black hat USA 2018

AUGUST 4-9, 2018
MANDALAY BAY / LAS VEGAS

Detecting Malicious Cloud Account Behavior:

A Look at the New Native Platform Capabilities

@bradgeesaman

Bio

Previously

- Network Security Engineer
- Penetration Tester/Security Consultant

Past 8+ Years

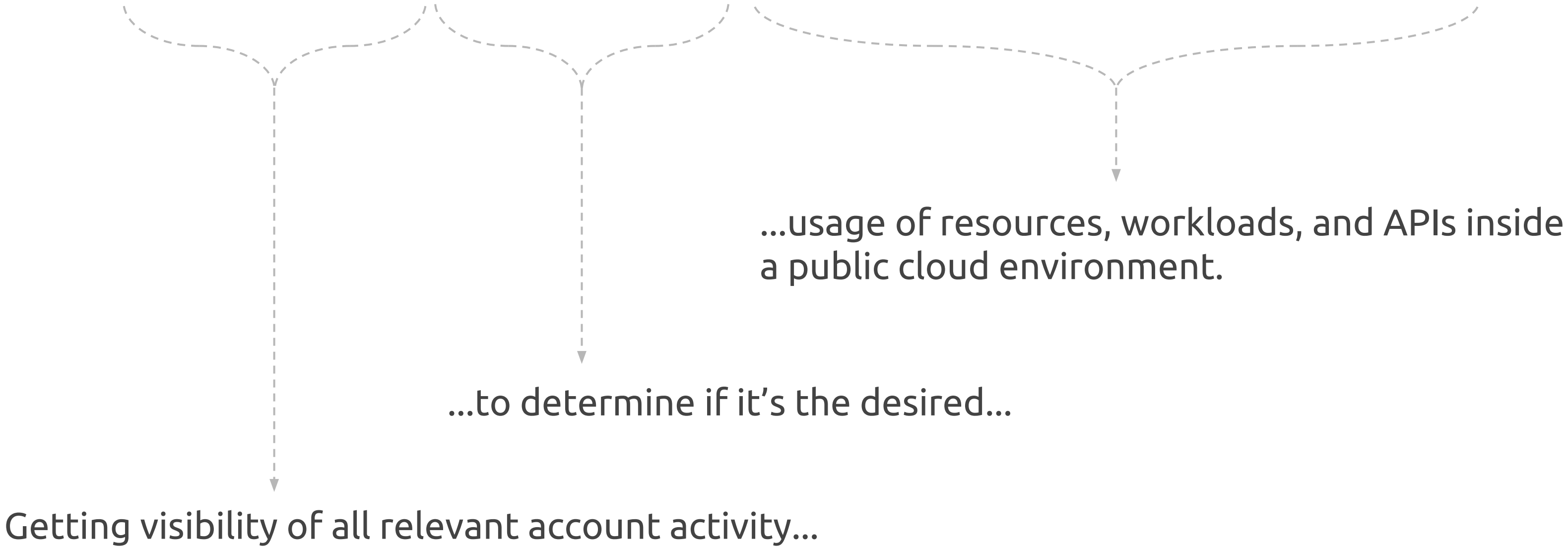
- Cloud Infrastructure Administrator
- “DevOps” practitioner *
- Ethical Hacking Educator
  - CTF Scenario design
  - Running CTF/Hacking competition workloads inside public clouds using containers **

Past Two Years

- Researching Cloud Security Issues with Containers and Container Orchestrators
  - *Hacking and Hardening Kubernetes Clusters by Example*: https://youtu.be/vTgQLzeBfRU
- Independent Consulting - Securing Containers and Kubernetes

* Sorry
** Not recommended. It seemed like a good idea then.

Detecting Malicious Cloud Account Behavior:



Getting visibility of all relevant account activity...

...to determine if it’s the desired...

...usage of resources, workloads, and APIs inside a public cloud environment.

This Talk is Aimed at

Attackers

Penetration Testers/Security Consultants who want to know how malicious activity is being analyzed and detected with and without the latest services enabled.

Defenders

Security practitioners who want to know more about cloud-specific threats, attack patterns, and how to gain better visibility and streamline detection workflows.

Business Leaders

Leaders who want to better understand cloud-specific threats, the cloud shared responsibility model, and where to focus to improve detections with a better grasp of the capabilities offered.

Security Architects/Ops/Builders

Those who design, build, and secure applications in cloud platforms who want to better understand how and when to leverage platform services vs DIY.

Roadmap

Explore the Problem Space

- Review two recent breaches
- Highlight cloud attack behavior

Understand the Challenges

- Discuss Pace of Innovation and Skills Gap
- Revisit the Cloud Shared Responsibility Model
- Determining “Normal” vs “Suspicious/Malicious”

The Latest “Native” Cloud Security Services

- Amazon GuardDuty (and supporting services)
- Microsoft Azure Security Center
- Google Cloud Security Command Center

Key Takeaways and Looking Ahead

- What the New Capabilities Offer
- Adoption and Perspectives

https://flic.kr/p/afRuwn

Explore the Problem Space

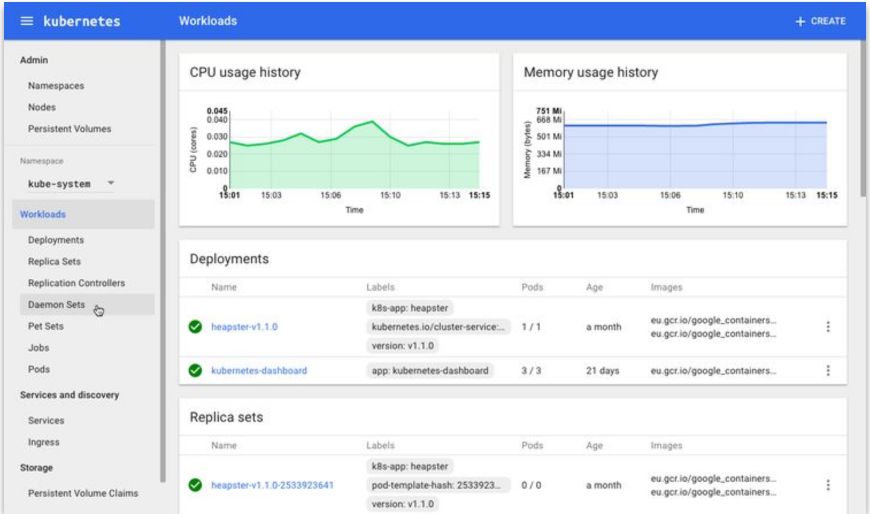
An Electric Car Manufacturer

Exposed Kubernetes Dashboard

- Kubernetes Cluster on AWS
- Installed CPU-throttled crypto-mining workers
- Tight integration with AWS Access Keys led to S3 data exfiltration
- Masked their sources behind a CDN

Not Alone

- Aviva and Gemalto



Deployments

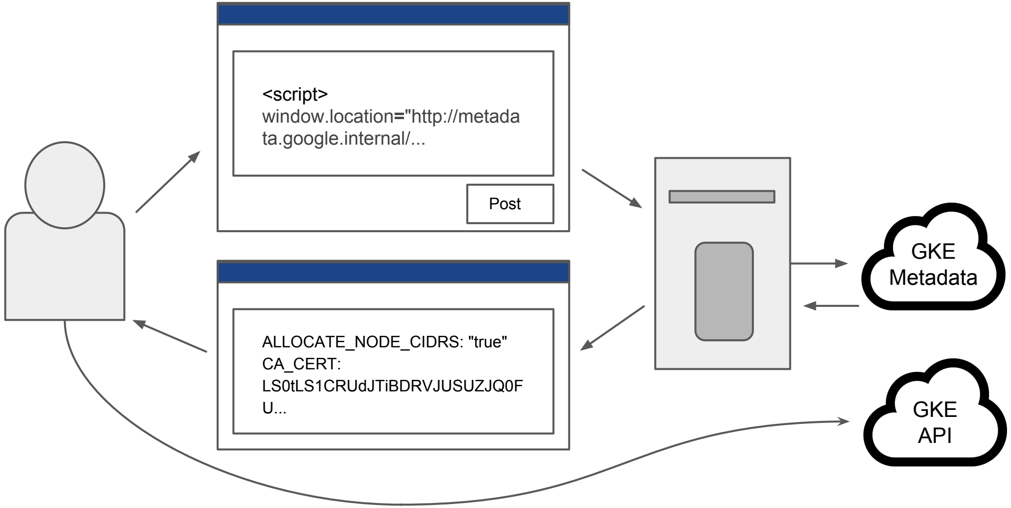
Name	Labels	Pods	Age	Images
✓ heapster-v1.1.0	k8s-app: heapster kubernetes.io/cluster-service:... version: v1.1.0	1 / 1	a month	eu.gcr.io/google_containers... eu.gcr.io/google_containers...
✓ kubernetes-dashboard	app: kubernetes-dashboard	3 / 3	21 days	eu.gcr.io/google_containers...

Replica sets

Name	Labels	Pods	Age	Images
✓ heapster-v1.1.0-2533923641	k8s-app: heapster pod-template-hash: 2533923... version: v1.1.0	0 / 0	a month	eu.gcr.io/google_containers... eu.gcr.io/google_containers...

http://fortune.com/2018/02/20/tesla-hack-amazon-cloud-cryptocurrency-mining/

An E-Commerce Shopping Platform



```
<script>
window.location="http://metada
ta.google.internal/...
```

```
ALLOCATE_NODE_CIDRS: "true"
CA_CERT:
LS0tLS1CRUdJTiBDRVJUSUZJQ0F
U...
```

Server-side Request Forgery

- $25K Bug Bounty - André Baptista (0xacb)
- Application flaw fetched instance metadata which contained GKE cluster credentials.
- Credentials allowed for escalation and privileged/root access to all nodes in the entire cluster.

https://hackerone.com/reports/341876

Other Potential Concerns

Credential theft

- Phishing
- Malware
- Backdoored libraries/tools
- Password guessing/weak passwords

Malicious Outsiders

- Compromise of 3rd Party Services with integrated access
- Failure to disable, delete, rotate credentials post termination

Credential Leaks

- Checked into source code
- Technical support tickets
- Public Q&A Tech Help chat/forums
- Applications transmit keys in headers, messages, or logs of API calls

You may be a *single flaw* away from cloud account compromise

Indicators of Malicious Cloud Account Behavior*

Network

- Activity to/from known-bad IPs
- Unusual changes to traffic patterns
- Unusual outbound port usage

DNS

- Queries to known-bad domains (CnC, bots, malware, crypto-mining, etc)
- Queries that embed data in the lookup

Host-based

- OS, Application, Security/Audit logs
- Security endpoint solution events

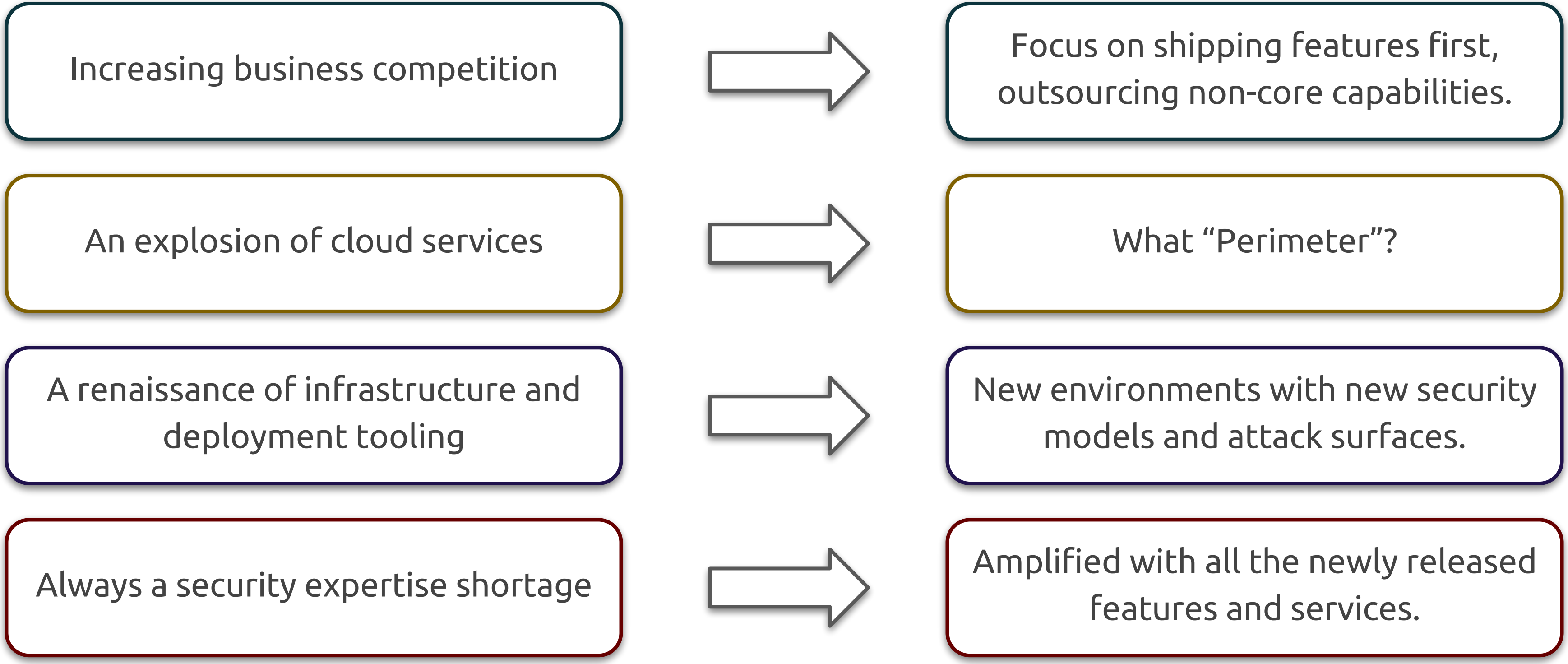
API Activity

- Multiple failed logins
- Simultaneous API access from different countries
- Attempted activity from terminated accounts/credentials/keys
- Uncommon service/API usage
- Credential/permission enumeration
- Changes to user accounts/logging/detection configurations
- Sensitive changes to user permissions
- Internal resource credentials used from external sources

* Not an exhaustive list.

Understand the Challenges

Pace of Innovation Leaves A Wake



Increasing business competition → Focus on shipping features first, outsourcing non-core capabilities.

An explosion of cloud services → What “Perimeter”?

A renaissance of infrastructure and deployment tooling → New environments with new security models and attack surfaces.

Always a security expertise shortage → Amplified with all the newly released features and services.

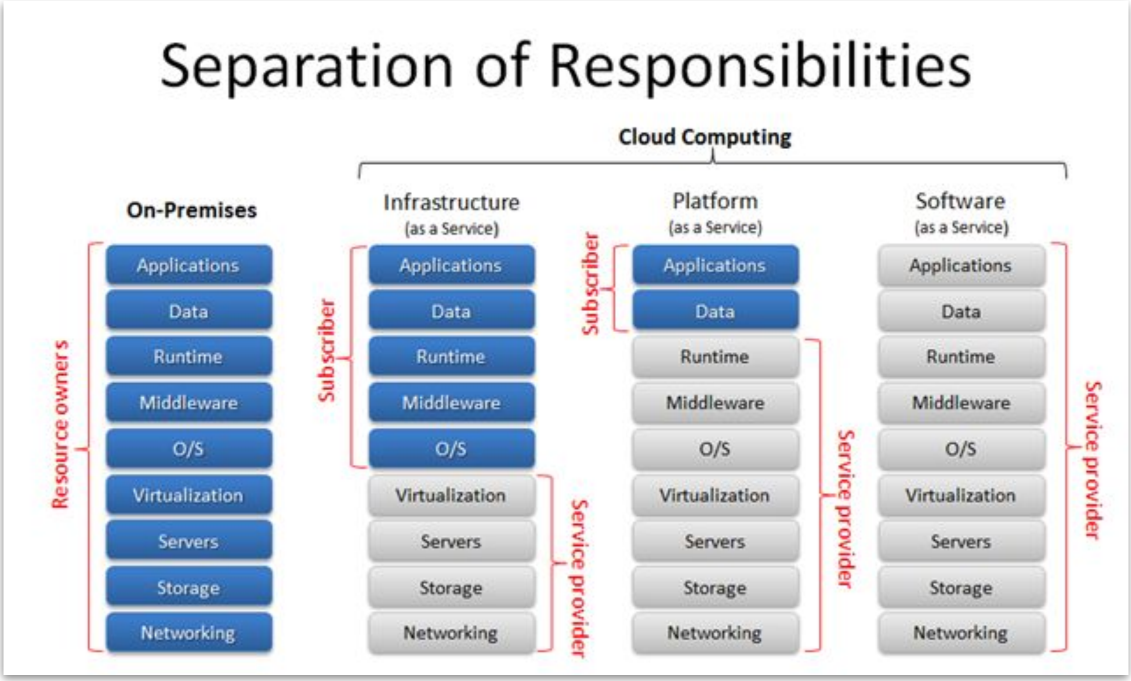
Some Challenges Unique to the Cloud

- Automation amplifies human and configuration errors.
- Inventory is extremely fluid.
- Basic security assumptions invalidate lots of approaches by traditional security products.
- Most cloud services logging mechanisms are very verbose.
- Actions performed against the cloud provider APIs often are hard to combine coherently.
- Some managed cloud services offer little to no security visibility.
- Integration of log and event data from cloud with on-premise SIEM systems.
- Response and Forensics capabilities are difficult to integrate.

Challenges Unique to the Cloud

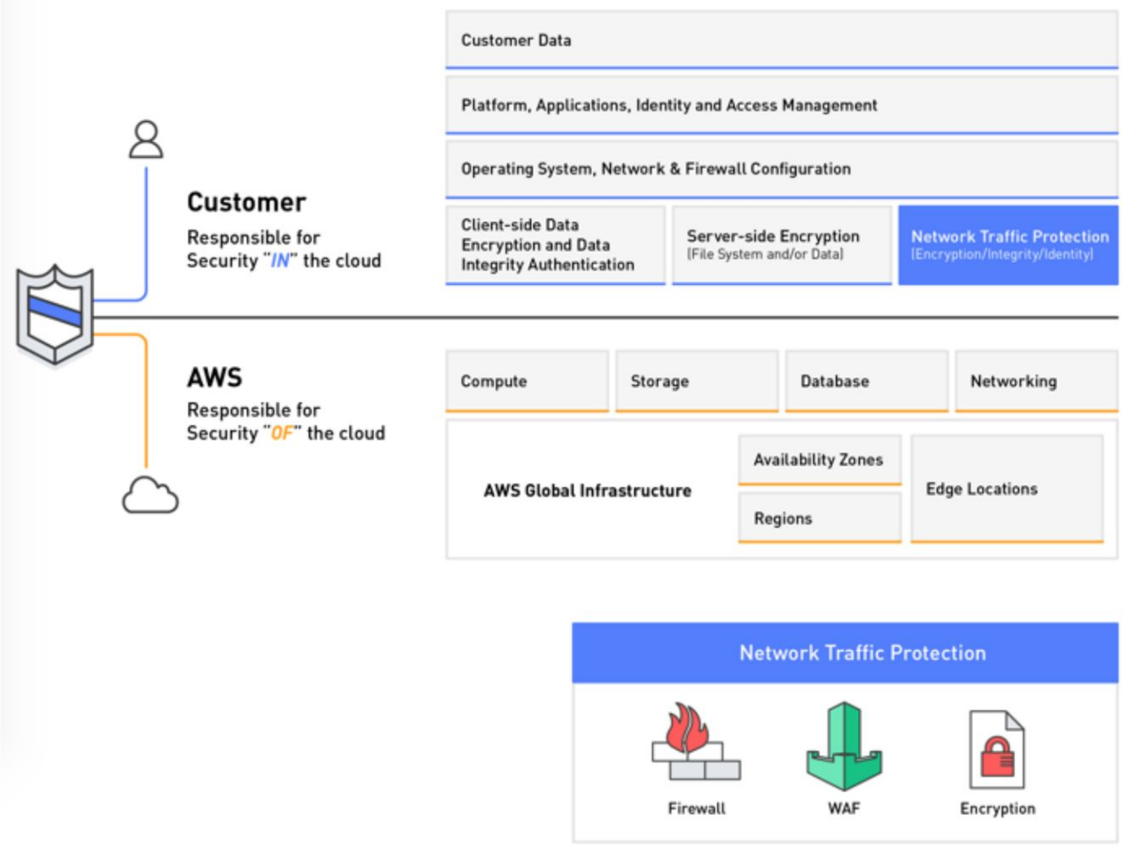
- Traditional security professionals and/or tooling lacking cloud-specific experience.
- Cloud-oriented professionals lacking traditional security experience and/or tooling.
- Traditional security implementation strategies cost time and money with high switching costs.
- Security vendors looking to go “cloud-native” have to heavily modify their approach--per cloud provider, per environment.

Cloud Shared Responsibility Model (2010)



https://blogs.technet.microsoft.com/yungchou/2010/12/17/cloud-computing-for-it-pros-26-what-is-cloud/

AWS Shared Responsibility Model



Customer Data

Platform, Applications, Identity and Access Management

Operating System, Network & Firewall Configuration

Client-side Data Encryption and Data Integrity Authentication

Server-side Encryption
(File System and/or Data)

Network Traffic Protection
(Encryption/Integrity/Identity)

Customer

Responsible for Security "IN" the cloud

AWS

Responsible for Security "OF" the cloud

Compute

Storage

Database

Networking

AWS Global Infrastructure

Availability Zones

Regions

Edge Locations

Network Traffic Protection

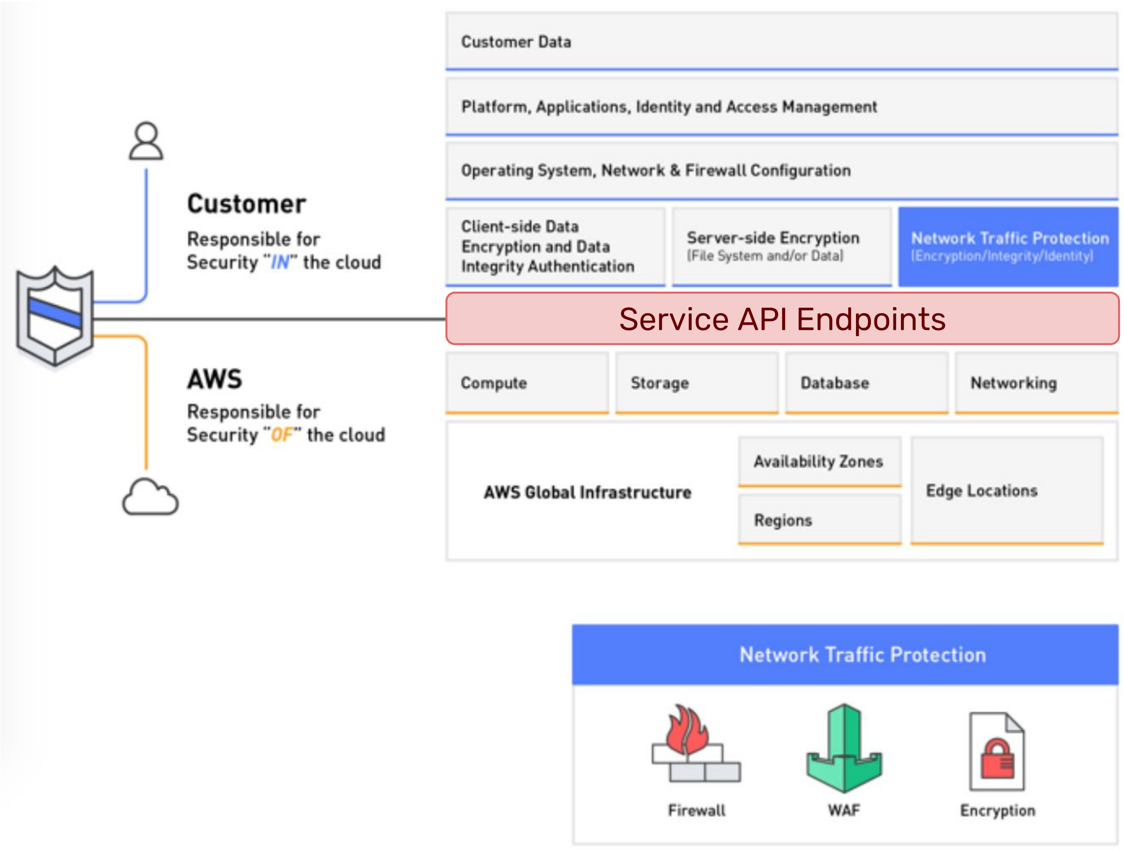
Firewall

WAF

Encryption

https://aws.amazon.com/mp/scenarios/security/malware/

AWS Shared Responsibility Model (Adapted)



Customer Data

Platform, Applications, Identity and Access Management

Operating System, Network & Firewall Configuration

Client-side Data Encryption and Data Integrity Authentication

Server-side Encryption [File System and/or Data]

Network Traffic Protection [Encryption/Integrity/Identity]

Service API Endpoints

Implied

Customer

Responsible for Security "IN" the cloud

AWS

Responsible for Security "OF" the cloud

Compute

Storage

Database

Networking

AWS Global Infrastructure

Availability Zones

Regions

Edge Locations

Network Traffic Protection

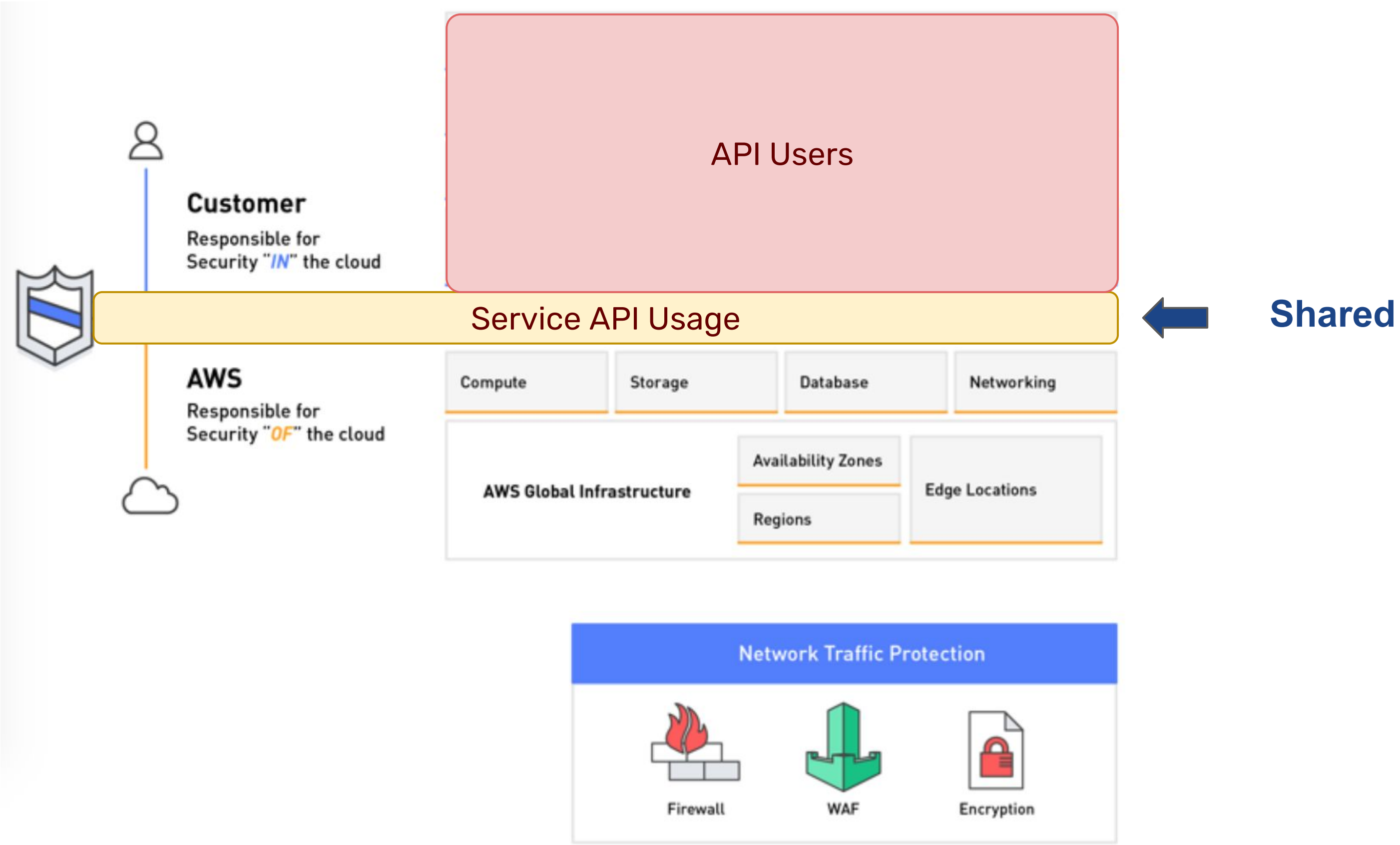
Firewall

WAF

Encryption

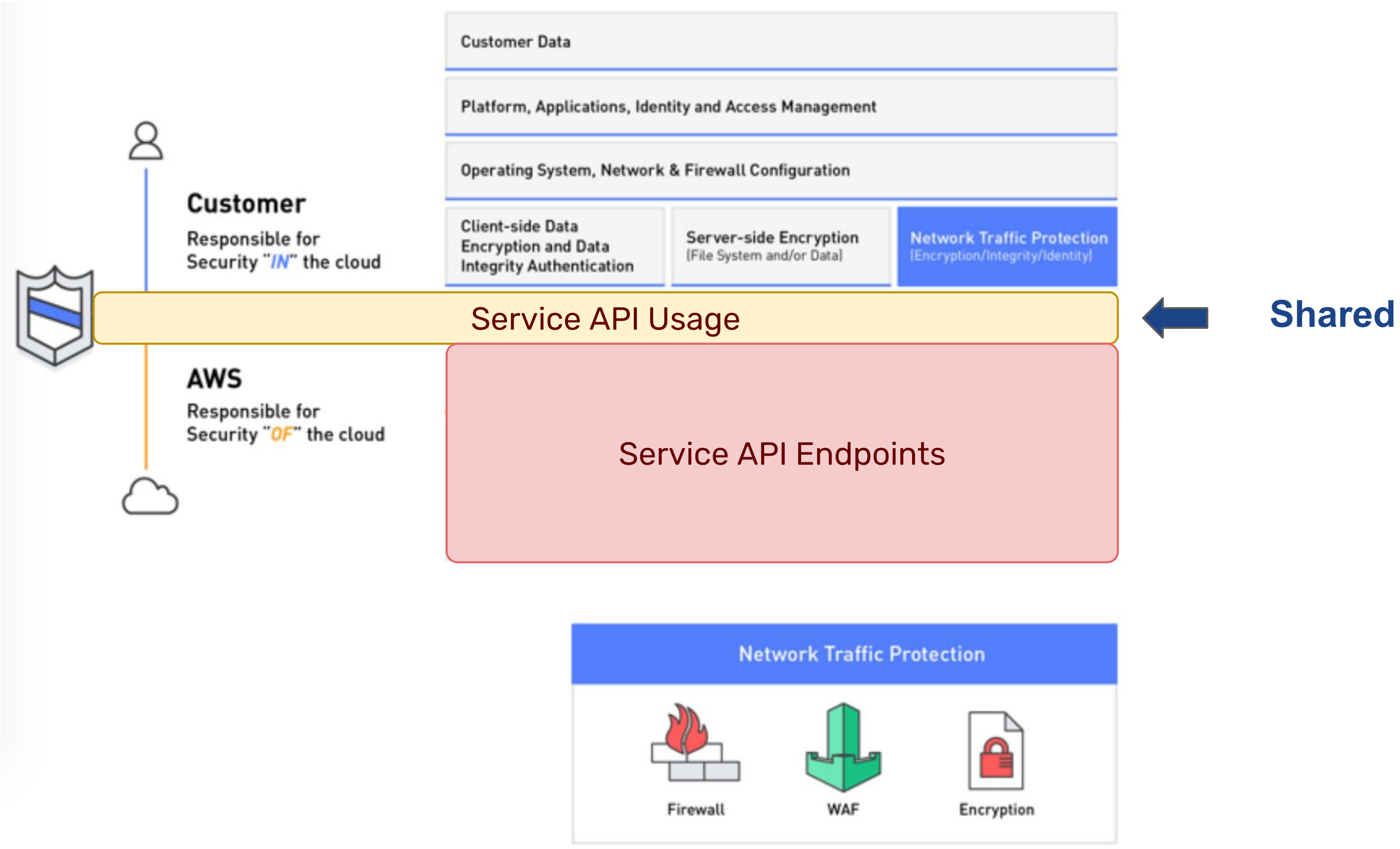
Adapted from https://aws.amazon.com/mp/scenarios/security/malware/

Shared Responsibility Model - Provider’s View



Adapted from https://aws.amazon.com/mp/scenarios/security/malware/

Shared Responsibility Model - Tenant's View



Customer Data

Platform, Applications, Identity and Access Management

Operating System, Network & Firewall Configuration

Client-side Data Encryption and Data Integrity Authentication

Server-side Encryption (File System and/or Data)

Network Traffic Protection (Encryption/Integrity/Identity)

Customer

Responsible for Security "*IN*" the cloud

Service API Usage

Shared

AWS

Responsible for Security "*OF*" the cloud

Service API Endpoints

Network Traffic Protection

Adapted from https://aws.amazon.com/mp/scenarios/security/malware/

Ambiguity Abounds

A “get all instances” API request is successfully authenticated from an IP never before seen in this cloud account.

Admin from a hotel while travelling abroad?

OR

Malicious user with stolen credentials.

Ambiguity Abounds

The API was just used to start up 10 large GPU-backed instances in a never-before used region.

A new project working with ML?

OR

A compromised account spinning up crypto-mining instances.

Ambiguity Abounds

Network traffic showing repeated HTTP connections on a high port to an external server on a routine interval.

A recurring task sending telemetry data every 30 minutes?

OR

A command and control channel.

Consider: **Many Third Party Services Have Some Form of Access to Your Cloud Account**

The Latest “Native” Cloud Security Services

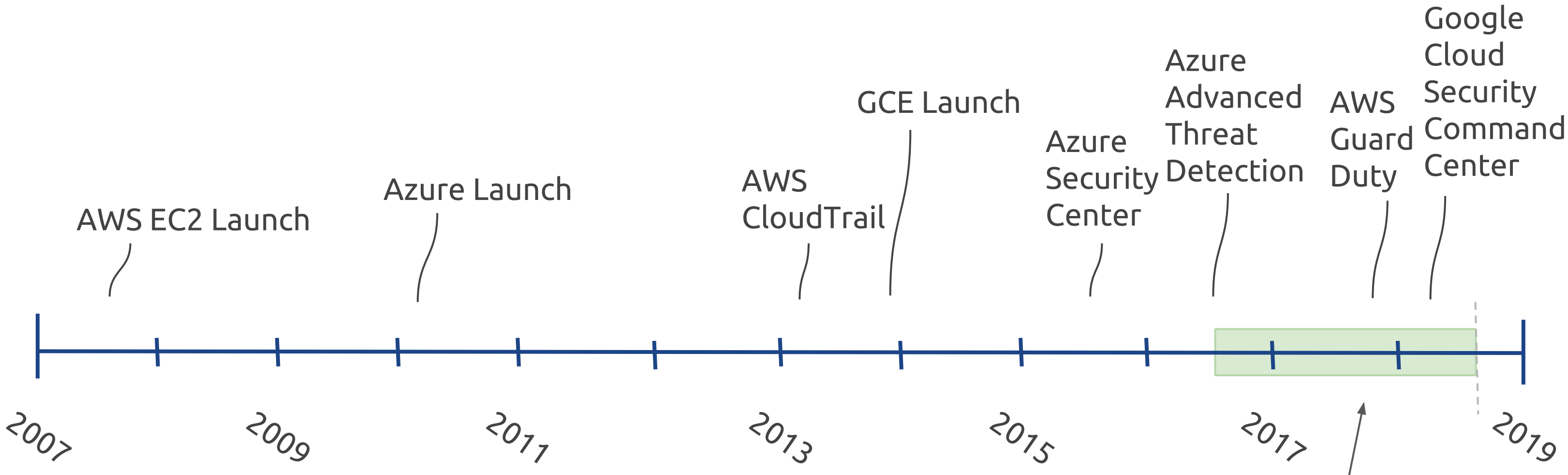
Services In Scope

Microsoft Azure Security Center, Advanced Threat Protection

AWS GuardDuty (and CloudTrail, CloudWatch)

Google Cloud Security Command Center

Service Launches



Very Recently Released

Questions Asked During This Review

- What data sources do they use?
- How do they operate on that data?
- What visibility does that data provide?
- What is not covered in the service?
- What is needed for onboarding?
- What’s the cost structure?
- How does it integrate with other internal services and partners?
- How accessible are these services to customization?
- How do you validate the detection capabilities?

Different Questions for Different Roles

Attackers

- What methods and tactics need to change to remain undetected?

Defenders

- What visibility do I now have?
- How much effort is required?
- What is still not covered in the service?

Business Leaders

- What exposure do I have?
- What's the ROI on enabling and maintaining these services

Security Architects/Ops/Builders

- How does this change my infrastructure design?
- What do I no longer have to DIY?

https://flic.kr/p/eX7ybV

Azure Security Center

Azure Security Center - ATP

Released

- Initial - Fall 2015
- Generally Available - Spring/Summer 2016

Description

- Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads. With Security Center, you can apply security policies across your workloads, limit your exposure to threats, and detect and respond to attacks.

Links and Documentation

- https://docs.microsoft.com/en-us/azure/security-center/

Key Features

Unified Security Dashboard

- Common Windows-style management experience in the cloud and on-premise in a single place.

Security Recommendation Engine

- Suggests a lot of security hygiene items to address proactively. Offers customizable policy (XML) for user-supplied checks.

Microsoft Provided Agent

- OS, Application, Security/Audit logs, missing patches, weak configurations and more supplement network-based detections. Can be automatically enabled for all VMs.

Key Features (Cont’d)

Third-Party Security Tool Integration Marketplace

- Centrally integrate your choice of multiple security endpoint solutions, host-based vulnerability management agents, and network-security devices with a few clicks and some license keys.

Custom Alert Rules

- Custom queries on all log event types to trigger notification alerts.

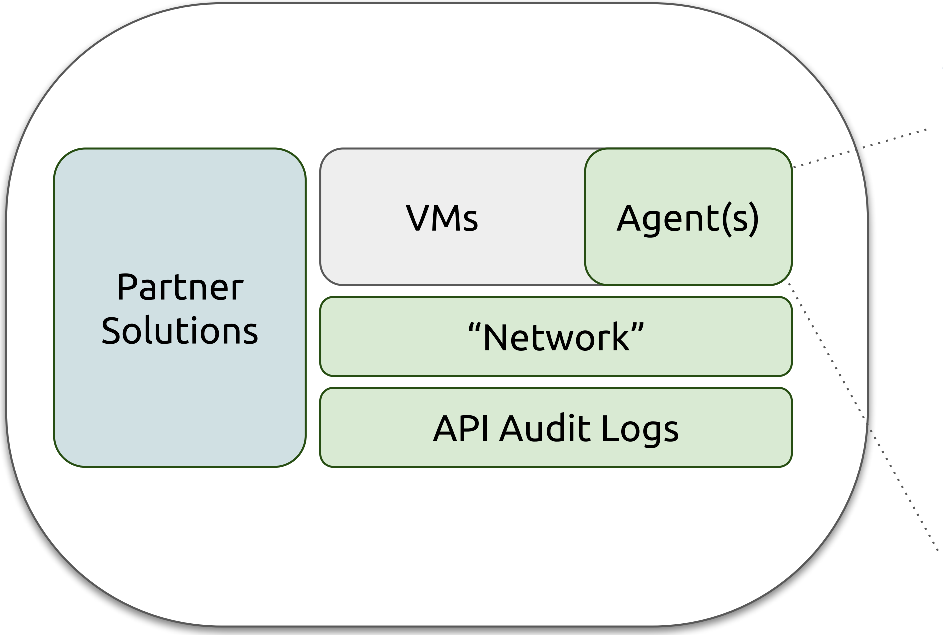
File Integrity Monitoring (Preview)

- Validates the integrity of Windows files, Windows registry, and Linux files

REST API

- Integration with your existing security systems and workflows for inserting and pulling events.

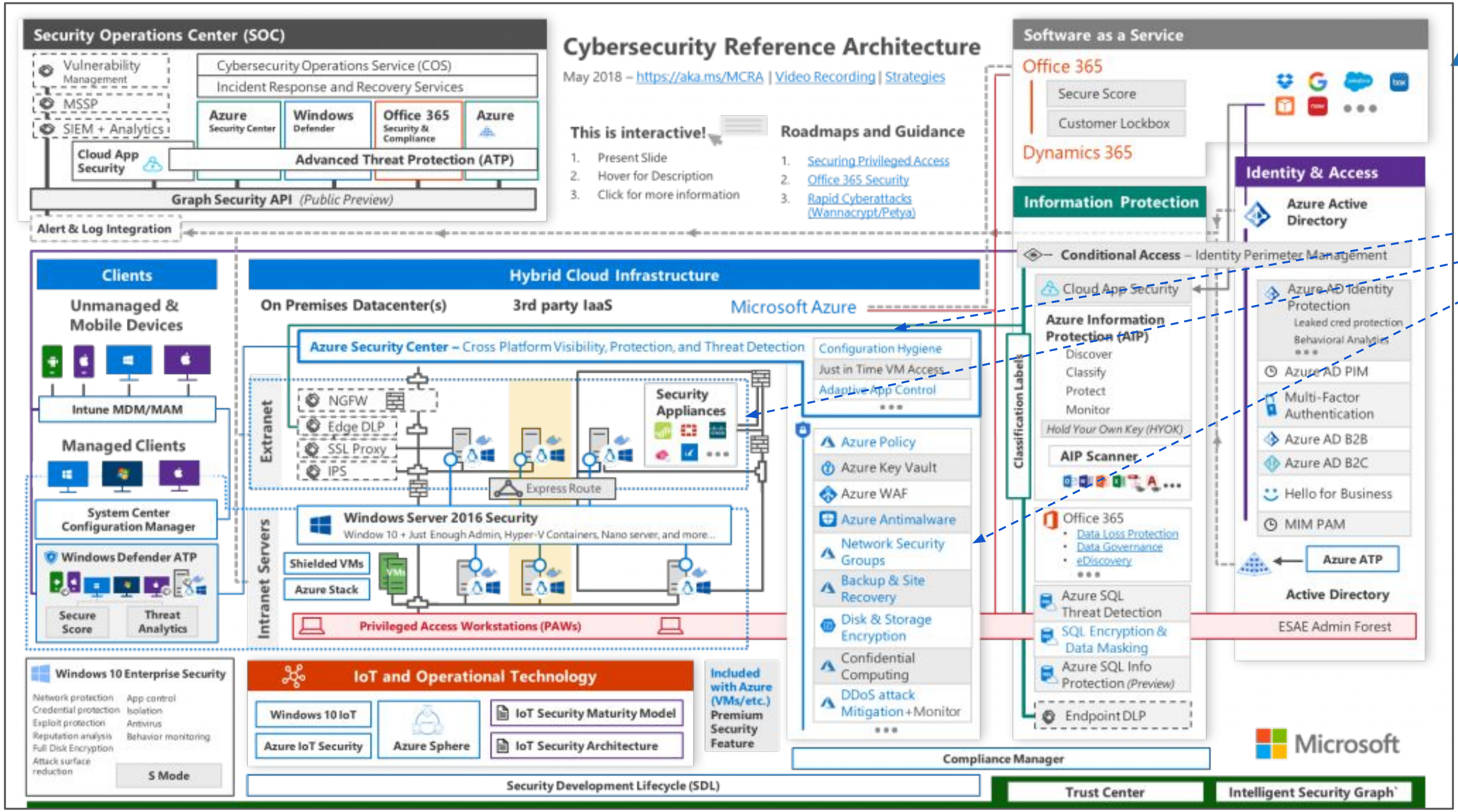
Detection Data Sources



Microsoft Agent Operating Systems

- Windows Server (of course)
- Amazon Linux 2012.09 --> 2017
- CentOS Linux 5,6, and 7
- Oracle Linux 5,6, and 7
- Red Hat Enterprise Linux Server 5,6 and 7
- Debian GNU/Linux 6, 7, 8, and 9
- Ubuntu 12.04, 14.04, 16.04 LTS
- SUSE Linux Enterprise Server 11/ 12

Architecture



Cybersecurity Reference Architecture

May 2018 – https://aka.ms/MCRA | Video Recording | Strategies

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks (Wannacrypt/Petya)

Security Operations Center (SOC)

- Vulnerability Management
- MSSP
- SIEM + Analytics
- Cybersecurity Operations Service (COS)
- Incident Response and Recovery Services
- Azure Security Center
- Windows Defender
- Office 365 Security & Compliance
- Azure
- Cloud App Security
- Advanced Threat Protection (ATP)
- Graph Security API *(Public Preview)*
- Alert & Log Integration

Clients

- Unmanaged & Mobile Devices
- Intune MDM/MAM
- Managed Clients
- System Center Configuration Manager
- Windows Defender ATP
- Secure Score
- Threat Analytics

Windows 10 Enterprise Security

- Network protection
- Credential protection
- Exploit protection
- Reputation analysis
- Full Disk Encryption
- Attack surface reduction
- App control
- Isolation
- Antivirus
- Behavior monitoring
- S Mode

Hybrid Cloud Infrastructure

On Premises Datacenter(s) | 3rd party IaaS | Microsoft Azure

Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection

- Configuration Hygiene
- Just in Time VM Access
- Adaptive App Control
- •••

Extranet: NGFW, Edge DLP, SSL Proxy, IPS

Security Appliances

Express Route

Intranet Servers: Windows Server 2016 Security – Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more…

- Shielded VMs
- Azure Stack

Privileged Access Workstations (PAWs)

- Azure Policy
- Azure Key Vault
- Azure WAF
- Azure Antimalware
- Network Security Groups
- Backup & Site Recovery
- Disk & Storage Encryption
- Confidential Computing
- DDoS attack Mitigation + Monitor
- •••

IoT and Operational Technology

- Windows 10 IoT
- Azure IoT Security
- Azure Sphere
- IoT Security Maturity Model
- IoT Security Architecture

Included with Azure (VMs/etc.) Premium Security Feature

Security Development Lifecycle (SDL)

Compliance Manager

Software as a Service

Office 365

- Secure Score
- Customer Lockbox

Dynamics 365

•••

Information Protection

Conditional Access – Identity Perimeter Management

- Cloud App Security
- Azure Information Protection (AIP)
  - Discover
  - Classify
  - Protect
  - Monitor
- *Hold Your Own Key (HYOK)*
- AIP Scanner
- Office 365
  - Data Loss Protection
  - Data Governance
  - eDiscovery
  - •••
- Azure SQL Threat Detection
- SQL Encryption & Data Masking
- Azure SQL Info Protection *(Preview)*
- Endpoint DLP

Classification Labels

Identity & Access

- Azure Active Directory
- Azure AD Identity Protection
  - Leaked cred protection
  - Behavioral Analytics
  - •••
- Azure AD PIM
- Multi-Factor Authentication
- Azure AD B2B
- Azure AD B2C
- Hello for Business
- MIM PAM
- Azure ATP
- Active Directory
- ESAE Admin Forest

Microsoft

Trust Center | Intelligent Security Graph

Here

https://aka.ms/MCRA

Detections

Threat Intelligence

- Outbound communication to a malicious IP address
- Threat intelligence monitoring and signal sharing across all their services

Behavioral Analytics

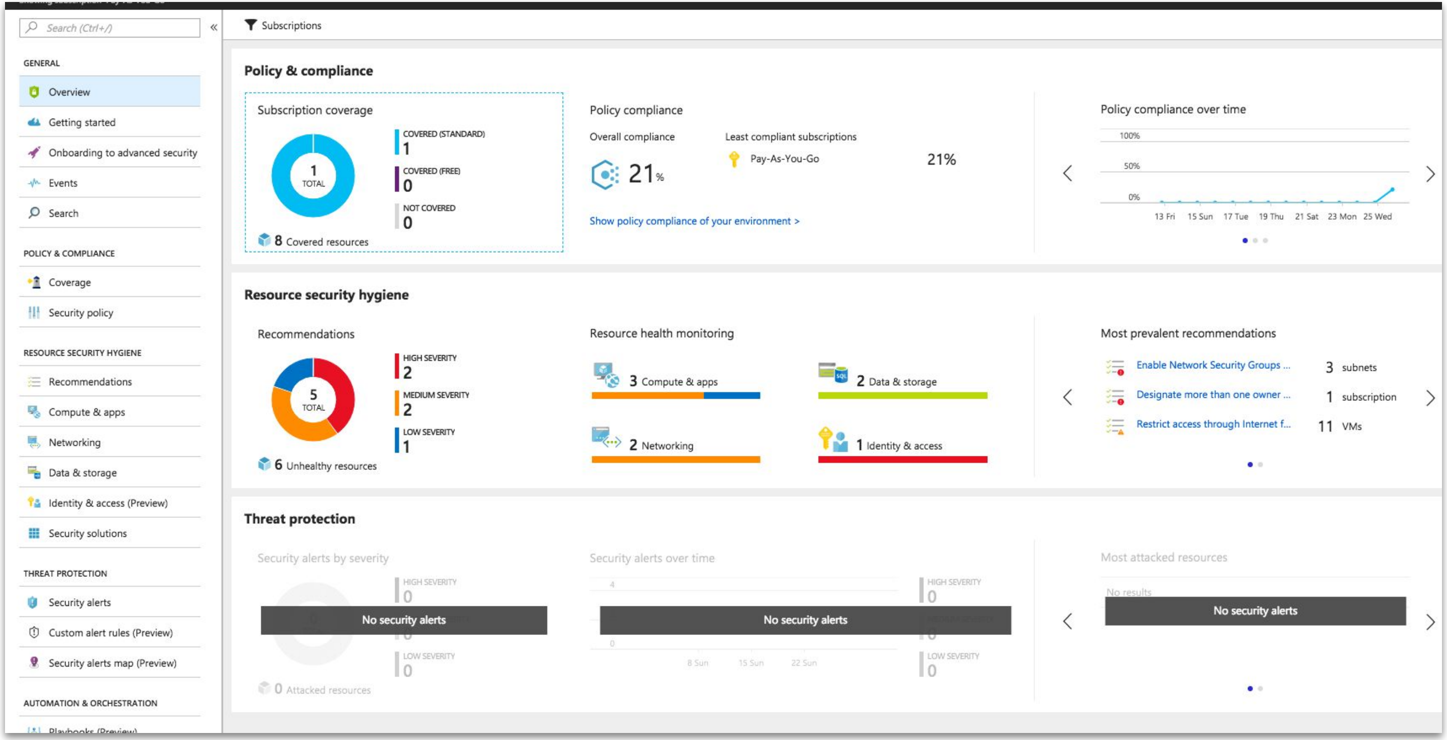
- Suspicious process execution: models processes behaviors and monitors process executions to detect outliers
- Hidden malware and exploitation attempts: memory analysis, crash dump analysis
- Lateral movement and internal reconnaissance: monitors process and login activities such as remote command execution network probing, and account enumeration
- Malicious PowerShell Scripts: inspects PowerShell activity for evidence of suspicious activity
- Outgoing attacks: take part in brute force, scanning, DDoS, and Spam sending campaigns

Anomaly Detection

- Inbound RDP/SSH brute force attacks

https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities

Dashboard



Search (Ctrl+/)

Subscriptions

GENERAL

- Overview
- Getting started
- Onboarding to advanced security
- Events
- Search

POLICY & COMPLIANCE

- Coverage
- Security policy

RESOURCE SECURITY HYGIENE

- Recommendations
- Compute & apps
- Networking
- Data & storage
- Identity & access (Preview)
- Security solutions

THREAT PROTECTION

- Security alerts
- Custom alert rules (Preview)
- Security alerts map (Preview)

AUTOMATION & ORCHESTRATION

- Playbooks (Preview)

Policy & compliance

Subscription coverage

1 TOTAL

COVERED (STANDARD) 1

COVERED (FREE) 0

NOT COVERED 0

8 Covered resources

Policy compliance

Overall compliance 21 %

Least compliant subscriptions	
Pay-As-You-Go	21%

Show policy compliance of your environment >

Policy compliance over time

Resource security hygiene

Recommendations

5 TOTAL

HIGH SEVERITY 2

MEDIUM SEVERITY 2

LOW SEVERITY 1

6 Unhealthy resources

Resource health monitoring

3 Compute & apps

2 Data & storage

2 Networking

1 Identity & access

Most prevalent recommendations

Enable Network Security Groups ...	3	subnets
Designate more than one owner ...	1	subscription
Restrict access through Internet f...	11	VMs

Threat protection

Security alerts by severity

HIGH SEVERITY 0

No security alerts

LOW SEVERITY 0

0 Attacked resources

Security alerts over time

HIGH SEVERITY 0

No security alerts

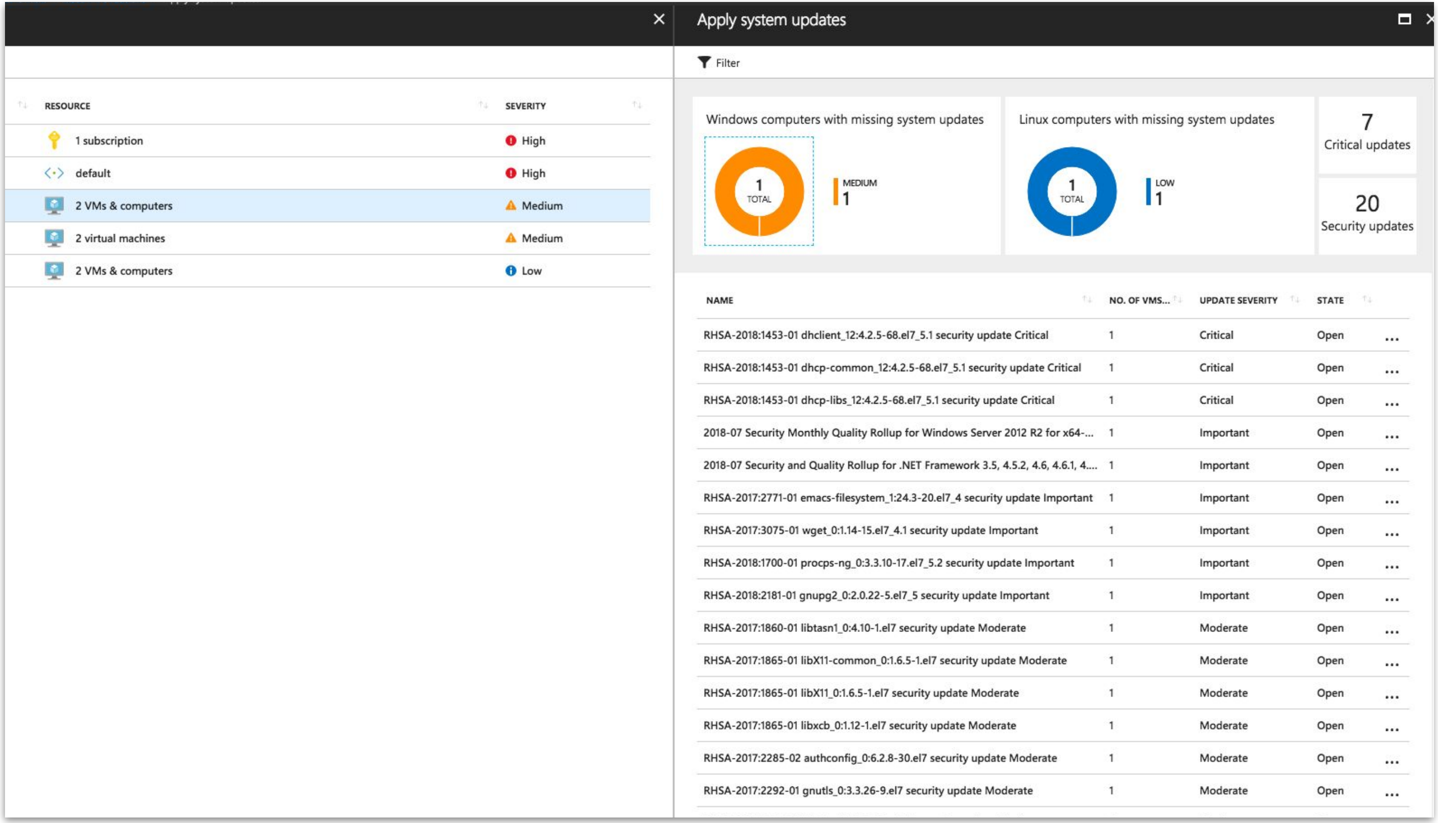
LOW SEVERITY 0

Most attacked resources

No results

No security alerts

Dashboard



RESOURCE	SEVERITY
1 subscription	❗ High
default	❗ High
2 VMs & computers	⚠ Medium
2 virtual machines	⚠ Medium
2 VMs & computers	ℹ Low

Apply system updates

Filter

Windows computers with missing system updates

1 TOTAL

MEDIUM 1

Linux computers with missing system updates

1 TOTAL

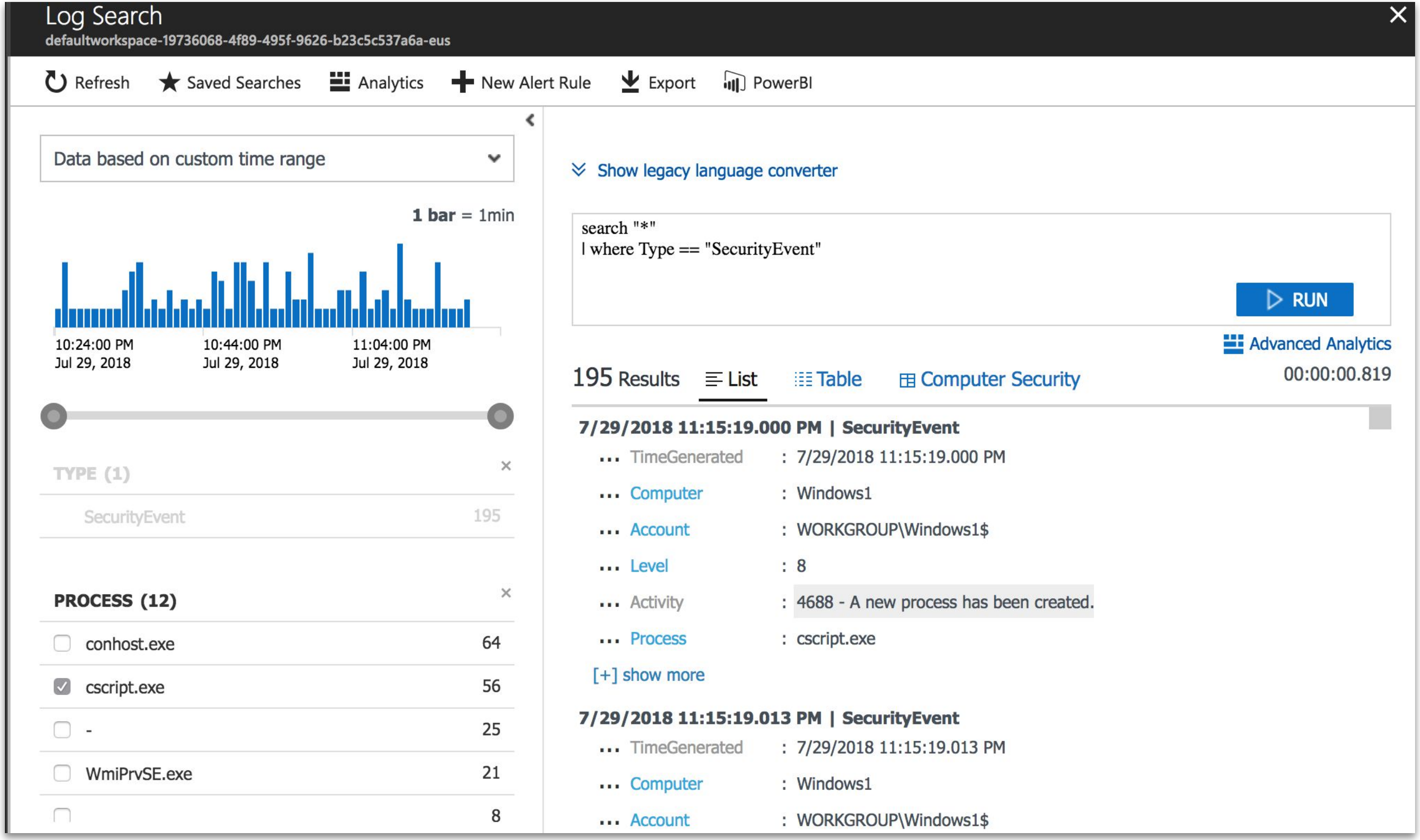
LOW 1

7 Critical updates

20 Security updates

NAME	NO. OF VMS...	UPDATE SEVERITY	STATE	
RHSA-2018:1453-01 dhclient_12:4.2.5-68.el7_5.1 security update Critical	1	Critical	Open	...
RHSA-2018:1453-01 dhcp-common_12:4.2.5-68.el7_5.1 security update Critical	1	Critical	Open	...
RHSA-2018:1453-01 dhcp-libs_12:4.2.5-68.el7_5.1 security update Critical	1	Critical	Open	...
2018-07 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-...	1	Important	Open	...
2018-07 Security and Quality Rollup for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4....	1	Important	Open	...
RHSA-2017:2771-01 emacs-filesystem_1:24.3-20.el7_4 security update Important	1	Important	Open	...
RHSA-2017:3075-01 wget_0:1.14-15.el7_4.1 security update Important	1	Important	Open	...
RHSA-2018:1700-01 procps-ng_0:3.3.10-17.el7_5.2 security update Important	1	Important	Open	...
RHSA-2018:2181-01 gnupg2_0:2.0.22-5.el7_5 security update Important	1	Important	Open	...
RHSA-2017:1860-01 libtasn1_0:4.10-1.el7 security update Moderate	1	Moderate	Open	...
RHSA-2017:1865-01 libX11-common_0:1.6.5-1.el7 security update Moderate	1	Moderate	Open	...
RHSA-2017:1865-01 libX11_0:1.6.5-1.el7 security update Moderate	1	Moderate	Open	...
RHSA-2017:1865-01 libxcb_0:1.12-1.el7 security update Moderate	1	Moderate	Open	...
RHSA-2017:2285-02 authconfig_0:6.2.8-30.el7 security update Moderate	1	Moderate	Open	...
RHSA-2017:2292-01 gnutls_0:3.3.26-9.el7 security update Moderate	1	Moderate	Open	...

Dashboard



TYPE (1)

SecurityEvent	195

PROCESS (12)

□ conhost.exe	64
☑ cscript.exe	56
□ -	25
□ WmiPrvSE.exe	21
□	8

```
search "*"
| where Type == "SecurityEvent"
```

195 Results

00:00:00.819

7/29/2018 11:15:19.000 PM | SecurityEvent

... TimeGenerated : 7/29/2018 11:15:19.000 PM
... Computer : Windows1
... Account : WORKGROUP\Windows1$
... Level : 8
... Activity : 4688 - A new process has been created.
... Process : cscript.exe

[+] show more

7/29/2018 11:15:19.013 PM | SecurityEvent

... TimeGenerated : 7/29/2018 11:15:19.013 PM
... Computer : Windows1
... Account : WORKGROUP\Windows1$

Value Added

Hybrid-first approach

- Leverages the vast amount of enterprise management features and capabilities applied to Azure resources.

Provides a Microsoft-supported Windows/Linux Agent

- Supported OSes get enhanced detection capabilities (logs, process monitoring, crash dump analysis)

Integrated, Self-Service Partner Marketplace

- Adding a solution is a few clicks and a license away in many cases.

Leverages the Azure Log Analytics Service

- Mature integrations, advanced querying, and full-featured REST API

Areas for Improvement

Areas for Improvement

- A detailed list of anomalous detection capabilities is not yet available.
- Ability to see and therefore tune parameters and settings for all detections, per detection.
- Ability to add custom detections into the native analytics engine/flow
- There can be a significant delay from agent deployment to it reporting in the Dashboard.
- The Security Center UI can be overwhelming at times and options tucked several layers deep in configuration workflows.
- The Security Center UI allows for direct modification of live VMs to install agents/partner solutions which breaks the rules of immutable infrastructure.
  - The “feel” is distinctly Enterprise-focused and drives work primarily through the UI, not as much emphasis in the documentation on using code/APIs for automation.
- The ability to supply custom threat/IP feeds to aid in improving detection accuracy.

Amazon GuardDuty et al

Amazon GuardDuty et al

Released

- AWS CloudTrail: Spring 2013
- AWS VPC Flow Logs: Summer 2015
- Amazon GuardDuty: Winter 2017

Description

- Amazon GuardDuty offers threat detection that enables you to continuously monitor and protect your AWS accounts and workloads.

Links and Documentation

- https://aws.amazon.com/guardduty/

Key Features

Watches Data Streams

- Analyzes continuous streams of meta-data generated from your account and network activity found in AWS CloudTrail Events, Amazon VPC Flow Logs, and DNS Logs.

Integrates Threat Intelligence Feeds

- Uses integrated threat intelligence such as known malicious IP addresses, anomaly detection, and machine learning to better identify threats.
- You can supply your own IP lists for “good” and “bad” hosts.

Generates Findings

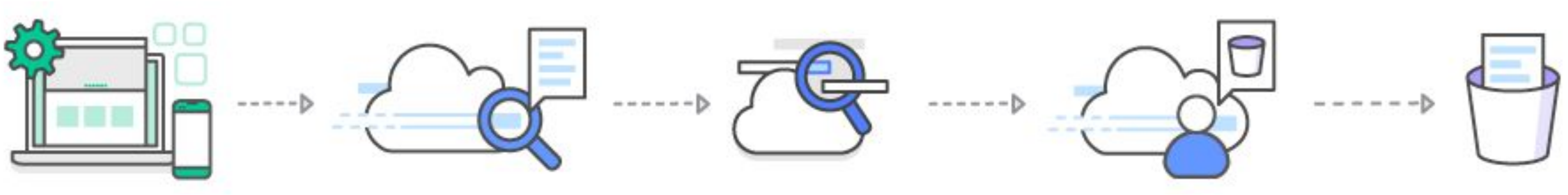
- Creation action creates CloudWatch events useful for triggering Lambda functions for further processing and sending notifications.

Cross-Account Visibility

- Events can be centralized across multiple “member” accounts to a centralized “master” account.

How it Works

Amazon CloudTrail



Account activity occurs

CloudTrail records a CloudTrail Event

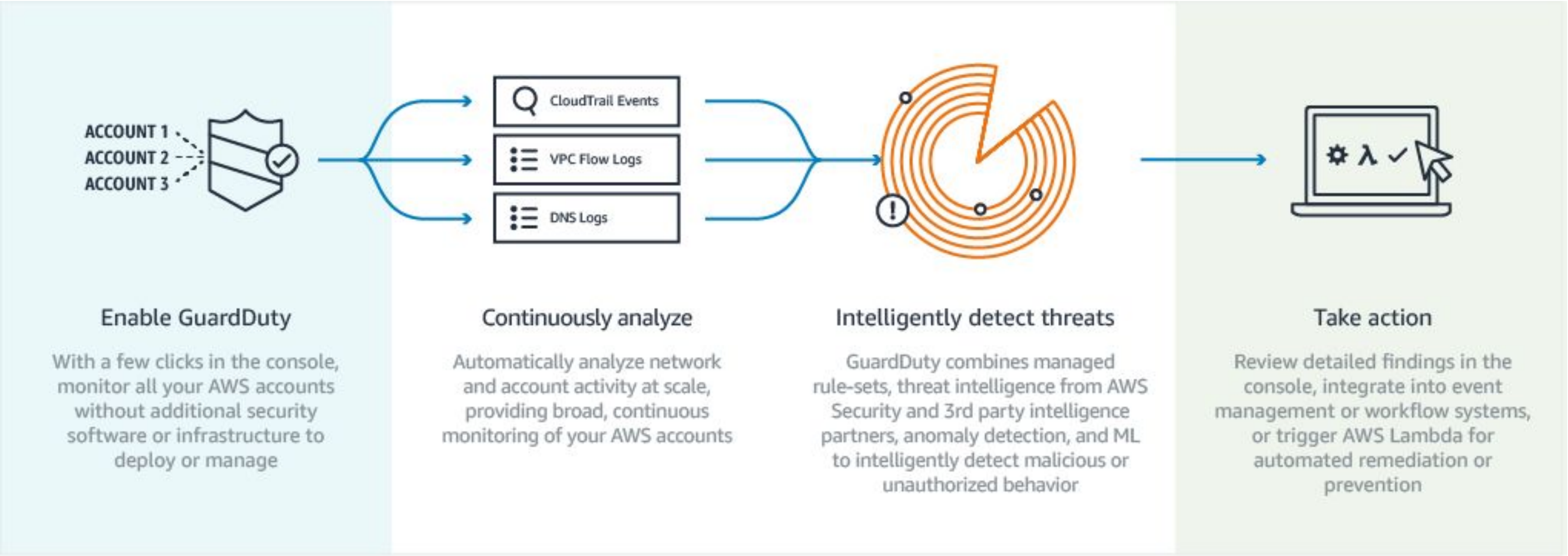
You can view/download your activity in the CloudTrail Event History

You can set up CloudTrail and define an Amazon S3 bucket for storage

A log of CloudTrail Events is delivered to an S3 bucket and optionally to CloudWatch Logs and CloudWatch Events

How it Works

Amazon GuardDuty



Enable GuardDuty

With a few clicks in the console, monitor all your AWS accounts without additional security software or infrastructure to deploy or manage

Continuously analyze

Automatically analyze network and account activity at scale, providing broad, continuous monitoring of your AWS accounts

Intelligently detect threats

GuardDuty combines managed rule-sets, threat intelligence from AWS Security and 3rd party intelligence partners, anomaly detection, and ML to intelligently detect malicious or unauthorized behavior

Take action

Review detailed findings in the console, integrate into event management or workflow systems, or trigger AWS Lambda for automated remediation or prevention

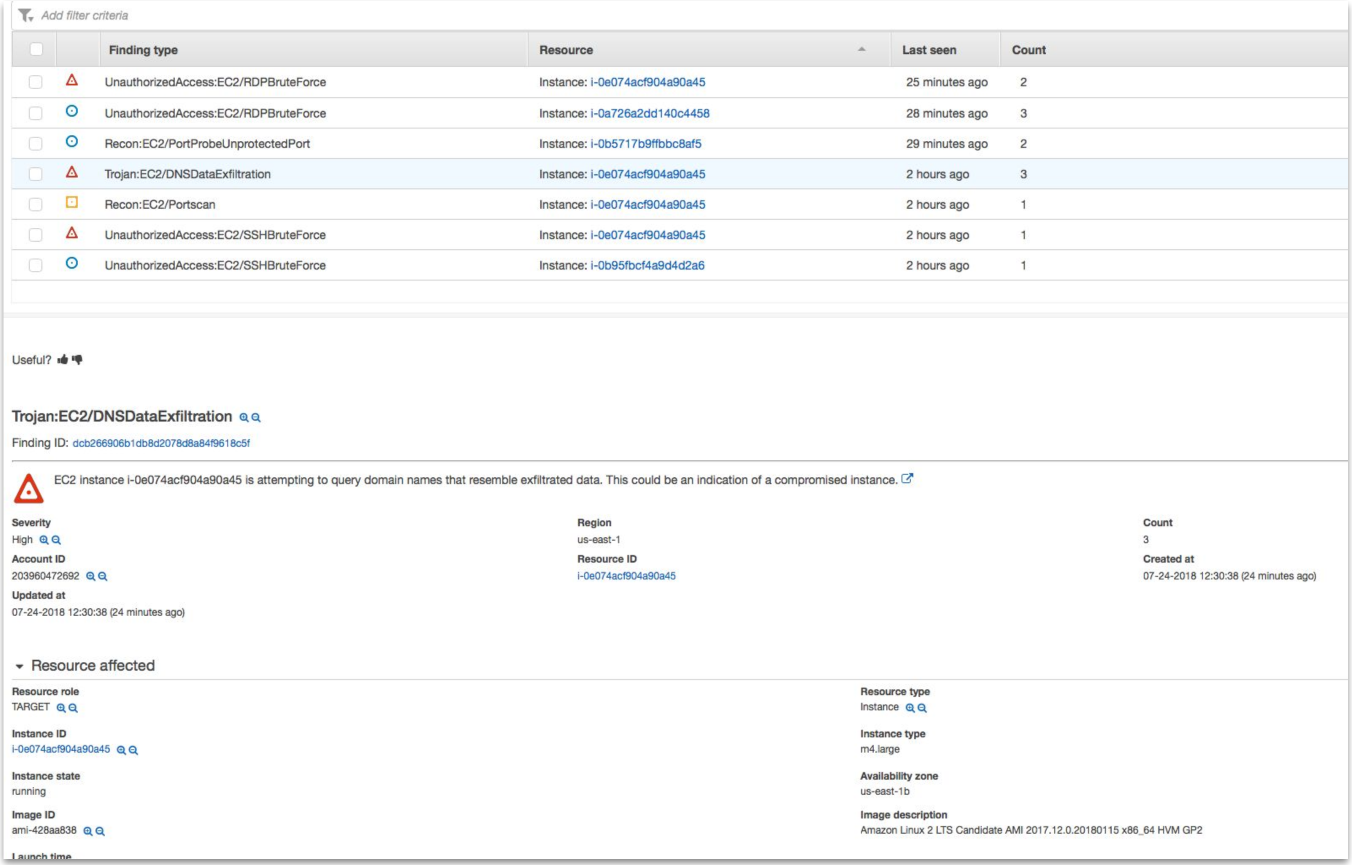
Detections

“Threat Purposes” (Types of Findings)

- **Backdoor** - Compromised AWS resource contacting its C&C server.
- **Behavior** - Activity patterns that are different from the established baseline.
- **Cryptocurrency** - Detecting software that is associated with cryptocurrencies.
- **Pentest** - Potential attack activity generated by known pen testing tools.
- **Persistence** - An IAM user is behaving differently from the established baseline.
- **Recon** - Reconnaissance attack underway probing ports, listing users, database tables, etc.
- **Resource Consumption** - An IAM user is behaving differently from the established baseline to create new resources, such as EC2 instances.
- **Stealth** - Detects attacks leveraging an anonymizing proxy server, disguising the true nature of the activity.
- **Trojan** - Malicious activity associated with certain Trojan applications.
- **Unauthorized Access** - A suspicious activity pattern by an unauthorized individual.

https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-types.html

Dashboard



Add filter criteria

□		Finding type	Resource	Last seen	Count
□	△	UnauthorizedAccess:EC2/RDPBruteForce	Instance: i-0e074acf904a90a45	25 minutes ago	2
□	○	UnauthorizedAccess:EC2/RDPBruteForce	Instance: i-0a726a2dd140c4458	28 minutes ago	3
□	○	Recon:EC2/PortProbeUnprotectedPort	Instance: i-0b5717b9ffbbc8af5	29 minutes ago	2
□	△	Trojan:EC2/DNSDataExfiltration	Instance: i-0e074acf904a90a45	2 hours ago	3
□	□	Recon:EC2/Portscan	Instance: i-0e074acf904a90a45	2 hours ago	1
□	△	UnauthorizedAccess:EC2/SSHBruteForce	Instance: i-0e074acf904a90a45	2 hours ago	1
□	○	UnauthorizedAccess:EC2/SSHBruteForce	Instance: i-0b95fbcf4a9d4d2a6	2 hours ago	1

Useful?

Trojan:EC2/DNSDataExfiltration

Finding ID: dcb266906b1db8d2078d8a84f9618c5f

△ EC2 instance i-0e074acf904a90a45 is attempting to query domain names that resemble exfiltrated data. This could be an indication of a compromised instance.

Severity
High

Account ID
203960472692

Updated at
07-24-2018 12:30:38 (24 minutes ago)

Region
us-east-1

Resource ID
i-0e074acf904a90a45

Count
3

Created at
07-24-2018 12:30:38 (24 minutes ago)

▾ Resource affected

Resource role
TARGET

Instance ID
i-0e074acf904a90a45

Instance state
running

Image ID
ami-428aa838

Launch time

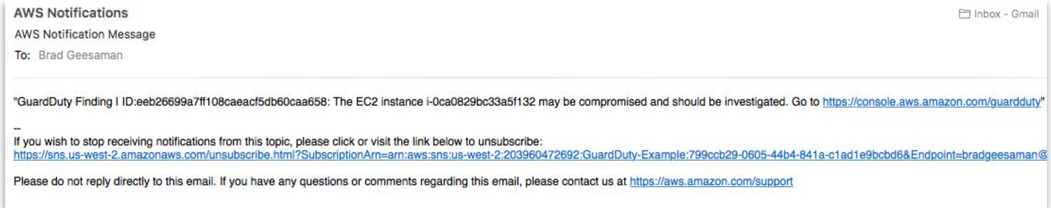
Resource type
Instance

Instance type
m4.large

Availability zone
us-east-1b

Image description
Amazon Linux 2 LTS Candidate AMI 2017.12.0.20180115 x86_64 HVM GP2

Sample Notification and IP Lists



AWS Notifications

Inbox - Gmail

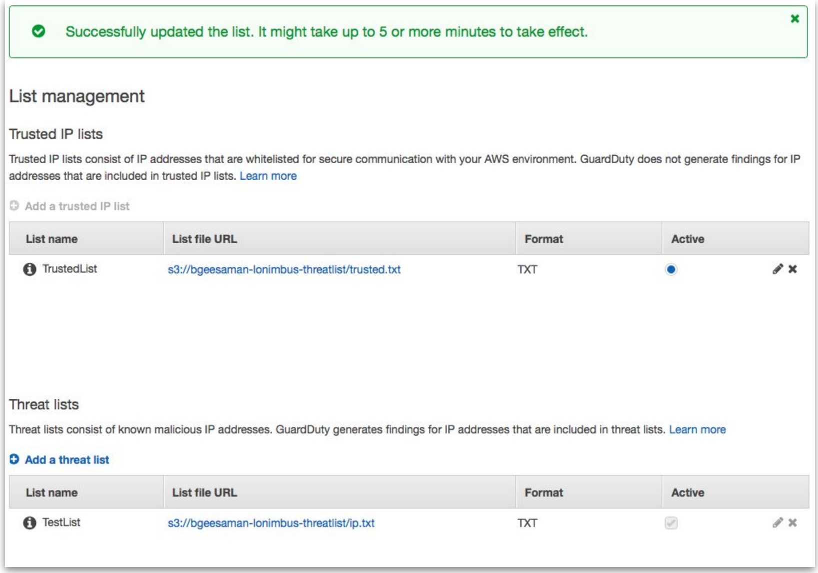
AWS Notification Message

To: Brad Geesaman

"GuardDuty Finding I ID:eeb26699a7ff108caeacf5db60caa658: The EC2 instance i-0ca0829bc33a5f132 may be compromised and should be investigated. Go to https://console.aws.amazon.com/guardduty"

--
If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:
https://sns.us-west-2.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-west-2:203960472692:GuardDuty-Example:799ccb29-0605-44b4-841a-c1ad1e9bcbd6&Endpoint=bradgeesaman@

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at https://aws.amazon.com/support



Successfully updated the list. It might take up to 5 or more minutes to take effect.

List management

Trusted IP lists

Trusted IP lists consist of IP addresses that are whitelisted for secure communication with your AWS environment. GuardDuty does not generate findings for IP addresses that are included in trusted IP lists. Learn more

Add a trusted IP list

List name	List file URL	Format	Active
TrustedList	s3://bgeesaman-lonimbus-threatlist/trusted.txt	TXT	●

Threat lists

Threat lists consist of known malicious IP addresses. GuardDuty generates findings for IP addresses that are included in threat lists. Learn more

Add a threat list

List name	List file URL	Format	Active
TestList	s3://bgeesaman-lonimbus-threatlist/ip.txt	TXT	☑

Demo

Value Added

Zero-Impact Setup

- Nearly a “one-click” installation process that does not affect any running workflows.

Clear Listing of GuardDuty Detections

- Allows you to know what AWS is monitoring and what you may want a partner to supplement.

Extremely Broad Partner Ecosystem

- Many options to choose from in many different areas of security, not just detection.

Strong Detection of API Misuse

- Several key detections for behaviors associated with compromised credentials.

Areas for Improvement

Areas for Improvement

- Ability to tune parameters for all settings and detections
- Ability to add custom detections into the native analytics engine/flow
- API ability to create custom findings, not just view them.
  - Would allow GuardDuty to be the aggregation interface from many sources.
  - Would allow for user-created integrations to drive through the same interface.

Google Cloud Security Command Center

Google Cloud Security Command Center

Released

- Google StackDriver: Spring 2016
- Google Cloud VPC Flow logs: Spring 2018
- Google Cloud Security Command Center (Alpha): Spring 2018

Description

- The Cloud Security Command Center (Cloud SCC) is the canonical security and data risk database for Google Cloud Platform (GCP). Cloud SCC enables you to understand your security and data attack surface by providing asset inventory, discovery, search, and management.

Links and Documentation

- https://cloud.google.com/security-command-center/

Key Features

Asset Discovery/Inventory

- Across App Engine, Compute Engine, Cloud Storage, and Cloud Datastore

Anomaly Detection

- Identifies threats like botnets, cryptocurrency mining, anomalous reboots, and suspicious network traffic.

Sensitive Data Identification

- Scans storage buckets that may contain sensitive and regulated data using the DLP API.

Application Vulnerability Detection

- Scan App Engine applications for web vulnerabilities using Cloud Security Scanner.

Key Features (Cont'd)

Access Control Monitoring

- Forseti validates access control policies and alerts when policies are misconfigured or unexpectedly change.

Third-Party Security Tool Integration

- Centrally integrate output from tools such as Cloudflare, CrowdStrike, Palo Alto Networks, Qualys, and RedLock into the Cloud SCC

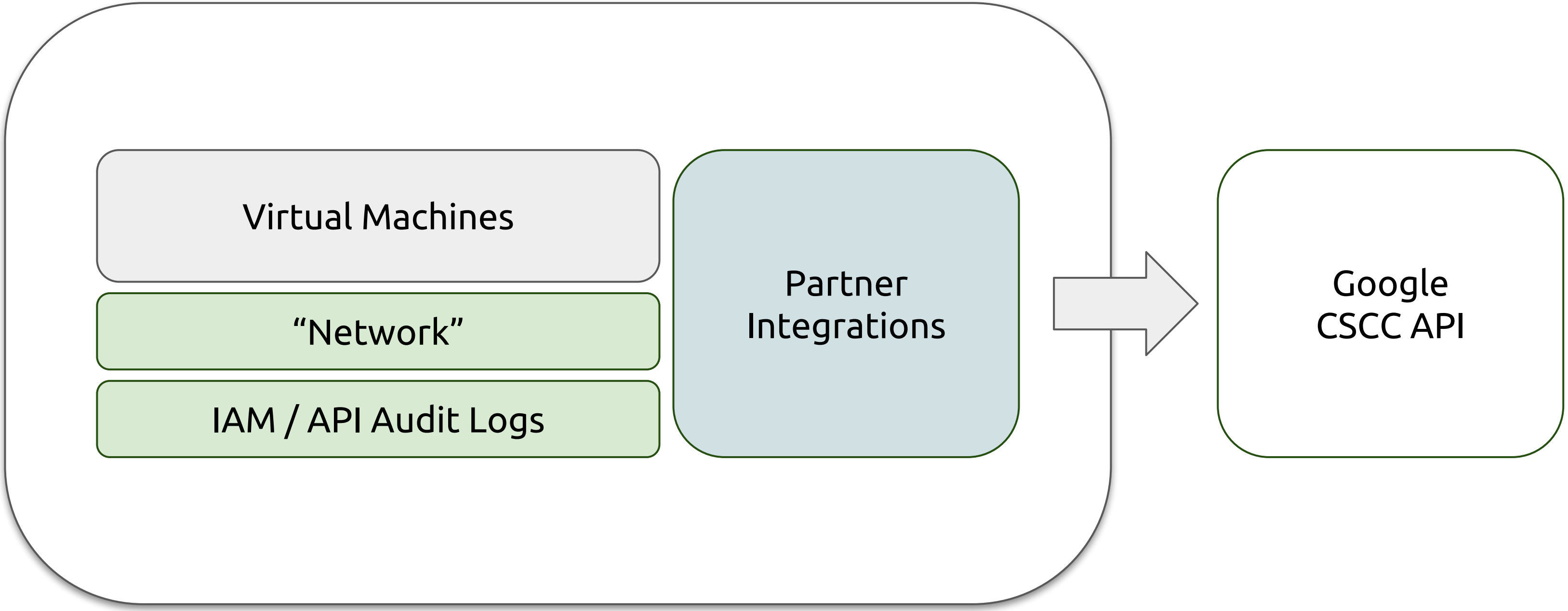
Real-Time Notifications

- Receive Cloud SCC alerts via Gmail, SMS, and Jira with Cloud Pub/Sub notification integration.

REST API

- Integration with your existing security systems and workflows.

Detection Data Sources

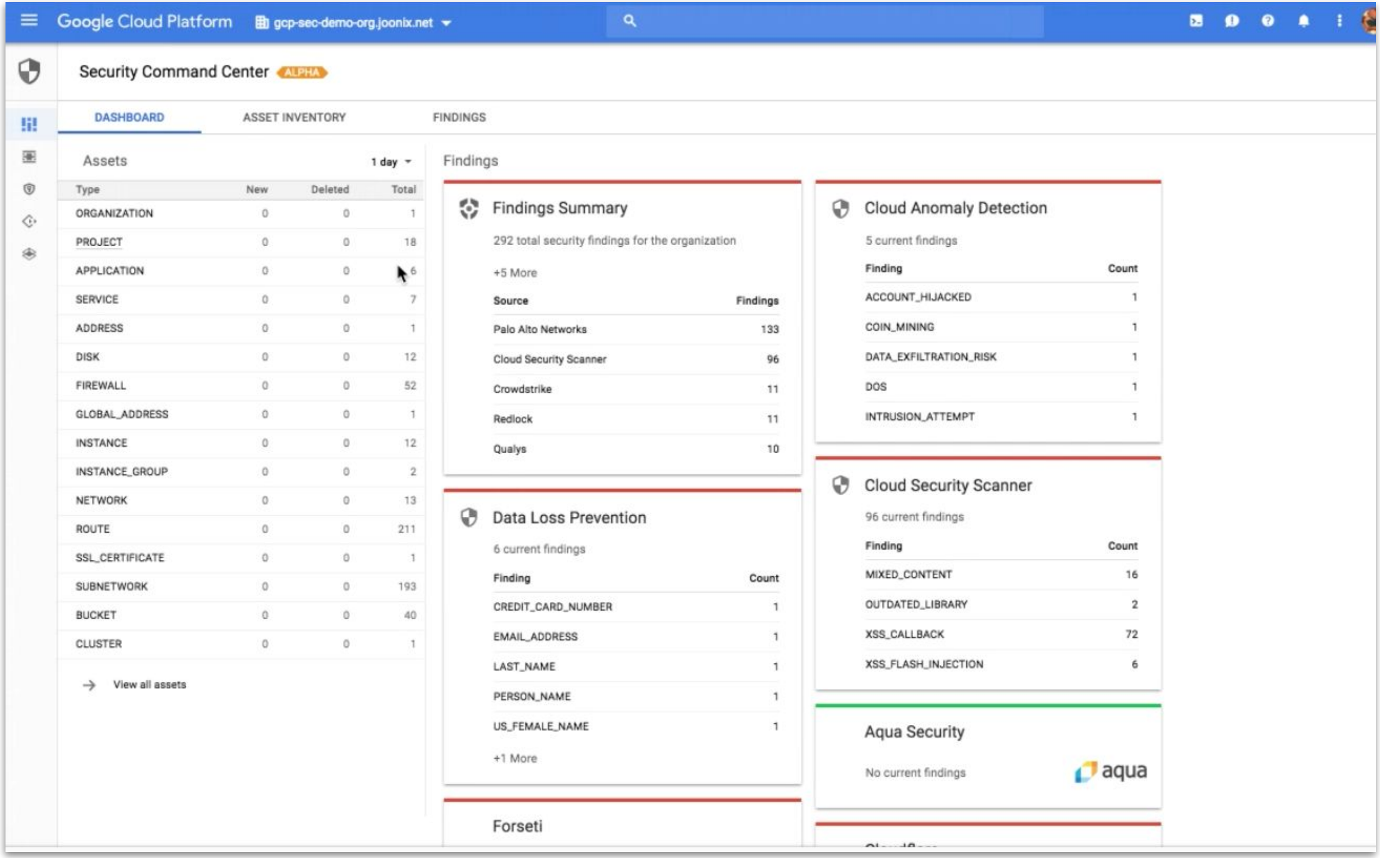


Detections

As Listed but not Detailed

- Botnets
- Cryptocurrency mining
- Anomalous reboots
- Suspicious/anomalous network traffic

Dashboard



Assets — 1 day

Type	New	Deleted	Total
ORGANIZATION	0	0	1
PROJECT	0	0	18
APPLICATION	0	0	6
SERVICE	0	0	7
ADDRESS	0	0	1
DISK	0	0	12
FIREWALL	0	0	52
GLOBAL_ADDRESS	0	0	1
INSTANCE	0	0	12
INSTANCE_GROUP	0	0	2
NETWORK	0	0	13
ROUTE	0	0	211
SSL_CERTIFICATE	0	0	1
SUBNETWORK	0	0	193
BUCKET	0	0	40
CLUSTER	0	0	1

→ View all assets

Findings

Findings Summary

292 total security findings for the organization

+5 More

Source	Findings
Palo Alto Networks	133
Cloud Security Scanner	96
Crowdstrike	11
Redlock	11
Qualys	10

Cloud Anomaly Detection

5 current findings

Finding	Count
ACCOUNT_HIJACKED	1
COIN_MINING	1
DATA_EXFILTRATION_RISK	1
DOS	1
INTRUSION_ATTEMPT	1

Data Loss Prevention

6 current findings

Finding	Count
CREDIT_CARD_NUMBER	1
EMAIL_ADDRESS	1
LAST_NAME	1
PERSON_NAME	1
US_FEMALE_NAME	1

+1 More

Cloud Security Scanner

96 current findings

Finding	Count
MIXED_CONTENT	16
OUTDATED_LIBRARY	2
XSS_CALLBACK	72
XSS_FLASH_INJECTION	6

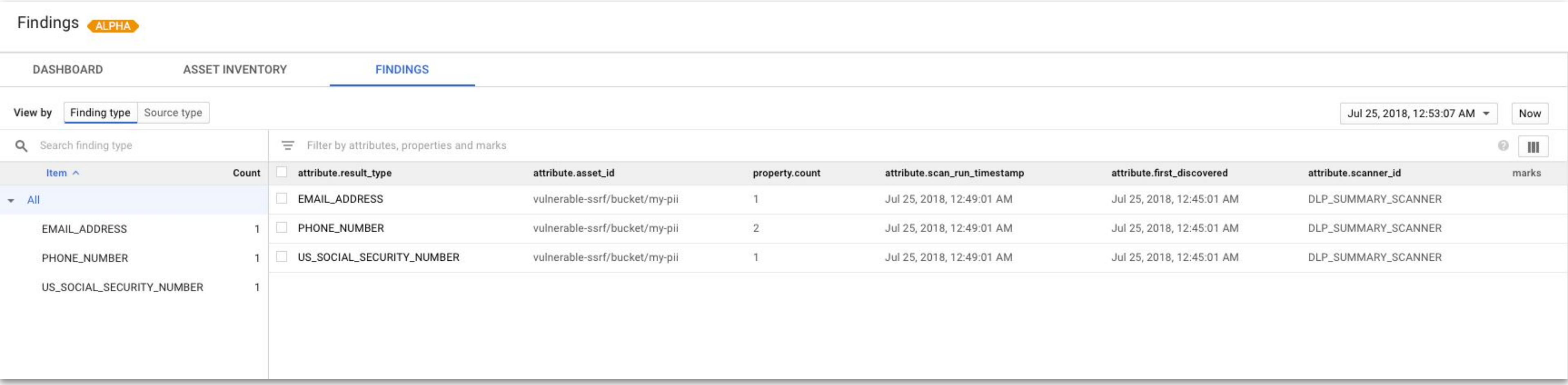
Aqua Security

No current findings

aqua

Forseti

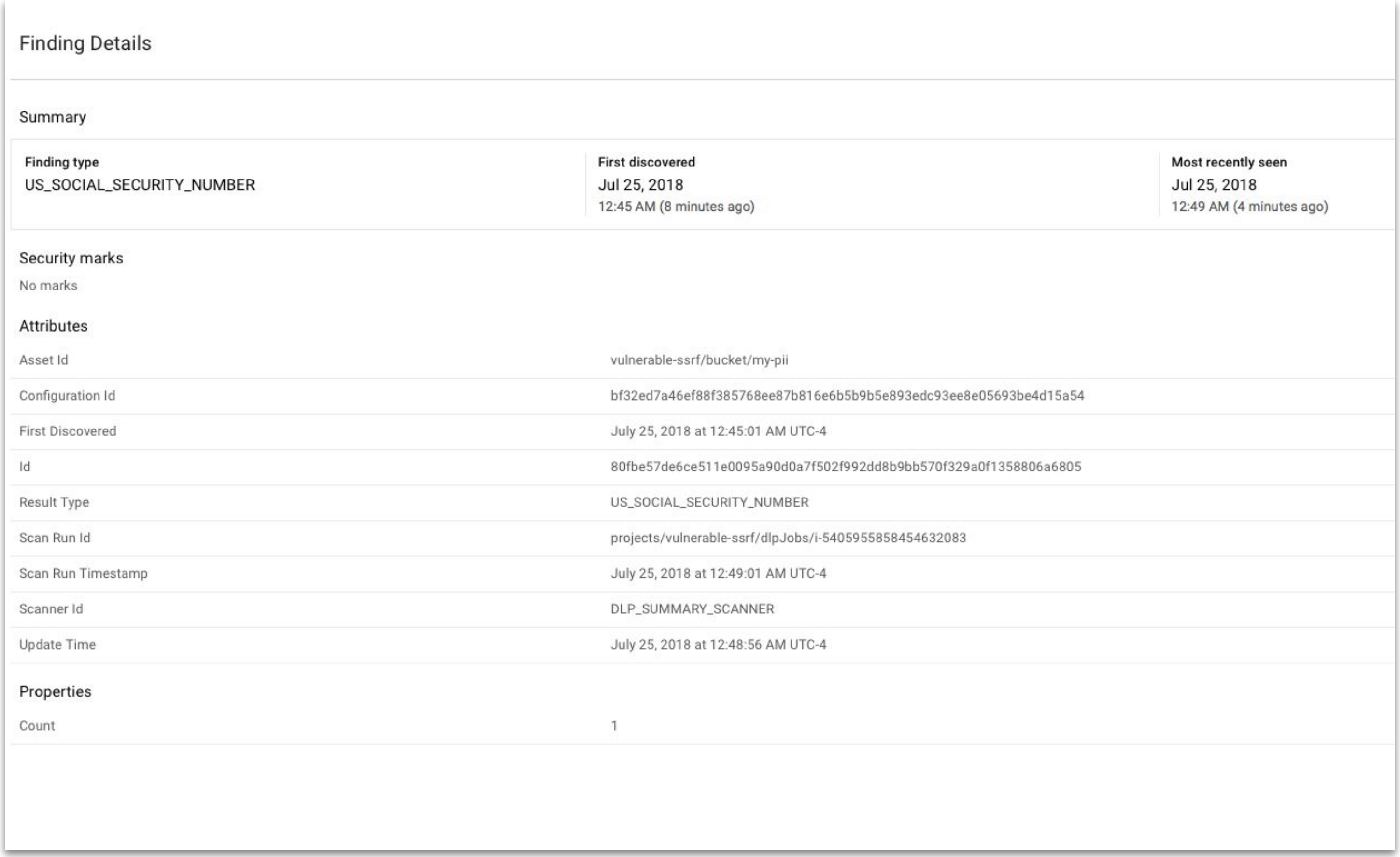
Dashboard



Item	Count
All	
EMAIL_ADDRESS	1
PHONE_NUMBER	1
US_SOCIAL_SECURITY_NUMBER	1

attribute.result_type	attribute.asset_id	property.count	attribute.scan_run_timestamp	attribute.first_discovered	attribute.scanner_id	marks
EMAIL_ADDRESS	vulnerable-ssrf/bucket/my-pii	1	Jul 25, 2018, 12:49:01 AM	Jul 25, 2018, 12:45:01 AM	DLP_SUMMARY_SCANNER	
PHONE_NUMBER	vulnerable-ssrf/bucket/my-pii	2	Jul 25, 2018, 12:49:01 AM	Jul 25, 2018, 12:45:01 AM	DLP_SUMMARY_SCANNER	
US_SOCIAL_SECURITY_NUMBER	vulnerable-ssrf/bucket/my-pii	1	Jul 25, 2018, 12:49:01 AM	Jul 25, 2018, 12:45:01 AM	DLP_SUMMARY_SCANNER	

Dashboard



Finding Details

Summary

Finding type	First discovered	Most recently seen
US_SOCIAL_SECURITY_NUMBER	Jul 25, 2018 12:45 AM (8 minutes ago)	Jul 25, 2018 12:49 AM (4 minutes ago)

Security marks

No marks

Attributes

Asset Id	vulnerable-ssrf/bucket/my-pii
Configuration Id	bf32ed7a46ef88f385768ee87b816e6b5b9b5e893edc93ee8e05693be4d15a54
First Discovered	July 25, 2018 at 12:45:01 AM UTC-4
Id	80fbe57de6ce511e0095a90d0a7f502f992dd8b9bb570f329a0f1358806a6805
Result Type	US_SOCIAL_SECURITY_NUMBER
Scan Run Id	projects/vulnerable-ssrf/dlpJobs/i-5405955858454632083
Scan Run Timestamp	July 25, 2018 at 12:49:01 AM UTC-4
Scanner Id	DLP_SUMMARY_SCANNER
Update Time	July 25, 2018 at 12:48:56 AM UTC-4

Properties

Count	1

Value Added

Zero-Impact Setup

- Alpha setup process requires a few manual steps, but they do not affect any running workflows.

Strong Partner Focus

- The API and Interface feature partner solutions and integrate their output streams into a single management interface.

Framework-Oriented

- Similar to the Stackdriver logging service in that it’s a framework for handling all security events across all applicable services.

Limitations and Suggestions

Limitations

- Still in Alpha, so anomalous detection capabilities are still in the early stages.
- Not yet a comprehensive or detailed list of detection capabilities.

Suggestions

- Ability to tune all settings and detections
- Ability to add custom detections into the native flow
- Ability to see total permission scope vs actual usage and recommend policy restrictions
- Integrate security detections for all managed services (Database, BigData, Storage, Kubernetes)
- Integrate the notification and alerting functionality natively
- Cross-project management

Key Takeaways and Looking Ahead

Key Takeaways

Attackers

There are still opportunities for exploitation, pivoting/lateral movement, and escalation. But, the time is soon approaching where stealth must be applied and detection windows are shrinking. Have to get in and get out quickly as persisting now greatly increases the chances of discovery.

Defenders

Greatly increased visibility without roadblocking development teams that want to move quickly.

Can deal you in at the “DevSecOps” table.

Can reduce or eliminate a lot of manual or brittle integration efforts/tooling already in place.

Can allow for multiple solutions to run in parallel with minimal additional effort.

Key Takeaways

Security Architects/Ops/Builders

If I’m not implementing these capabilities in my systems and designs, I will want to revisit that.

There may be new opportunities to simplify and offload customized integration efforts on new designs.

Business Leaders

Add capabilities and visibility previously ignored for very low cost

Remove undifferentiated heavy lifting and take advantage of

Position my computing environments using a shared/common understanding for integration points

More easily bring in my trusted vendor partners in to add value

Recognize there are network effects of a thriving ecosystem of easily integrated solutions that can keep up with the accelerated pace of innovation

Reduce switching costs--Even run in parallel

Should I Adopt?

Have you just started your cloud adoption journey?

- Most likely, yes. There are immediate and cost-effective benefits.
- Do explore the natively-integrated partner/vendor space to supplement capabilities to meet the security needs of your workloads.
- Ensure that your solution choices work well with the current development and operations processes and don’t diminish their ability to cleanly automate and maintain their applications.

Should I Adopt?

Have you been building your own log/event analysis pipelines using your own internal capabilities?

- Even if you are satisfied with your implementation, you may want to revisit and explore opportunities to refactor and simplify using the newer patterns and APIs.
- Also, consider running it in parallel. The detection benefits offered by the providers will continue to improve, and the cost is reasonable in most cases.

Should I Adopt?

Have you been building your own log/event analysis pipelines using only third-party vendors that don’t directly integrate into the platform console?

- Talk to your vendors about their plans to offer their solutions directly in the cloud provider’s marketplaces. Standardizing and streamlining the onboarding processes and administration mechanisms has mutual benefits: easier for you and the vendor reaches more customers directly.
- Assess any gaps in your detection capabilities to see if the vendor solution helps cover them.

Should I Adopt?

Are you a mature, cloud-native organization with a balanced portfolio of well implemented security solutions, a strong grasp of your risk and exposure, and a highly-qualified staff of well-funded cloud security professionals who are threat-hunting geniuses?

- Congratulations on your Unicorn status!
- Keep a close eye on the developments and improvements as the providers mature their solutions and capabilities--especially on the aspects that you don’t have control over as a tenant in their cloud.

Wherever possible, avoid
undifferentiated heavy lifting

The *Framework* is the Key

Watch this space closely

Security solution vendors -- Take note

black hat®
USA 2018

AUGUST 4-9, 2018
MANDALAY BAY / LAS VEGAS

Thank you!

Questions?

@bradgeesaman

#BHUSA / @BLACK HAT EVENTS