



Be Secure. Be Resilient.

Synthesizing Threat-Informed Defense: When Cloud Attack Emulation Meets Detection Engineering

*Kennedy Torkura
Co-Founder & CTO
Mitigant*

About Me

- CTO/co-founder @Mitigant
- 12+ years in cyber security
- Various cloud security positions
- One of the pioneers of Security Chaos Engineering
- AWS Community Builder



Agenda

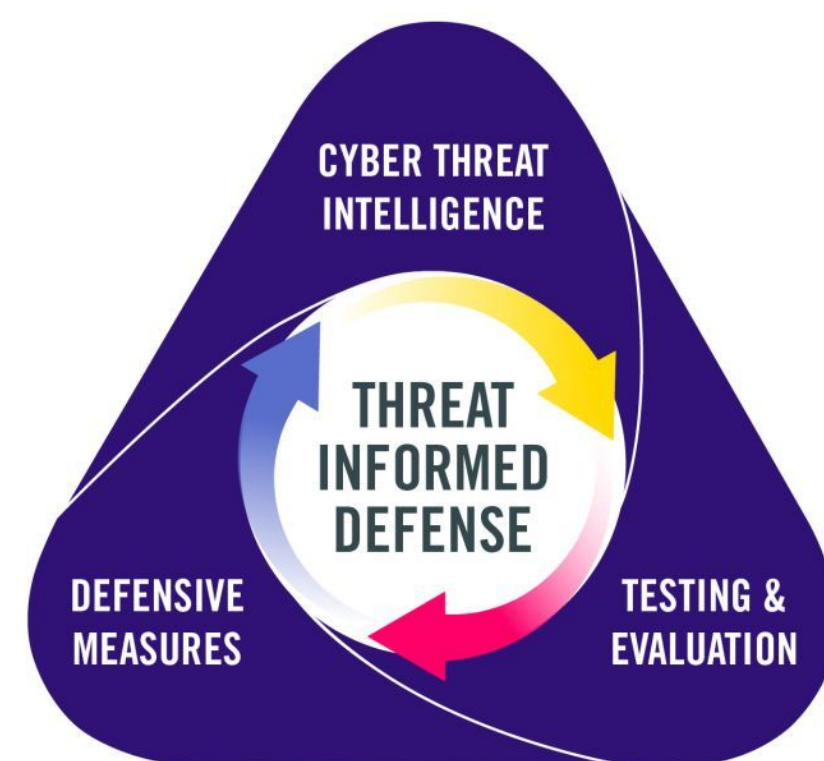
- Threat-Informed Defense
- Three Pillars of Threat-Informed Defense
- Adversary Emulation
- Cloud Attack Emulation
- Use Case: Validating Cloud Threat Detection
- Demo of Mitigant Cloud Attack Emulation

Cybersecurity: Low Signals to Noise Ratio

- Cybersecurity is a NOISY domain.
- Sifting SIGNALs from NOISE is one of the most challenging aspects of cybersecurity.
- It is comparable to the needle in the haystack problem.
- SIGNALs must be efficiently sifted from noise in order enable effective defenses.



Threat-informed defense is the **systematic application** of a deep understanding of **adversary tradecraft and technology** to **improve** defenses.



- MITRE ENGENUITY

Pillar 01: Defensive Measures

MITRE ATT&CK is a globally-accessible knowledge base of **adversary tactics** and **techniques** based on **real-world observations**.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	17 techniques	9 techniques	14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Content Injection	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Encoding (2)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Client Software Binary	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Data Obfuscation (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Create or Modify System Process (4)	Create or Modify System Process (4)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Dynamic Resolution (3)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (4)	Domain Policy Modification (2)	Direct Volume Access	Modify Authentication Process (8)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Financial Theft
Search Open Websites/Domains (3)	Valid Accounts (4)	Trusted Relationship	Serverless Execution	Event Triggered Execution (14)	Escape to Host	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Failback Channels	Exfiltration Over Web Service (4)	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Inhibit System Recovery
			Software Deployment Tools	System Services (2)	Hijack Execution Flow (12)	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Network Denial of Service (2)
			System Services (2)	Hijack Execution Flow (12)	Hijack Execution Flow (12)	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	File and Directory Discovery		Data from Removable Media	Non-Application Layer Protocol		Resource Hijacking
			User Execution (3)	Implant Internal Image	Process Injection (12)	Hide Artifacts (11)	Steal Application Access Token	Group Policy Discovery		Data from Staged (2)	Non-Standard Port		Service Stop
			Windows Management Instrumentation	Modify Authentication Process (8)	Scheduled Task/Job (5)	Hijack Execution Flow (12)	Steal or Forge Authentication Certificates	Log Enumeration		Email Collection (3)	Protocol Tunneling		System Shutdown/Reboot
				Office Application Startup (6)	Valid Accounts (4)	Impair Defenses (11)	Steal or Forge Certificates	Network Service Discovery		Input Capture (4)	Proxy (4)		
				Power Settings		Impersonation	Peripheral Device Discovery	Network Share Discovery		Screen Capture	Remote Access Software		
						Indicator Removal (9)		Network Sniffing			Traffic Signaling (2)		
						Indirect Command Execution		Password Policy Discovery					
						Masquerading (9)		Peripheral Device Discovery					
						Modify Authentication Process (8)		Steal or Forge Credentials					

Pillar 01: Defensive Measures

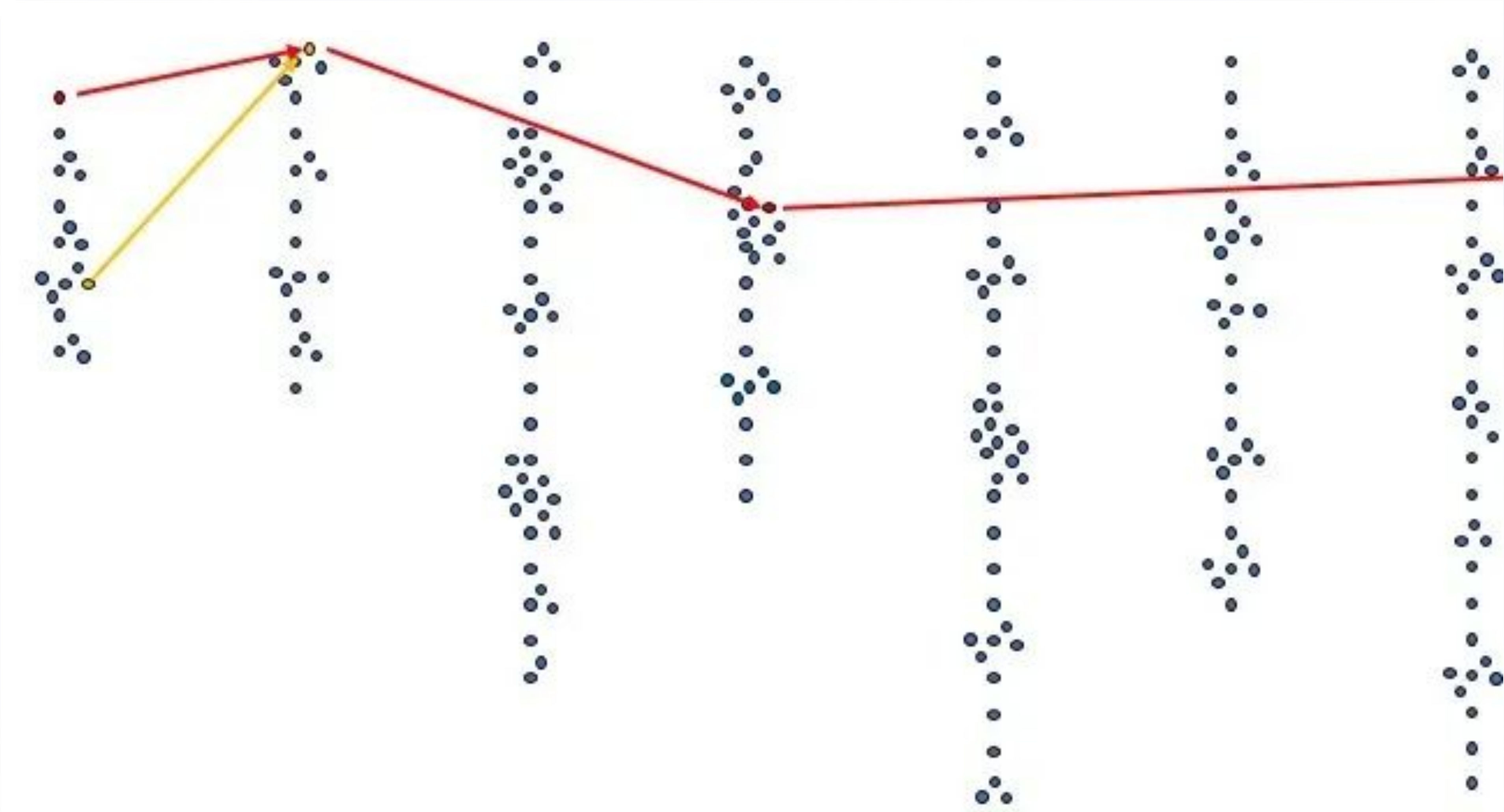
Matrices (Technological Categories)

- Enterprise Matrix : 14 Tactics & 234 Techniques
- Mobile Matrix
- ICS Matrix

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 17 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Content Injection	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Encoding (2)	Exfiltration Over Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Client Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Create or Modify System Process (4)	Create or Modify System Process (4)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Event Triggered Execution (16)	Domain Policy Modification (2)	Direct Volume Access	Modify Authentication Process (8)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Financial Theft
Search Open Websites/Domains (3)	Trusted Relationship	Shared Modules	Serverless Execution	External Remote Services	Escape to Host	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Failback Channels	Exfiltration Over Web Service (4)	Firmware Corruption
Search Victim-Owned Websites	Valid Accounts (4)	Software Deployment Tools	System Services (2)	Hijack Execution Flow (12)	Event Triggered Execution (16)	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	Device Driver Discovery		Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Inhibit System Recovery
		Windows Management Instrumentation	User Execution (3)	Implant Internal Image	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Network Denial of Service (2)
			Windows Management Instrumentation	Modify Authentication Process (8)	Hijack Execution Flow (12)	Hide Artifacts (11)	OS Credential Dumping (8)	File and Directory Discovery		Data from Removable Media	Non-Application Layer Protocol	Non-Standard Port	Resource Hijacking
				Office Application Startup (6)	Process Injection (12)	Hijack Execution Flow (12)	Steal Application Access Token	Group Policy Discovery		Data Staged (2)	Non-Application Layer Protocol	Protocol Tunneling	Service Stop
				Power Settings	Scheduled Task/Job (5)	Impair Defenses (11)	Steal or Forge Authentication Certificates	Log Enumeration		Email Collection (3)	Proxy (4)	Remote Access Software	System Shutdown/Reboot
					Valid Accounts (4)	Impersonation	Steal or Forge Certificates	Network Service Discovery		Input Capture (4)	Remote Access Software	Traffic Signaling (2)	
						Indirect Command Execution	Steal or Forge Credentials	Network Share Discovery		Screen Capture	Traffic Signaling (2)		
						Masquerading (9)	Steal or Forge Credentials	Password Policy Discovery					
						Modify Authentication Process (8)	Steal or Forge Credentials	Peripheral Device Discovery					

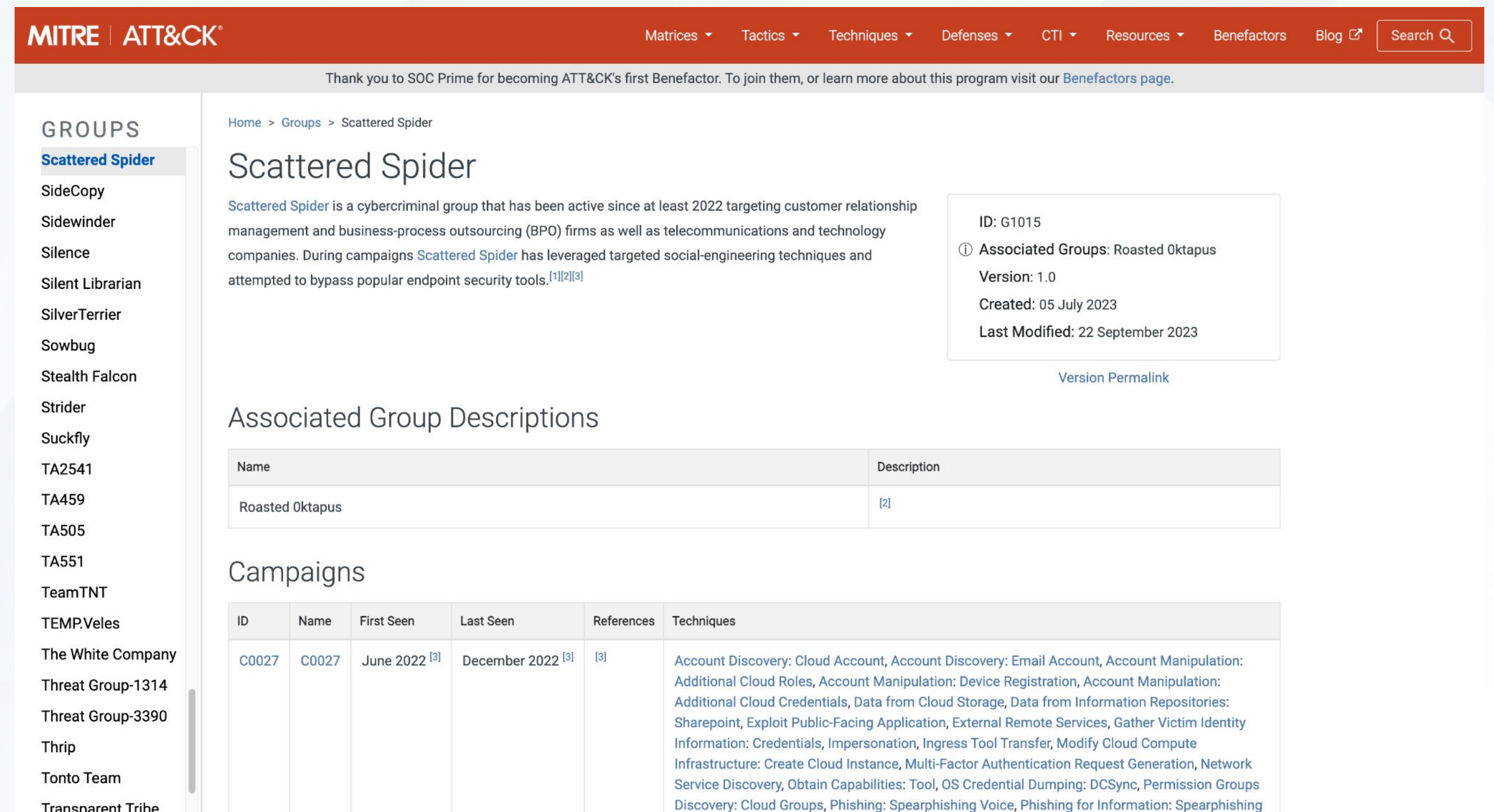
MITRE ATT&CK Matrix for Enterprise

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 17 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Client Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Create Account (3)	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (4)	Execution Guardrails (1)	Direct Volume Access	Modify Authentication Process (8)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Scheduled Transfer	Financial Theft
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Escape to Host	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Ingress Tool Transfer	Transfer Data to Cloud Account	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	Event Triggered Execution (16)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Multi-Stage Channels		Inhibit System Recovery
			Software Deployment Tools	External Remote Services	Hijack Execution Flow (12)	File and Directory Permissions Modification (2)	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Non-Application Layer Protocol		Network Denial of Service (2)
			System Services (2)	Hijack Execution Flow (12)	Implant Internal Image	Hide Artifacts (11)	OS Credential Dumping (8)	File and Directory Discovery		Data from Removable Media	Protocol Tunneling		Resource Hijacking
			User Execution (3)	Hijack Execution Flow (12)	Modify Authentication Process (8)	Hijack Execution Flow (12)	Steal Application Access Token	Group Policy Discovery		Data Staged (2)	Proxy (4)		Service Stop
			Windows Management Instrumentation	Process Injection (12)	Office Application Startup (6)	Impersonation	Steal or Forge Authentication Certificates	Log Enumeration		Email Collection (3)	Remote Access Software		System Shutdown/Reboot
				Scheduled Task/Job (5)	Power Settings	Indicator Removal (9)		Network Service Discovery		Input Capture (4)	Traffic Signaling (2)		
				Valid Accounts (4)		Indirect Command Execution		Network Share Discovery		Screen Capture			
						Masquerading (9)		Network Sniffing					
						Modify Authentication Process (8)		Password Policy Discovery					
								Peripheral Device Discovery					



Pillar 02: Cyber Threat Intelligence

Threat information that has been **aggregated, transformed, analyzed, interpreted, or enriched** to provide the necessary context for decision-making.



The screenshot shows the MITRE ATT&CK website interface. At the top, there is a navigation bar with links for Matrices, Tactics, Techniques, Defenses, CTI, Resources, Benefactors, and Blog. A search bar is also present. Below the navigation bar, a message thanks SOC Prime for becoming ATT&CK's first Benefactor. The main content area is titled "Scattered Spider" and includes a description of the group, its ID (G1015), associated groups (Roasted Oktapus), version (1.0), creation date (05 July 2023), and last modified date (22 September 2023). There is also a section for "Associated Group Descriptions" with a table showing the name "Roasted Oktapus" and a description link. Finally, there is a "Campaigns" table with columns for ID, Name, First Seen, Last Seen, References, and Techniques.

GROUPS

- Scattered Spider
- SideCopy
- Sidewinder
- Silence
- Silent Librarian
- SilverTerrier
- Sowbug
- Stealth Falcon
- Strider
- Suckfly
- TA2541
- TA459
- TA505
- TA551
- TeamTNT
- TEMP.Veles
- The White Company
- Threat Group-1314
- Threat Group-3390
- Thrip
- Tonto Team
- Transparent Tribe

Home > Groups > Scattered Spider

Scattered Spider

Scattered Spider is a cybercriminal group that has been active since at least 2022 targeting customer relationship management and business-process outsourcing (BPO) firms as well as telecommunications and technology companies. During campaigns Scattered Spider has leveraged targeted social-engineering techniques and attempted to bypass popular endpoint security tools.^{[1][2][3]}

ID: G1015
 ⓘ Associated Groups: Roasted Oktapus
 Version: 1.0
 Created: 05 July 2023
 Last Modified: 22 September 2023

[Version Permalink](#)

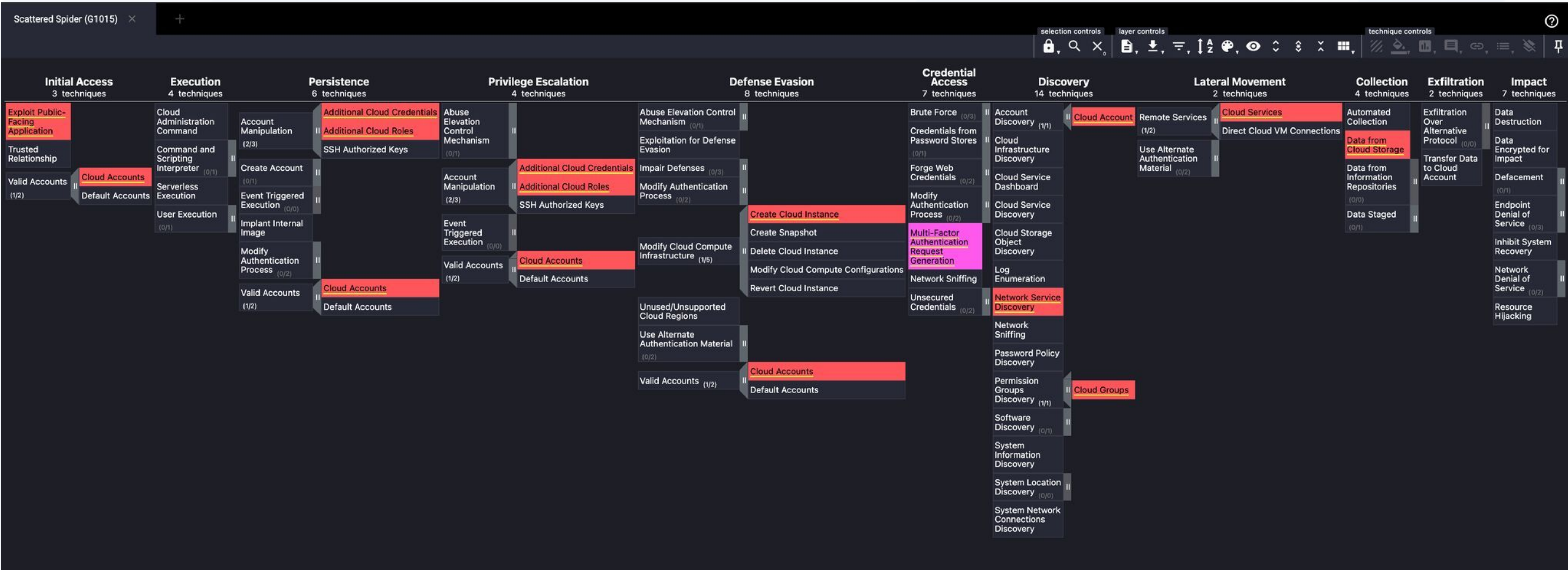
Associated Group Descriptions

Name	Description
Roasted Oktapus	[2]

Campaigns

ID	Name	First Seen	Last Seen	References	Techniques
C0027	C0027	June 2022 ^[3]	December 2022 ^[3]	[3]	Account Discovery: Cloud Account, Account Discovery: Email Account, Account Manipulation: Additional Cloud Roles, Account Manipulation: Device Registration, Account Manipulation: Additional Cloud Credentials, Data from Cloud Storage, Data from Information Repositories: Sharepoint, Exploit Public-Facing Application, External Remote Services, Gather Victim Identity Information: Credentials, Impersonation, Ingress Tool Transfer, Modify Cloud Compute Infrastructure: Create Cloud Instance, Multi-Factor Authentication Request Generation, Network Service Discovery, Obtain Capabilities: Tool, OS Credential Dumping: DCSync, Permission Groups Discovery: Cloud Groups, Phishing: Spearphishing Voice, Phishing for Information: Spearphishing

Cyber Threat Intelligence - Threat Actor Context



The screenshot displays the MITRE ATT&CK Navigator interface for the threat actor Scattered Spider (G1015). The interface is organized into columns representing different stages of an attack: Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Exfiltration, and Impact. A specific attack path is highlighted in red, showing the following sequence of techniques:

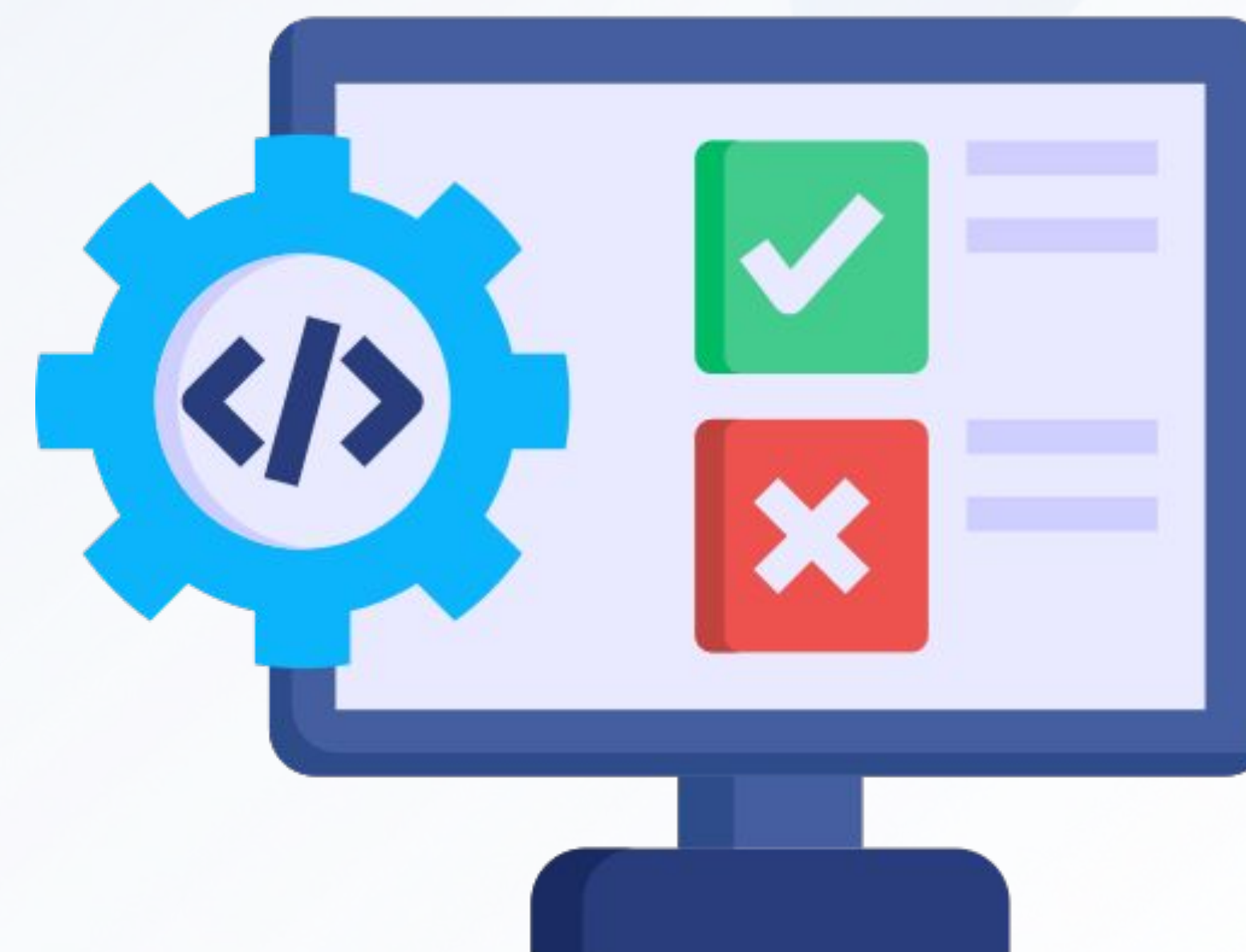
- Initial Access:** Exploit Public-Facing Application, Trusted Relationship, Valid Accounts (1/2).
- Execution:** Cloud Administration Command, Command and Scripting Interpreter (0/1), Serverless Execution, User Execution (0/1).
- Persistence:** Account Manipulation (2/3), SSH Authorized Keys, Create Account (0/1), Event Triggered Execution (0/0), Implant Internal Image, Modify Authentication Process (0/2), Valid Accounts (1/2).
- Privilege Escalation:** Abuse Elevation Control Mechanism (0/1), Account Manipulation (2/3), Event Triggered Execution (0/0), Valid Accounts (1/2), Default Accounts.
- Defense Evasion:** Abuse Elevation Control Mechanism (0/1), Exploitation for Defense Evasion, Impair Defenses (0/3), Modify Authentication Process (0/2), Modify Cloud Compute Infrastructure (1/5), Delete Cloud Instance, Modify Cloud Compute Configurations, Revert Cloud Instance, Unused/Unsupported Cloud Regions, Use Alternate Authentication Material (0/2), Valid Accounts (1/2).
- Credential Access:** Brute Force (0/3), Credentials from Password Stores (0/1), Forge Web Credentials (0/2), Modify Authentication Process (0/2), Multi-Factor Authentication Request Generation, Network Sniffing, Unsecured Credentials (0/2).
- Discovery:** Account Discovery (1/1), Cloud Infrastructure Discovery, Cloud Service Dashboard, Cloud Service Discovery, Cloud Storage Object Discovery, Log Enumeration, Network Service Discovery, Network Sniffing, Password Policy Discovery, Permission Groups Discovery (1/1), Software Discovery (0/1), System Information Discovery, System Location Discovery (0/0), System Network Connections Discovery.
- Lateral Movement:** Remote Services (1/2), Use Alternate Authentication Material (0/2), Direct Cloud VM Connections.
- Collection:** Automated Collection, Data from Cloud Storage, Data from Information Repositories (0/0), Data Staged (0/1).
- Exfiltration:** Exfiltration Over Alternative Protocol (0/0), Transfer Data to Cloud Account.
- Impact:** Data Destruction, Data Encrypted for Impact, Defacement (0/1), Endpoint Denial of Service (0/3), Inhibit System Recovery, Network Denial of Service (0/2), Resource Hijacking.

Key techniques highlighted in red include: Cloud Accounts, Additional Cloud Credentials, Additional Cloud Roles, SSH Authorized Keys, Create Cloud Instance, Create Snapshot, Delete Cloud Instance, Modify Cloud Compute Configurations, Revert Cloud Instance, Cloud Accounts, Default Accounts, Cloud Groups, Cloud Account, Remote Services, Cloud Services, Data from Cloud Storage, and Network Service Discovery.

Pillar 03: Testing & Evaluation

MITRE ENGENUITY recommends the use of **Adversary emulation** for testing and evaluating defenses.

Adversary emulation mimics the behaviour of real world threat actors in a safe and repeatable manner.

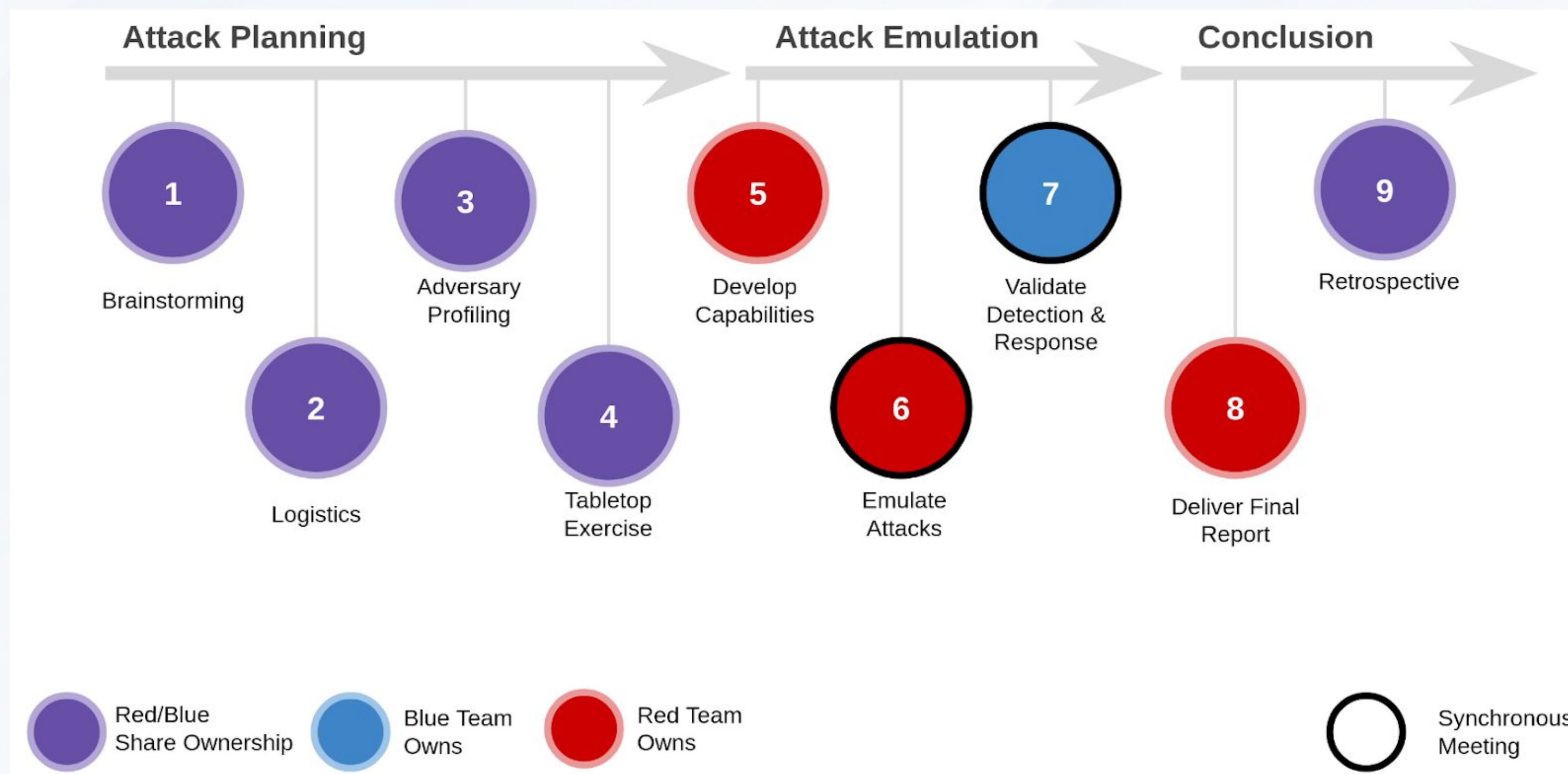


Why Adversary Emulation ?

- How do we build a resilient defense that is not based on **static** (and easily evaded) Indicators of Compromise ?
- How do we **detect, mitigate, respond to, or prevent** against **threat actor X**?
- Are we collecting **the right data** and **run the right queries** to detect technique Y?
- How do we build **the experience and skills** on our team to defend against real-world threats?
- How do we tune our **tools and processes** to maximize efficacy against real-world threats ?



Adversary Emulation Workflow



[GitLab Security team's Attack Emulation Workflow](#)

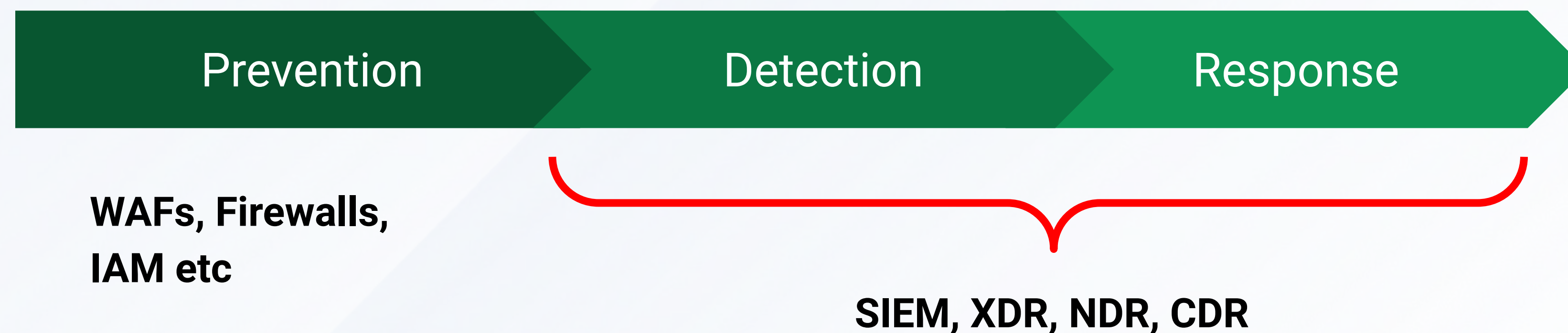
Cloud Attack Emulation

- Adversary emulation for the cloud.
- Efficient of mimicking of real world threat that target cloud-native infrastructure.
- Cloud attack emulation is designed to address cloud-specific challenges.

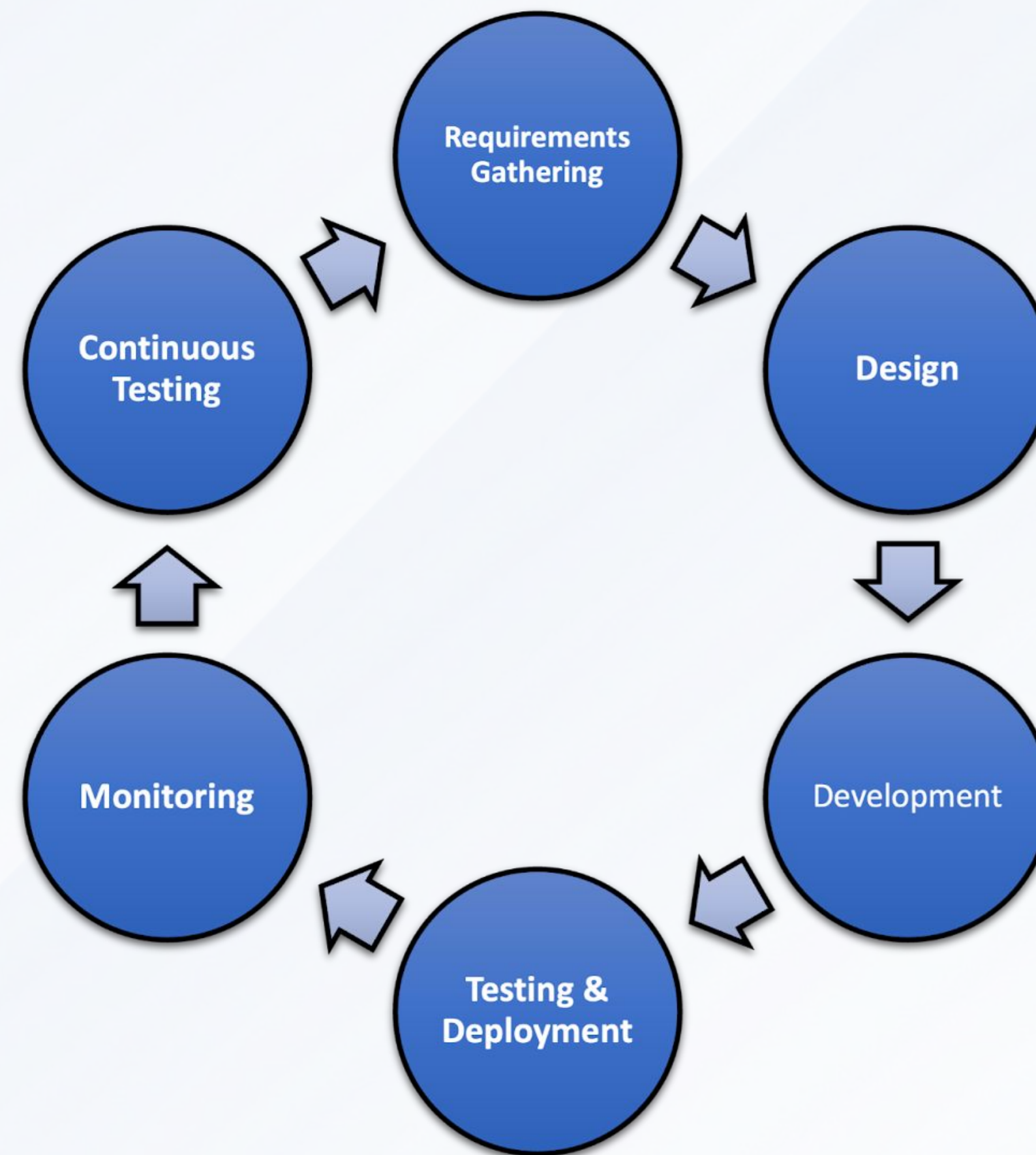


Detection Engineering

Detection Engineering is an aspect of cybersecurity that focuses on **developing, fine-tuning, and maintaining** systems designed to identify and alert organizations to potential security threats, breaches, and malicious/suspicious activities.



Detection Development Lifecycle




```
1  title: AWS CloudTrail Important Change
2  id: 4db60cc0-36fb-42b7-9b58-a5b53019fb74
3  status: test
4  description: Detects disabling, deleting and updating of a Trail
5  references:
6    - https://docs.aws.amazon.com/awscloudtrail/latest/userguide/best-practices-security.html
7  author: vitaliy0x1
8  date: 2020/01/21
9  modified: 2022/10/09
10 tags:
11   - attack.defense_evasion
12   - attack.t1562.001
13 logsource:
14   product: aws
15   service: cloudtrail
16 detection:
17   selection_source:
18     eventSource: cloudtrail.amazonaws.com
19     eventName:
20       - StopLogging
21       - UpdateTrail
22       - DeleteTrail
23   condition: selection_source
24 falsepositives:
25   - Valid change in a Trail
26 level: medium
```

Example Sigma Rule For detecting Several Potentially Malicious Events Against AWS CloudTrail

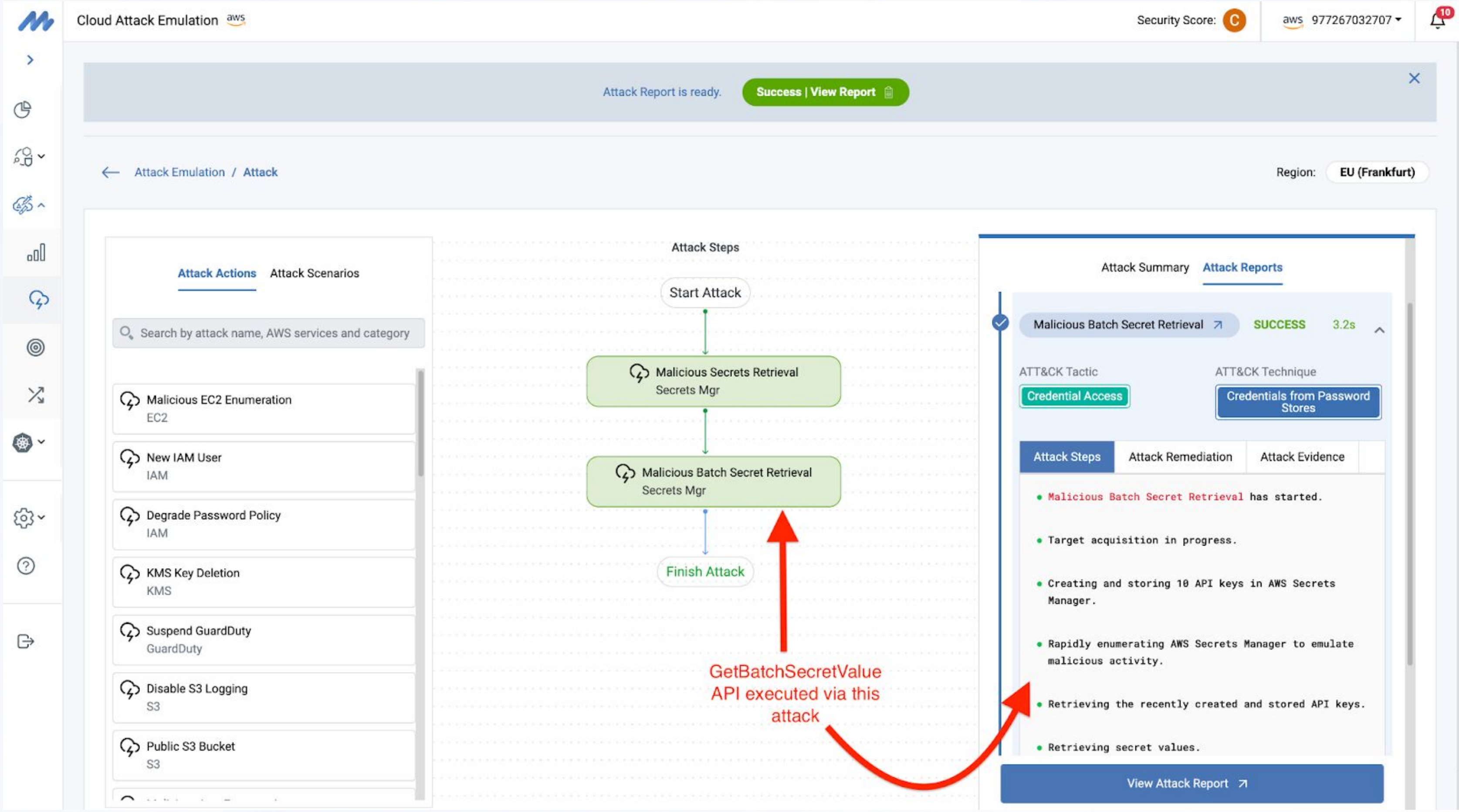
Example - Validating Detections



Credential from Password Stores: Cloud Secrets Management Stores (T1555.006)



Emulating The Cloud Attack





The screenshot displays the Mitigant Cloud Attack Emulation interface. At the top, it shows the security score as 'C' and the AWS account ID '977267032707'. A notification banner indicates 'Attack Report is ready' with a 'Success | View Report' button. The main content area is divided into three sections:

- Attack Actions:** A list of attack actions including Malicious EC2 Enumeration, New IAM User, Degrade Password Policy, KMS Key Deletion, Suspend GuardDuty, Disable S3 Logging, and Public S3 Bucket.
- Attack Steps:** A flowchart showing the sequence of the attack: Start Attack → Malicious Secrets Retrieval (Secrets Mgr) → Malicious Batch Secret Retrieval (Secrets Mgr) → Finish Attack. A red arrow points from the 'Attack Evidence' section to the 'Malicious Batch Secret Retrieval' step, with the text 'GetBatchSecretValue API executed via this attack'.
- Attack Summary:** Details for the 'Malicious Batch Secret Retrieval' attack, which is marked as 'SUCCESS' and took 3.2s. It lists the ATT&CK Tactic as 'Credential Access' and the ATT&CK Technique as 'Credentials from Password Stores'. The 'Attack Evidence' section contains a list of events: 'Malicious Batch Secret Retrieval has started.', 'Target acquisition in progress.', 'Creating and storing 10 API keys in AWS Secrets Manager.', 'Rapidly enumerating AWS Secrets Manager to emulate malicious activity.', 'Retrieving the recently created and stored API keys.', and 'Retrieving secret values.'

CloudTrail Record

```
"eventTime": "2024-03-17T08:26:34Z",  
"eventSource": "secretsmanager.amazonaws.com",  
"eventName": "BatchGetSecretValue",  
"awsRegion": "eu-central-1",  
"sourceIPAddress": "84.173.248.182",  
"userAgent": "aws-sdk-java/1.12.97 Mac_OS_X/13.6.1 OpenJDK_64-Bit_Server_VM/11.0.15+9-LTS java/11.0.15 vendor/Amazon.com_Inc. cfg/retry-mode/legacy",  
"requestParameters": {  
  "secretIdList": [  
    "mitigator-X_API_KEY_1BPWKB",  
    "mitigator-X_API_KEY_F5FAZW",  
    "mitigator-X_API_KEY_UHAAWW",  
    "mitigator-X_API_KEY_MVV9EU",  
    "mitigator-X_API_KEY_NTWS23",  
    "mitigator-X_API_KEY_MKQBD1",  
    "mitigator-X_API_KEY_JTWSKU",  
    "mitigator-X_API_KEY_7FAWMK",  
    "mitigator-X_API_KEY_7MG88B",  
    "mitigator-X_API_KEY_S2EOR0"  
  ]  
},
```



Undetected Threats !

Cloud SIEM Overview | Content Packs | Signals | Detection Rules | **Investigator**

aws AWS | gcp GCP | azure Azure

In Assumed Role investigate MitigantChaosRolec714f8... Search for service:secretsmanager

```
graph LR; A["MitigantChaosRole...  
Type: Assumed Role  
Account: 977267032707"] -.- uses -.-> B["secretsmanager  
Type: Service"]; B -.- performs -.-> C["4 event types  
20 CreateSecret  
20 DeleteSecret  
30 GetSecretValue"]; C --- D["4 event types  
20 CreateSecret  
20 DeleteSecret  
30 GetSecretValue  
51 ListSecrets"]; E["GetBatchSecretValue  
Not Detected"] --> C;
```

The diagram illustrates the relationship between an assumed role and the secretsmanager service. The role, identified as 'MitigantChaosRole...' (Type: Assumed Role, Account: 977267032707), uses the 'secretsmanager' service (Type: Service). This service performs four event types: 20 CreateSecret, 20 DeleteSecret, and 30 GetSecretValue. A comparison shows that the actual events include an additional 51 ListSecrets events. A red arrow points to a missing event type, 'GetBatchSecretValue', which is noted as 'Not Detected'.


```
86 tags = [  
87     "Domain: Cloud",  
88     "Data Source: AWS",  
89     "Data Source: Amazon Web Services",  
90     "Tactic: Credential Access",  
91     "Resources: Investigation Guide",  
92 ]  
93 timestamp_override = "event.ingested"  
94 type = "new_terms"  
95  
96 query = '''  
97 event.dataset:aws.cloudtrail and event.provider:secretsmanager.amazonaws.com and  
98     event.action:GetSecretValue and event.outcome:success and aws.cloudtrail.user_identity.session_context.session_issuer.type: Role and  
99     not user_agent.name: ("Chrome" or "Firefox" or "Safari" or "Edge" or "Brave" or "Opera")  
100 '''  
101  
102  
103 [[rule.threat]]  
104 framework = "MITRE ATT&CK"  
105 [[rule.threat.technique]]  
106 id = "T1528"  
107 name = "Steal Application Access Token"  
108 reference = "https://attack.mitre.org/techniques/T1528/"  
109  
110  
111 [rule.threat.tactic]  
112 id = "TA0006"  
113 name = "Credential Access"  
114 reference = "https://attack.mitre.org/tactics/TA0006/"  
115  
116 [rule.new_terms]  
117 field = "new_terms_fields"  
118 value = ["user.id", "aws.cloudtrail.request_parameters"]  
119 [[rule.new_terms.history_window_start]]  
120 field = "history_window_start"  
121 value = "now-15d"
```


Resources

- MITRE ATT&CK Cloud Matrix: New Techniques & Why You Should Care ([Link](#))
- Threat Led Attack Emulation ([Link](#))
- Cloud Attack Emulation & Detection Engineering: A Match Made in Heaven ([Link](#))
- Cloud Attack Emulation: Enhancing Cloud-Native Security With Threat-Informed Defense ([Link](#))
- Threat Detection Strategy: A Visual Model ([Link](#))

Thank you for your attention

 kennedy@mitigant.io

 [@run2obtain](https://twitter.com/run2obtain)