Be Secure. Be Resilient.

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

Kennedy Torkura
Co-Founder & CTO
Mitigant

Mitigant
Be Secure. Be Resilient.

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

Mitigant
Be Secure. Be Resilient.

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

Mitigant
Be Secure. Be Resilient.

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.

Mitigant
Be Secure. Be Resilient.

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

- MITRE ENGENUITY

https://mitre-engenuity.org/cybersecurity/

Mitigant
Be Secure. Be Resilient.

Pillar 01: Defensive Measures

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

Mitigant
Be Secure. Be Resilient.

Pillar 01: Defensive Measures

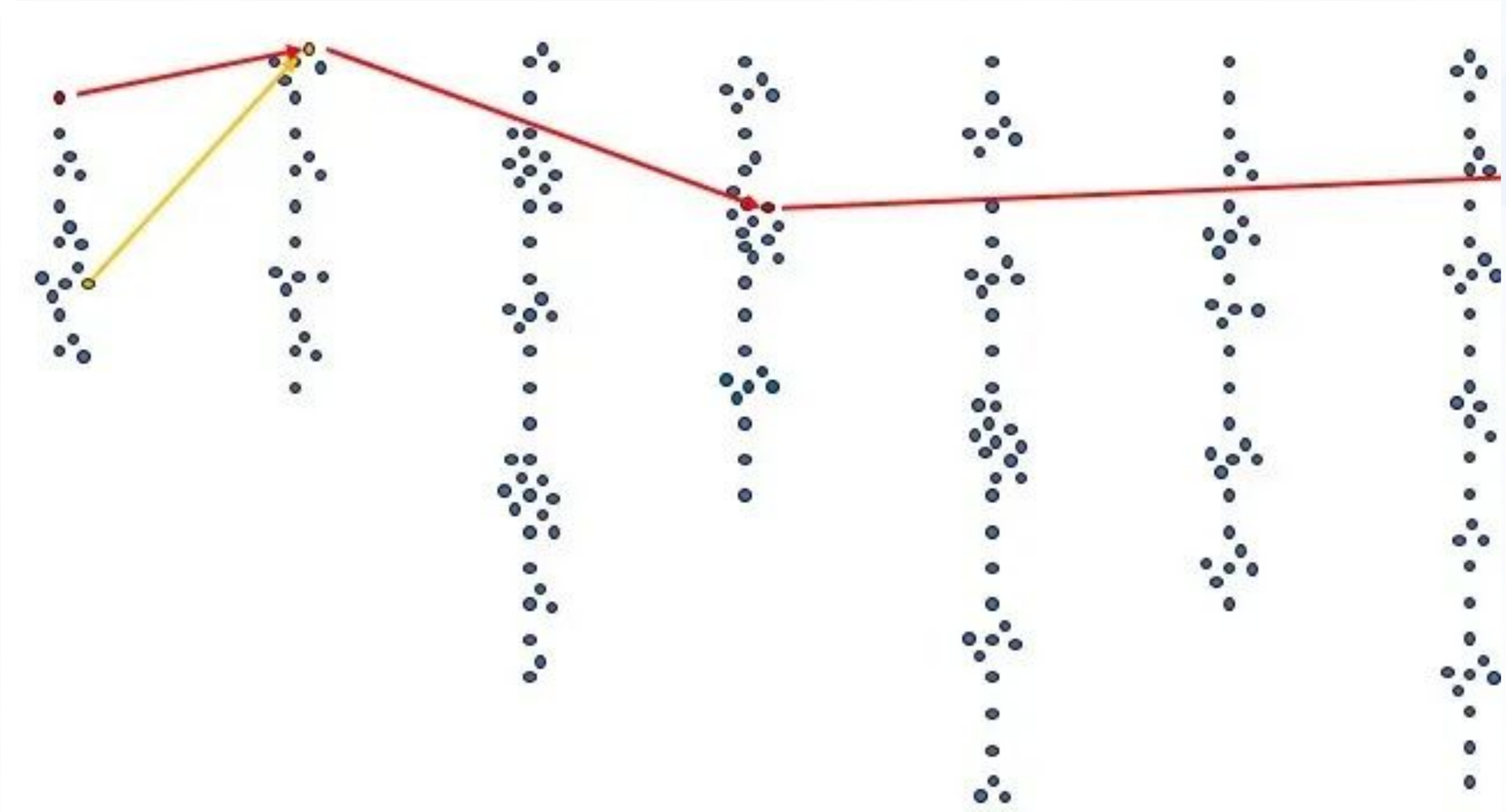
<u>Matrices (Technological Categories)</u>

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

Mitigant
Be Secure. Be Resilient.

MITRE ATT&CK Matrix for Enterprise

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	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)	Escape to Host	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)	Event Triggered Execution (16)	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	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Multi-Stage Channels		Inhibit System Recovery
			Software Deployment Tools	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Non-Application Layer Protocol		Network Denial of Service (2)
			System Services (2)	Implant Internal Image	Process Injection (12)	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	File and Directory Discovery		Data from Removable Media	Non-Standard Port		Resource Hijacking
			User Execution (3)	Modify Authentication Process (8)	Scheduled Task/Job (5)	Hide Artifacts (11)	Steal Application Access Token	Group Policy Discovery		Data Staged (2)	Protocol Tunneling		Service Stop
			Windows Management Instrumentation	Office Application Startup (6)	Valid Accounts (4)	Hijack Execution Flow (12)	Steal or Forge Authentication Certificates	Log Enumeration		Email Collection (3)	Proxy (4)		System Shutdown/Reboot
				Power Settings		Impair Defenses (11)	Steal or Forge	Network Service Discovery		Input Capture (4)	Remote Access Software		
						Impersonation		Network Share Discovery		Screen Capture	Traffic Signaling (2)		
						Indicator Removal (9)		Network Sniffing					
						Indirect Command Execution		Password Policy Discovery					
						Masquerading (9)		Peripheral Device Discovery					
						Modify Authentication Process (8)							

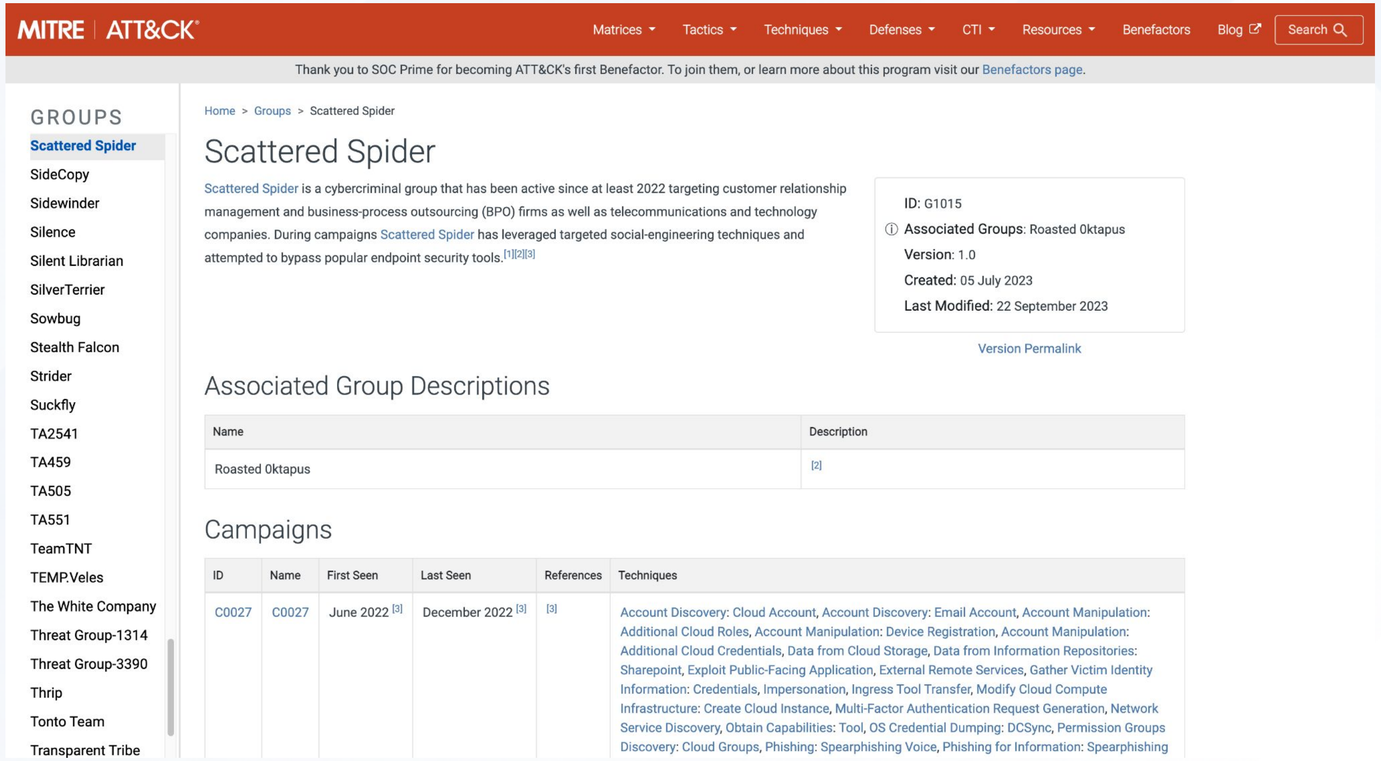


https://medium.com/@vanvleet/threat-detection-strategy-a-visual-model-b8f4fa518441

Mitigant
Be Secure. Be Resilient.

Pillar 02: Cyber Threat Intelligence

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



MITRE | ATT&CK

Matrices Tactics Techniques Defenses CTI Resources Benefactors Blog Search

Thank you to SOC Prime for becoming ATT&CK's first Benefactor. To join them, or learn more about this program visit our Benefactors page.

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 0ktapus
Version: 1.0
Created: 05 July 2023
Last Modified: 22 September 2023

Version Permalink

Associated Group Descriptions

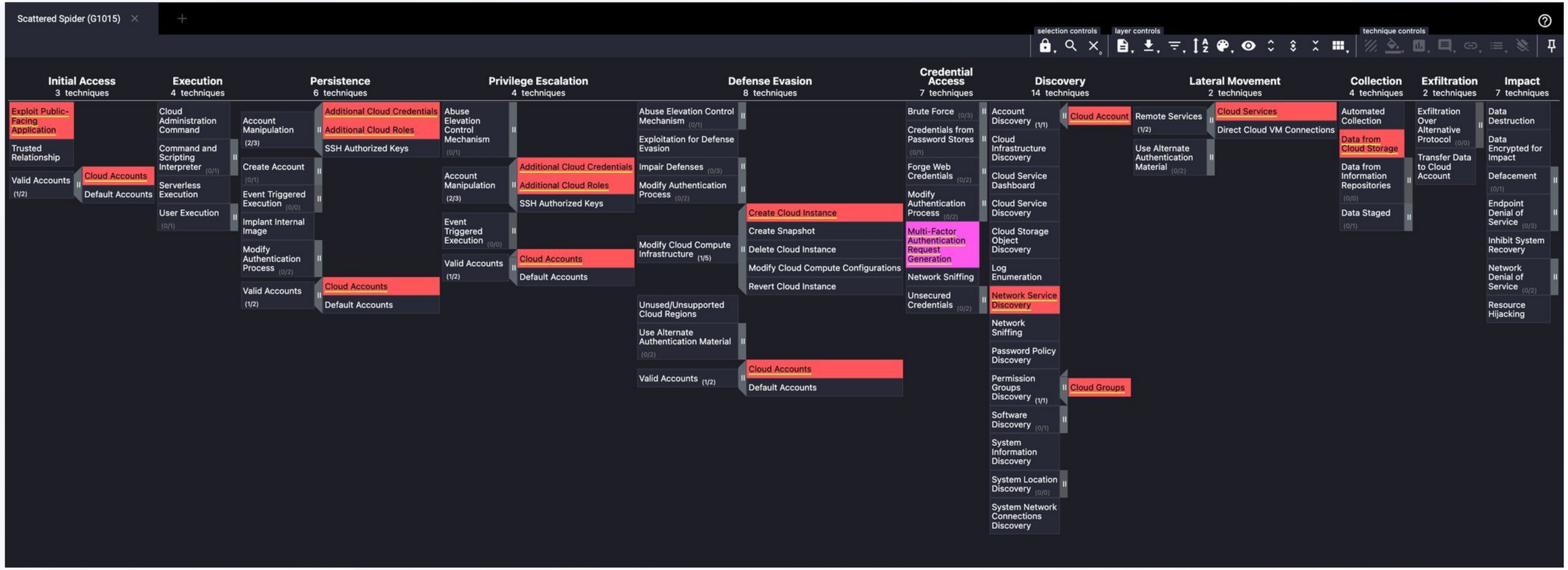
Name	Description
Roasted 0ktapus	[2]

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

Mitigant
Be Secure. Be Resilient.

Cyber Threat Intelligence - Threat Actor Context



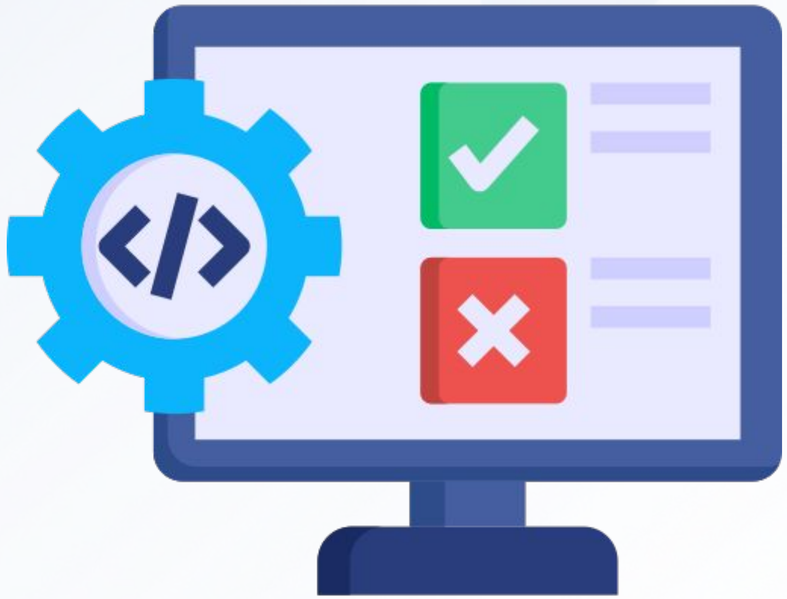
MITRE ATT&CK Navigator

Mitigant
Be Secure. Be Resilient.

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.



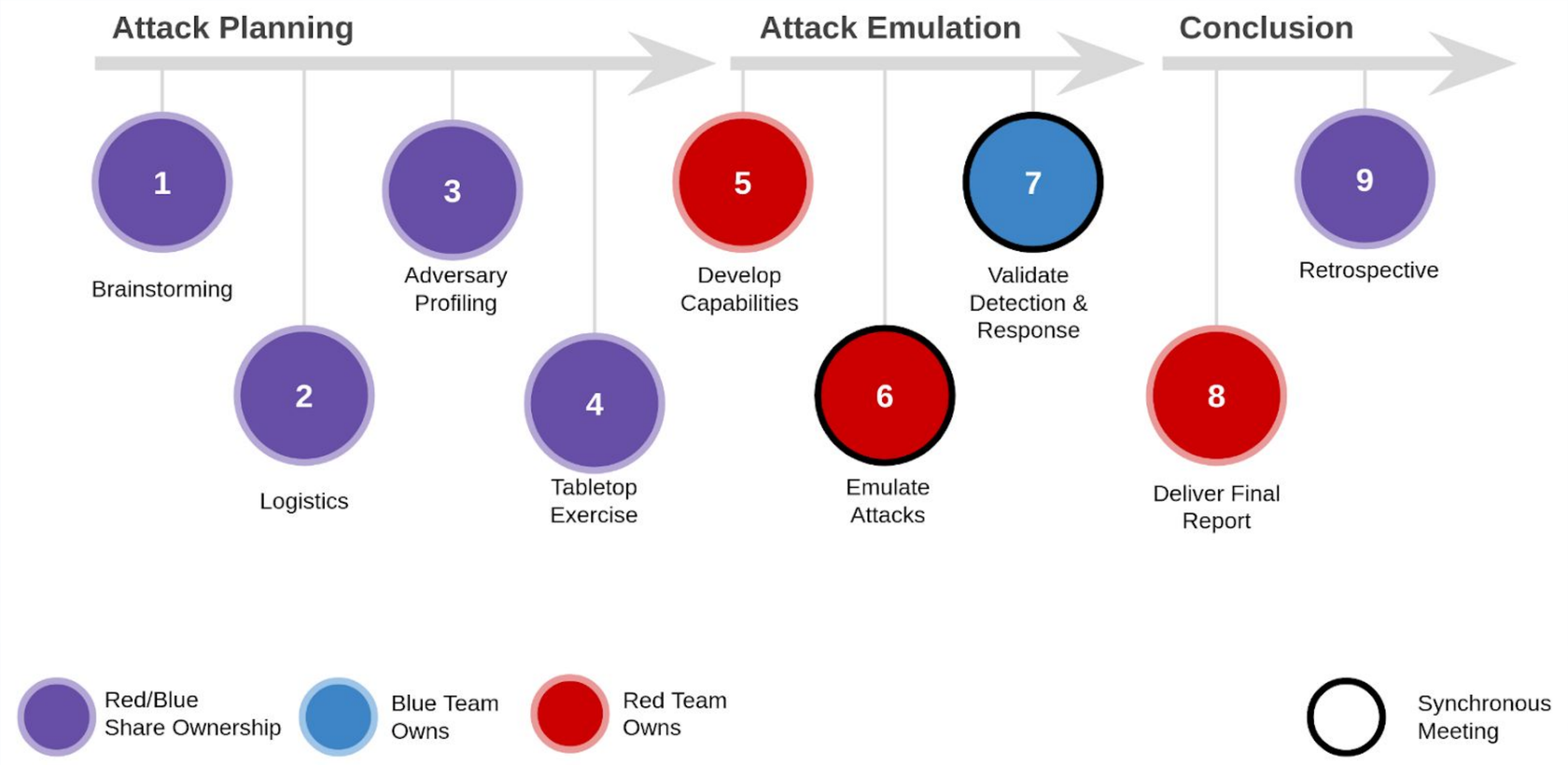
Mitigant
Be Secure. Be Resilient.

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 ?

https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/adversary-emulation-library/

Adversary Emulation Workflow

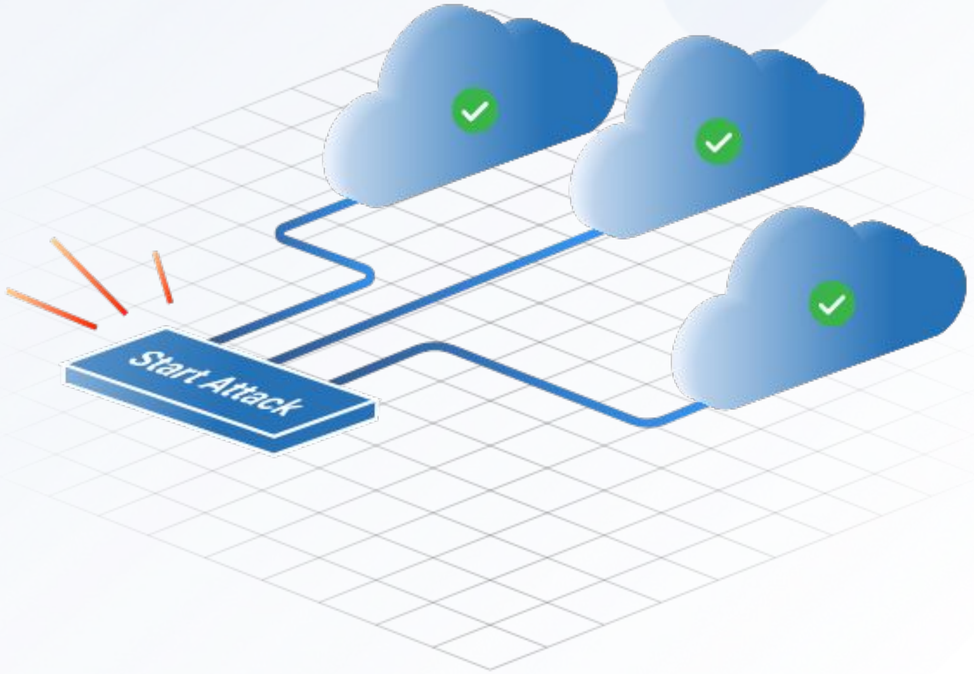


[GitLab Security team's Attack Emulation Workflow]

Mitigant
Be Secure. Be Resilient.

Cloud Attack Emulation

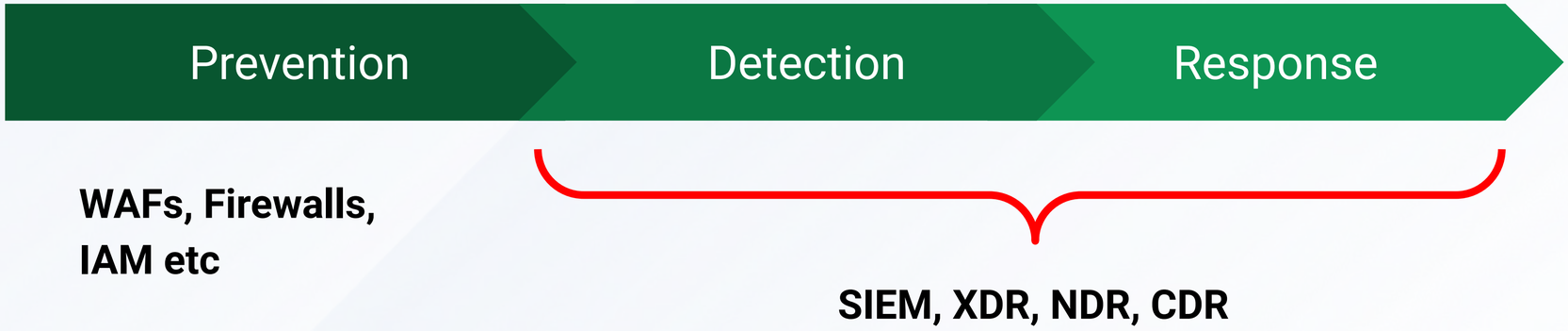
- Adversary emulation for the cloud.
- Efficient of mimicking of real world threat that target cloud-native infrastructure.
- Cloud attack emulation is designed to address cloud-specific challenges.



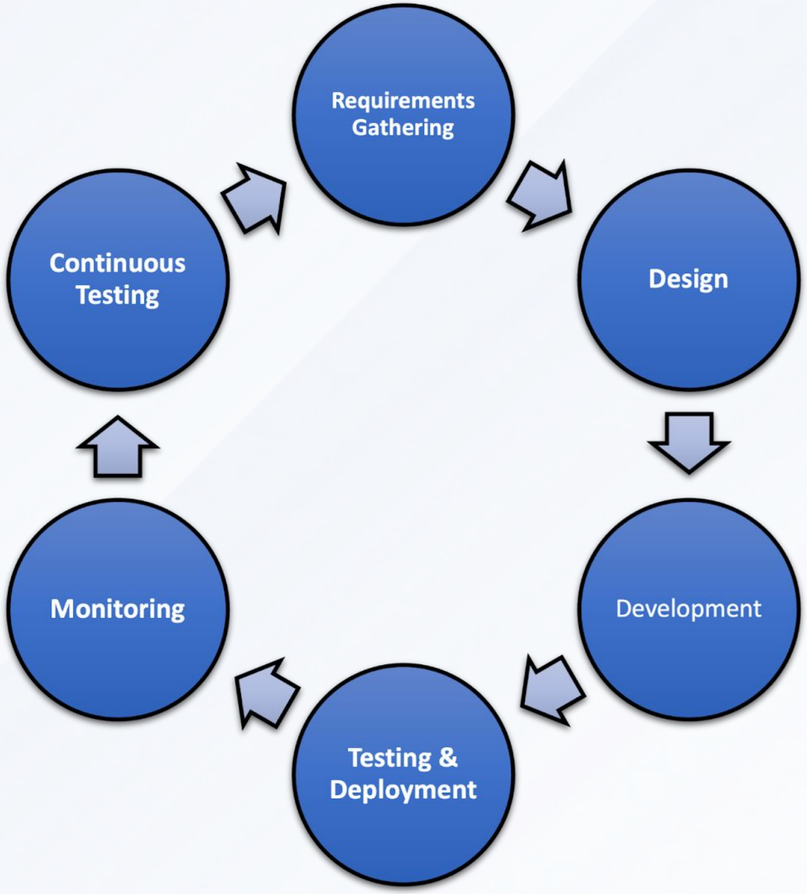
Mitigant
Be Secure. Be Resilient.

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



https://medium.com/snowflake/detection-development-lifecycle-af166fffb3bc

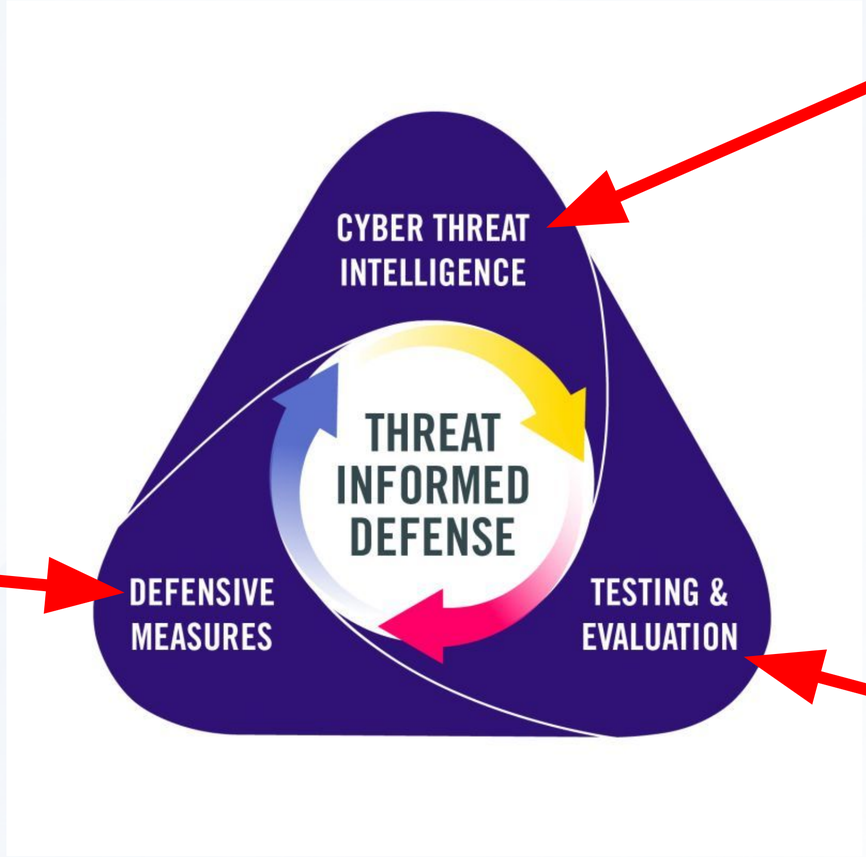
Mitigant
Be Secure. Be Resilient.

```yaml
title: AWS CloudTrail Important Change
id: 4db60cc0-36fb-42b7-9b58-a5b53019fb74
status: test
description: Detects disabling, deleting and updating of a Trail
references:
    - https://docs.aws.amazon.com/awscloudtrail/latest/userguide/best-practices-security.html
author: vitaliy0x1
date: 2020/01/21
modified: 2022/10/09
tags:
    - attack.defense_evasion
    - attack.t1562.001
logsource:
    product: aws
    service: cloudtrail
detection:
    selection_source:
        eventSource: cloudtrail.amazonaws.com
        eventName:
            - StopLogging
            - UpdateTrail
            - DeleteTrail
    condition: selection_source
falsepositives:
    - Valid change in a Trail
level: medium
```

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

Example - Validating Detections

Scattered Spider Threat Actor



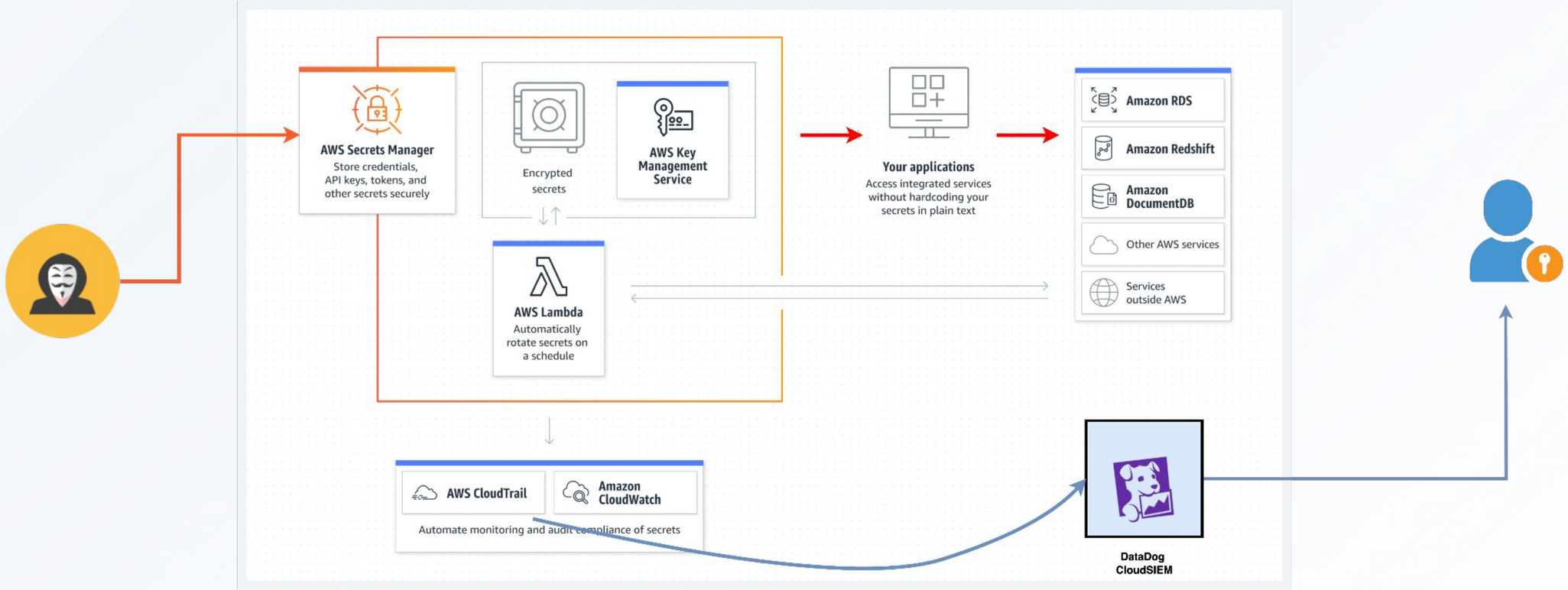
Scattered Spider Techniques

- T1555.006

Adversary Emulation of Scattered Spider TTPs

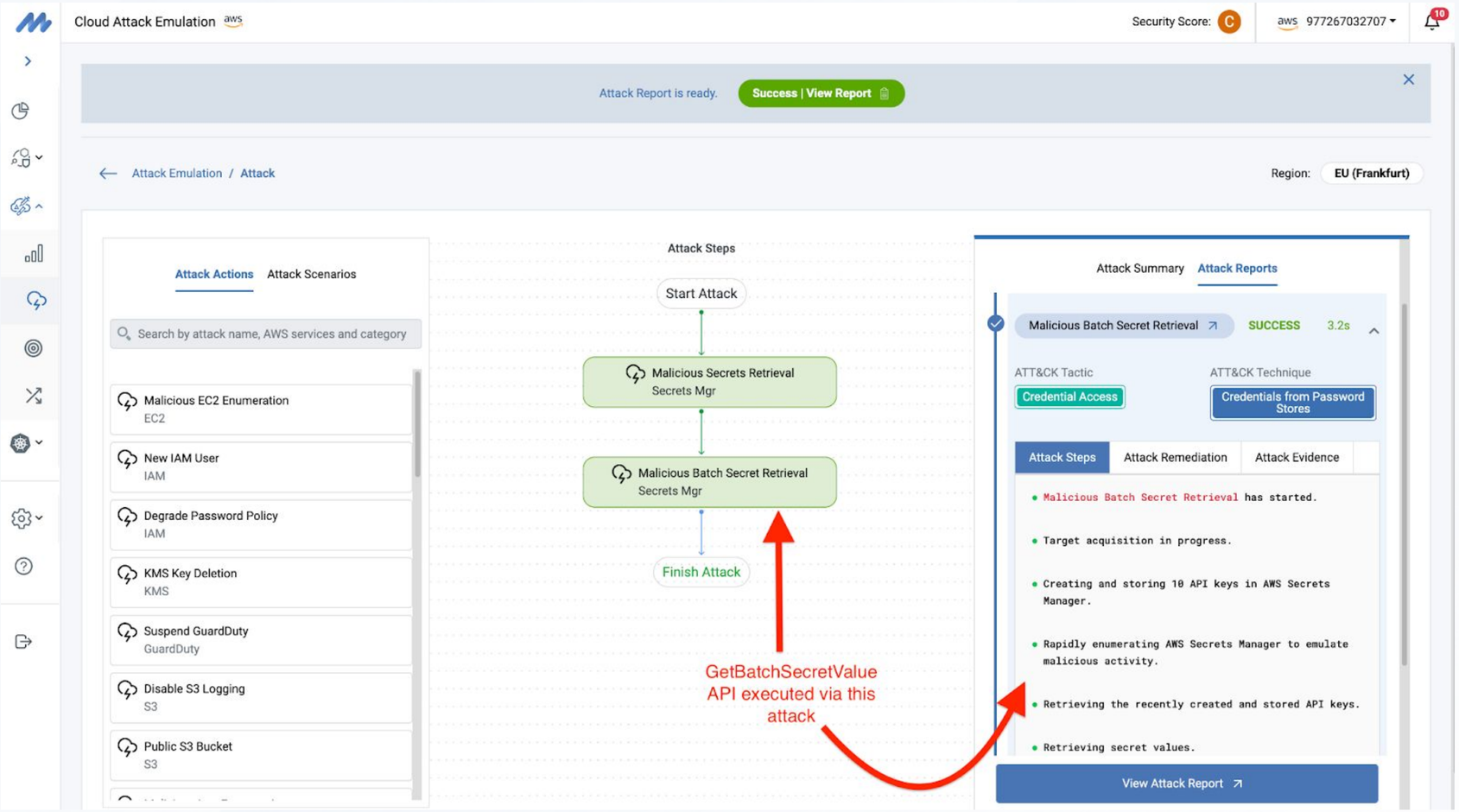
Mitigant
Be Secure. Be Resilient.

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



Mitigant
Be Secure. Be Resilient.

Emulating The Cloud Attack



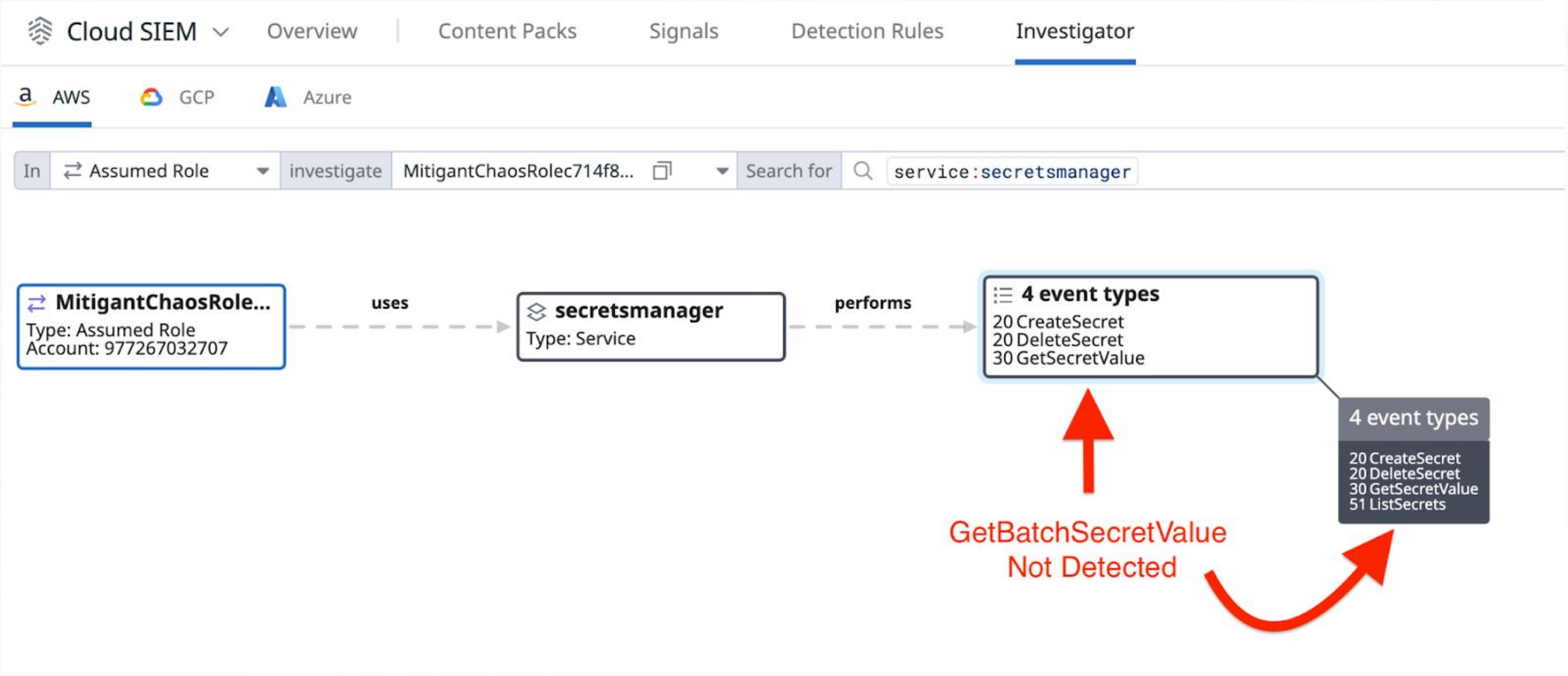
Mitigant
Be Secure. Be Resilient.

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"
    ]
},
```

Mitigant
Be Secure. Be Resilient.

Undetected Threats !



Mitigant
Be Secure. Be Resilient.

```
tags = [
    "Domain: Cloud",
    "Data Source: AWS",
    "Data Source: Amazon Web Services",
    "Tactic: Credential Access",
    "Resources: Investigation Guide",
]
timestamp_override = "event.ingested"
type = "new_terms"

query = '''
event.dataset:aws.cloudtrail and event.provider:secretsmanager.amazonaws.com and
    event.action:GetSecretValue and event.outcome:success and aws.cloudtrail.user_identity.session_context.session_issuer.type: Role and
    not user_agent.name: ("Chrome" or "Firefox" or "Safari" or "Edge" or "Brave" or "Opera")
'''


[[rule.threat]]
framework = "MITRE ATT&CK"
[[rule.threat.technique]]
id = "T1528"
name = "Steal Application Access Token"
reference = "https://attack.mitre.org/techniques/T1528/"


[rule.threat.tactic]
id = "TA0006"
name = "Credential Access"
reference = "https://attack.mitre.org/tactics/TA0006/"

[rule.new_terms]
field = "new_terms_fields"
value = ["user.id", "aws.cloudtrail.request_parameters"]
[[rule.new_terms.history_window_start]]
field = "history_window_start"
value = "now-15d"
```

https://github.com/elastic/detection-rules/blob/main/rules/integrations/aws/credential_access_new_terms_secretsmanager_getsecretvalue.toml

Mitigant
Be Secure. Be Resilient.

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)

Mitigant
Be Secure. Be Resilient.

Thank you for your attention

kennedy@mitigant.io
@run2obtain