German-American IT Security Forum

IT Security Association Germany (TeleTrusT) in cooperation with GACC – German American Chamber of Commerce

San Francisco, 06.05.2024

Cloud Attack Emulation: A Pragmatic Threat-Informed Defense Approach for Cloud Infrastructure

Kennedy Torkura, 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

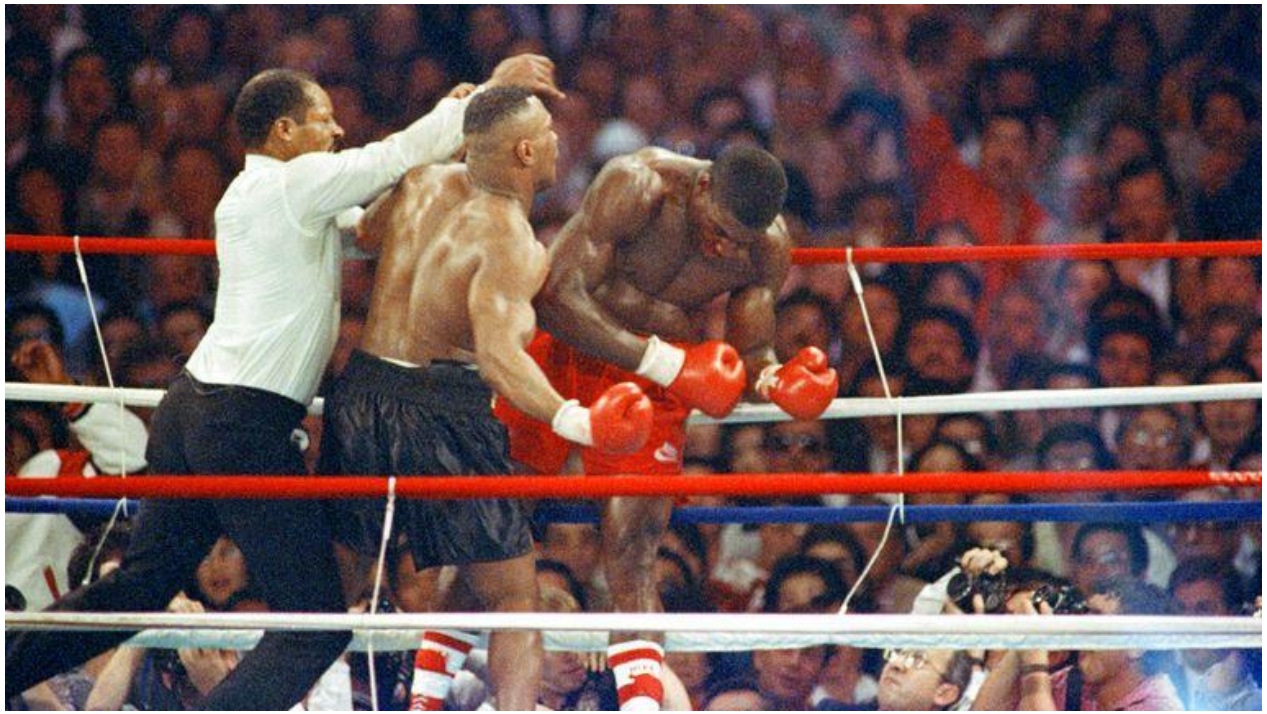
- Introduction
- Threat-Informed Defense
- Three Pillars of Threat-Informed Defense
- Adversary Emulation
- Cloud Attack Emulation
- Use Case: Validating Cloud Threat Detection

Every one has a plan until they get punched in the face.

- Mike Tyson

- Our aim in cybersecurity boils down to “keeping our organizations safe from cyberattacks”
- Keeping our eyes focused on the opponent is critical. .
- Misunderstanding or underestimating the capabilities of our opponent could be disastrous.

- A boxer’s focus in neither on the spectators nor on the referee.
- Boxers train for bouts with a tunnel focus on defeating their opponents, every other thing is secondary.



Learnings for Cybersecurity

- Focusing on our opponent (the attackers) is paramount for success.
- Other things are secondary, complementary.
- De-emphasize and/or balance focus on referees & spectators e.g. compliance-driven cybersecurity.

Getting Punched In the Face

Kennedy Torkura
Co-Founder & CTO at Mitigant | Cloud Attack Emulation
2 articles

April 27, 2024

Open Immersive Reader

All-time boxing legend Mike Tyson once said, "Everyone has a plan until they get punched in the face."

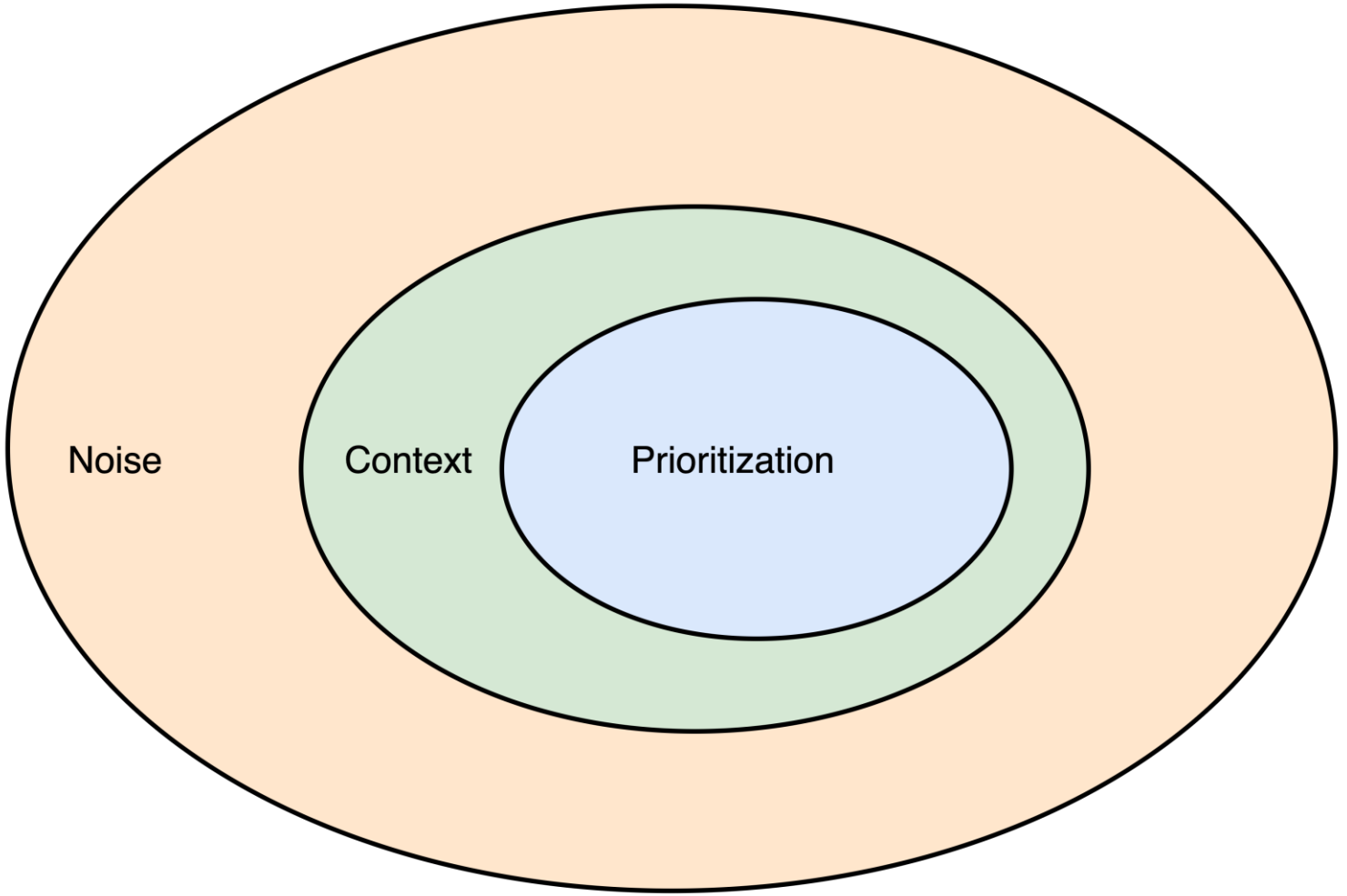
> Everyone has a plan until they get punched in the face.

Preparation is crucial, but what are you preparing for? This is the essence of Tyson's quote. It emphasizes the need for practical preparation and pl
without loosing sight of the opponent's inherent and unexpected capa
about ensuring that our efforts and resources are brutally geared towa
the inevitable confusion that appears in the face of the true realities of
preparing for ; *aka the aim of our preparation*.

Cybersecurity: Low Signals to Noise Ration

- 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.

Eventually what matters most MUST be prioritized !



.... But PRIORITIZATION is an age-old Cybersecurity Problem

Stakeholder Specific Vulnerability Categorization (SSVC)

CWE

CVSS
COMMON VULNERABILITY SCORING SYSTEM

MITRE | ATT&CK®

OWASP TOP10

CAPEC™

Known Exploited Vulnerabilities Catalog
cisa.gov

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

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

Pillar 01: Defensive Measures

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

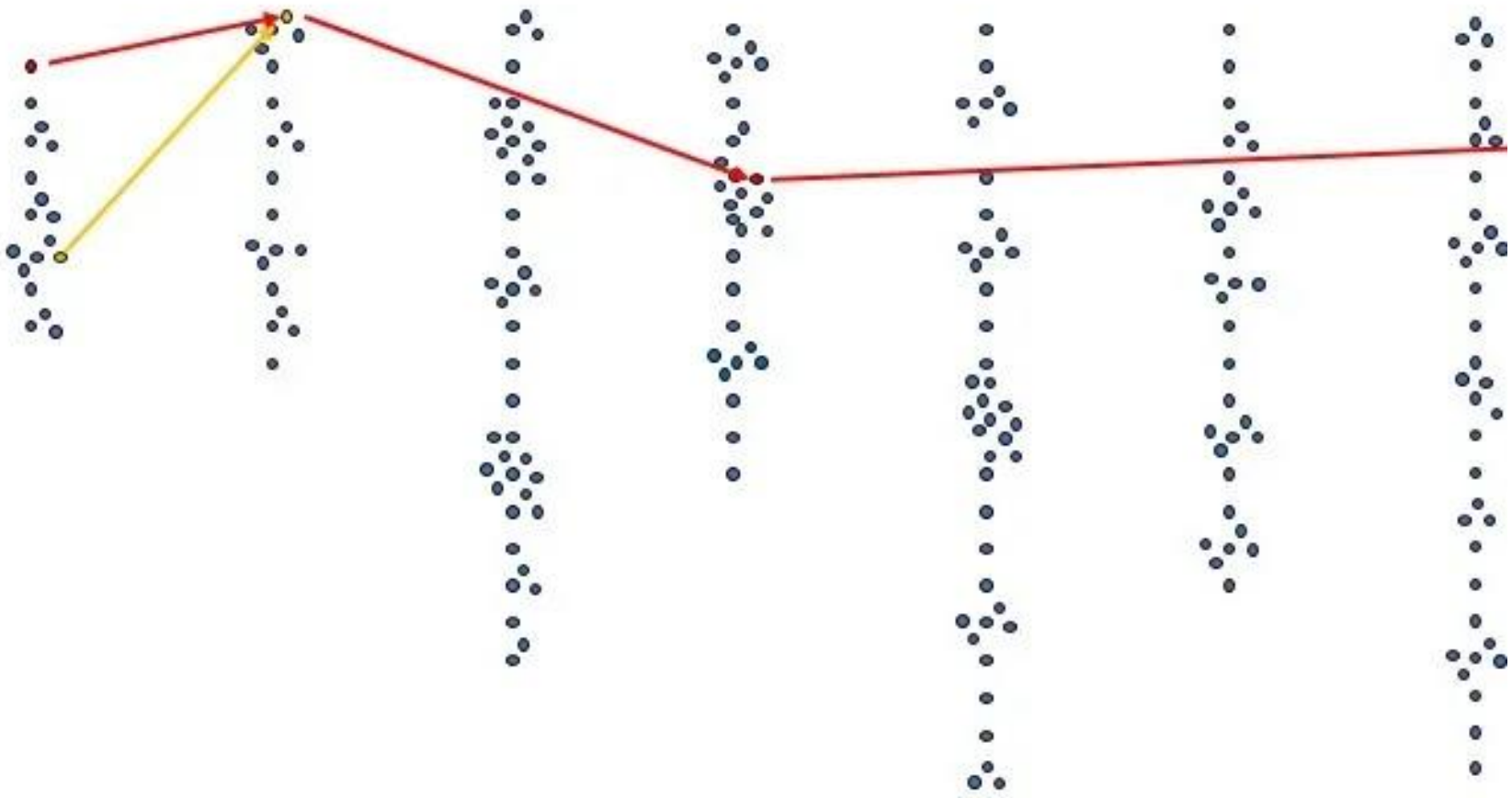
Pillar 01: Defensive Measures

Matrices (Technological Categories)

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

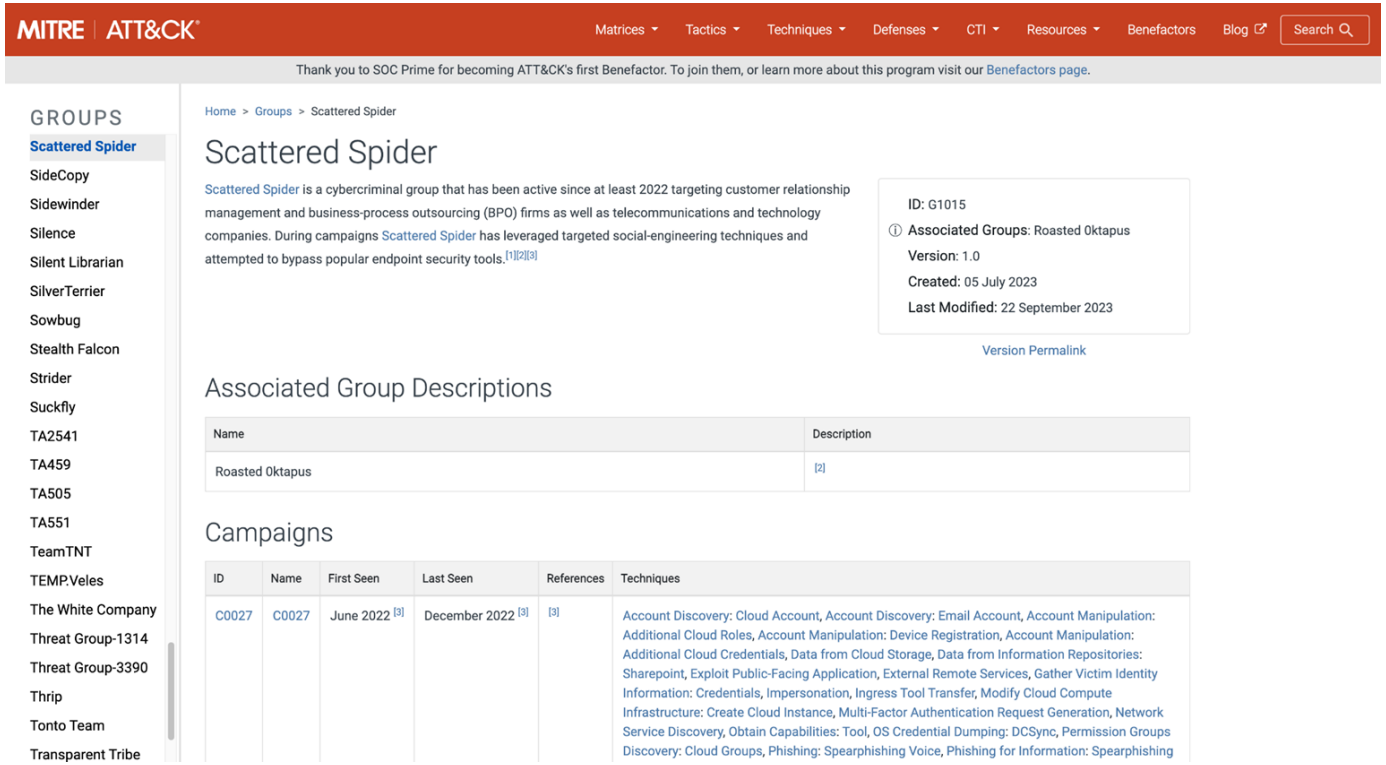
MITRE ATT&CK Matrix for Enterprises

MITRE ATT&CK Matrix for Enterprises



Pillar 02: Cyber Threat Intelligence

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



MGM Resorts breached by 'Scattered Spider' hackers: sources

By **Zeba Siddiqui** and **Christopher Bing**

September 13, 2023 4:15 PM PDT · Updated 8 months ago

[1/6] A view of MGM Grand hotel and casino signage, after MGM Resorts shut down some computer systems due to a cyber attack in Las Vegas, Nevada, U.S., September 13, 2023. REUTERS/Bridget Bennett *Purchase Licensing Rights*

MGM Resorts says cyberattack cost $100 million, resulted in theft of customer info

A recent cyberattack cost MGM Resorts about $100 million, the Las Vegas company said in a regulatory filing on Thursday.

In its filings with the Securities and Exchange Commission (SEC), the company also acknowledged that customer information ranging from Social Security numbers to passport data was stolen during the attack.

The company did not respond to requests for comment about how many people were affected. It filed breach notification documents with regulators in Maine but left the section related to the number of people affected empty.

After discovering the attack on September 11, MGM Resorts shut down all of its systems so that the hackers could not get access to customer information, disrupting several of their properties. They said about $100 million was lost in collective damage.

In addition to its namesake resort, the company owns Mandalay Bay, the Bellagio, The Cosmopolitan and the Aria. For days, everything from slot machines to restaurant management systems and even key cards for rooms were shut off due to the attack.

America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home / News & Events / Cybersecurity Advisories / Cybersecurity Advisory

CYBERSECURITY ADVISORY

Scattered Spider

Release Date: November 16, 2023 **Alert Code:** AA23-320A

RELATED TOPICS: CYBER THREATS AND ADVISORIES, MALWARE, PHISHING, AND RANSOMWARE

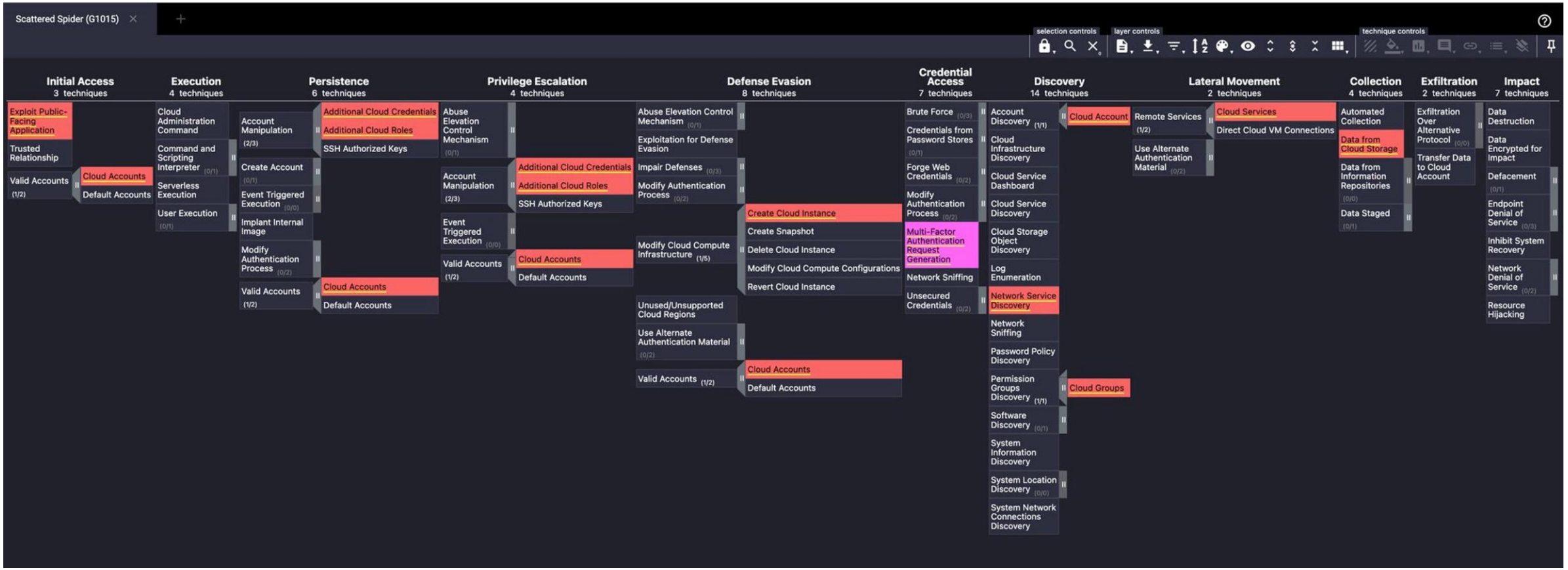
SUMMARY

The Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint Cybersecurity Advisory (CSA) in response to recent activity by Scattered Spider threat actors against the commercial facilities sectors and subsectors. This advisory provides tactics, techniques, and procedures (TTPs) obtained through FBI investigations as recently as November 2023.

Scattered Spider is a cybercriminal group that targets large companies and their contracted information technology (IT) help desks. Scattered Spider threat actors, per trusted third parties, have typically engaged in data theft for extortion and have also been known to utilize BlackCat/ALPHV ransomware alongside their usual TTPs.

The FBI and CISA encourage critical infrastructure organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of a cyberattack by Scattered Spider actors.

Cyber Threat Intelligence- Threat Actor Context (Scattered Spider)



Pillar 03: Testing and Evaluation

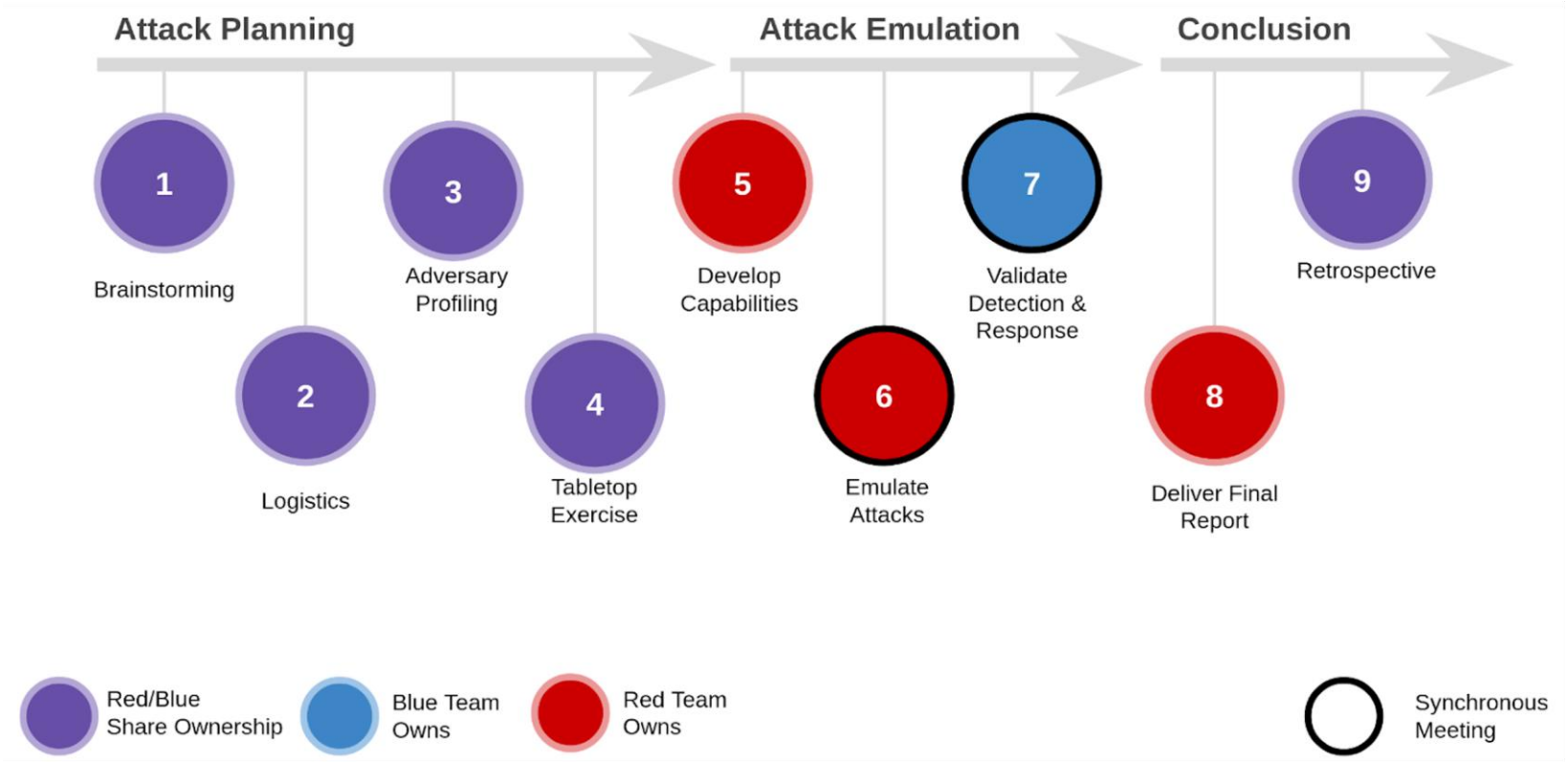
MITRE ENGENUITY recommends the use of Adversary emulation for testing and evaluating defenses.

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 ?

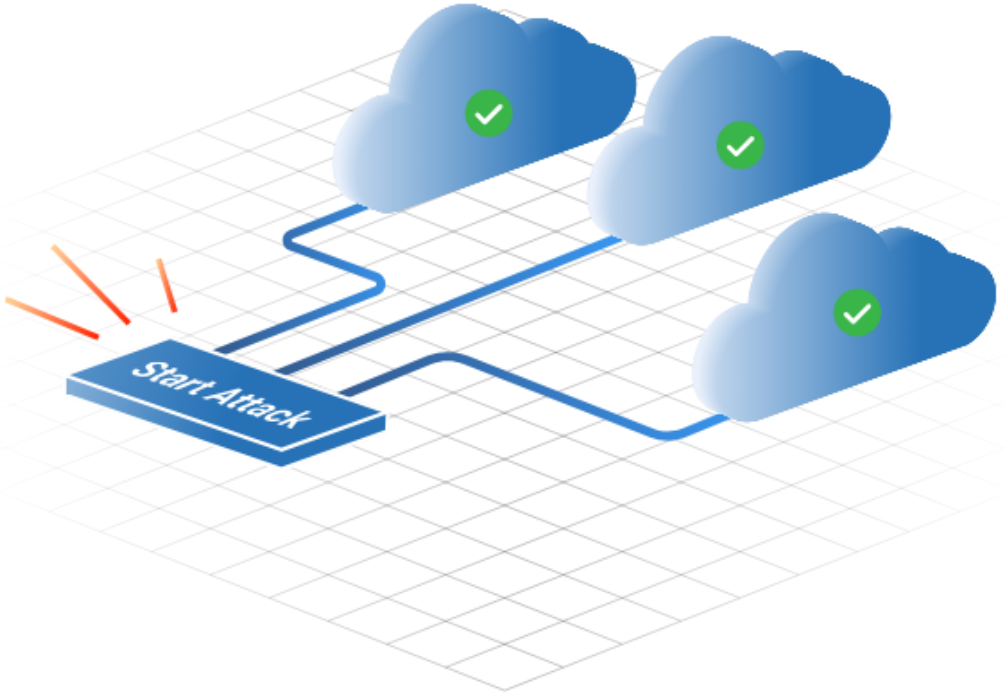
Adversary Emulation Workflow



GitLab Security team's Attack Emulation Workflow

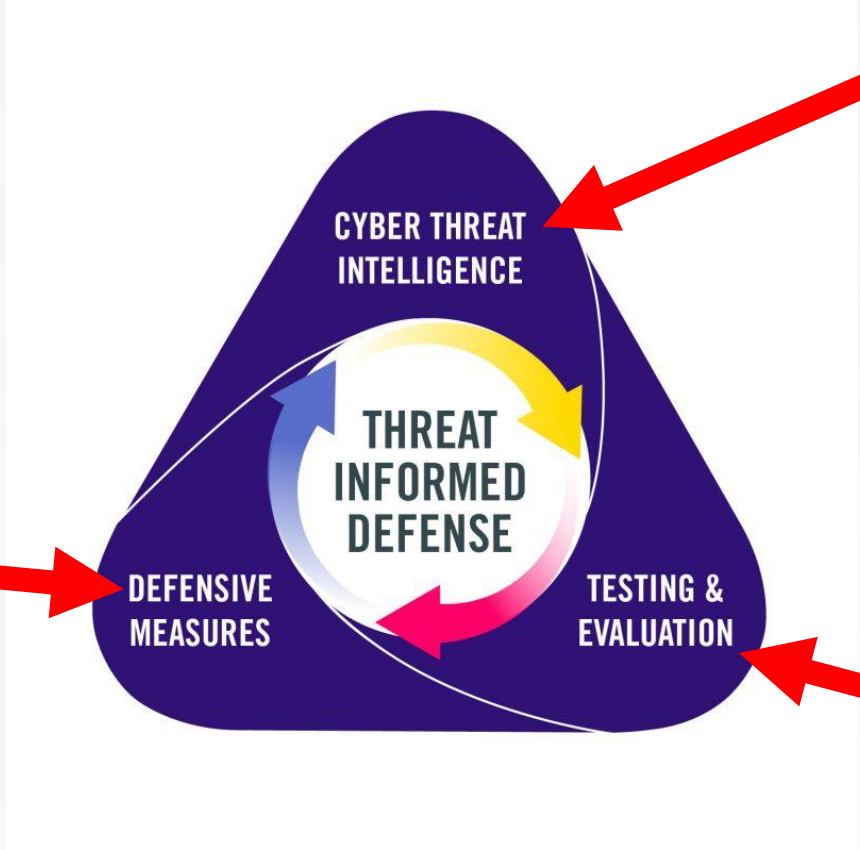
Cloud Attack Emulation – Adversary Emulation for the Cloud

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



Example Use-Case: Validating Threat Actors

Scattered Spider Threat Actor

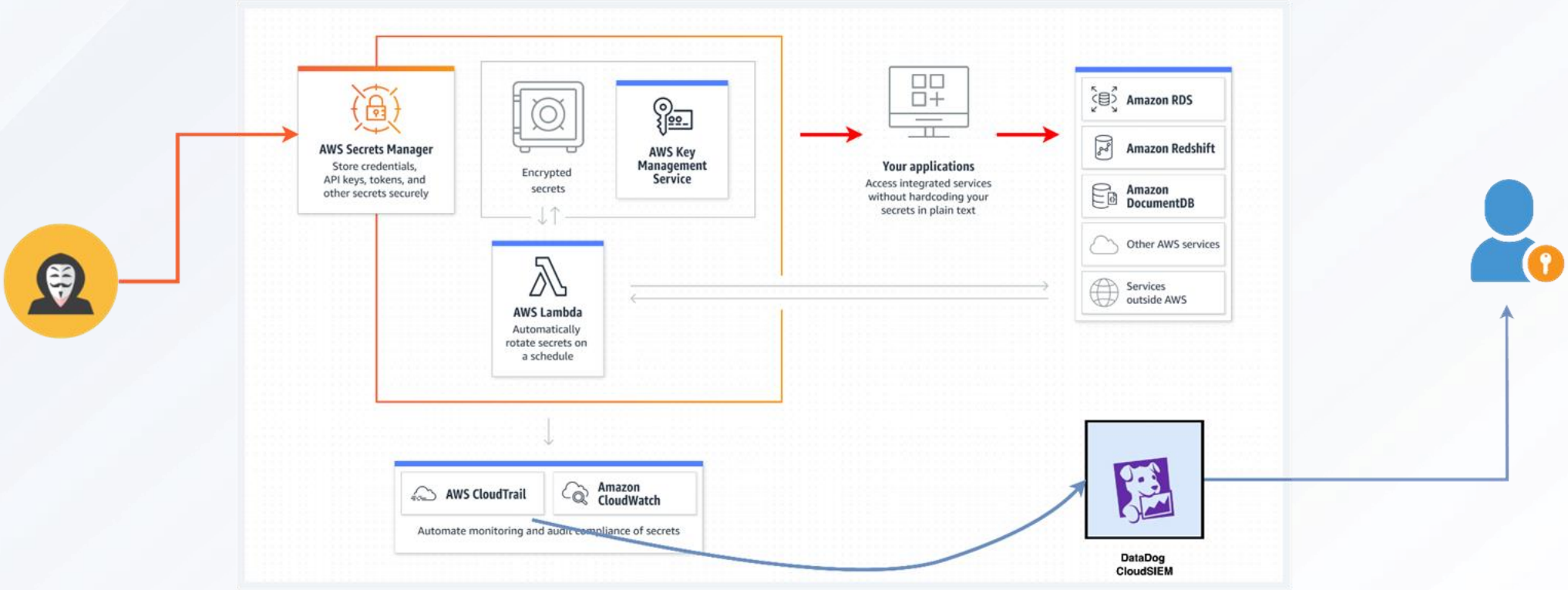


Scattered Spider Techniques

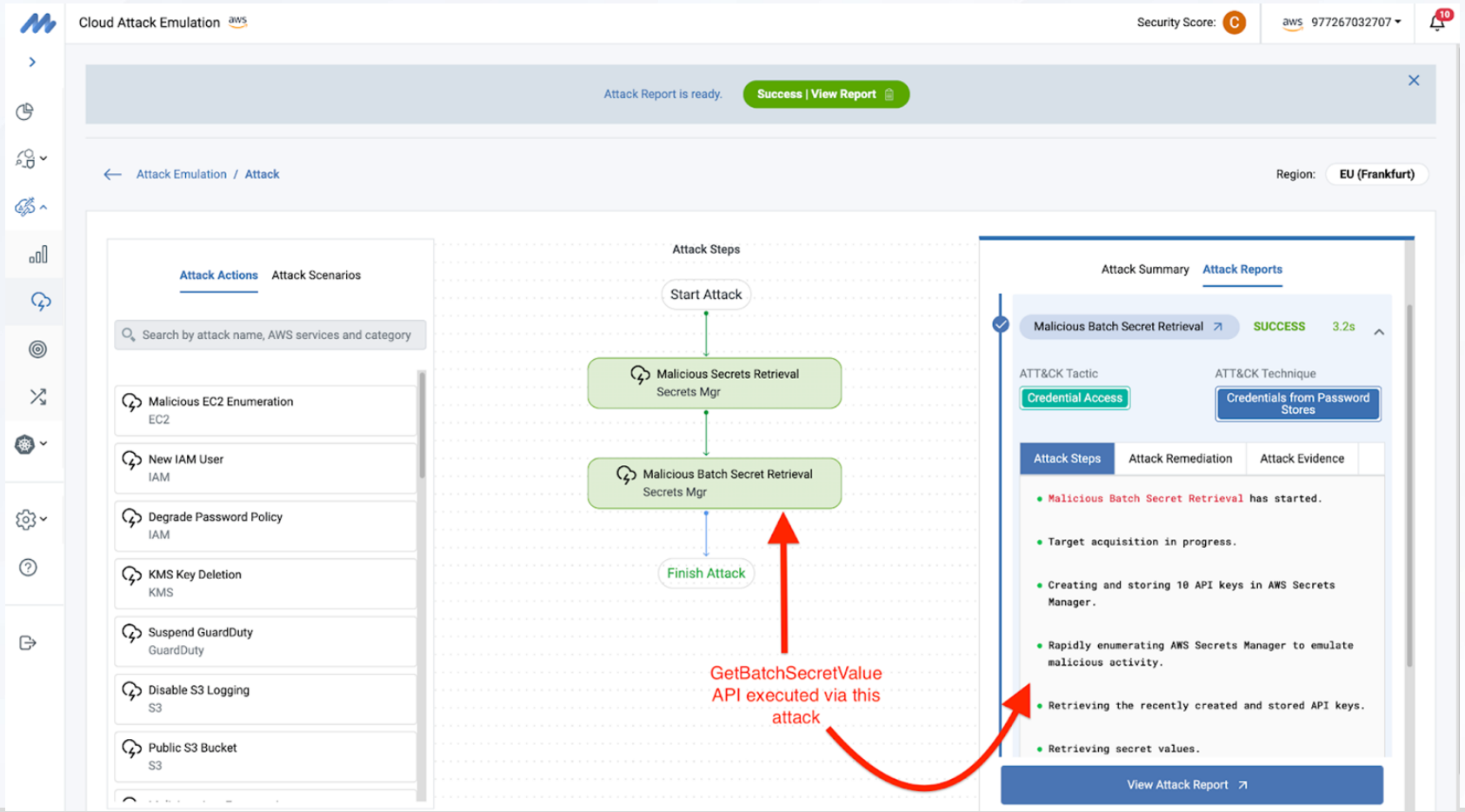
- **T1555.006**

Adversary Emulation of Scattered Spider TTPs

Credential from Password Stores: Cloud Secrets Management Stores

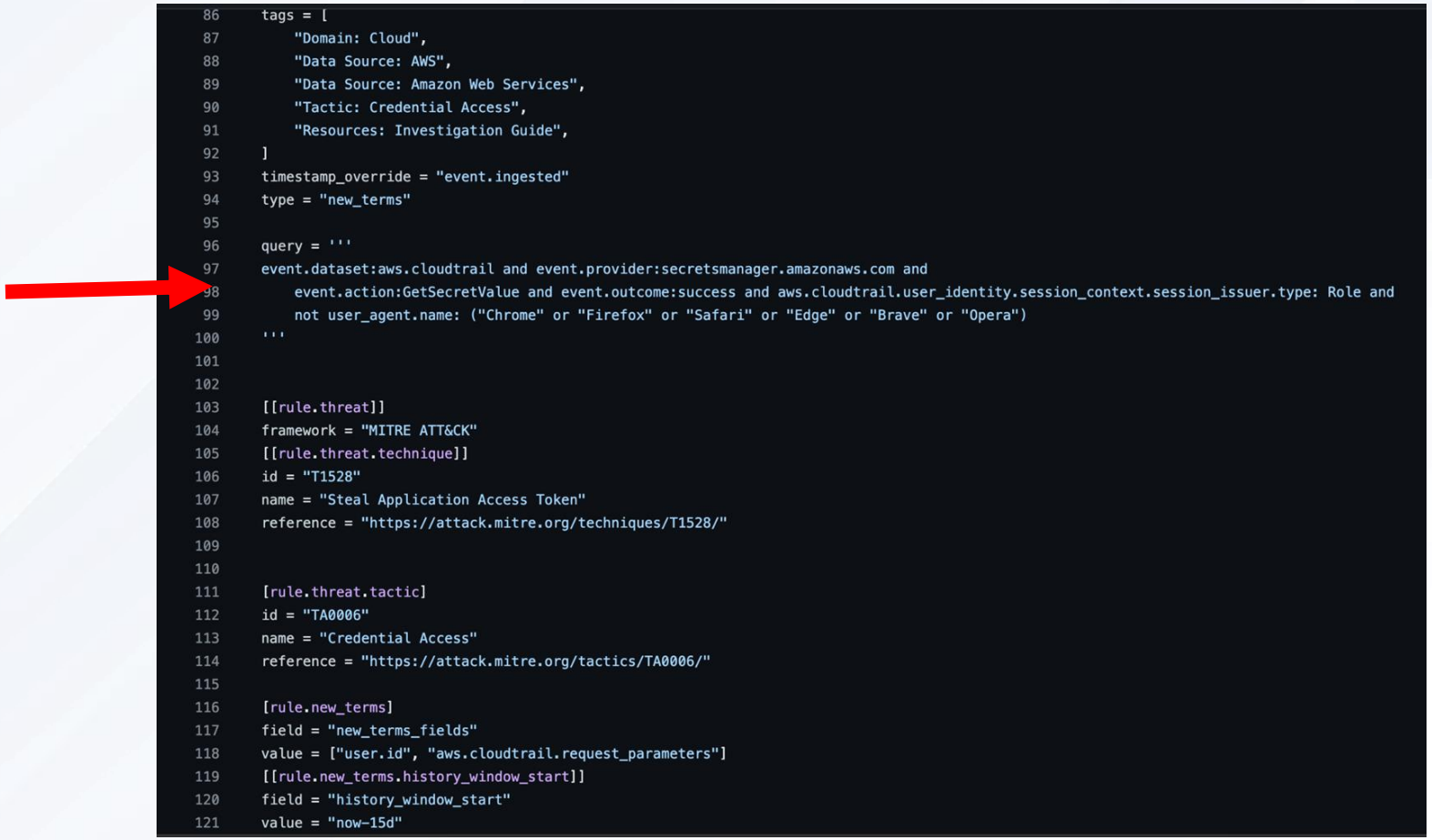


Emulating the Attack



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"
    ]
},
```



```
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"
```

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

Conclusion

- Identifying and focusing on the most important threats is important for efficient cybersecurity
- Most prioritization approaches still suffer from realism and aren't threat-focused.
- Threat-Informed Defense allows organizations to leverage real-world insights to identify and focus on the threats that really matter.
- Cloud Attack Emulation enhances Threat-Informed Defense by further cutting down noise and validating cybersecurity measures and reducing alert fatigue.

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