Forward-Looking Statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries.
All other brand names, product names or trademarks belong to their respective owners. © 2023 Splunk Inc. All rights reserved.

© 2023 SPLUNK INC.

Securing the Cloudscape

Resilient Multi-Cloud Detection Engineering
SEC1225B

Mauricio Velazco

Principal Threat Research Engineer | Splunk

Bhavin Patel

Senior Threat Research Engineer | Splunk

splunk> .conf23

© 2023 SPLUNK INC.

Mauricio Velazco

Principal Threat Researcher | Splunk

Bhavin Patel

Senior Threat Researcher | Splunk

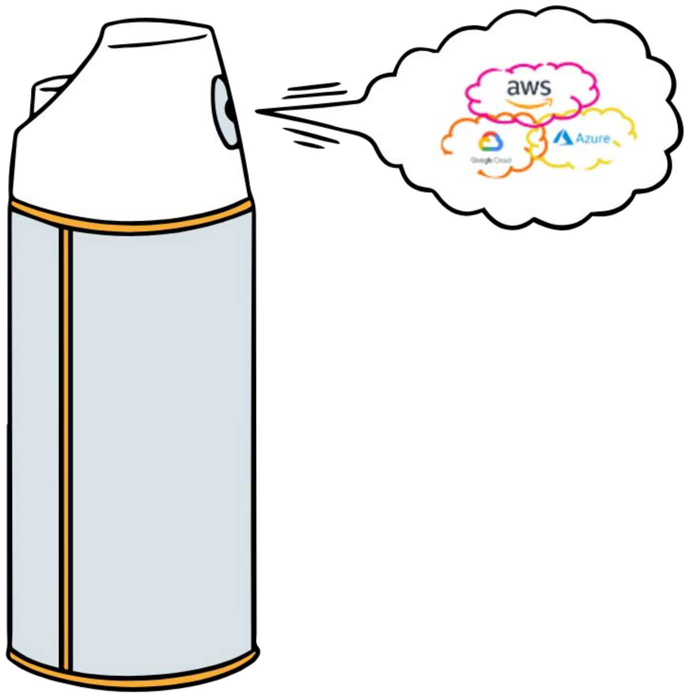
© 2023 SPLUNK INC.

Splunk Threat Research Team (STRT)

- Study Threats
- Create Datasets
- Build Detections
- Release Tools
- Share with Community

https://research.splunk.com

© 2023 SPLUNK INC.



Source: bit.ly/3p5RjtE

Agenda

- Introduction
- Cloud Telemetry
- Multi-Cloud Detection Engineering
- Demo
- Takeaways

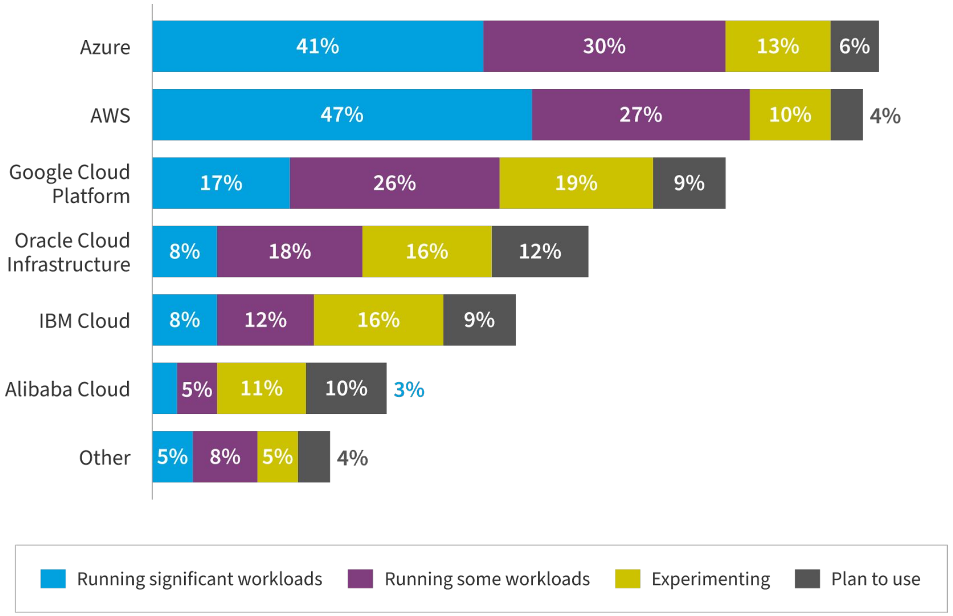
All trademarks, logos, and brand names are the property of their respective owners.

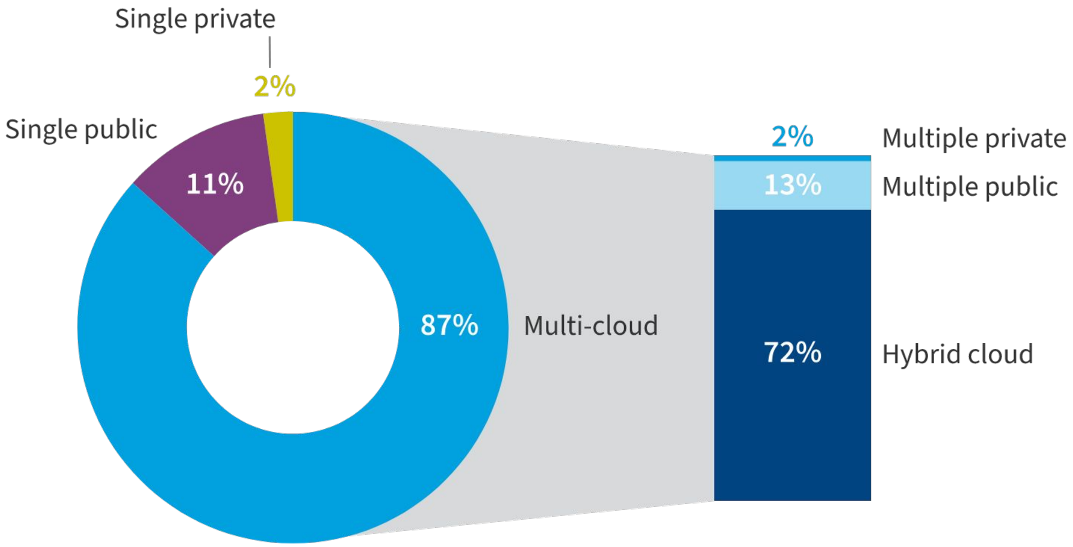
© 2023 SPLUNK INC.

Introduction

© 2023 SPLUNK INC.

Cloudy with a Chance of Multi-Cloud





Source: Flexera 2023 State of the Cloud Report; N=750.

© 2023 SPLUNK INC.

Why Organizations Use Multiple Clouds

Different stacks for different tasks

aws
Google Cloud
Azure

AWS for development
Microservices
Containers
EC2, Storage

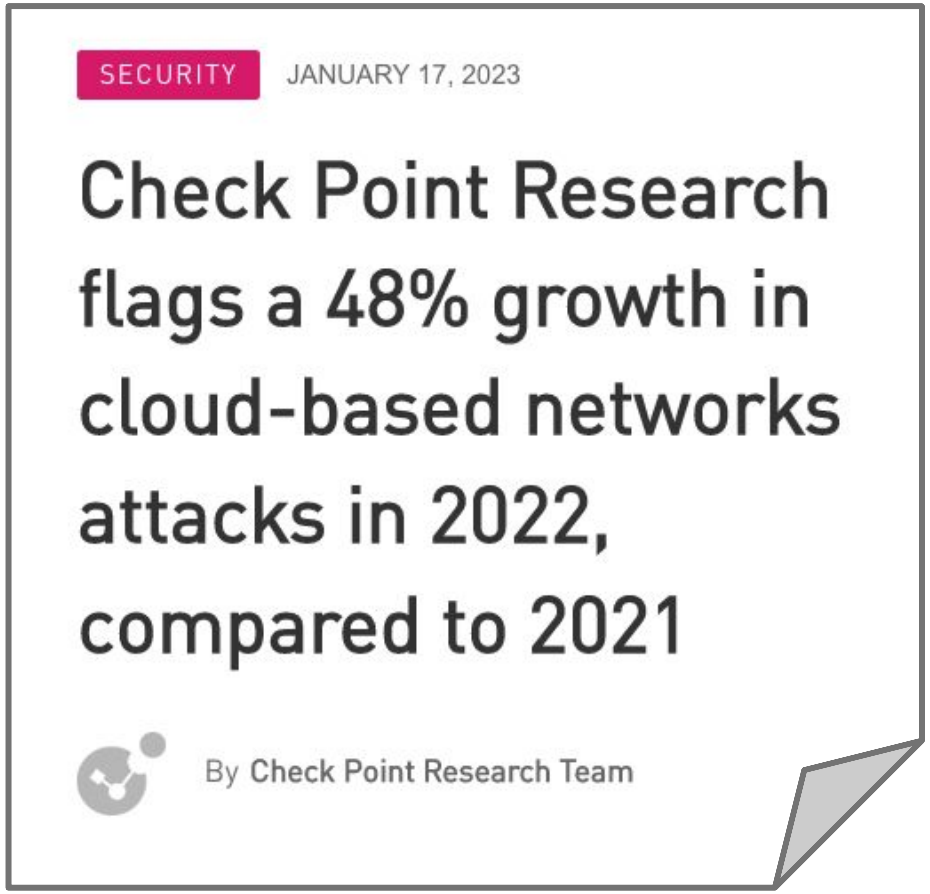
GCP for internal services
Google Workspace
Workday
Salesforce

Azure for lift and shift
Reduce costs
Disaster recovery

All trademarks, logos, and brand names are the property of their respective owners.

© 2023 SPLUNK INC.

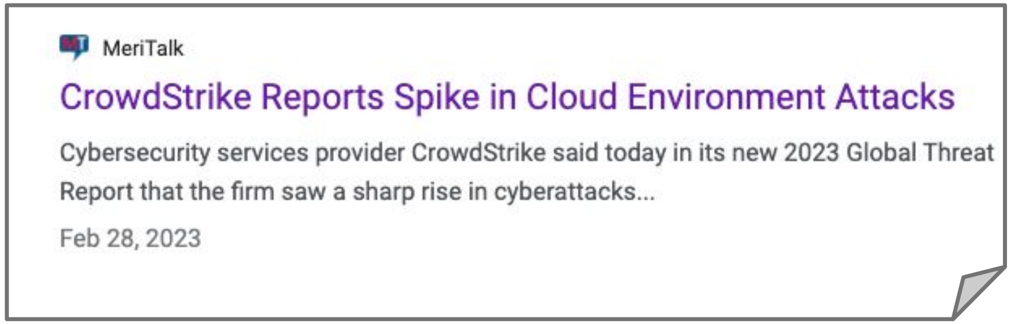
Turbulence in the Clouds



SECURITY JANUARY 17, 2023

Check Point Research flags a 48% growth in cloud-based networks attacks in 2022, compared to 2021

By Check Point Research Team

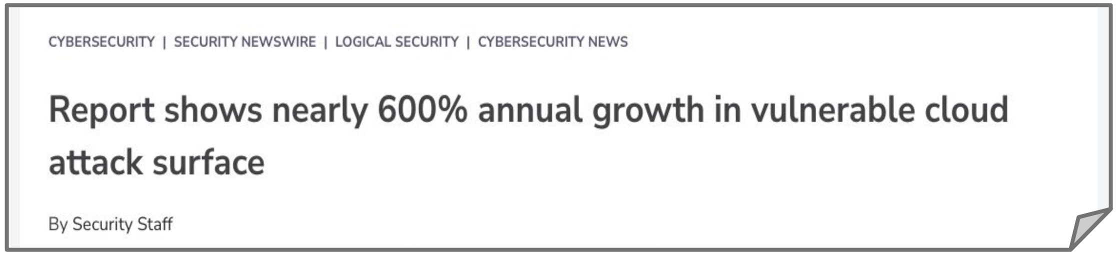


MeriTalk

CrowdStrike Reports Spike in Cloud Environment Attacks

Cybersecurity services provider CrowdStrike said today in its new 2023 Global Threat Report that the firm saw a sharp rise in cyberattacks...

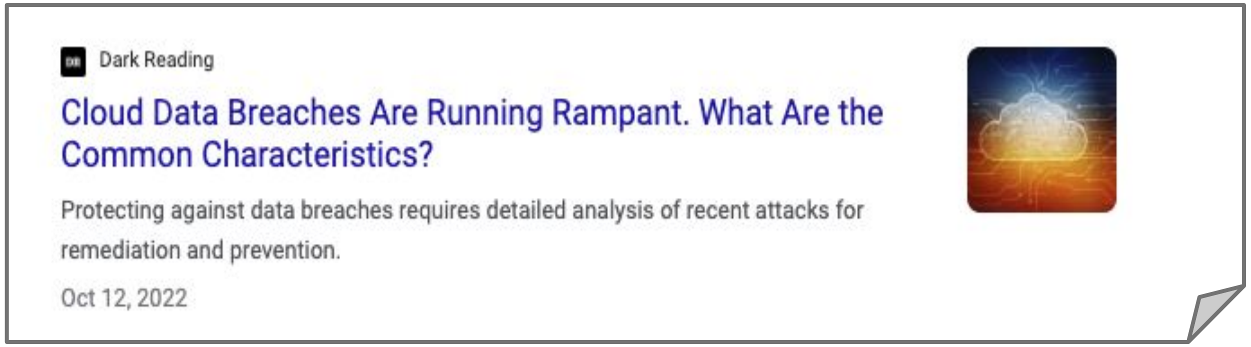
Feb 28, 2023



CYBERSECURITY | SECURITY NEWSWIRE | LOGICAL SECURITY | CYBERSECURITY NEWS

Report shows nearly 600% annual growth in vulnerable cloud attack surface

By Security Staff



Dark Reading

Cloud Data Breaches Are Running Rampant. What Are the Common Characteristics?

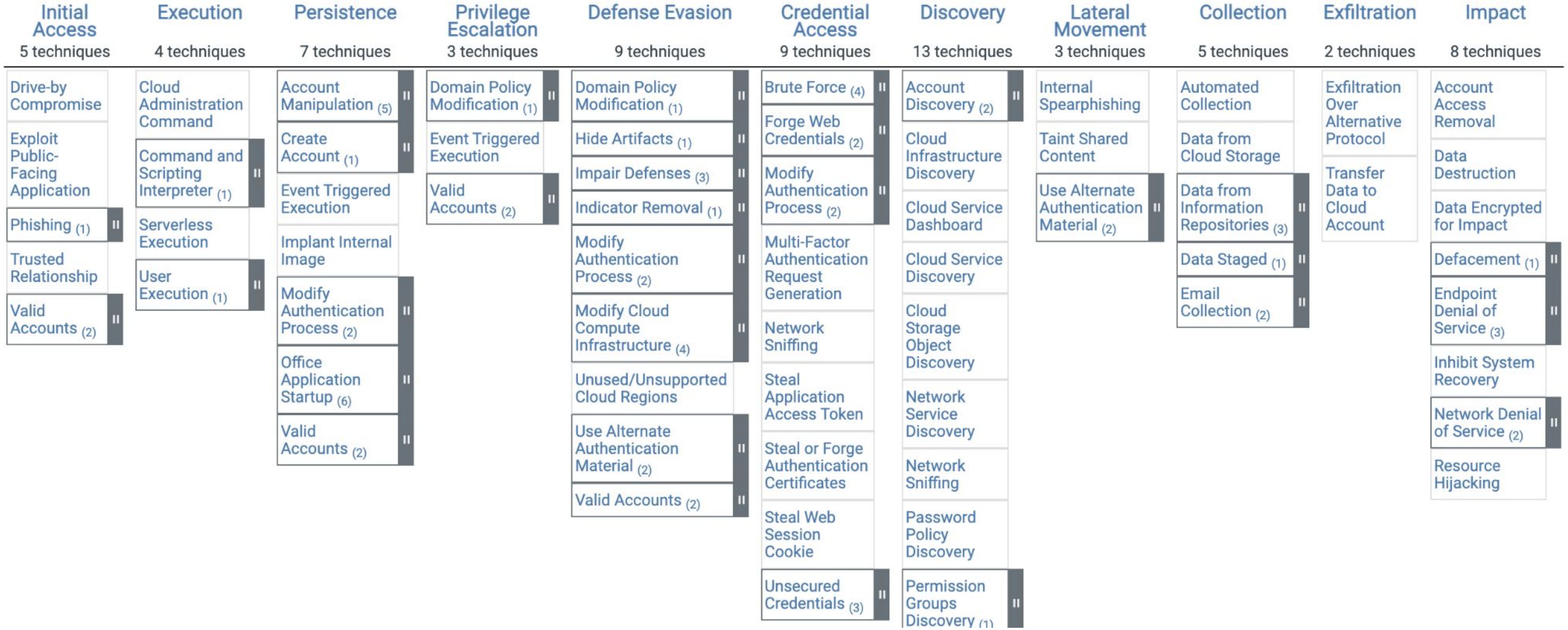
Protecting against data breaches requires detailed analysis of recent attacks for remediation and prevention.

Oct 12, 2022

© 2023 SPLUNK INC.

MITRE Cloud Matrix

Cloud-based techniques for Azure AD, Office 365, Google Workspace, SaaS, IaaS (v13)

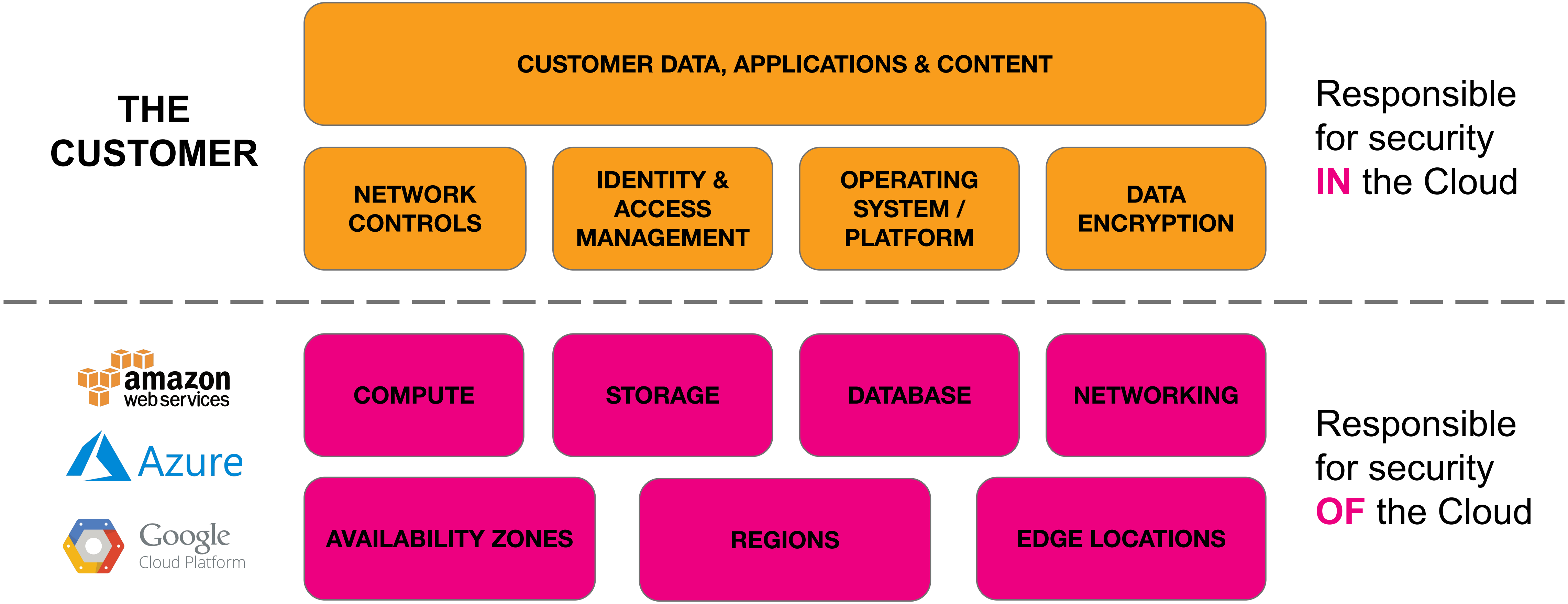


Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
5 techniques	4 techniques	7 techniques	3 techniques	9 techniques	9 techniques	13 techniques	3 techniques	5 techniques	2 techniques	8 techniques
Drive-by Compromise	Cloud Administration Command	Account Manipulation (5)	Domain Policy Modification (1)	Domain Policy Modification (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)	Create Account (1)	Event Triggered Execution	Hide Artifacts (1)	Forge Web Credentials (2)	Cloud Infrastructure Discovery	Taint Shared Content	Data from Cloud Storage	Transfer Data to Cloud Account	Data Destruction
Phishing (1)	Serverless Execution	Event Triggered Execution	Valid Accounts (2)	Impair Defenses (3)	Modify Authentication Process (2)	Cloud Service Dashboard	Use Alternate Authentication Material (2)	Data from Information Repositories (3)		Data Encrypted for Impact
Trusted Relationship	User Execution (1)	Implant Internal Image		Indicator Removal (1)	Multi-Factor Authentication Request Generation	Cloud Service Discovery		Data Staged (1)		Defacement (1)
Valid Accounts (2)		Modify Authentication Process (2)		Modify Authentication Process (2)	Network Sniffing	Cloud Storage Object Discovery		Email Collection (2)		Endpoint Denial of Service (3)
		Office Application Startup (6)		Modify Cloud Compute Infrastructure (4)	Steal Application Access Token	Network Service Discovery				Inhibit System Recovery
		Valid Accounts (2)		Unused/Unsupported Cloud Regions	Steal or Forge Authentication Certificates	Network Sniffing				Network Denial of Service (2)
				Use Alternate Authentication Material (2)	Steal Web Session Cookie	Password Policy Discovery				Resource Hijacking
				Valid Accounts (2)	Unsecured Credentials (3)	Permission Groups Discovery (1)				

Source: https://attack.mitre.org/matrices/enterprise/cloud/

© 2023 SPLUNK INC.

Bottom Line – Security is a Shared Responsibility in the Cloud



THE CUSTOMER

CUSTOMER DATA, APPLICATIONS & CONTENT

NETWORK CONTROLS

IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM / PLATFORM

DATA ENCRYPTION

Responsible for security **IN** the Cloud

amazon web services

Azure

Google Cloud Platform

COMPUTE

STORAGE

DATABASE

NETWORKING

AVAILABILITY ZONES

REGIONS

EDGE LOCATIONS

Responsible for security **OF** the Cloud

All trademarks, logos, and brand names are the property of their respective owners.

© 2023 SPLUNK INC.

Challenges of Monitoring Multi-Cloud

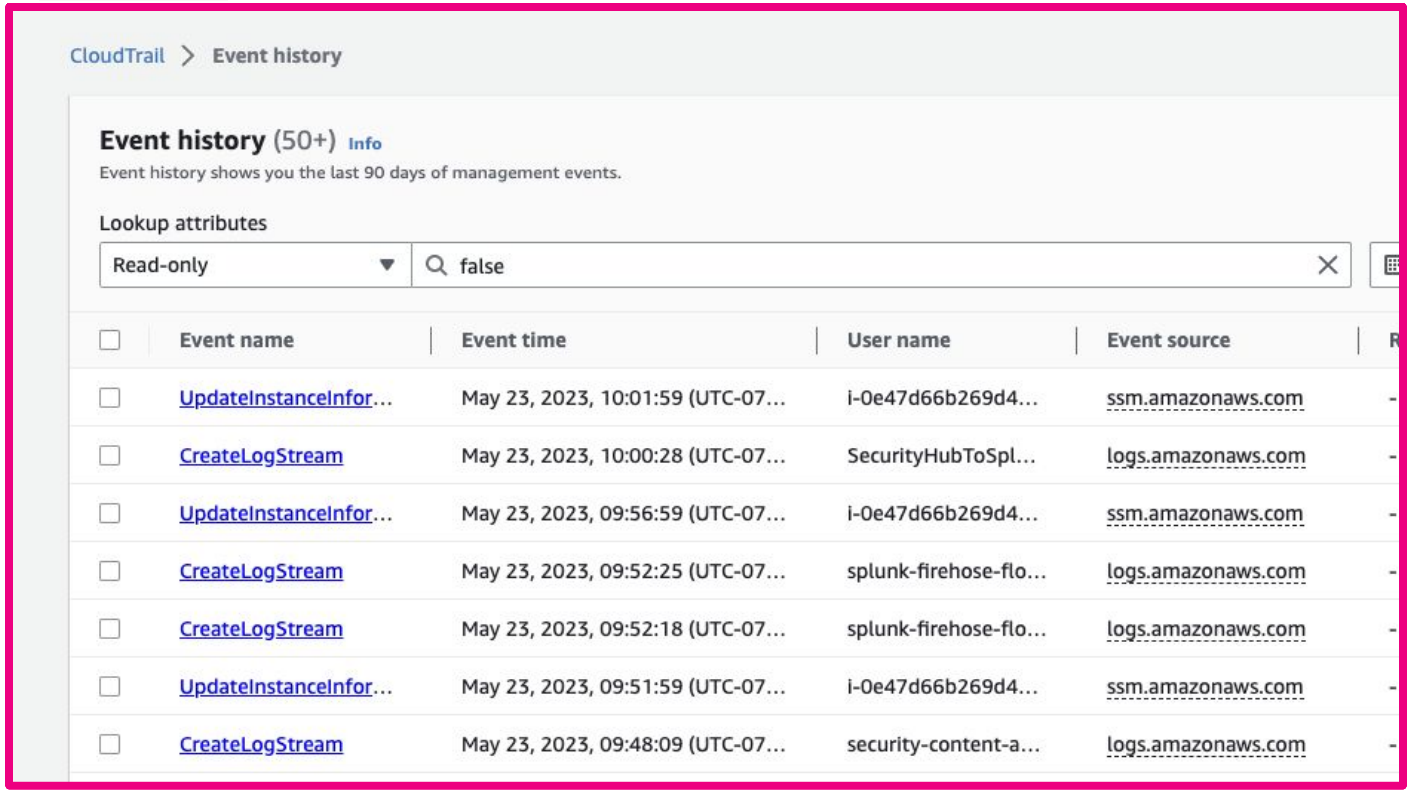
- Holistic visibility
- Complexity and differences across platforms
- Query languages and log schemas (SQL,KQL,etc)
- (Near) real time alerting
- Threat intelligence integration
- Multiple vendors and tools to manage

Source: https://www.shutterstock.com/search/cyber-security-cartoon

© 2023 SPLUNK INC.

Console?

Amazon
CloudTrail



CloudTrail > Event history

Event history (50+) Info

Event history shows you the last 90 days of management events.

Lookup attributes

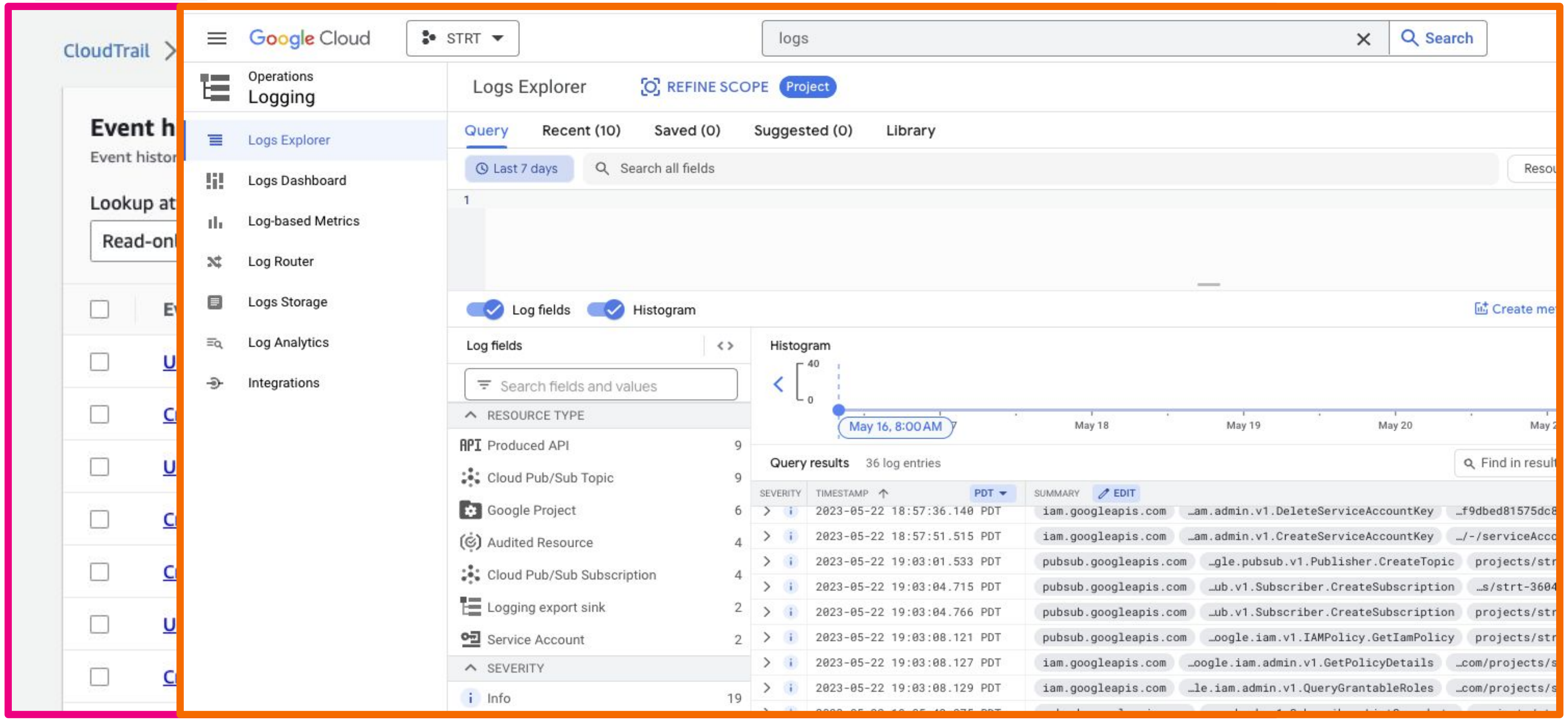
Read-only ▼ | false ✕

□	Event name	Event time	User name	Event source	R
□	UpdateInstanceInfor...	May 23, 2023, 10:01:59 (UTC-07...	i-0e47d66b269d4...	ssm.amazonaws.com	-
□	CreateLogStream	May 23, 2023, 10:00:28 (UTC-07...	SecurityHubToSpl...	logs.amazonaws.com	-
□	UpdateInstanceInfor...	May 23, 2023, 09:56:59 (UTC-07...	i-0e47d66b269d4...	ssm.amazonaws.com	-
□	CreateLogStream	May 23, 2023, 09:52:25 (UTC-07...	splunk-firehose-flo...	logs.amazonaws.com	-
□	CreateLogStream	May 23, 2023, 09:52:18 (UTC-07...	splunk-firehose-flo...	logs.amazonaws.com	-
□	UpdateInstanceInfor...	May 23, 2023, 09:51:59 (UTC-07...	i-0e47d66b269d4...	ssm.amazonaws.com	-
□	CreateLogStream	May 23, 2023, 09:48:09 (UTC-07...	security-content-a...	logs.amazonaws.com	-

© 2023 SPLUNK INC.

Console? Another Console?

Amazon CloudTrail



CloudTrail >

Event h
Event histor

Lookup at
Read-onl

E
U
C
U
C
C
U
C

Logs Explorer

```
1
```

Log fields

RESOURCE TYPE	
Produced API	9
Cloud Pub/Sub Topic	9
Google Project	6
Audited Resource	4
Cloud Pub/Sub Subscription	4
Logging export sink	2
Service Account	2
SEVERITY	
Info	19

Histogram

Query results 36 log entries

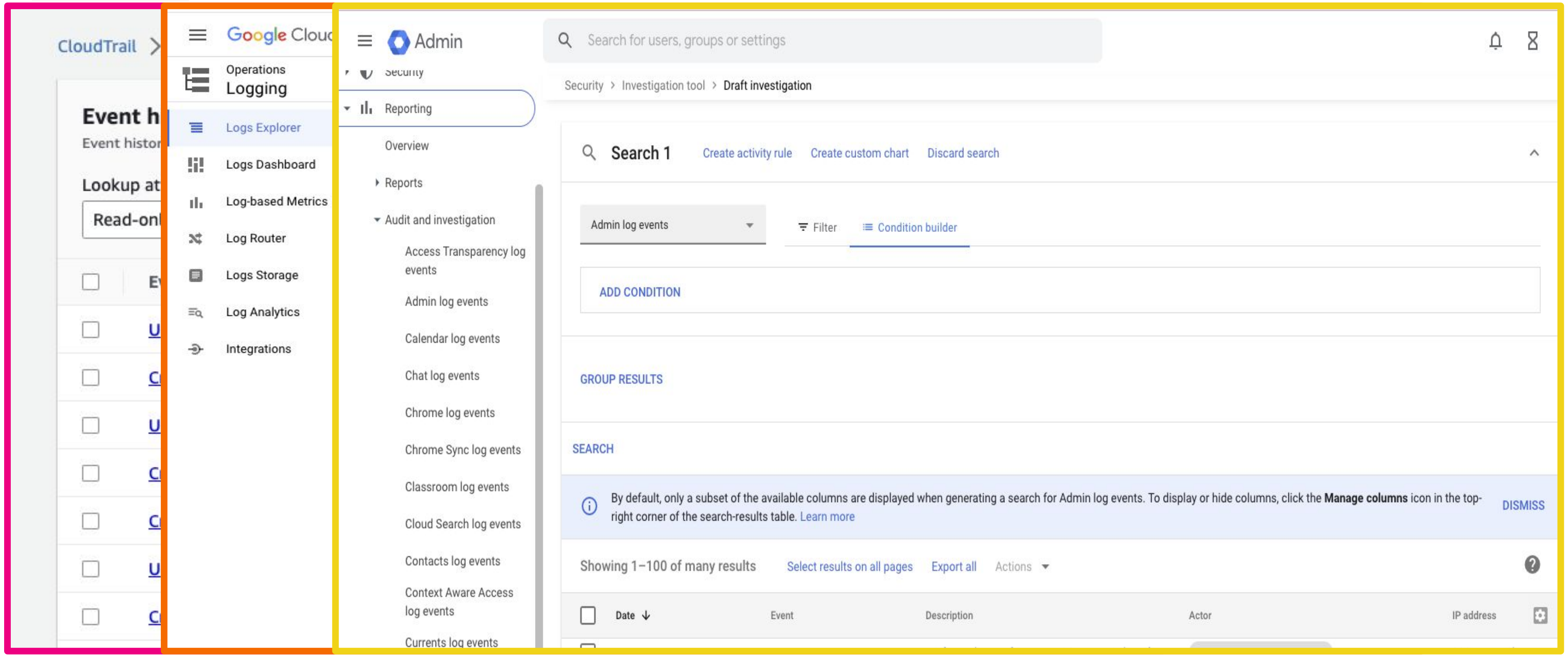
```
SEVERITY  TIMESTAMP                      PDT   SUMMARY
          2023-05-22 18:57:36.140 PDT   iam.googleapis.com     …am.admin.v1.DeleteServiceAccountKey     …f9dbed81575dc8
          2023-05-22 18:57:51.515 PDT   iam.googleapis.com     …am.admin.v1.CreateServiceAccountKey     …/-/serviceAcco
          2023-05-22 19:03:01.533 PDT   pubsub.googleapis.com  …gle.pubsub.v1.Publisher.CreateTopic     projects/str
          2023-05-22 19:03:04.715 PDT   pubsub.googleapis.com  …ub.v1.Subscriber.CreateSubscription     …s/strt-3604
          2023-05-22 19:03:04.766 PDT   pubsub.googleapis.com  …ub.v1.Subscriber.CreateSubscription     projects/str
          2023-05-22 19:03:08.121 PDT   pubsub.googleapis.com  …oogle.iam.v1.IAMPolicy.GetIamPolicy     projects/str
          2023-05-22 19:03:08.127 PDT   iam.googleapis.com     …oogle.iam.admin.v1.GetPolicyDetails     …com/projects/s
          2023-05-22 19:03:08.129 PDT   iam.googleapis.com     …le.iam.admin.v1.QueryGrantableRoles     …com/projects/s
```

© 2023 SPLUNK INC.

Console? Another Console? One More?

Amazon CloudTrail

Google Workspace



By default, only a subset of the available columns are displayed when generating a search for Admin log events. To display or hide columns, click the **Manage columns** icon in the top-right corner of the search-results table. Learn more

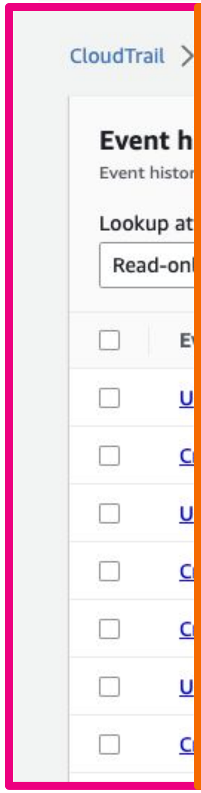
Showing 1–100 of many results

© 2023 SPLUNK INC.

A Portal to What?

Amazon CloudTrail

Google Workspace



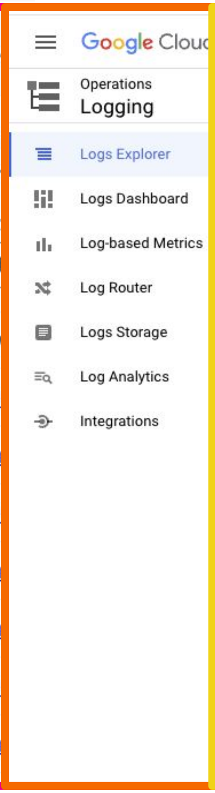
CloudTrail >

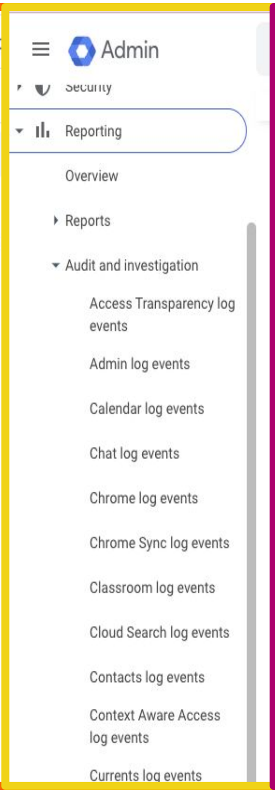
Event h

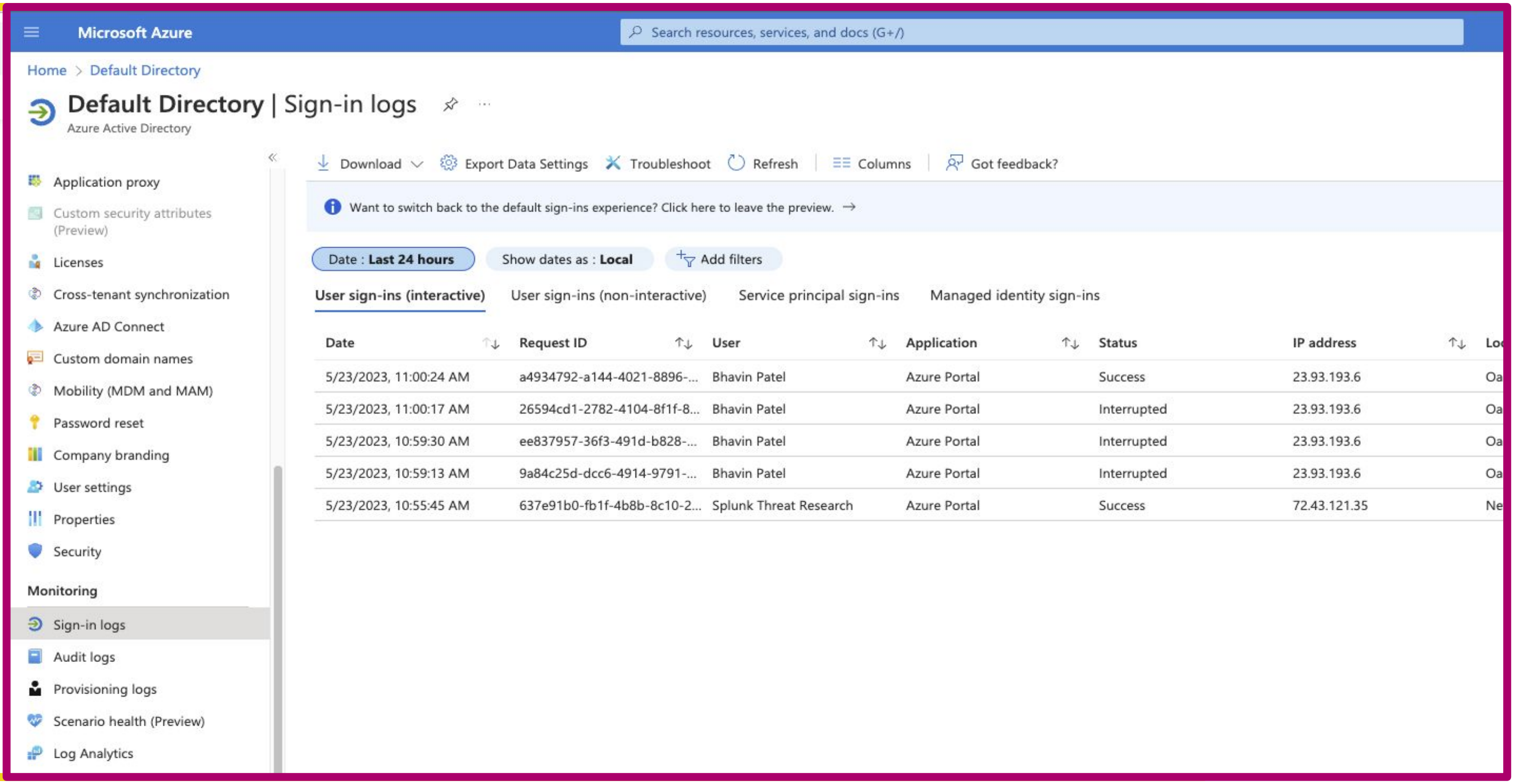
Event histor

Lookup at

Read-onl







Default Directory | Sign-in logs

Azure Active Directory

Want to switch back to the default sign-ins experience? Click here to leave the preview. →

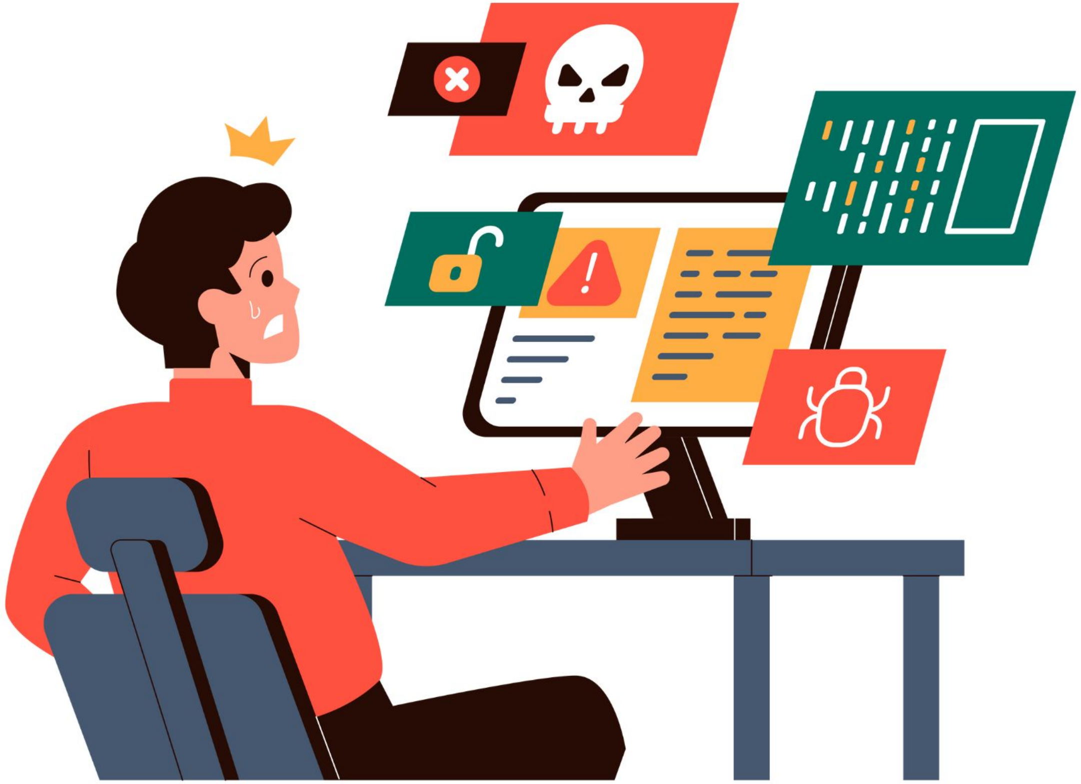
Date : **Last 24 hours** Show dates as : **Local** Add filters

User sign-ins (interactive) User sign-ins (non-interactive) Service principal sign-ins Managed identity sign-ins

Date	Request ID	User	Application	Status	IP address	Lo
5/23/2023, 11:00:24 AM	a4934792-a144-4021-8896-...	Bhavin Patel	Azure Portal	Success	23.93.193.6	Oa
5/23/2023, 11:00:17 AM	26594cd1-2782-4104-8f1f-8...	Bhavin Patel	Azure Portal	Interrupted	23.93.193.6	Oa
5/23/2023, 10:59:30 AM	ee837957-36f3-491d-b828-...	Bhavin Patel	Azure Portal	Interrupted	23.93.193.6	Oa
5/23/2023, 10:59:13 AM	9a84c25d-dcc6-4914-9791-...	Bhavin Patel	Azure Portal	Interrupted	23.93.193.6	Oa
5/23/2023, 10:55:45 AM	637e91b0-fb1f-4b8b-8c10-2...	Splunk Threat Research	Azure Portal	Success	72.43.121.35	Ne

© 2023 SPLUNK INC.

uhhh, well….?

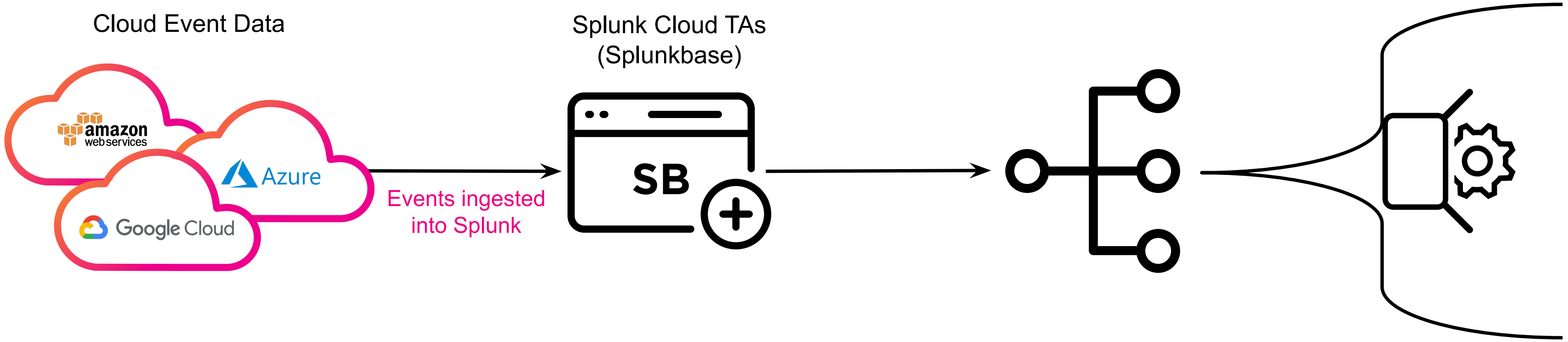


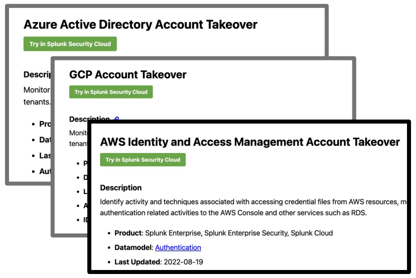
Source: bit.ly/3XjpquI

© 2023 SPLUNK INC.

Don’t Fear, Splunk is Here!

Collect Cloud Events → Analyze Telemetry → Write Detections!





Azure Active Directory Account Takeover

Try in Splunk Security Cloud

Descri

Monitor
tenants.

- Pro
- Dat
- Las
- Aut

GCP Account Takeover

Try in Splunk Security Cloud

Description

Monit
tenant

- P
- D
- L
- A
- ID

AWS Identity and Access Management Account Takeover

Try in Splunk Security Cloud

Description

Identify activity and techniques associated with accessing credential files from AWS resources, m
authentication related activities to the AWS Console and other services such as RDS.

- **Product**: Splunk Enterprise, Splunk Enterprise Security, Splunk Cloud
- **Datamodel**: Authentication
- **Last Updated**: 2022-08-19

Pre-packaged security content (searches, detection models, reports, dashboards, automation playbooks, and more.)

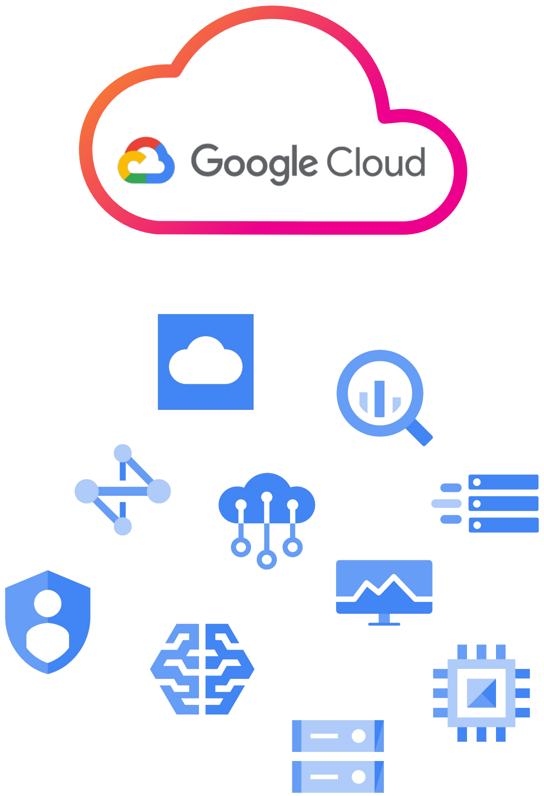
All trademarks, logos, and brand names are the property of their respective owners.

© 2023 SPLUNK INC.

Cloud Telemetry

© 2023 SPLUNK INC.

Technologies and Features



All trademarks, logos, and brand names are the property of their respective owners.

© 2023 SPLUNK INC.

Available Log Sources

AWS

- AWS Cloudtrail
- AWS IAM Access Analyzer
- Amazon CloudWatch Logs
- Amazon Security Lake
- Amazon Security Hub
- Amazon Guarduty

Azure

- Sign-ins
- Audit
- Provisioning
- Resource Logs
- Activity Logs

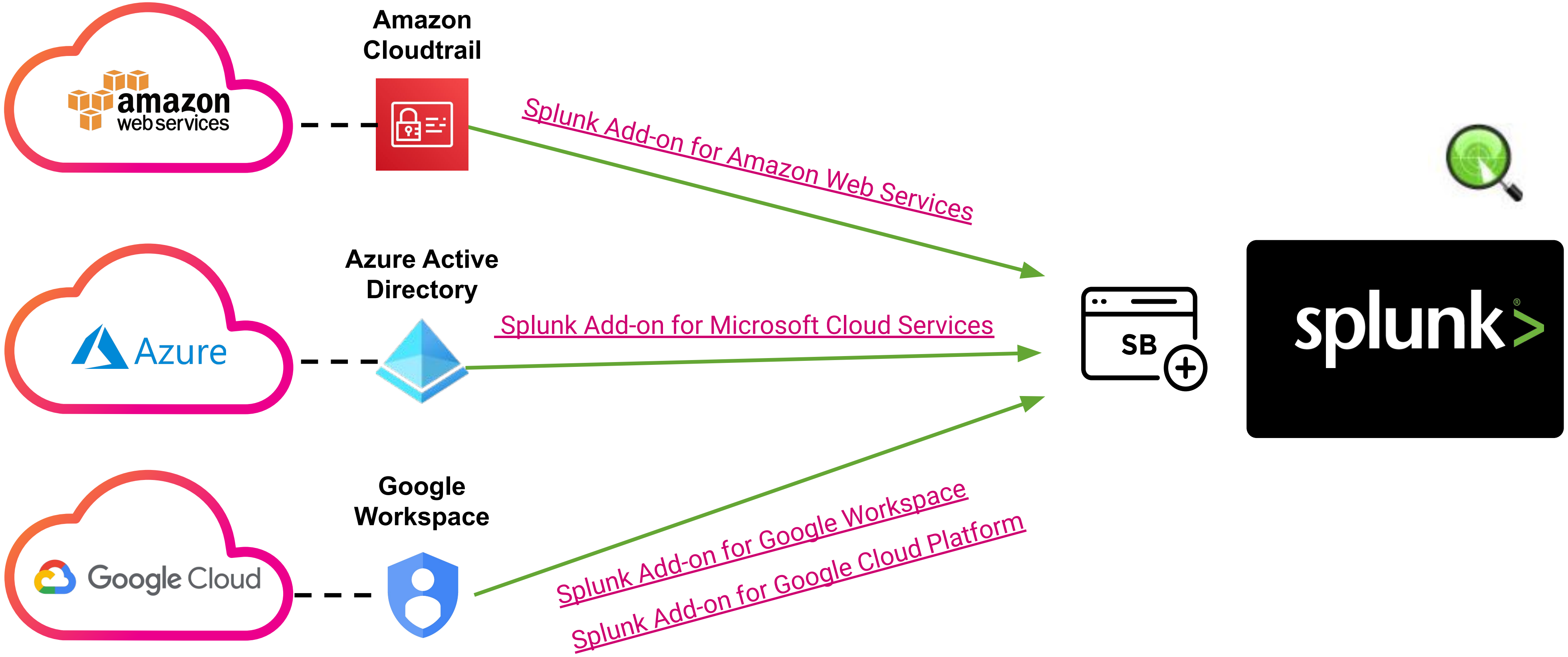
GCP/GWS

- Admin Log Events
- User Log Events
- Audit Logs Events
- Admin Activity audit logs
- Data Access audit logs
- System Event audit logs
- Policy Denied audit logs

All trademarks, logos, and brand names are the property of their respective owners.

© 2023 SPLUNK INC.

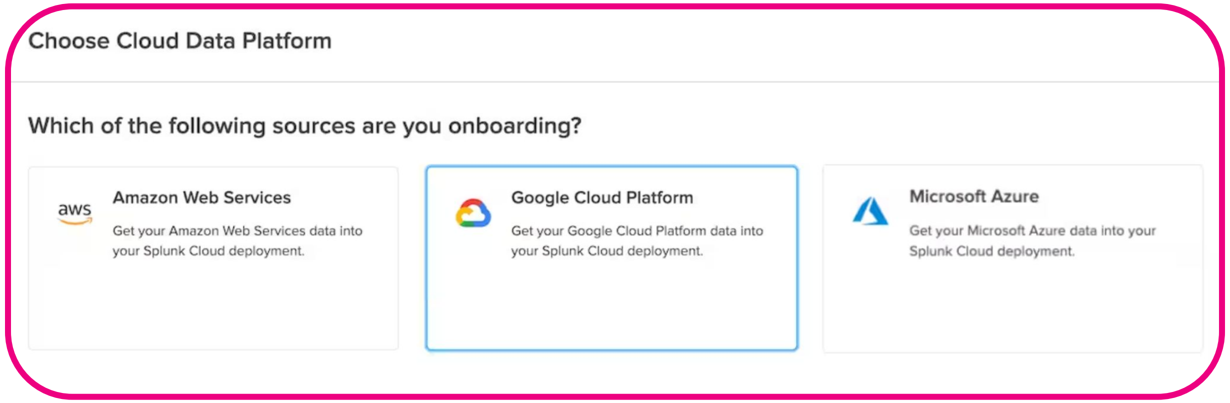
Splunk Technology Add-Ons


amazon web services
Amazon Cloudtrail
Splunk Add-on for Amazon Web Services
Azure
Azure Active Directory
Splunk Add-on for Microsoft Cloud Services
Google Cloud
Google Workspace
Splunk Add-on for Google Workspace
Splunk Add-on for Google Cloud Platform
SB
splunk>

All trademarks, logos, and brand names are the property of their respective owners.

© 2023 SPLUNK INC.

Data Manager for Splunk Cloud



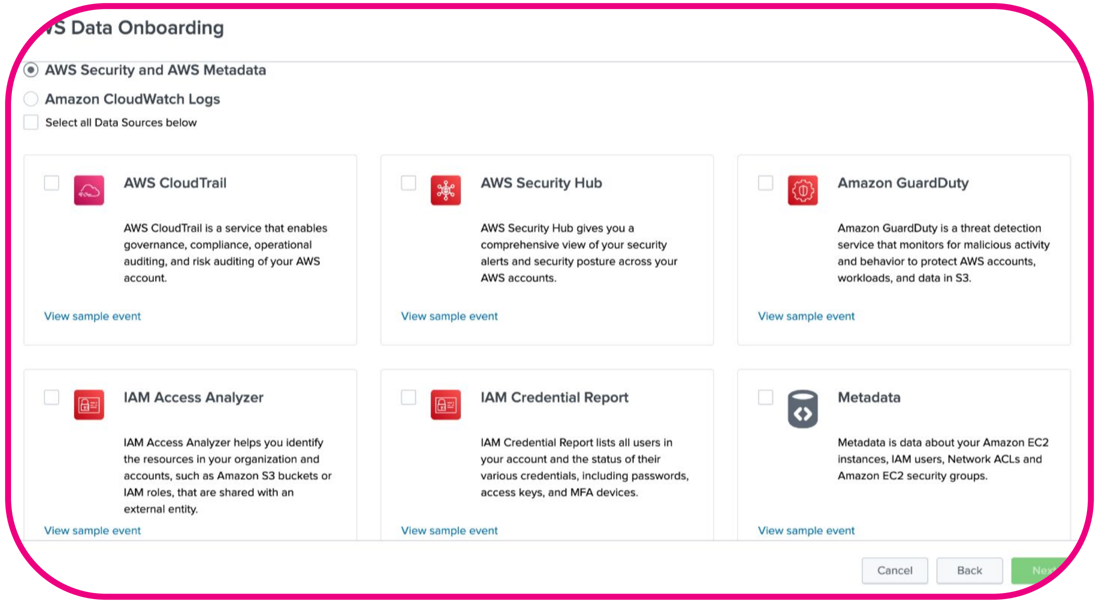
Choose Cloud Data Platform

Which of the following sources are you onboarding?

Amazon Web Services
Get your Amazon Web Services data into your Splunk Cloud deployment.

Google Cloud Platform
Get your Google Cloud Platform data into your Splunk Cloud deployment.

Microsoft Azure
Get your Microsoft Azure data into your Splunk Cloud deployment.



S Data Onboarding

● AWS Security and AWS Metadata
○ Amazon CloudWatch Logs
□ Select all Data Sources below

□ **AWS CloudTrail**
AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account.
View sample event

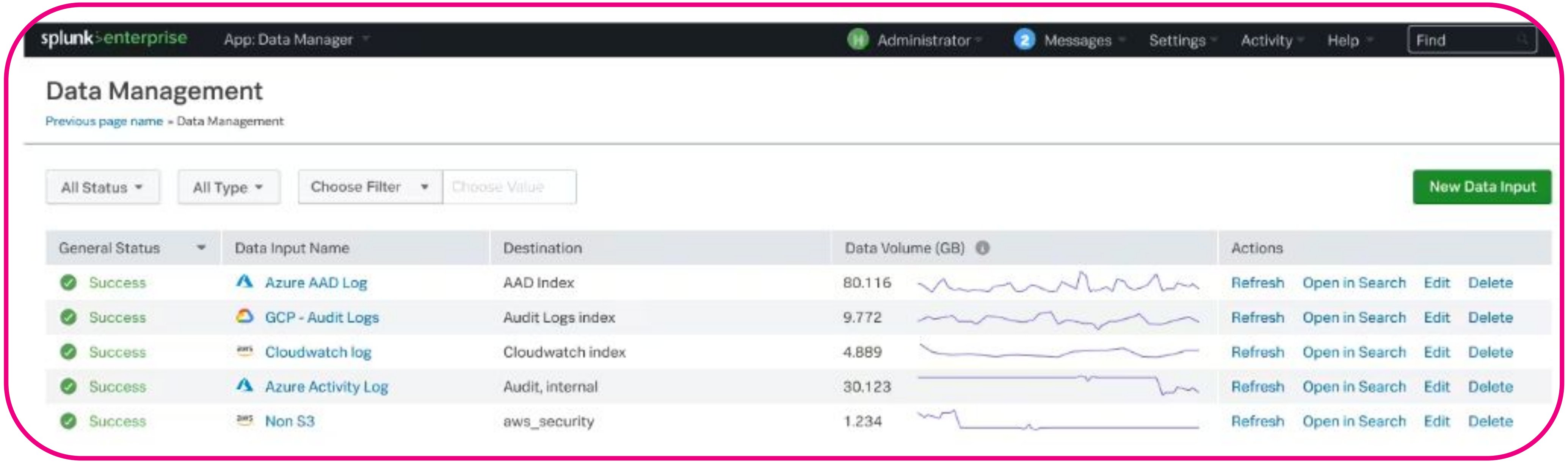
□ **AWS Security Hub**
AWS Security Hub gives you a comprehensive view of your security alerts and security posture across your AWS accounts.
View sample event

□ **Amazon GuardDuty**
Amazon GuardDuty is a threat detection service that monitors for malicious activity and behavior to protect AWS accounts, workloads, and data in S3.
View sample event

□ **IAM Access Analyzer**
IAM Access Analyzer helps you identify the resources in your organization and accounts, such as Amazon S3 buckets or IAM roles, that are shared with an external entity.
View sample event

□ **IAM Credential Report**
IAM Credential Report lists all users in your account and the status of their various credentials, including passwords, access keys, and MFA devices.
View sample event

□ **Metadata**
Metadata is data about your Amazon EC2 instances, IAM users, Network ACLs and Amazon EC2 security groups.
View sample event



Data Management

Previous page name » Data Management

General Status	Data Input Name	Destination	Data Volume (GB)	Actions
✓ Success	Azure AAD Log	AAD Index	80.116	Refresh Open in Search Edit Delete
✓ Success	GCP - Audit Logs	Audit Logs index	9.772	Refresh Open in Search Edit Delete
✓ Success	Cloudwatch log	Cloudwatch index	4.889	Refresh Open in Search Edit Delete
✓ Success	Azure Activity Log	Audit, internal	30.123	Refresh Open in Search Edit Delete
✓ Success	Non S3	aws_security	1.234	Refresh Open in Search Edit Delete

© 2023 SPLUNK INC.

Source: bit.ly/3p9kT1d

© 2023 SPLUNK INC.

Multi-Cloud Detection Engineering

splunk> .conf23

© 2023 SPLUNK INC.

Multi-Cloud Detection Engineering Workflow

Analyze Threats

Define a Detection Opportunity

Create a Detection Template

//pseudo spl

Create Analytics

Source: bit.ly/3XzKGwF

© 2023 SPLUNK INC.

Cloud Identity Attack

A cloud identity attack involves unauthorized actions or attempts to compromise the identities, credentials, or privileges associated with users, administrators, or service accounts within a cloud environment.

Source: bit.ly/3NF10J4

© 2023 SPLUNK INC.

Identity Providers

"An identity provider is a system entity that creates, maintains, and manages identity information for principals"

What are the different Identity Providers?

- **AWS Identity and Access Management (IAM)**
- **Azure® Active Directory**
- **Google Workspace™**
- **Cloud Identity™**

Source: bit.ly/3XnMTuQ

© 2023 SPLUNK INC.

Password Spraying

Technique by which adversaries leverage a single password against a large group of user accounts with the goal of acquiring valid account credentials.

Source: bit.ly/466yWoS

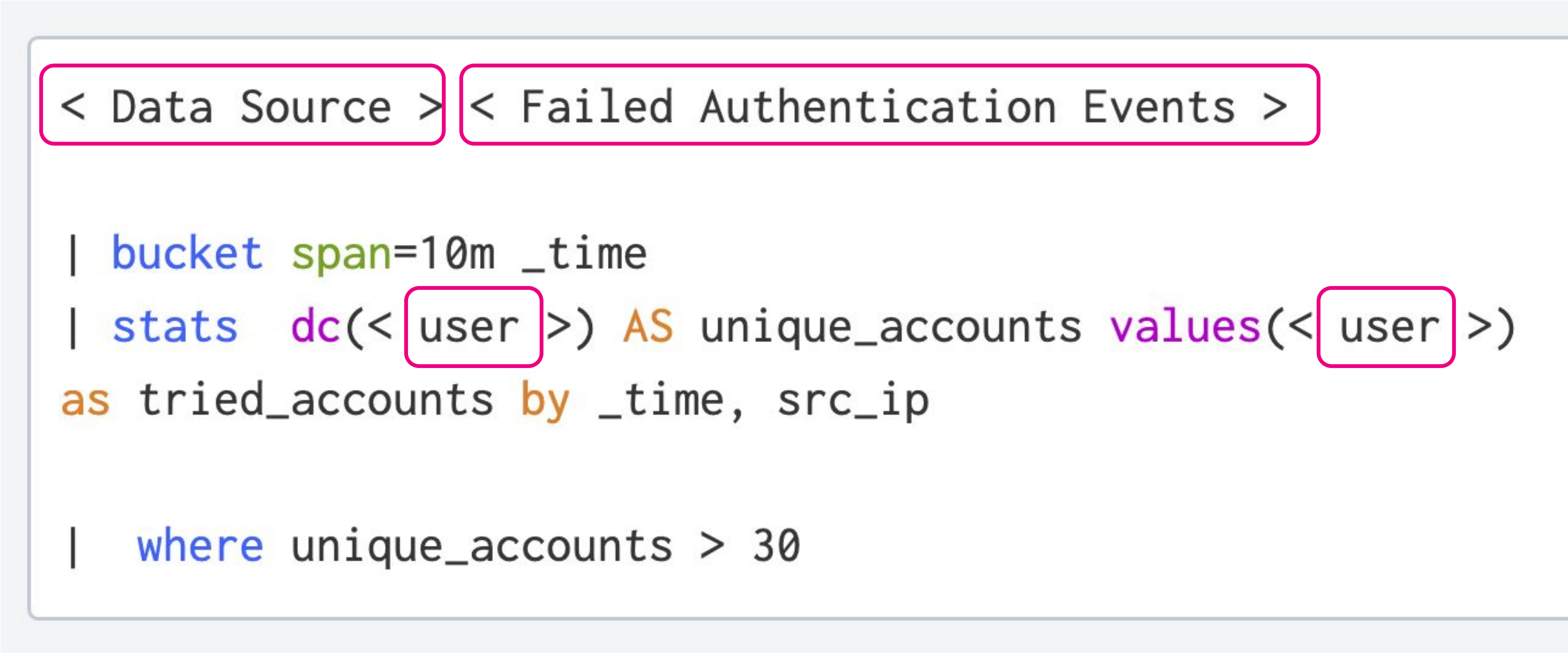
© 2023 SPLUNK INC.

Detection Template

Password Spraying

Password Spraying

Identify one IP Address failing to authenticate with more than 30 users in a 10 minute time span

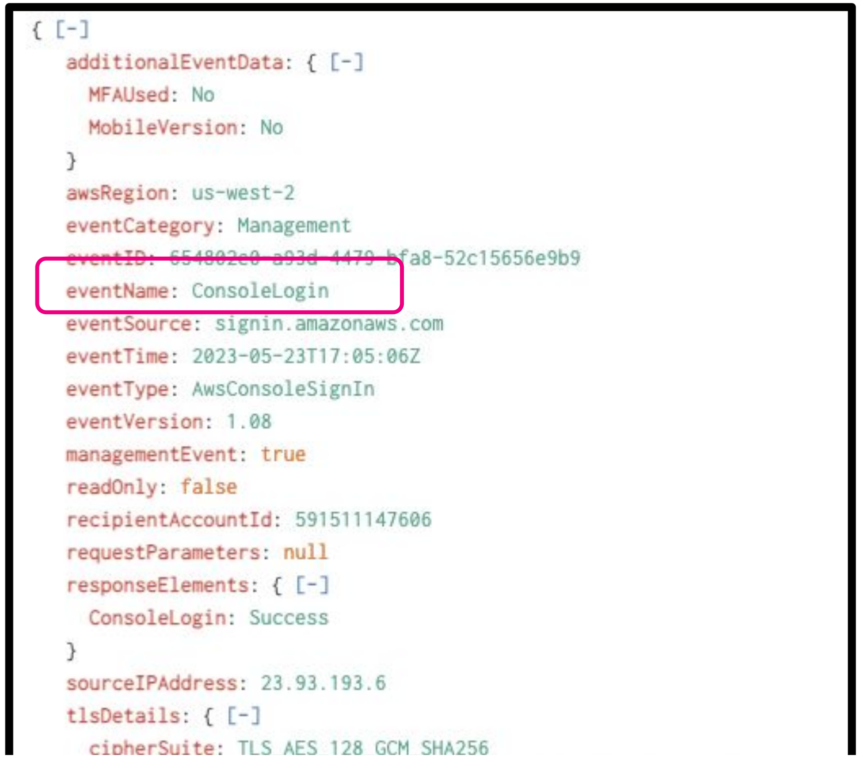


```
< Data Source >< Failed Authentication Events >


| bucket span=10m _time
| stats  dc(< user >) AS unique_accounts values(< user >)
as tried_accounts by _time, src_ip


|  where unique_accounts > 30
```

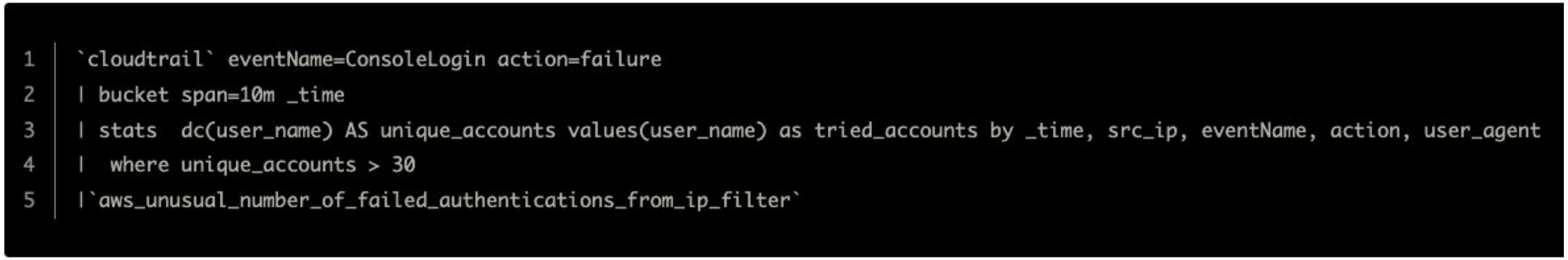
© 2023 SPLUNK INC.

AWS Cloudtrail

sourcetype= aws:cloudtrail



```
{ [-]
  additionalEventData: { [-]
    MFAUsed: No
    MobileVersion: No
  }
  awsRegion: us-west-2
  eventCategory: Management
  eventID: 654802c0-a93d-4479-bfa8-52c15656e9b9
  eventName: ConsoleLogin
  eventSource: signin.amazonaws.com
  eventTime: 2023-05-23T17:05:06Z
  eventType: AwsConsoleSignIn
  eventVersion: 1.08
  managementEvent: true
  readOnly: false
  recipientAccountId: 591511147606
  requestParameters: null
  responseElements: { [-]
    ConsoleLogin: Success
  }
  sourceIPAddress: 23.93.193.6
  tlsDetails: { [-]
    cipherSuite: TLS_AES_128_GCM_SHA256
```



```
`cloudtrail` eventName=ConsoleLogin action=failure
| bucket span=10m _time
| stats  dc(user_name) AS unique_accounts values(user_name) as tried_accounts by _time, src_ip, eventName, action, user_agent
|  where unique_accounts > 30
|`aws_unusual_number_of_failed_authentications_from_ip_filter`
```

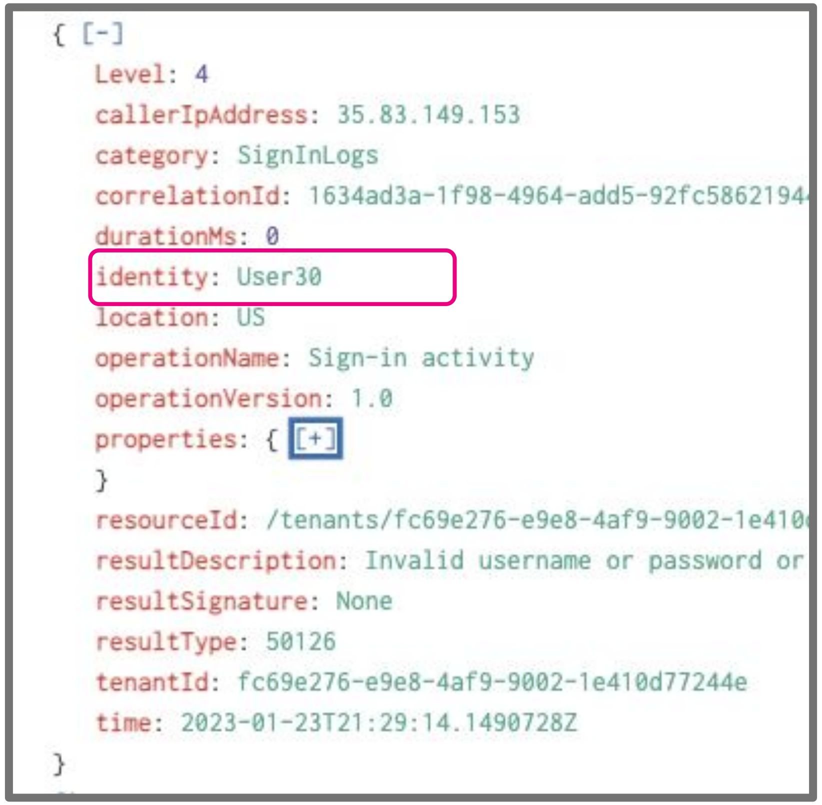
```
    type: AssumedRole
  }
}
```

All trademarks, logos, and brand names
are the property of their respective owners.

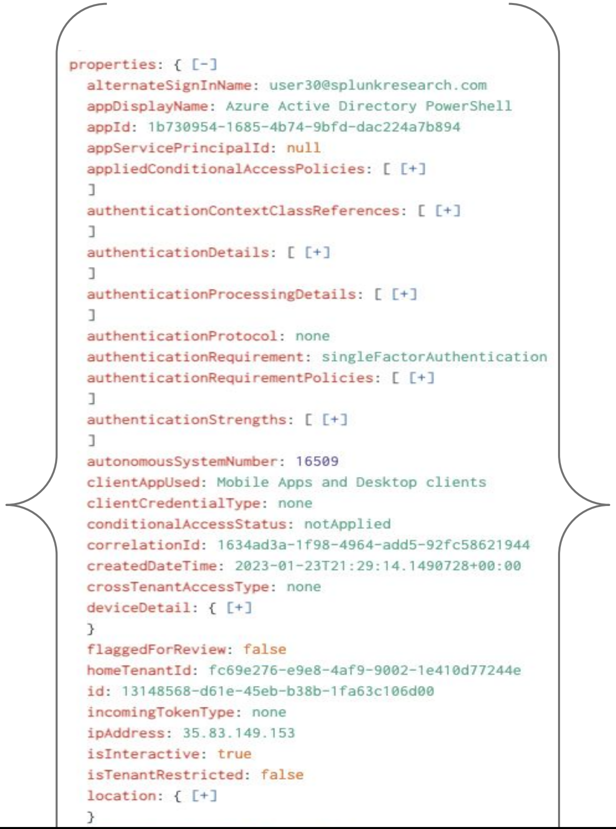
© 2023 SPLUNK INC.

Azure Active Directory

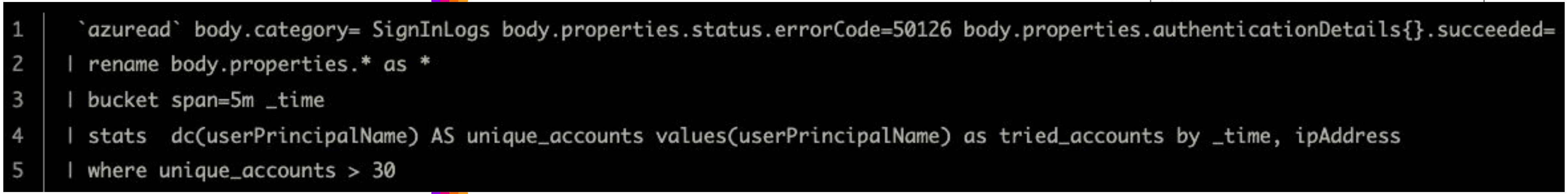
sourcetype = mscs:azure:eventhub



```
{ [-]
   Level: 4
   callerIpAddress: 35.83.149.153
   category: SignInLogs
   correlationId: 1634ad3a-1f98-4964-add5-92fc5862194
   durationMs: 0
   identity: User30
   location: US
   operationName: Sign-in activity
   operationVersion: 1.0
   properties: { [+]
   }
   resourceId: /tenants/fc69e276-e9e8-4af9-9002-1e410
   resultDescription: Invalid username or password or
   resultSignature: None
   resultType: 50126
   tenantId: fc69e276-e9e8-4af9-9002-1e410d77244e
   time: 2023-01-23T21:29:14.1490728Z
}
```



```
properties: { [-]
  alternateSignInName: user30@splunkresearch.com
  appDisplayName: Azure Active Directory PowerShell
  appId: 1b730954-1685-4b74-9bfd-dac224a7b894
  appServicePrincipalId: null
  appliedConditionalAccessPolicies: [ [+]
  ]
  authenticationContextClassReferences: [ [+]
  ]
  authenticationDetails: [ [+]
  ]
  authenticationProcessingDetails: [ [+]
  ]
  authenticationProtocol: none
  authenticationRequirement: singleFactorAuthentication
  authenticationRequirementPolicies: [ [+]
  ]
  authenticationStrengths: [ [+]
  ]
  autonomousSystemNumber: 16509
  clientAppUsed: Mobile Apps and Desktop clients
  clientCredentialType: none
  conditionalAccessStatus: notApplied
  correlationId: 1634ad3a-1f98-4964-add5-92fc58621944
  createdDateTime: 2023-01-23T21:29:14.1490728+00:00
  crossTenantAccessType: none
  deviceDetail: { [+]
  }
  flaggedForReview: false
  homeTenantId: fc69e276-e9e8-4af9-9002-1e410d77244e
  id: 13148568-d61e-45eb-b38b-1fa63c106d00
  incomingTokenType: none
  ipAddress: 35.83.149.153
  isInteractive: true
  isTenantRestricted: false
  location: { [+]
  }
```



```
 `azuread` body.category= SignInLogs body.properties.status.errorCode=50126 body.properties.authenticationDetails{}.succeeded=
| rename body.properties.* as *
| bucket span=5m _time
| stats  dc(userPrincipalName) AS unique_accounts values(userPrincipalName) as tried_accounts by _time, ipAddress
| where unique_accounts > 30
```

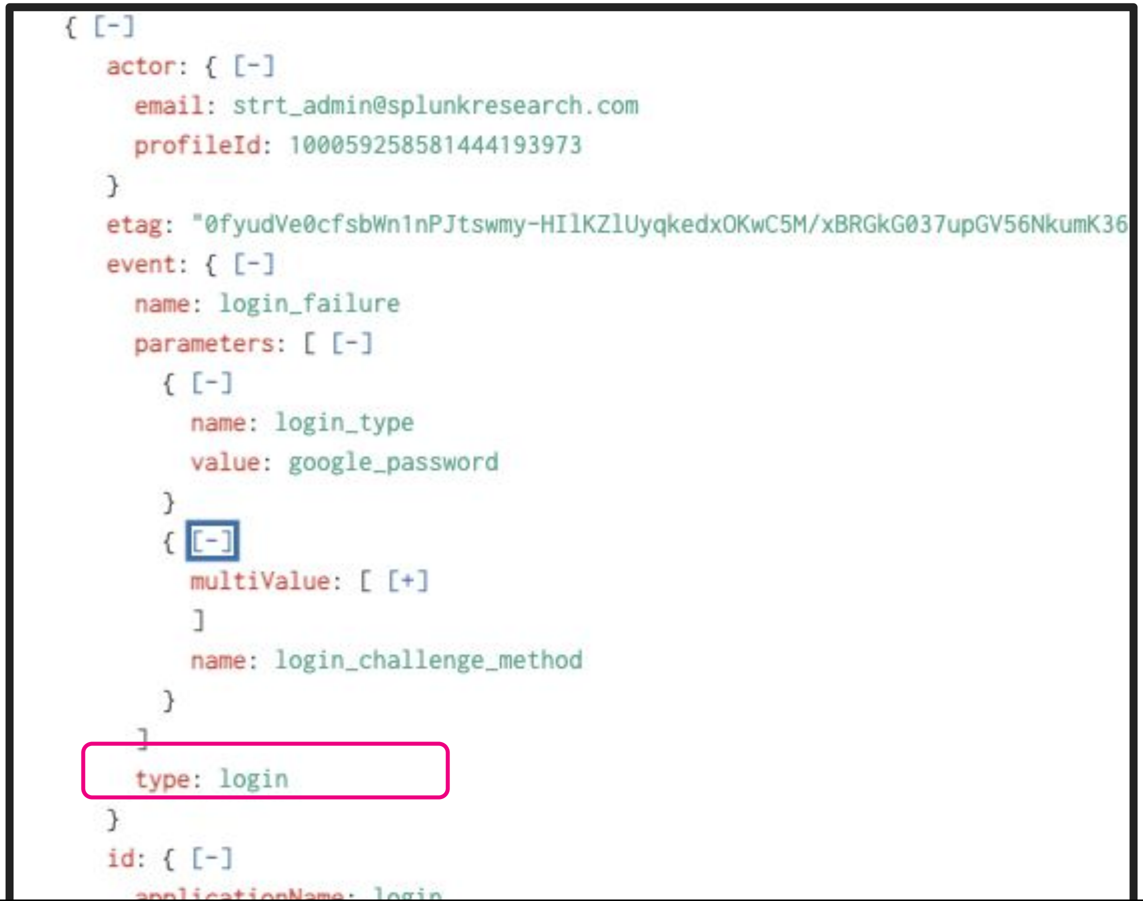
All trademarks, logos, and brand names
are the property of their respective owners.

© 2023 SPLUNK INC.

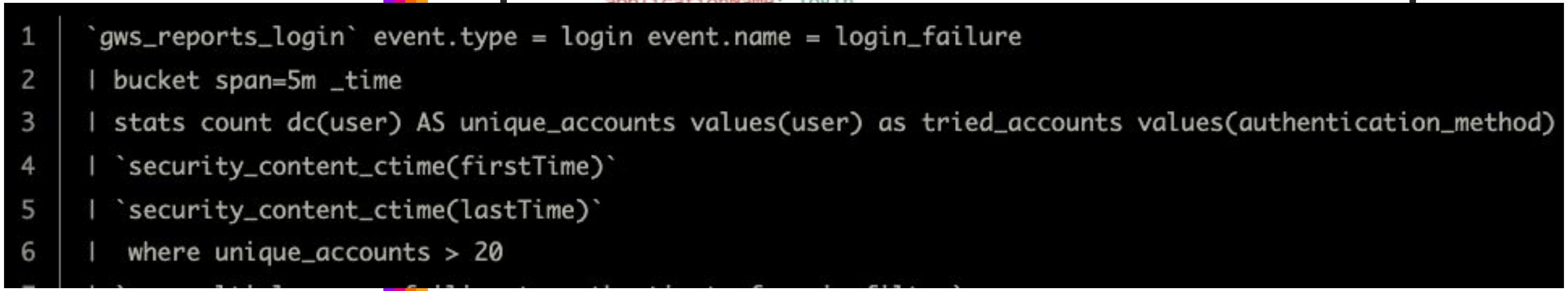
Google Workspace

Google Login Reports

sourcetype = gws:reports:login



```
{ [-]
  actor: { [-]
    email: strt_admin@splunkresearch.com
    profileId: 100059258581444193973
  }
  etag: "0fyudVe0cfsbWn1nPJtswmy-HIlKZlUyqkedxOKwC5M/xBRGkG037upGV56NkumK36
  event: { [-]
    name: login_failure
    parameters: [ [-]
      { [-]
        name: login_type
        value: google_password
      }
      { [-]
        multiValue: [ [+]
        ]
        name: login_challenge_method
      }
    ]
    type: login
  }
  id: { [-]
    applicationName: login
```



```
`gws_reports_login` event.type = login event.name = login_failure
| bucket span=5m _time
| stats count dc(user) AS unique_accounts values(user) as tried_accounts values(authentication_method)
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
|  where unique_accounts > 20
```

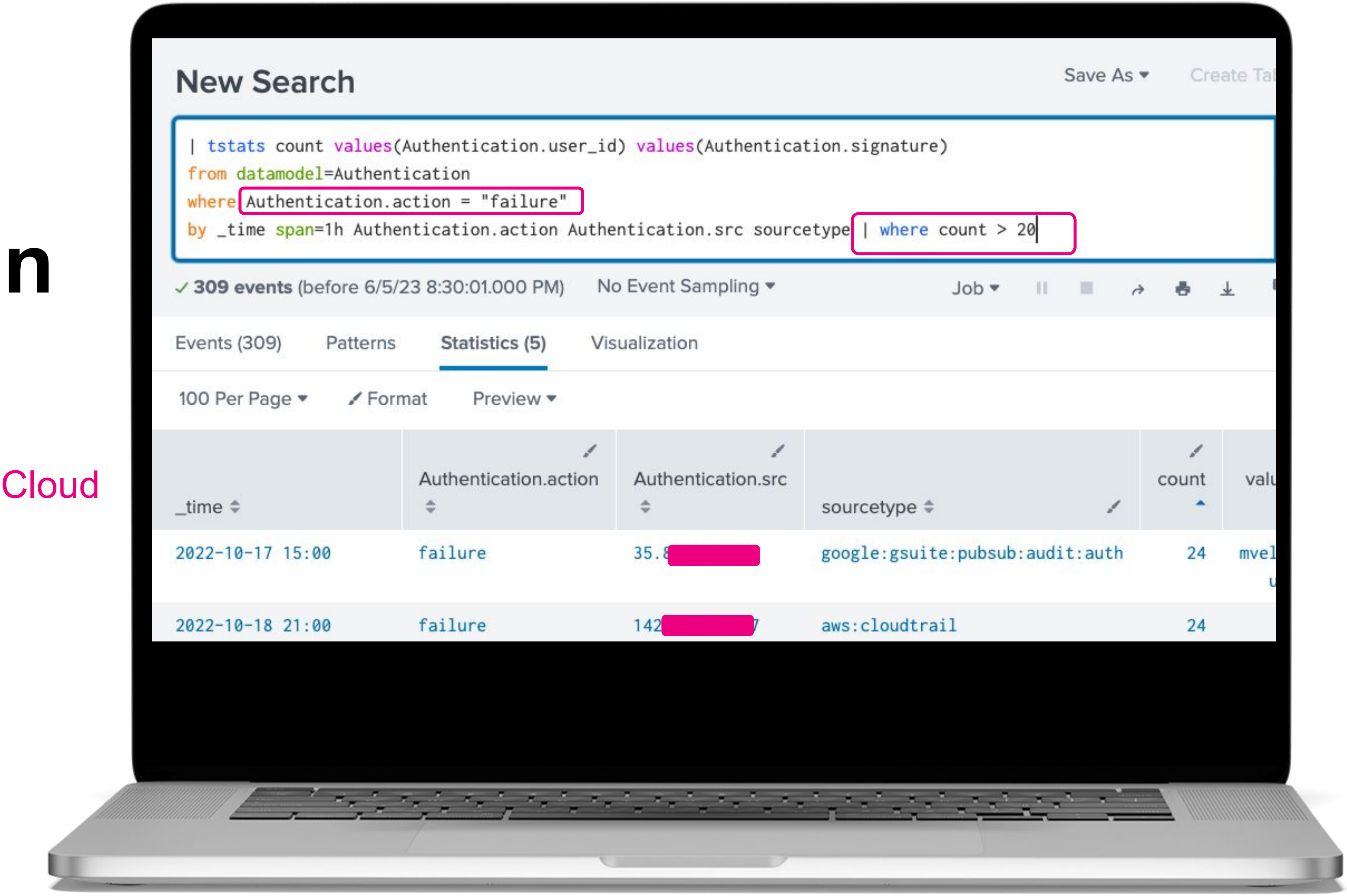
All trademarks, logos, and brand names are the property of their respective owners.

splunk> .conf23

© 2023 SPLUNK INC.

Authentication Data Model

High number of login failures in Cloud



```
| tstats count values(Authentication.user_id) values(Authentication.signature)
from datamodel=Authentication
where Authentication.action = "failure"
by _time span=1h Authentication.action Authentication.src sourcetype | where count > 20
```

✓ 309 events (before 6/5/23 8:30:01.000 PM)

_time	Authentication.action	Authentication.src	sourcetype	count	valu
2022-10-17 15:00	failure	35.[redacted]	google:gsuite:pubsub:audit:auth	24	mvel u
2022-10-18 21:00	failure	142[redacted]	aws:cloudtrail	24	

© 2023 SPLUNK INC.

MFA Fatigue

An MFA Fatigue attack is when a threat actor attempts to log in with stolen credentials over and over, causing what feels like an endless stream of MFA push requests to be sent to the account's owner's mobile device.

Source: bit.ly/3CHKP7C

© 2023 SPLUNK INC.

Detection Opportunity

MFA Fatigue

MFA Fatigue

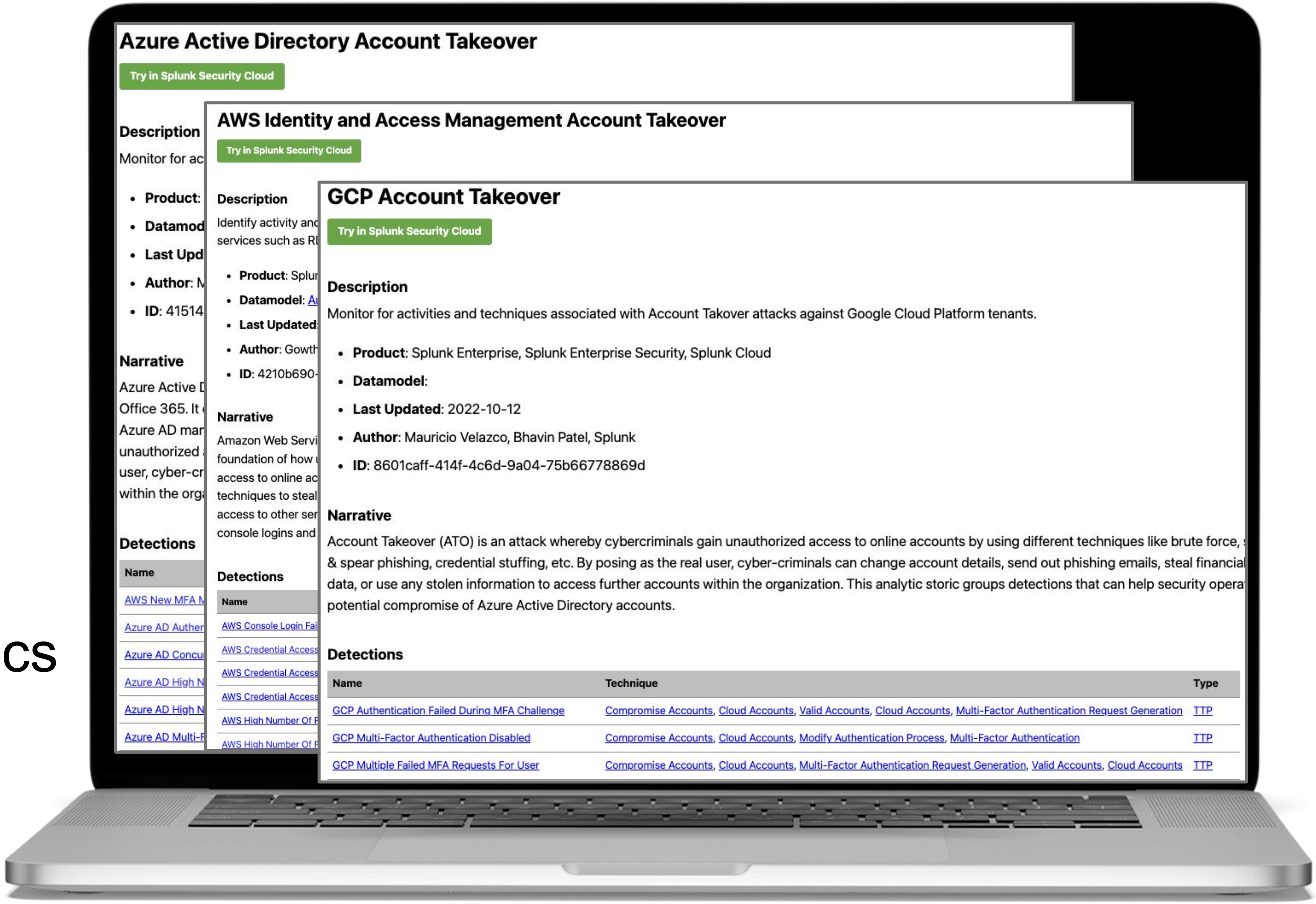
“Identify one user failing on the second factor authentication more than 10 times in a 5 minute time span”

© 2023 SPLUNK INC.

Account Takeover Analytic Stories

https://research.splunk.com

30+ detection analytics covering the 3 major cloud providers



Azure Active Directory Account Takeover

Try in Splunk Security Cloud

Description

Monitor for ac

- **Product**:
- **Datamod**
- **Last Upd**
- **Author**: M
- **ID**: 41514

Narrative

Azure Active D
Office 365. It
Azure AD mar
unauthorized
user, cyber-cr
within the orga

Detections

Name
AWS New MFA M
Azure AD Auther
Azure AD Concu
Azure AD High N
Azure AD High N
Azure AD Multi-F

AWS Identity and Access Management Account Takeover

Try in Splunk Security Cloud

Description

Identify activity and
services such as RI

- **Product**: Splur
- **Datamodel**: Au
- **Last Updated**:
- **Author**: Gowth
- **ID**: 4210b690-

Narrative

Amazon Web Servi
foundation of how
access to online ac
techniques to steal
access to other ser
console logins and

Detections

Name
AWS Console Login Fai
AWS Credential Access
AWS Credential Access
AWS Credential Access
AWS High Number Of F
AWS High Number Of F

GCP Account Takeover

Try in Splunk Security Cloud

Description

Monitor for activities and techniques associated with Account Takover attacks against Google Cloud Platform tenants.

- **Product**: Splunk Enterprise, Splunk Enterprise Security, Splunk Cloud
- **Datamodel**:
- **Last Updated**: 2022-10-12
- **Author**: Mauricio Velazco, Bhavin Patel, Splunk
- **ID**: 8601caff-414f-4c6d-9a04-75b66778869d

Narrative

Account Takeover (ATO) is an attack whereby cybercriminals gain unauthorized access to online accounts by using different techniques like brute force, s
& spear phishing, credential stuffing, etc. By posing as the real user, cyber-criminals can change account details, send out phishing emails, steal financial
data, or use any stolen information to access further accounts within the organization. This analytic storic groups detections that can help security opera
potential compromise of Azure Active Directory accounts.

Detections

Name	Technique	Type
GCP Authentication Failed During MFA Challenge	Compromise Accounts, Cloud Accounts, Valid Accounts, Cloud Accounts, Multi-Factor Authentication Request Generation	TTP
GCP Multi-Factor Authentication Disabled	Compromise Accounts, Cloud Accounts, Modify Authentication Process, Multi-Factor Authentication	TTP
GCP Multiple Failed MFA Requests For User	Compromise Accounts, Cloud Accounts, Multi-Factor Authentication Request Generation, Valid Accounts, Cloud Accounts	TTP

splunk> .conf23

© 2023 SPLUNK INC.

Demos

© 2023 SPLUNK INC.

Demo

© 2023 SPLUNK INC.

Takeaways

© 2023 SPLUNK INC.

Takeaways

research.splunk.com

- The Splunk ecosystem enables security teams obtain a holistic cloud visibility
- Centralizing cloud telemetry provides many benefits for cloud detection engineering
- Prioritize comprehension of the threat and identifying detection opportunities
- The workflow can also be applied to threat hunting and incident response
- You don’t have to start from scratch. STRT has your back!
- Related .conf 2023 sessions:
  - **SEC1228B - Gloves Off/Hands On: Threat Simulation and Detection Engineering With Splunk**
  - **PLA1962A - Accelerate the Value of Your Data Using Splunk® Cloud Platform’s New Data Processing Features**

© 2023 SPLUNK INC.

Thank You

splunk> .conf23