0.4,65078,3389,T,I,A"
                        ]
                    }
                ]
            }
        ]
    }
},
```

Use-case: Automated Agent Deployment

HashiCorp Terraform

Azure Policy

Azure Monitor

Use-case: Network & Resource visibility for Security Events

HashiCorp Terraform

Automation Account

Take Away Checklist

Ç Establish a cloud security governance program

Ç Understand organizational constraints

Ç Establish cloud risks and threats

Ç Identify critical cloud logs and events

Ç Develop logging strategy based on business requirements

Ç Logging varies across CSPs, understand various CSP logging strategies

Ç Develop security log integration Architecture
(Native vs Cloud vs On-premise)

Ç Establish cloud log monitoring processes

Ç Automate using infrastructure as code and event driven architecture

Ç Focus on using AI/ML based insights

Useful Links

TD Ameritrade Cloud Security Github

https://github.com/TDAmeritrade/cloud-and-data-security

Cloud Security Governance

https://cloudsecurityalliance.org/research/cloud-controls-matrix/
https://www.sans.org/reading-room/whitepapers/cloud/paper/37960

Cloud Security Logging

https://aws.amazon.com/answers/logging/aws-native-security-logging-capabilities/
https://aws.amazon.com/answers/logging/
https://docs.microsoft.com/en-us/azure/security/fundamentals/log-audit
https://azure.microsoft.com/en-us/resources/videos/security-logging-and-audit-log-collection/