Security Monitoring in the Cloud

Who am I ?

tim.mannai@datadoghq.com

Vulnerability Management @ Datadog

+10 Years Experience In Cybersecurity with focus on Cloud Security (CSP Auditor, DevSecOps, Cloud Security Architect, Incident Detection & Response)

ENSTA Paris 2015

Why this course ?

- Cloud **adoption** is **redefining** how organizations build and secure infrastructure.
- **Traditional** on-prem security tools don’t provide full **visibility** in cloud environments.
- Future cybersecurity engineers must **detect**, **analyze**, and **respond** to threats in **dynamic**, **multi-cloud** systems.

Course Program

~ 1h30 Lecture   ~1h30 Lab

- **Session 1:** Cloud Security & Monitoring Foundations (IAM + Network)
- **Session 2:** Container Security & Observability (Docker + Kubernetes on GCP)
- **Session 3:** Application & Data Security Monitoring
- **Session 4:** Threat Detection, Incident Response

Course resources are accessible on https://github.com/0x74696D/security_monitoring_tp

Security Monitoring in the Cloud
Session #1

Cloud Security & Monitoring Foundations

Jan 2026

Key Outcomes

- Understand Observability pillars
- Understand and configure GCP audit logs for IAM and network activity.
- Detect anomalous login attempts and privilege escalations.
- Use VPC Flow Logs to identify suspicious network behavior.

Agenda

01 **Understand cloud risks**:
Shared responsibility model & cloud security

02 **Get familiar with observability**:
logs, metrics, traces

03 **Identity as the new perimeter**:
IAM monitoring (least privilege, service accounts, escalation attempts).

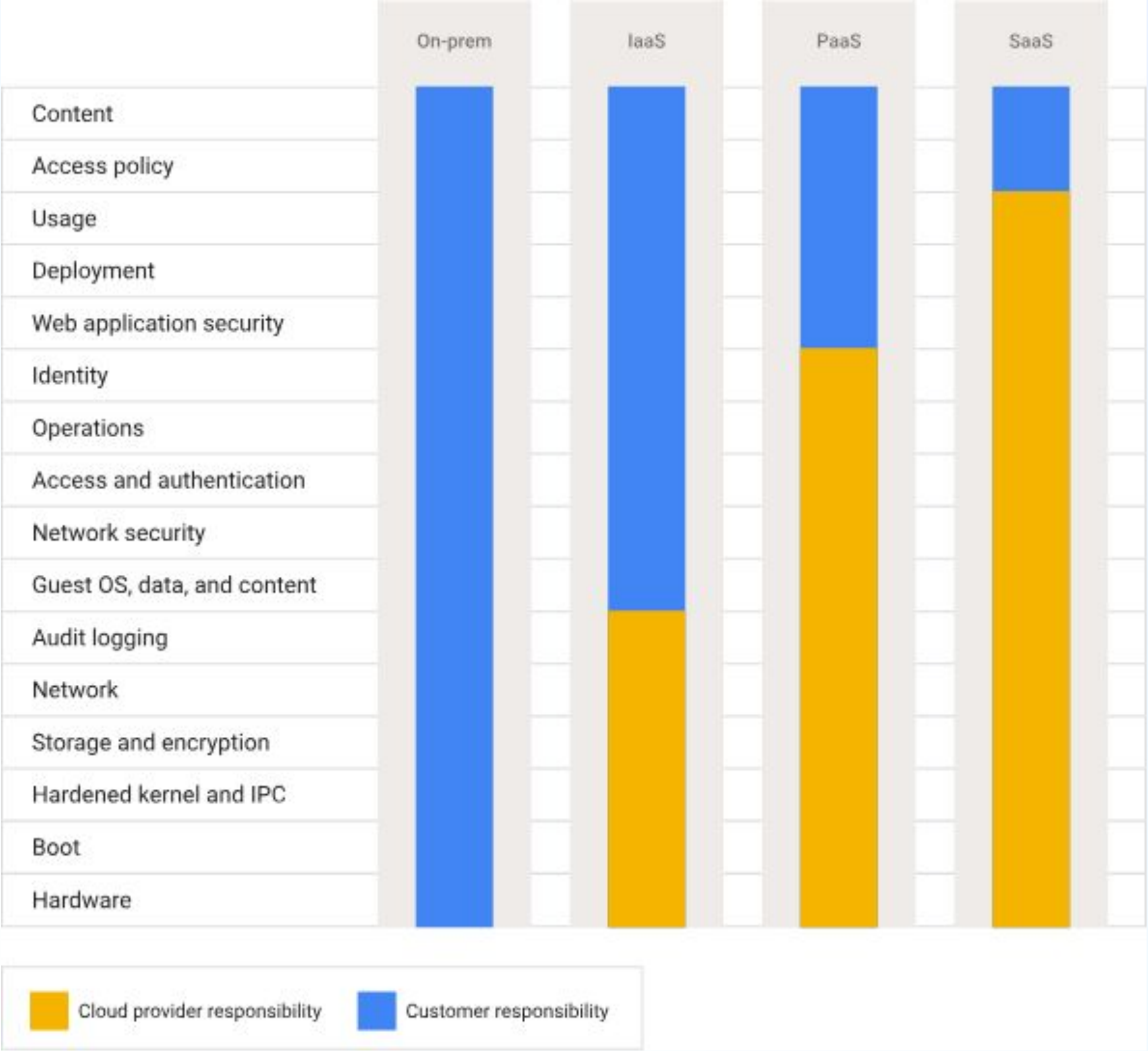
04 **Revisit the basics**:
Network monitoring (VPC Flow Logs, anomalous traffic).

1. Cloud Security Risks

Shared Responsibility Model

1.0.0

Perimeter



Security of the cloud (CSP)

Traditional On Premise model

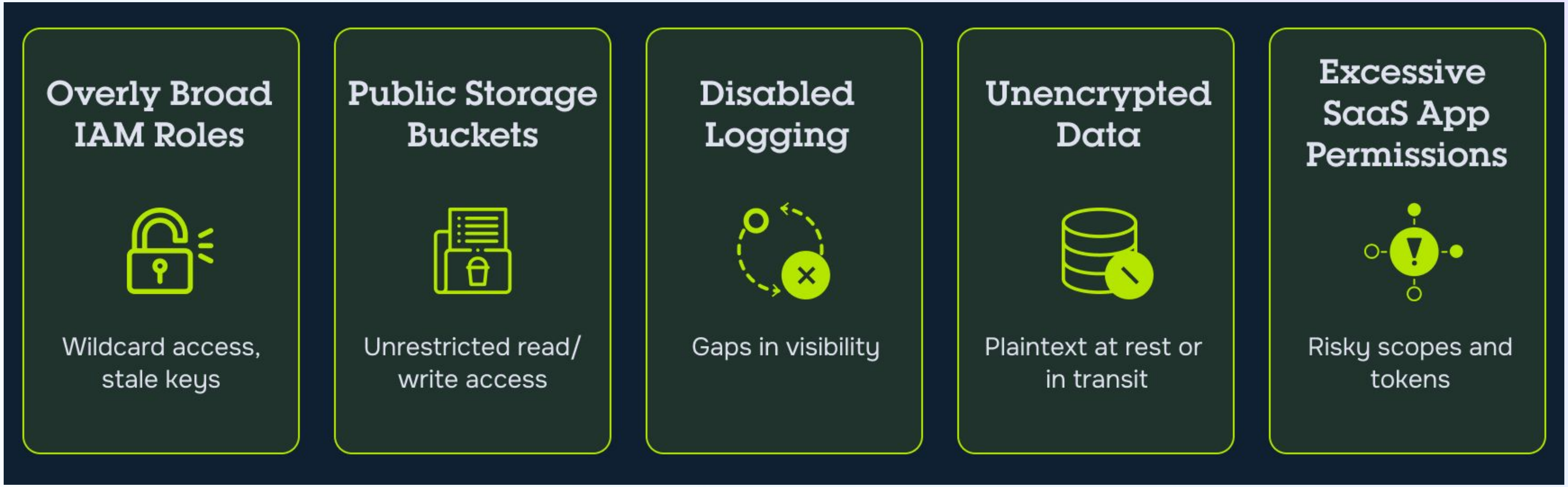
- You control everything: hardware, network, identity, data, and physical access.
- Boundaries are static, and trust zones are well-defined.

VS Security in the cloud (You)

- You delegate part of the stack to the provider (GCP, AWS, etc.).
- You gain agility and scalability — but lose visibility and traditional control planes.

Cloud Security Risks

Misconfiguration Exposure



Overly Broad IAM Roles

Wildcard access, stale keys

Public Storage Buckets

Unrestricted read/ write access

Disabled Logging

Gaps in visibility

Unencrypted Data

Plaintext at rest or in transit

Excessive SaaS App Permissions

Risky scopes and tokens

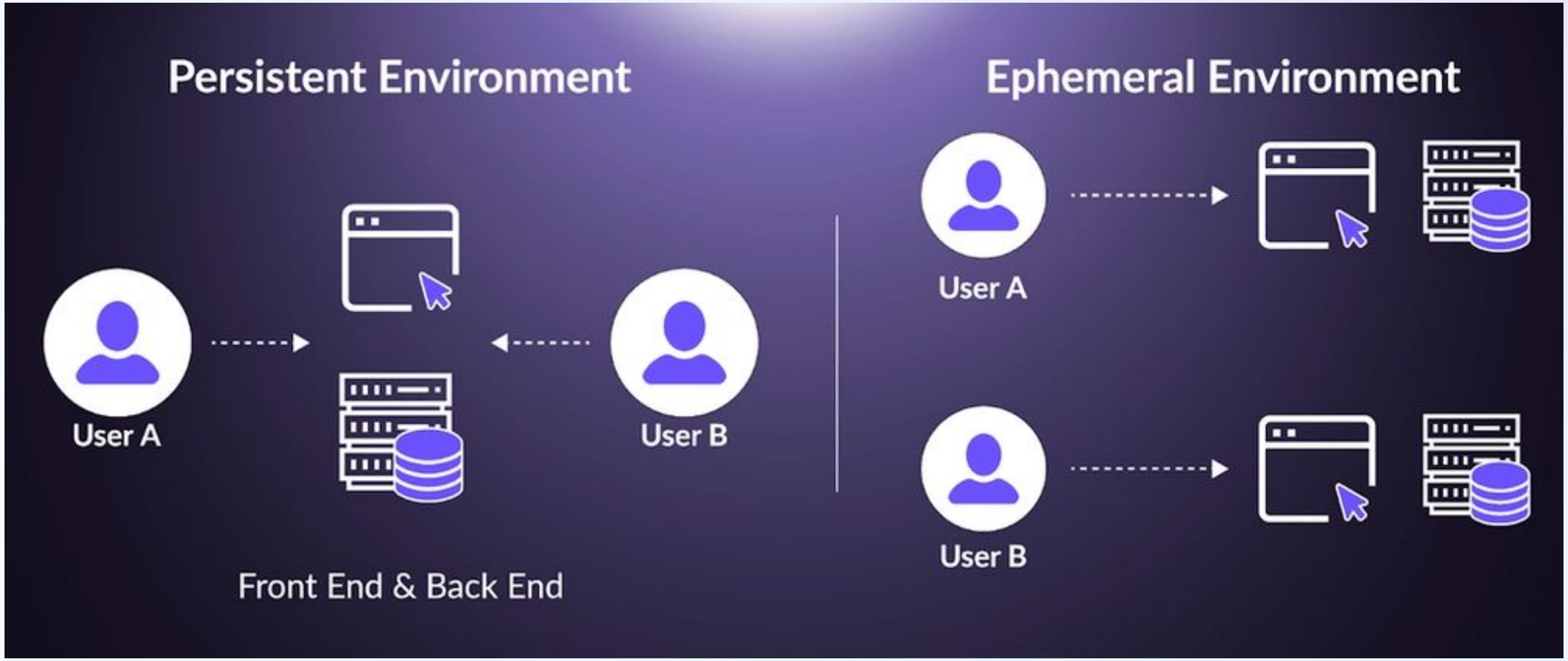
Self-service infrastructure leads to human error.

Case study:
Verizon & Accenture (2017–2018) – NICE Systems left **multiple S3 and GCS buckets found exposed** with sensitive internal data (credentials, configs).

Cloud Security Risks

1.1.1

Ephemeral Infrastructure

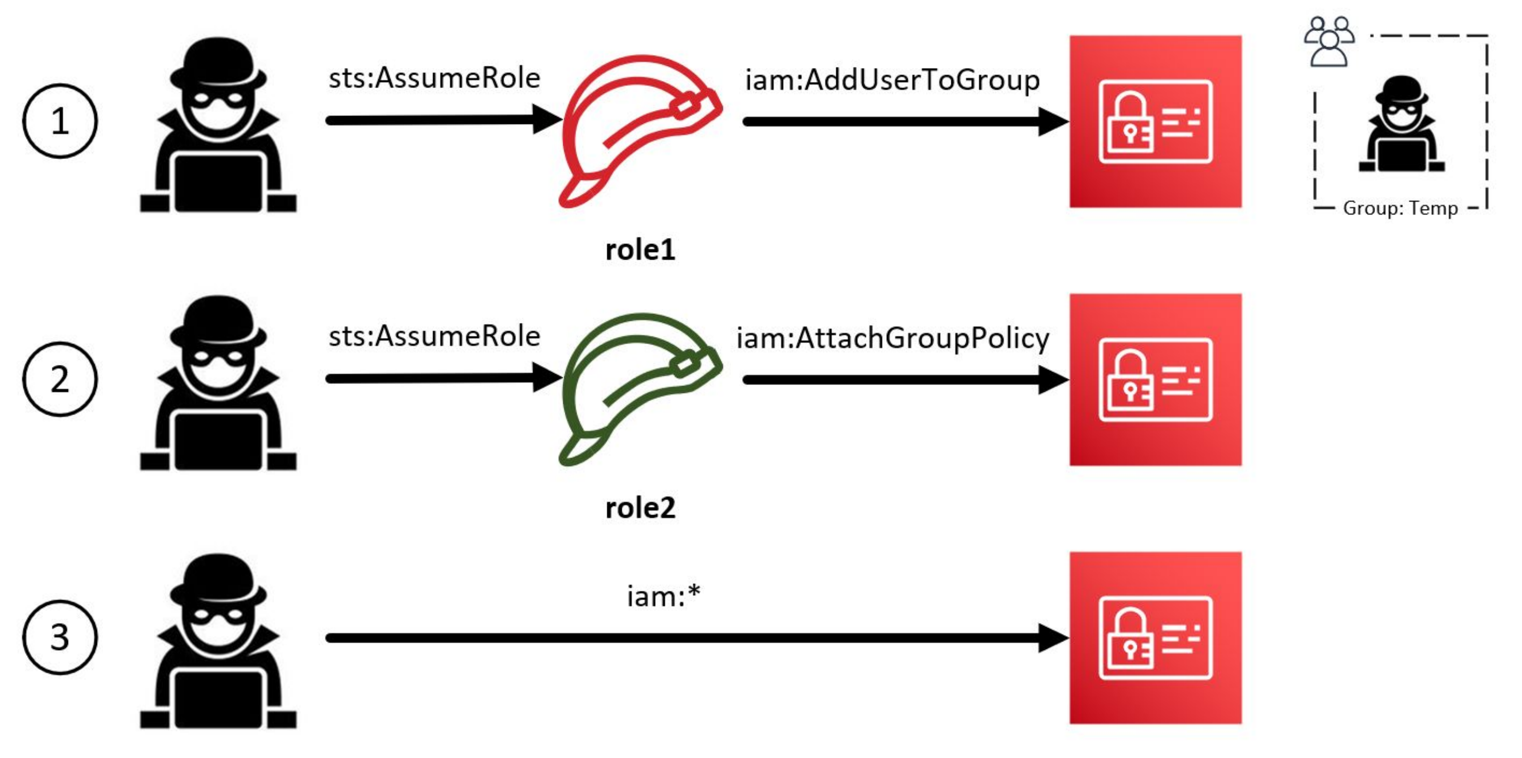


Short-lived workloads (e.g., Cloud Run) evade traditional scans.

Threat example:
Attacker deploys malicious container for data exfil and deletes it.

Cloud Security Risks

Over-Privileged IAM Roles



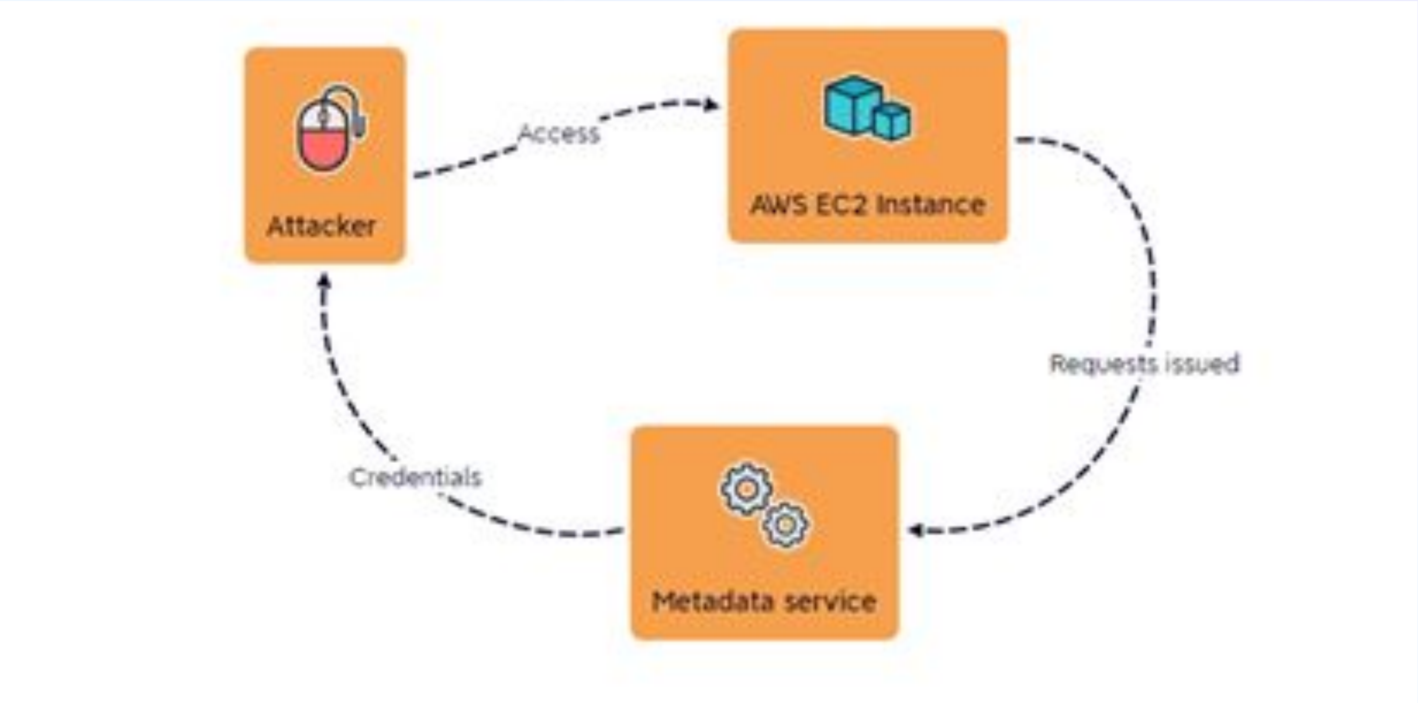
Lack of granular roles or inherited policies.
Example: User escalates privileges via SetIamPolicy.

Case study:
Capital One (2019) – an IAM role attached to the EC2 instance had broader permissions than necessary, including read access to S3 buckets containing sensitive customer data.

Cloud Security Risks

Metadata API Exploitation

1.1.3



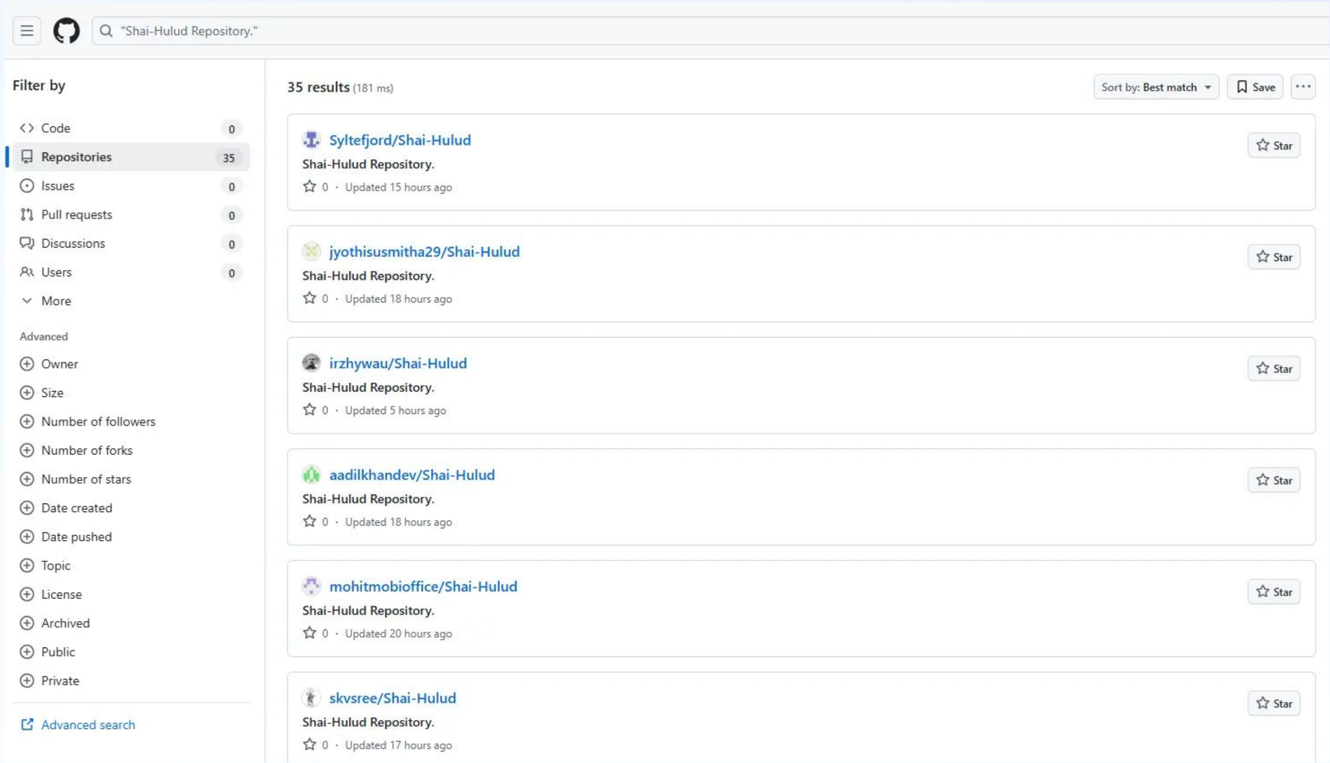
Cloud VMs expose tokens via internal metadata endpoints.
Example: SSRF attack steals access token from 169.254.169.254.

Case study:
Tesla Cloud Breach (2018) – Cryptojacking group compromised Kubernetes admin console exposed to the internet, accessed GCP credentials via the metadata API.

Cloud Security Risks

1.1.4

Service Account Key Leak



"Shai-Hulud Repository."

35 results (181 ms)

Syltefjord/Shai-Hulud
Shai-Hulud Repository.
0 · Updated 15 hours ago

jyothisusmitha29/Shai-Hulud
Shai-Hulud Repository.
0 · Updated 18 hours ago

irzhywau/Shai-Hulud
Shai-Hulud Repository.
0 · Updated 5 hours ago

aadilkhandev/Shai-Hulud
Shai-Hulud Repository.
0 · Updated 18 hours ago

mohitmobioffice/Shai-Hulud
Shai-Hulud Repository.
0 · Updated 20 hours ago

skvsree/Shai-Hulud
Shai-Hulud Repository.
0 · Updated 17 hours ago

Long-lived cloud credentials are exposed, allowing attackers to impersonate trusted services and access cloud resources without detection

Case study:
Code Spaces (GitHub competitor 2014) – Attackers obtained AWS API keys stored in plaintext in an internal control panel, deleted entire AWS environment.

2. Observability

Observability Pillars

2.0.0

Visibility: first step toward detection

Logs

Who did **what** and **when**

Detailed record of events
→ Source of truth for forensic evidence

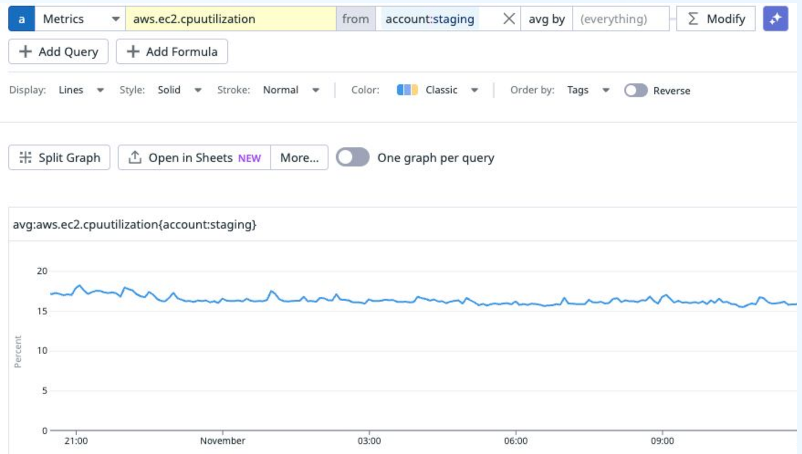
```
"connection": { "src_ip": "10.0.0.5",
"dest_ip": "8.8.8.8", "dest_port": 22 }
"bytes_sent": 12400
```

```
 "protoPayload.methodName":
 "SetIamPolicy"
 "principalEmail":
 "lord.nibbler@planetexpress.com"
 "resourceName": "projects/thuban "
```

Metrics

How the **system** behaves

Aggregated numerical indicators
→ Early anomaly detection, baselines



a Metrics aws.ec2.cpuutilization from account:staging avg by (everything)

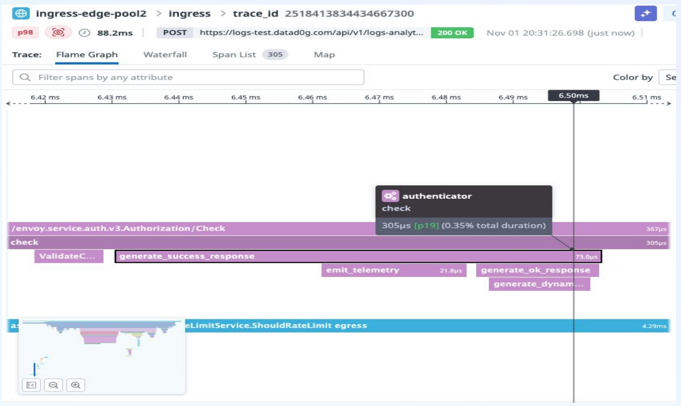
Display: Lines Style: Solid Stroke: Normal Color: Classic Order by: Tags

avg:aws.ec2.cpuutilization{account:staging}

Traces

Where and **how** the **request** flowed

End-to-end request visibility
→ Correlation between components and latency anomalies



ingress-edge-pool2 > ingress > trace_id 2518413834434667300

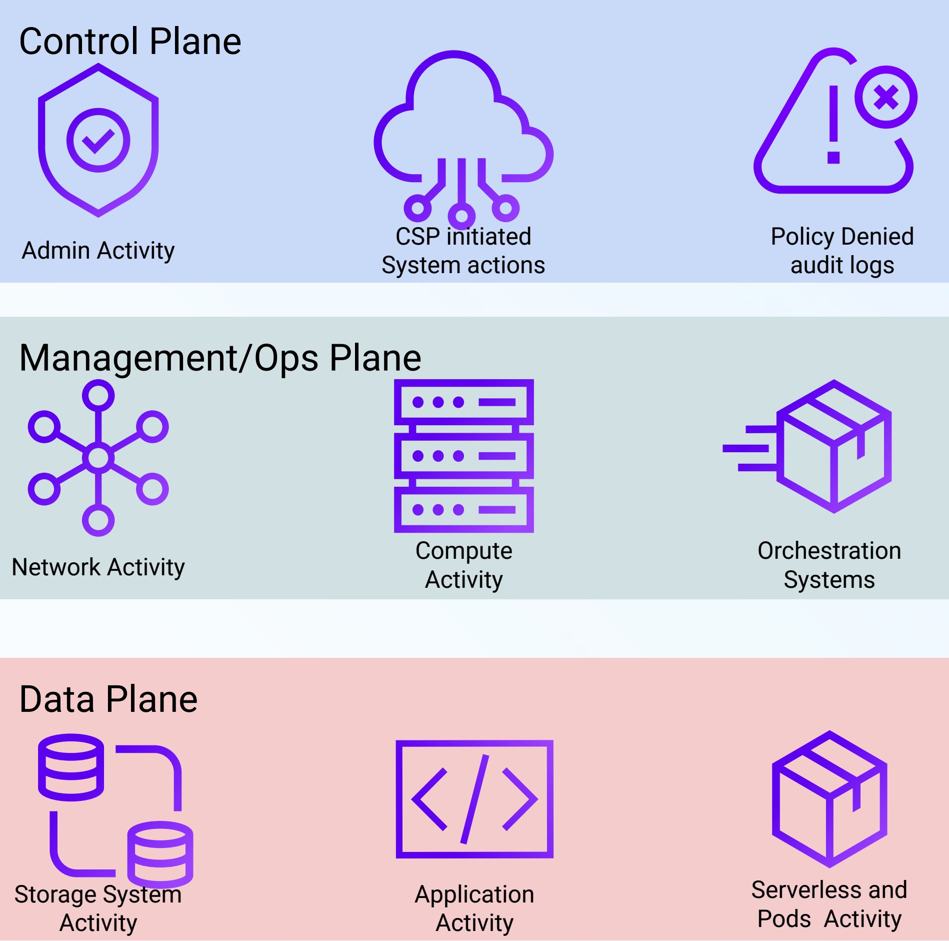
p98 88.2ms POST https://logs-test.datad0g.com/api/v1/logs-analyt... 200 OK Nov 01 20:31:26.698 (just now)

authenticator check 305μs [p19] (0.35% total duration)

Observability Pillars

Cloud Logs

2.1.0



Control Plane

Admin Activity

CSP initiated System actions

Policy Denied audit logs

Management/Ops Plane

Network Activity

Compute Activity

Orchestration Systems

Data Plane

Storage System Activity

Application Activity

Serverless and Pods Activity

Control-plane visibility

- the backbone of “who did what” for resource administration: API / IAM / resource changes
- Enabled by default cannot be disabled

Management & ops plane visibility

- platform health, networking, ingress/egress, runtime ops
- Needs additional configuration and sometimes agents

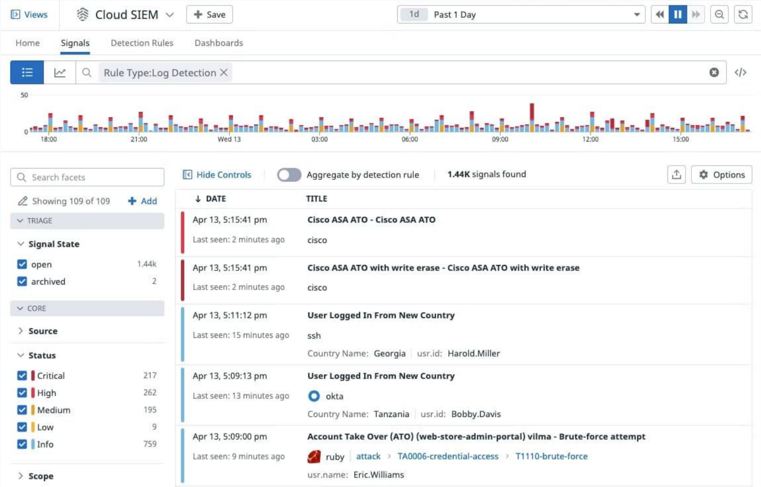
Data plane visibility

- Data Access audit logs are the key for “who accessed / read / changed the data
- disabled by default

Observability Pillars

2.2.0

Industry tools= dashboards + correlation + threat intelligence

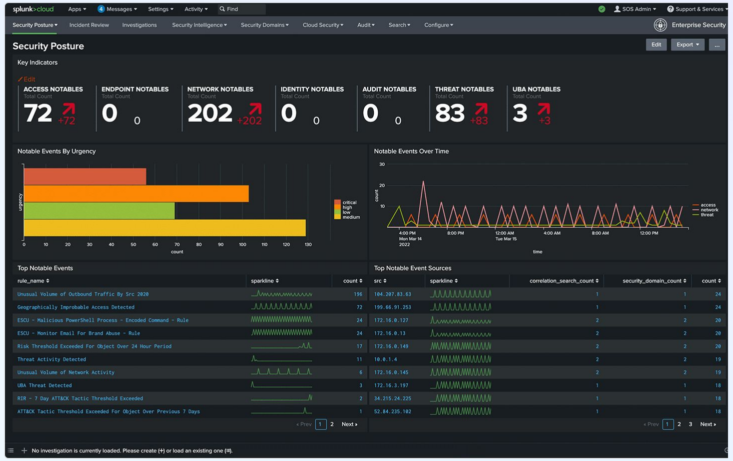


Cloud SIEM · Past 1 Day · Rule Type:Log Detection · 1.44K signals found

DATE	TITLE
Apr 13, 5:15:41 pm Last seen: 2 minutes ago	Cisco ASA ATO - Cisco ASA ATO cisco
Apr 13, 5:15:41 pm Last seen: 2 minutes ago	Cisco ASA ATO with write erase - Cisco ASA ATO with write erase cisco
Apr 13, 5:11:12 pm Last seen: 15 minutes ago	User Logged In From New Country ssh Country Name: Georgia usr.id: Harold.Miller
Apr 13, 5:09:13 pm Last seen: 13 minutes ago	User Logged In From New Country okta Country Name: Tanzania usr.id: Bobby.Davis
Apr 13, 5:09:00 pm Last seen: 9 minutes ago	Account Take Over (ATO) (web-store-admin-portal) vilma - Brute-force attempt ruby attack TA0006-credential-access T1110-brute-force usr.name: Eric.Williams

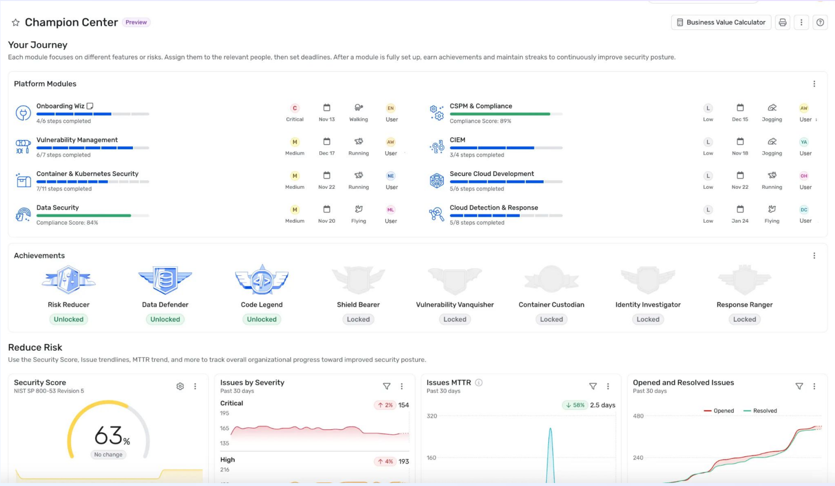
Status: Critical 217, High 262, Medium 195, Low 9, Info 759

Datadog SIEM



Security Posture — Key Indicators: ACCESS NOTABLES 72; ENDPOINT NOTABLES 0; NETWORK NOTABLES 202; IDENTITY NOTABLES 0; AUDIT NOTABLES 0; THREAT NOTABLES 83; UBA NOTABLES 3

Splunk

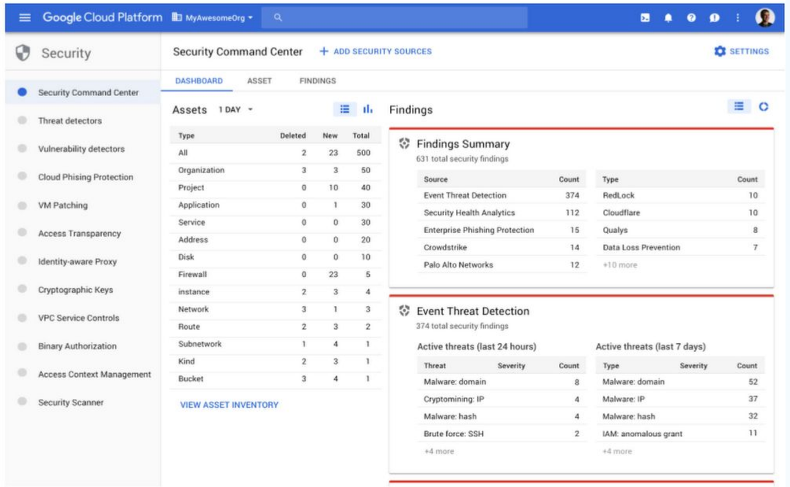


Champion Center — Your Journey — Platform Modules: Onboarding Wiz; Vulnerability Management; Container & Kubernetes Security; Data Security; CSPM & Compliance; CIEM; Secure Cloud Development; Cloud Detection & Response

Achievements: Risk Reducer (Unlocked); Data Defender (Unlocked); Code Legend (Unlocked); Shield Bearer (Locked); Vulnerability Vanquisher (Locked); Container Custodian (Locked); Identity Investigator (Locked); Response Ranger (Locked)

Reduce Risk — Security Score 63%; Issues by Severity; Issues MTTR; Opened and Resolved Issues

WIZ



Security Command Center — Assets (1 DAY)

Type	Deleted	New	Total
All	2	23	500
Organization	3	3	50
Project	0	10	40
Application	0	1	30
Service	0	0	30
Address	0	0	20
Disk	0	0	10
Firewall	0	23	5
instance	2	3	4
Network	3	1	3
Route	2	3	2
Subnetwork	1	4	1
Kind	2	3	1
Bucket	3	4	1

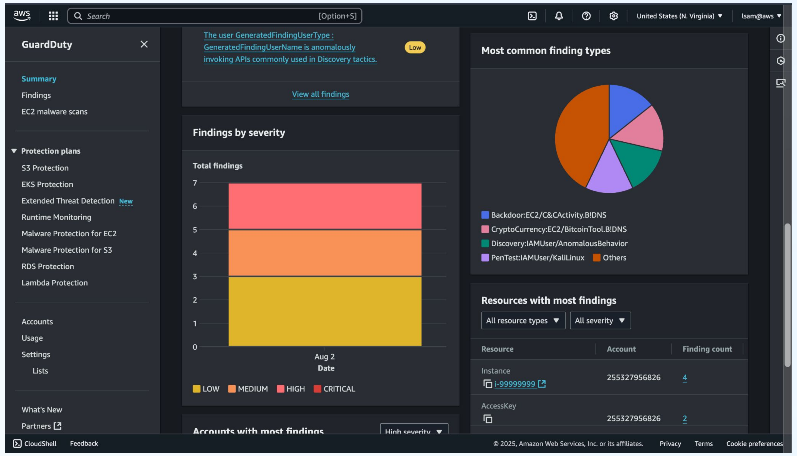
Findings Summary — 631 total security findings

Source	Count	Type	Count
Event Threat Detection	374	RedLock	10
Security Health Analytics	112	Cloudflare	10
Enterprise Phishing Protection	15	Qualys	8
Crowdstrike	14	Data Loss Prevention	7
Palo Alto Networks	12	+10 more	

Event Threat Detection — 374 total security findings

Threat	Count	Type	Count
Malware: domain	8	Malware: domain	52
Cryptomining: IP	4	Malware: IP	37
Malware: hash	4	Malware: hash	32
Brute force: SSH	2	IAM: anomalous grant	11

Google SCC



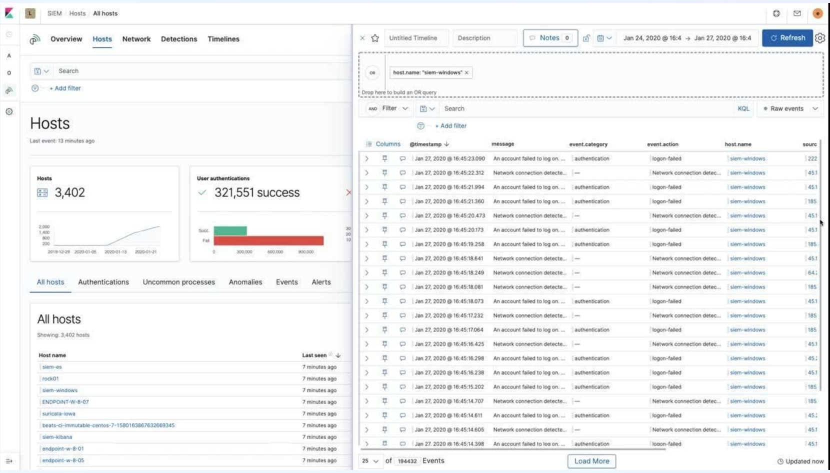
GuardDuty — The user GeneratedFindingUserType : GeneratedFindingUserName is anomalously invoking APIs commonly used in Discovery tactics. (Low)

Most common finding types: Backdoor:EC2/C&CActivity.B!DNS; CryptoCurrency:EC2/BitcoinTool.B!DNS; Discovery:IAMUser/AnomalousBehavior; PenTest:IAMUser/KaliLinux; Others

Findings by severity: LOW, MEDIUM, HIGH, CRITICAL

Resources with most findings: Instance i-99999999 255327956826 4; AccessKey 255327956826 2

Guardduty



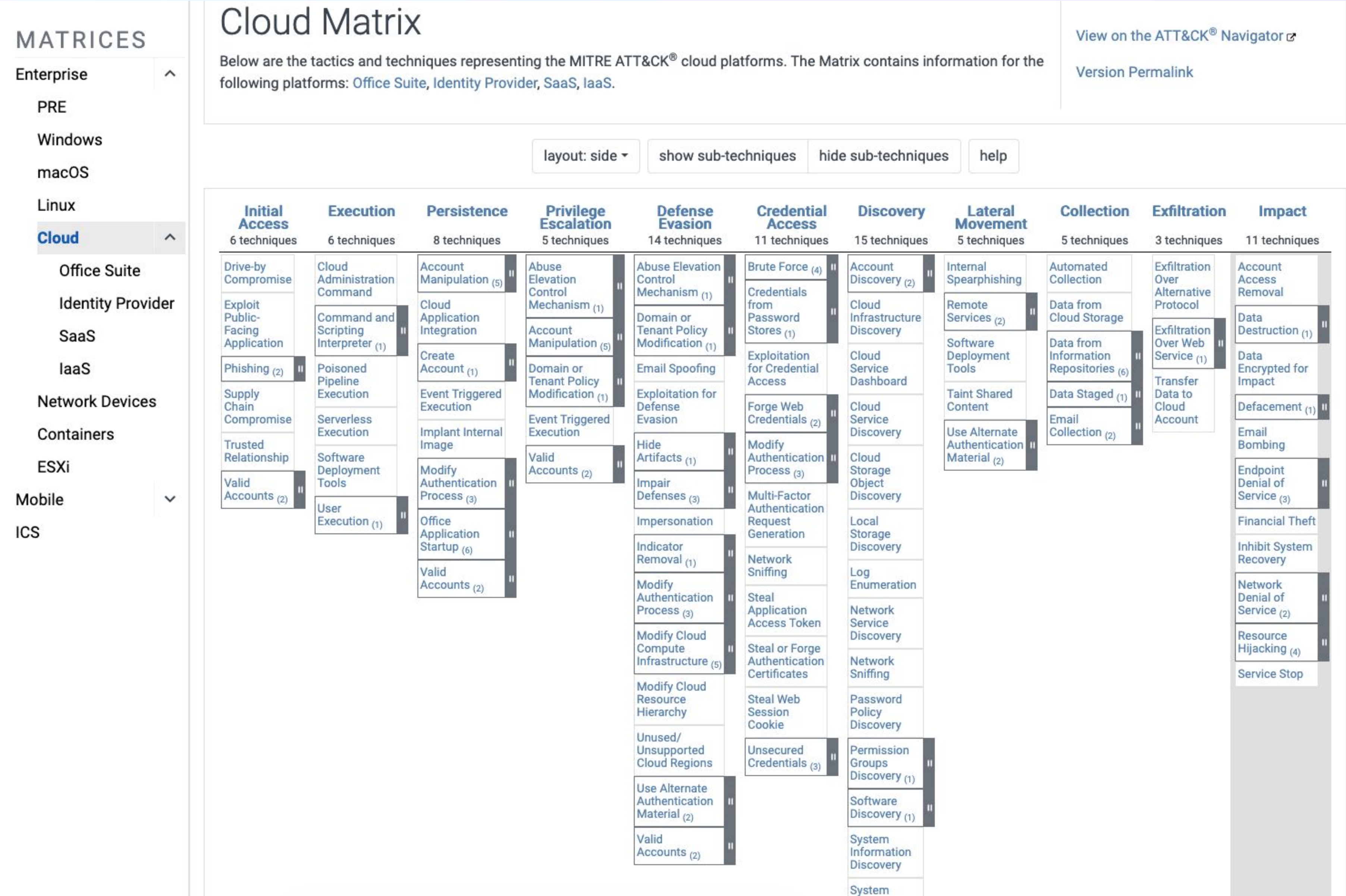
SIEM / Hosts / All hosts — Hosts 3,402; User authentications 321,551 success

ELK Stack

Observability Pillars

2.3.0

MITRE ATT&CK



Cloud Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® cloud platforms. The Matrix contains information for the following platforms: Office Suite, Identity Provider, SaaS, IaaS.

Initial Access 6 techniques	Execution 6 techniques	Persistence 8 techniques	Privilege Escalation 5 techniques	Defense Evasion 14 techniques	Credential Access 11 techniques	Discovery 15 techniques	Lateral Movement 5 techniques	Collection 5 techniques	Exfiltration 3 techniques	Impact 11 techniques
Drive-by Compromise	Cloud Administration Command	Account Manipulation (5)	Abuse Elevation Control Mechanism (1)	Abuse Elevation Control Mechanism (1)	Brute Force (4)	Account Discovery (2)	Internal Spearphishing	Automated Collection	Exfiltration Over Alternative Protocol	Account Access Removal
Exploit Public-Facing Application	Command and Scripting Interpreter (1)	Cloud Application Integration	Account Manipulation (5)	Domain or Tenant Policy Modification (1)	Credentials from Password Stores (1)	Cloud Infrastructure Discovery	Remote Services (2)	Data from Cloud Storage	Exfiltration Over Web Service (1)	Data Destruction (1)
Phishing (2)	Poisoned Pipeline Execution	Create Account (1)	Domain or Tenant Policy Modification (1)	Email Spoofing	Exploitation for Credential Access	Cloud Service Dashboard	Software Deployment Tools	Data from Information Repositories (6)	Transfer Data to Cloud Account	Data Encrypted for Impact
Supply Chain Compromise	Serverless Execution	Event Triggered Execution	Event Triggered Execution	Exploitation for Defense Evasion	Forge Web Credentials (2)	Cloud Service Discovery	Taint Shared Content	Data Staged (1)		Defacement (1)
Trusted Relationship	Software Deployment Tools	Implant Internal Image	Valid Accounts (2)	Hide Artifacts (1)	Modify Authentication Process (3)	Cloud Storage Object Discovery	Use Alternate Authentication Material (2)	Email Collection (2)		Email Bombing
Valid Accounts (2)	User Execution (1)	Modify Authentication Process (3)		Impair Defenses (3)	Multi-Factor Authentication Request Generation	Local Storage Discovery				Endpoint Denial of Service (3)
		Office Application Startup (6)		Impersonation	Network Sniffing	Log Enumeration				Financial Theft
		Valid Accounts (2)		Indicator Removal (1)	Steal Application Access Token	Network Service Discovery				Inhibit System Recovery
				Modify Authentication Process (3)	Steal or Forge Authentication Certificates	Network Sniffing				Network Denial of Service (2)
				Modify Cloud Compute Infrastructure (5)	Steal Web Session Cookie	Password Policy Discovery				Resource Hijacking (4)
				Modify Cloud Resource Hierarchy	Unsecured Credentials (3)	Permission Groups Discovery (1)				Service Stop
				Unused/ Unsupported Cloud Regions		Software Discovery (1)				
				Use Alternate Authentication Material (2)		System Information Discovery				
				Valid Accounts (2)		System				

3. IAM Monitoring

IAM Concepts

3.0.0

Concept	Description	GCP Example

Principals	Entities (users, groups, or service accounts) that request access.	`user:alice@company.com,`
		`serviceAccount:ci-bot@appspot.gserviceaccount.com`

Resources	GCP objects to protect (projects, buckets, VMs, etc.).	`projects/demo-project, buckets/customer-data`
Roles	Collections of permissions defining allowed actions.	`roles/viewer, roles/editor, custom roles`
Policies (Bindings)	Associate principals with roles on resources.	“Alice is granted roles/storage.admin on bucket X”
Inheritance	IAM policies cascade down the resource hierarchy.	Org → Folder → Project → Resource

Policies example

3.0.1

```
{
  "bindings": [
    {
      "role": "roles/storage.objectViewer",
      "members": [
        "user:alice@company.com",
        "group:data-analysts@company.com"
      ]
    },
    {
      "role": "roles/storage.objectAdmin",
      "members": [

"serviceAccount:data-loader@appspot.gserviceaccount.com"
      ],
      "condition": {
        "title": "RestrictToBusinessHours",
        "description": "Allow writes only during business hours",
        "expression": "request.time.getHours() >= 8 &&
request.time.getHours() <= 18"
      }
    }
  ],
  "etag": "BwWWja0YfJA=",
  "version": 3
}
```

Field	Meaning	Detection / Security Note
bindings	Array of role-member pairs	Each entry defines a trust relationship.
role	Permission set (predefined or custom)	Check for overprivileged roles like roles/editor or roles/owner.
members	Users, groups, or service accounts	Audit for external or wildcard members (allUsers, allAuthenticatedUsers).
condition	Contextual restriction (optional)	Great for reducing blast radius; monitor for missing conditions.
etag	Policy version checksum	Used to detect unauthorized overwrites.
version	Version (3 supports conditions)	Policies without conditions = less granular control.

Common Threats

3.1.0

Privilege Escalation

Attack Path:

A developer with partial admin rights modifies IAM policy to grant themselves the roles/owner role.

Detection:

Cloud Audit Logs → SetIamPolicy from non-admin principal.

MITRE: T1098 – Account Manipulation

GCP Logs Explorer

```
resource.type="project"
protoPayload.methodName="SetIamPolicy"
protoPayload.serviceData.policyDelta.bindingDeltas.action="ADD"
protoPayload.serviceData.policyDelta.bindingDeltas.role:("roles/owner
" OR "roles/editor" OR "roles/iam.admin")
protoPayload.authenticationInfo.principalEmail!="iamadmin@company.com
"
```

SCC Events examples

Anomalous Impersonation of Service Account for Admin Activity

Anomalous Impersonation of Service Account for Admin Activity

Common Threats

3.1.1

Service Account Key Creation & Abuse

Attack Path:

An attacker or insider creates a new service account key, downloads it, and uses it outside GCP (often from an external IP) to access APIs.

Detection:

CreateServiceAccountKey method called by unexpected principal or from unusual location

MITRE: T1078 – Valid Accounts

GCP Logs Explorer

```
protoPayload.methodName="google.iam.admin.v1.CreateServiceAccountKey"
protoPayload.status.code=0
protoPayload.authenticationInfo.principalEmail!="automation@datadoghq.com"
```

SCC Events examples

[Service Account Key Created](#)
[Service Account Created in sensitive namespace](#)

Common Threats

3.1.2

Cross-Project/Account Role Abuse

Attack Path:

Attacker compromises a service account in one GCP project and discovers it has IAM bindings to another project or organization, enabling lateral movement

Detection:

Repeated GetIamPolicy or ListProjects API calls from the same account across multiple unrelated projects

MITRE: T1086 – Cloud Service Discovery, T1098 – Account Manipulation

GCP Logs Explorer

```
protoPayload.methodName:("GetIamPolicy" OR "ListProjects")
protoPayload.status.code=0
protoPayload.authenticationInfo.principalEmail!="org-admin@datadoghq.
com"
```

SCC Events examples

Suspicious Cross-Project Permission Use

Service account self-investigation

Common Threats

3.1.3

OAuth or Access Token Abuse

Attack Path:

A valid OAuth access token or refresh token is stolen (e.g., from a developer laptop or browser) and used by an attacker from a new IP or location to impersonate a user or service account.

Detection:

AccessTokenUsage events from previously unseen IPs, regions, or clients.

MITRE: T1528 – Steal Application Access Token T1078 – Valid Accounts

GCP Logs Explorer

```
protoPayload.methodName:("GenerateAccessToken")
protoPayload.status.code=0
protoPayload.authenticationInfo.principalEmail!="trusted-sa@appspot.g
serviceaccount.com"
protoPayload.requestMetadata.callerIp!=("known-corp-ip-1" OR
"known-corp-ip-2")
```

SCC Events examples

Anomalous Service Account Impersonator for Data Access

Common Threats

3.1.4

Misconfigured or Overly Broad Roles

Attack Path:

An engineer or automation pipeline grants users or service accounts the roles/editor or roles/owner roles for convenience — effectively granting full control.

Detection:

Policy bindings contain excessive roles such as roles/editor applied to many members or groups.

T1068 – Exploitation for Privilege Escalation T1098 – Account Manipulation

GCP Logs Explorer

```
protoPayload.methodName:("SetIamPolicy")
protoPayload.serviceData.policyDelta.bindingDeltas.action="ADD"
protoPayload.serviceData.policyDelta.bindingDeltas.role=("roles/edito
r" OR "roles/owner")
protoPayload.serviceData.policyDelta.bindingDeltas.member:("allUsers"
OR "allAuthenticatedUsers")
protoPayload.status.code=0
```

SCC Events examples

New Service Account is Owner or Editor

Common Threats

Orphaned / Inactive Accounts

3.1.5

Attack Path:

A former employee’s account or unused service account remains active, retaining roles that can be exploited for persistence.

Detection:

Accounts with no recent activity still present in IAM policies or keys unused >90 days.

T1068 – T1078.004 – Cloud Accounts T1136 – Create Account

SCC Events examples

Dormant Service Account Action

Common Threats

Service Account Impersonation

3.1.6

Attack Path:

Attacker gains permission to impersonate a privileged service account (via roles/iam.serviceAccountTokenCreator or roles/iam.serviceAccountUser), and uses it to act as that account.

Detection:

GenerateAccessToken or ImpersonateServiceAccount calls by unusual or low-privilege users.

MITRE T1098.001 – Additional Cloud Credentials T1078 – Valid Accounts

GCP Logs Explorer

```
protoPayload.methodName:("GenerateAccessToken")
protoPayload.status.code=0
protoPayload.authenticationInfo.principalEmail!="ci-pipeline@appspot.gserviceaccount.com"
protoPayload.resourceName:"serviceAccounts/privileged-sa@appspot.gserviceaccount.com"
```

SCC Events examples

[Anomalous Impersonation of Service Account for Admin Activity]()

4. Network Monitoring

Network Monitoring

Logs categories

4.0.0

Category	What We Watch	Why It Matters	GCP Data Source
Traffic Flows	Who is talking to whom (IP, port, protocol, volume)	Detect lateral movement, scanning, or exfiltration	**VPC Flow Logs**
Connections & Sessions	Connection attempts (allowed/denied)	Identify brute-force or misconfigured firewall rules	**Firewall Logs**
Egress & Ingress Patterns	Data transfers leaving or entering VPCs	Detect data leaks or command & control (C2)	**VPC Flow Logs**, **Cloud Armor Logs**
DNS Activity	Domains queried by workloads	Identify suspicious domains, tunneling, or C2	**Cloud DNS Logs**
Application Access	Requests to public endpoints (HTTP(S), API Gateway)	Detect web attacks, abuse of APIs	**Load Balancer / Cloud Logging**

Network Monitoring

4.1.0

Core Network Telemetry

Observation Area	Description	Example Questions	GCP Component
VPC Flow Monitoring	Records metadata for every connection (src/dst IP, port, bytes).	Which instance connected to the internet? How much data was sent?	VPC Flow Logs
Firewall Enforcement	Captures allowed and denied traffic decisions.	Are there unexpected allows from unknown sources?	Firewall Logs
Egress/Ingress Visibility	Tracks data entering or leaving subnets.	Is a VM sending large outbound transfers to unknown IPs?	Flow Logs + Monitoring
DNS Requests	Tracks what domains workloads resolve.	Are workloads querying dynamic DNS or known malicious domains?	Cloud DNS Logs
Load Balancer Logs	Monitors HTTP(S) access to apps.	Are there signs of scanning or web exploitation attempts?	Load Balancer Access Logs
Routing and Peering Traffic	Observes cross-project or hybrid network flows.	Is unexpected traffic crossing VPC peering or Cloud VPN?	VPC Flow Logs + Route Logs

Common threats

4.2.0

Port Scanning / Reconnaissance

Attack Path:
An attacker or compromised VM scans internal or external IP ranges to identify open ports and services for further exploitation

Detection:
Same source IP connecting to many destinations or ports in a short timeframe.
High connection_count per reporting interval in VPC Flow Logs.

MITRE: T1046 – Network Service Scanning, T1595 – Active Scanning

SCC Events examples
[Log4J active scan]

Common threats

4.2.1

Data Exfiltration (Outbound Transfer Anomalies)

Attack Path:
A compromised workload exfiltrates sensitive data to an external IP address using allowed protocols (e.g., HTTPS, SFTP).

Detection:
Outbound data volume (bytes_sent) greatly exceeds baseline.
Destination IPs outside expected CIDR ranges.
Repeated long sessions to unknown destinations

MITRE: T1048 – Exfiltration Over Alternative Protocol T1567 – Exfiltration Over Web Services

SCC Events examples
Cloud SQL Data Exfiltration

Common threats

4.2.2

Command & Control (C2) via DNS or HTTP

Attack Path:

An attacker establishes a communication channel to an external domain through periodic DNS queries or HTTP callbacks from a compromised workload.

Detection:

Repetitive, timed outbound requests to rare or algorithmic (DGA-like) domains.
Unexpected DNS queries to dynamic domains or rare TLDs.
VMs connecting to known malicious IPs or domains.

MITRE: T1041 – Exfiltration Over C2 Channel

```
GCP Logs Explorer
resource.type="dns_query"
jsonPayload.query_name!~"(?i)(^|\.)(corp|google|gstatic|datadoghq)\."
jsonPayload.query_name=~"(?i)\.(top|xyz)\.?$"
```

SCC Events examples
[DNS Tunneling]

Common threats

4.2.3

Internal Lateral Movement

Attack Path:

An attacker attempts to pivot from a compromised VM to other internal hosts by connecting over SSH, RDP, or other management ports.

Detection:

Internal IP connecting to multiple internal destinations on admin ports (22, 3389, 5985).
Unusual cross-subnet connections between workloads.
Spikes in east–west traffic inside the VPC.

MITRE: T1049 – System Network Connections Discovery T1570 – Lateral Tool Transfer

GCP Logs Explorer

```
resource.type="gce_subnetwork"
logName:("vpc_flows")
jsonPayload.reporter="SRC"
jsonPayload.connection.dest_port=(22 OR 3389 OR 5985)
jsonPayload.connection.dest_ip=~"^(10\.|192\.168\.|172\.(1[6-9]|2[0-9
]|3[0-1])\.)"
```

SCC Events examples

DNS Tunneling

Common threats

4.2.4

Cryptomining Activity

Attack Path:

Compromised workloads are used for unauthorized cryptocurrency mining, causing CPU spikes and outbound connections to known mining pools.

Detection:

Sudden CPU usage spikes combined with sustained outbound traffic to known mining domains.
High outbound connections on mining protocols (3333, 4444, 5555).
Unexpected egress_bytes from idle workloads.

MITRE: T1496 – Resource Hijacking

```
GCP Logs Explorer
resource.type="gce_subnetwork"
logName:("vpc_flows")
jsonPayload.reporter="SRC"
jsonPayload.connection.dest_port=(3333 OR 4444)
```

SCC Events examples

[Cryptomining Bad IP](#)

Common threats

4.2.5

Denial of Service Attacks

Attack Path:
Attackers flood public-facing endpoints or load balancers with traffic to degrade performance or take services offline

Detection:
Sudden spike in inbound packets or requests.
Repeated connections from many unique IPs.
Abnormal error rates (HTTP 429, 503)

MITRE: T1498 – Network Denial of Service

GCP Logs Explorer

```
resource.type="http_load_balancer"
httpRequest.status>=500
httpRequest.latency>="1s"
```

Question ?

Hands-on time after a small break !

Detect suspicious IAM and Network activities in GCP

https://github.com/0x74696D/security_monitoring_tp