ATT&CK v16 has been released! Check out the blog post for more information.

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.

View on the ATT&CK® Navigator

Version Permalink

layout: side show sub-techniques hide sub-techniques
help

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collectio
5 techniques	5 techniques	7 techniques	5 techniques	13 techniques	11 techniques	14 techniques	5 techniques	5 techniqu
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
Exploit Public-Facing Application	Command and Scripting Interpreter (1)	Create Account (1)	Account Manipulation (5)	Domain or Tenant Policy Modification (1)	Credentials from Password Stores (1)	Cloud Infrastructure Discovery	Remote Services (2)	Data from Cloud Storag
Phishing (2)	Serverless Execution	Event Triggered Execution	Domain or Tenant Policy Modification (1)	Exploitation for Defense Evasion	Exploitation for Credential Access	Cloud Service Dashboard	Software Deployment Tools	Data from Information Repositories
Trusted Relationship	Software Deployment Tools	Implant Internal Image	Event Triggered Execution	Hide Artifacts (1)	Forge Web Credentials (2)	Cloud Service Discovery	Taint Shared Content	Data Staged
Valid Accounts (2)	User Execution (1)	Modify Authentication Process (3)	Valid Accounts (2)	Impair Defenses (3)	Modify Authentication Process (3)	Cloud Storage Object Discovery	Use Alternate Authentication Material (2)	Email Collection (2)
		Office Application Startup (6)		Impersonation	Multi-Factor Authentication Request Generation	Log Enumeration		
		Valid Accounts (2)		Indicator Removal (1)	Network Sniffing	Network Service Discovery		
				Modify Authentication Process (3)	Steal Application Access Token	Network Sniffing		
				Modify Cloud Compute Infrastructure (5)	Steal or Forge Authentication Certificates	Password Policy Discovery		
				Modify Cloud Resource Hierarchy	Steal Web Session Cookie	Permission Groups Discovery (1)		
				Unused/Unsupported Cloud Regions	Unsecured Credentials (3)	Software Discovery (1)		
				Use Alternate Authentication Material (2)		System Information Discovery		
				Valid Accounts (2)		System Location Discovery		
						System Network Connections Discovery		