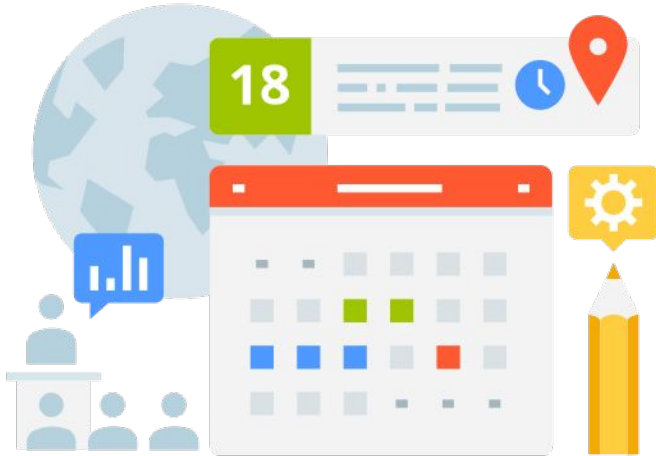




BLUE
TEAM
→ SECURITY INCIDENT RESPONSE

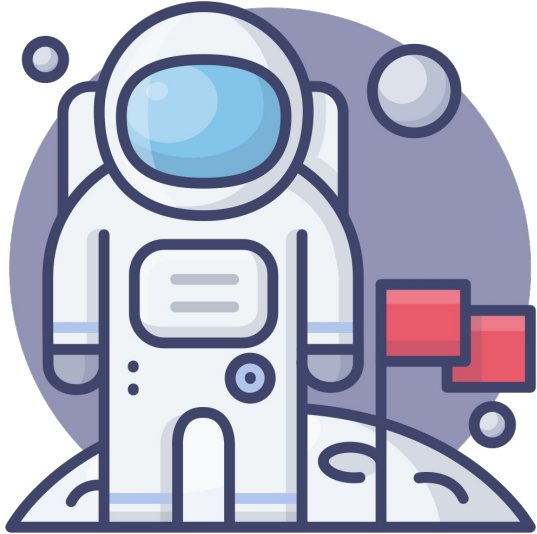
Incident Response
Google Cloud Platform

Agenda



- Mission
- Compromised credentials/keys Attacks
- Preparation
- Investigation
- Questions

Mission



- Identify suspicious/unauthorized access
- Identify new/suspicious/unauthorized accounts
- Identify unrecognized resources
- Identify escalation procedures
- Identify exposed secrets/keys/credentials

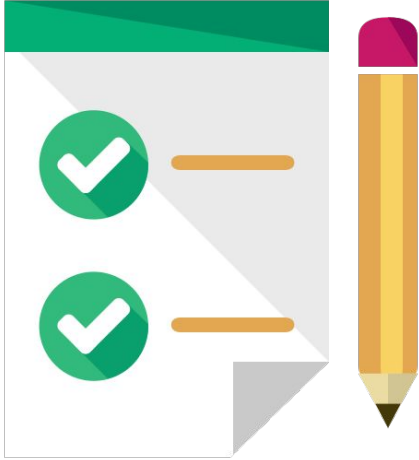


Investigating Compromised Credentials / Keys

Attacks

Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 30 techniques	Lateral Movement 9 techniques
Phishing (1/3)	Spearphishing Link	Modify Authentication Process (1/7)	Valid Accounts (1/4)	Modify Authentication Process (1/7)	Password Guessing	Account Discovery (0/4)	Exploitation of Remote Services
	Spearphishing Attachment	Valid Accounts (1/4)	Abuse Elevation Control Mechanism (0/4)	Valid Accounts (1/4)	Password Spraying	Application Window Discovery	Internal Spearphishing
	Spearphishing via Service	Container Administration Command	Access Token Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)	Credential Stuffing	Browser Bookmark Discovery	Lateral Tool Transfer
Valid Accounts (1/4)	Cloud Accounts	Deploy Container	Boot or Logon Autostart Execution (0/14)	Access Token Manipulation (0/5)	Password Cracking	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)
	Default Accounts	Exploitation for Client Execution	Device Registration	BITS Jobs	Password Managers	Cloud Service Dashboard	Remote Services (0/6)
	Domain Accounts	Account Manipulation (2/5)	SSH Authorized Keys	Build Image on Host	Credentials from Web Browsers	Cloud Storage Object Discovery	Replication Through Removable Media
	Local Accounts	Inter-Process Communication (0/3)		Debugger Evasion	Keychain	Container and Resource Discovery	Software Deployment Tools
Drive-by Compromise	Native API	BITS Jobs	Create or Modify System Process (0/4)	Deobfuscate/Decode Files or Information	Securityd Memory	Debugger Evasion	Taint Shared Content
Exploit Public-Facing Application	Scheduled Task/Job (0/5)	Boot or Logon Autostart Execution (0/14)	Domain Policy Modification (0/2)	Deploy Container	Windows Credential Manager	File and Directory Discovery	Use Alternate Authentication Material (0/4)
External Remote Services	Serverless Execution	Boot or Logon Initialization Scripts (0/5)	Escape to Host	Direct Volume Access	Multi-Factor Authentication	Group Policy Discovery	
Hardware Additions	Shared Modules	Browser Extensions	Event Triggered Execution (0/16)	Domain Policy Modification (0/2)	Domain Controller Authentication	Network Service Discovery	
Replication Through Removable Media	Software Deployment Tools	Compromise Client Software Binary	Exploitation for Privilege Escalation	Execution Guardrails (0/1)	Hybrid Identity	Network Share Discovery	
Supply Chain Compromise (0/3)	System Services (0/2)	Create Account (0/3)	Hijack Execution Flow (0/12)	Multi-Factor Authentication Interception	Network Device Authentication	Network Sniffing	
Trusted Relationship	User Execution (0/3)	Create or Modify System Process (0/4)	Process Injection (0/12)	Multi-Factor Authentication Request Generation	Password Filter DLL	Password Policy Discovery	
	Windows Management Instrumentation	Event Triggered Execution (0/16)	Scheduled Task/Job (0/5)	Hide Artifacts (0/10)	Pluggable Authentication Modules	Peripheral Device Discovery	
		External Remote Services	Impair Defenses (0/9)	Hijack Execution Flow (0/12)	Reversible Encryption	Permission Groups Discovery (0/3)	
		Hijack Execution Flow (0/12)	Indicator Removal (0/9)	Indirect Command Execution		Process Discovery	
		Implant Internal Image	Masquerading (0/7)	Masquerading (0/7)	Credentials in Files	Query Registry	
		Office Application Startup (0/6)	Modify Cloud Compute Infrastructure (0/4)	Modify Cloud Compute Infrastructure (0/4)	Private Keys	Remote System Discovery	
			Modify Registry	Modify Registry	Bash History		
					Cloud Instance Metadata API		
					Container API		
					Credentials in Registry		

Preparation



- Enforce MFA
- Least privilege principle
- Enable API logging
- Enabling identity logging!
enable Google Workspace data sharing within Google Cloud.

Preparation | Inventory



IAM & Admin



IAM



Identity & Organization



Policy Troubleshooter



Policy Analyzer **NEW**



Organization Policies



Service Accounts



Workload Identity Federat...



Labels



Tags



Manage Resources



Release Notes

IAM

GRANT ACCESS

REMOVE ACCESS

HELP ASSISTANT

L

PERMISSIONS

RECOMMENDATIONS HISTORY

VIEW BY PRINCIPALS

VIEW BY ROLES



Filter Enter property name or value



Type

Principal

Name

Role

Security insight



518782652219@cloudbuild.gserviceaccount.com

Organization Administrator

Owner

Project Billing Manager

Service Account Admin



717419762494-
compute@developer.gserviceaccount.com

Compute
Engine
default
service
account

Editor

6397/6400 excess permission



717419762494@cloudservices.gserviceaccount.com

Google
APIs
Service
Agent

Editor



6400/6400 excess permission



Preparation | Sharing Options

The screenshot shows the Google Admin console interface. The browser address bar displays `admin.google.com/ac/companyprofile/legal`. The left sidebar contains the 'Admin' menu with various options: Home, Dashboard, Directory, Devices, Apps, Security, Reporting, Billing, and Account. The 'Account settings' option is highlighted. The main content area is titled 'Account settings > Legal & Compliance'. It features a 'Sharing options' section with the text: 'Data stored or processed in Google Cloud Platform Services is subject to your organization's [Google Cloud Platform Terms of Service](#). [Learn more](#)'. Below this, it states 'Google Cloud Platform Sharing Options Enabled'. A large blue arrow points to this section. The 'Security and Privacy Additional Terms' section shows 'Review and agree to the amendment(s) below if applicable to your compliance needs. [Learn more](#)'. Below this, it states 'Cloud Data Processing Addendum (CDPA)' and 'Not accepted'.

Preparation | API Logging



Navigation menu

API API Library

logging

API Library > "logging"

Filter

Type to filter

Visibility

Public


(1)

Category

Google Enterprise APIs

(1)


1 result




Cloud Logging API

Google Enterprise API ?

Writes log entries and manages






Cloud Logging API

[Google Enterprise API](#)


Writes log entries and manages your Cloud Logging configuration.

MANAGE

TRY THIS API [↗](#)

 API Enabled

Incident Response in GCP | [dvirus.training](#)



Initial Access

^ RESOURCE TYPE	
 Audited Resource	62
 Google Organization	6

```
protoPayload.methodName="SetIamPolicy"  
protoPayload.methodName="google.login.LoginService.loginSuccess"
```

Persistence

Audit Logs

```
protoPayload.methodName="SetIamPolicy"
```

```
protoPayload.methodName="google.iam.admin.v1.CreateServiceAccountKey"
```

<https://cloud.google.com/logging/docs/view/query-library#iam-filters>

Cloud Functions

```
cloudfunctions.functions.create
```

```
cloudfunctions.functions.delete
```

```
cloudfunctions.functions.update
```

https://cloud.google.com/functions/docs/monitoring/audit-logging#audited_operations

Compute Engine

```
users.importSshPublicKey
```

```
users.sshPublicKeys.patch
```

```
gcloud alpha cloud-shell ssh
```

Privilege Escalation

Audit Logs

SetIamPolicy

iam.roles.update

iam.serviceAccounts.actAs

iam.serviceAccounts.getAccessToken

iam.serviceAccountKeys.implicitDelegation

iam.serviceAccountKeys.create

Investigation

```
resource.type="organization"  
protoPayload.methodName="SetIamPolicy"  
protoPayload.authenticationInfo.principalEmail="drodriguez"
```

(dvirus@gondor)-[~]
\$ whoami



Daniel Rodriguez

Security Consultant

Incident Response / Digital Forensics

Twitter @dvirus

Website: <https://dvirus.training/>



2600
MALMO