

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.**

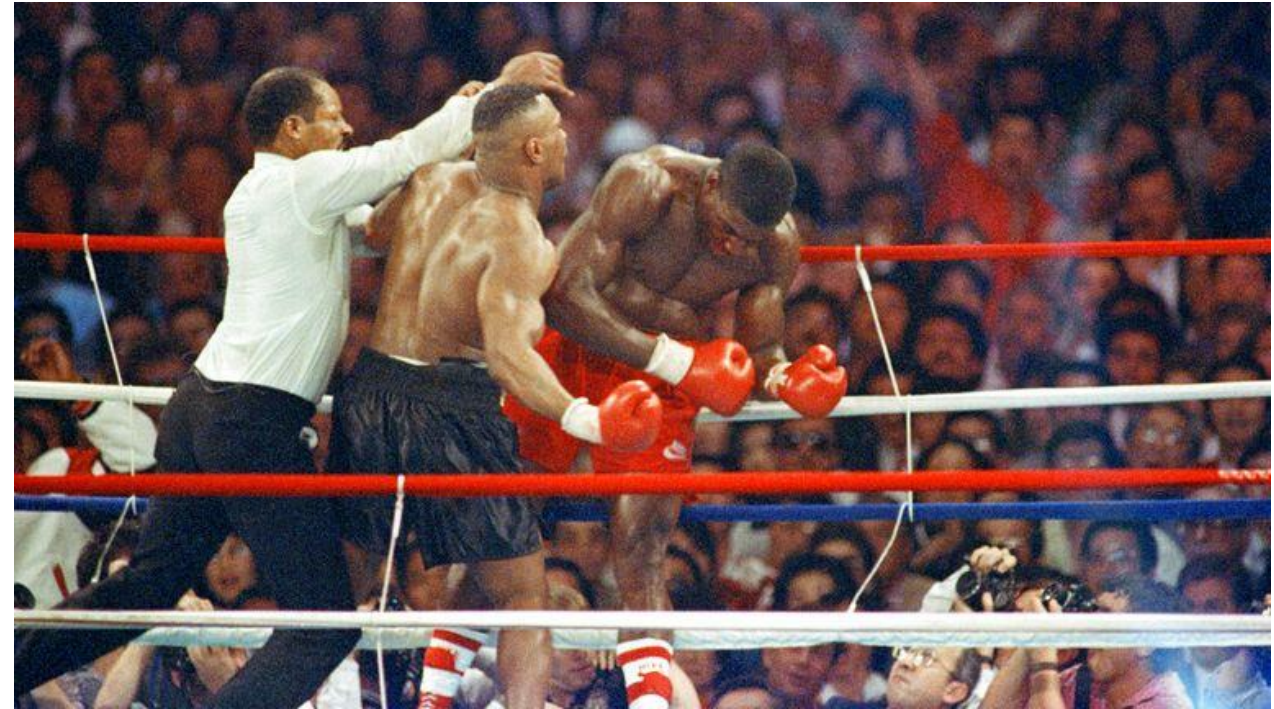
- Mike Tyson



- 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.

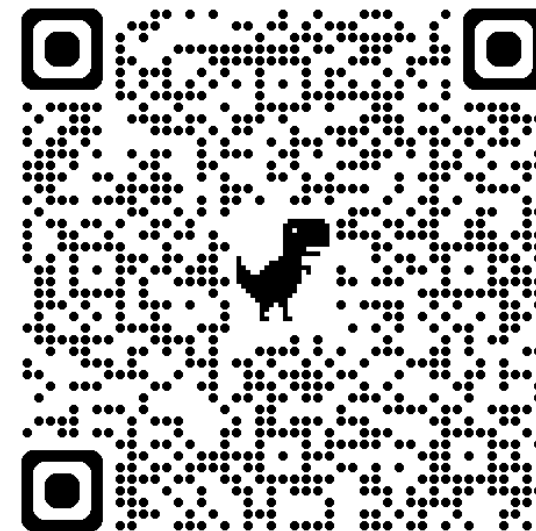
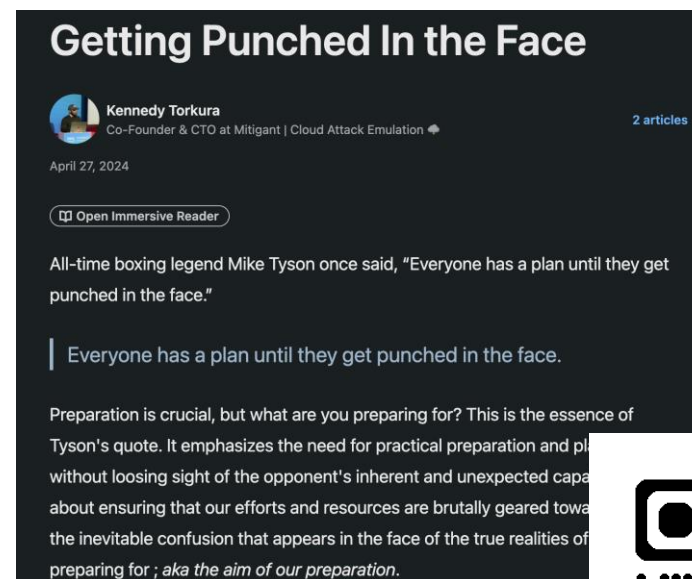


- A boxer's focus is neither on the spectators nor on the referee.
- Boxers train for bouts with a tunnel focus on defeating their opponents, every other thing is secondary.



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.

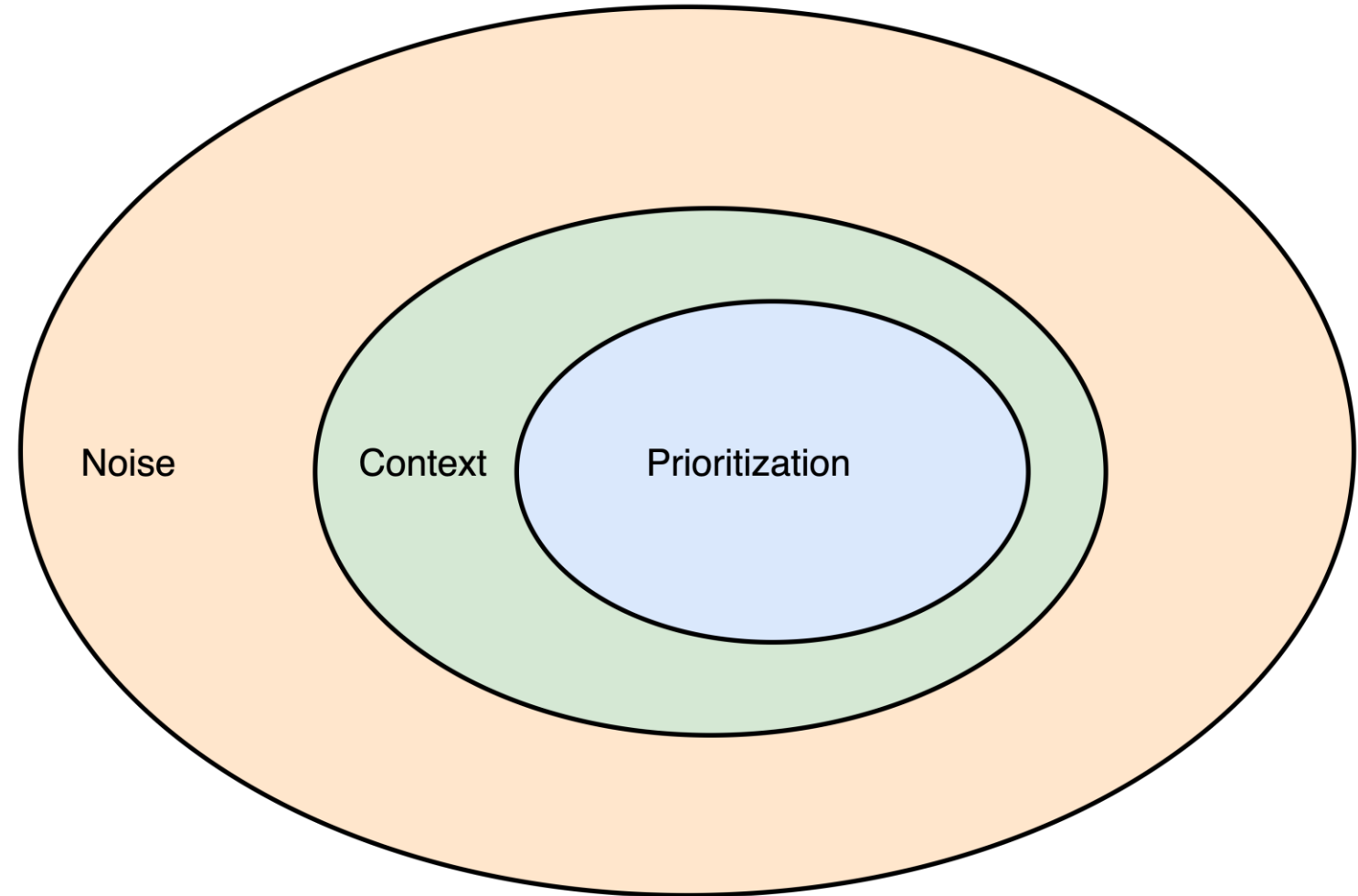


Cybersecurity: Low Signals to Noise Ratio

- 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)

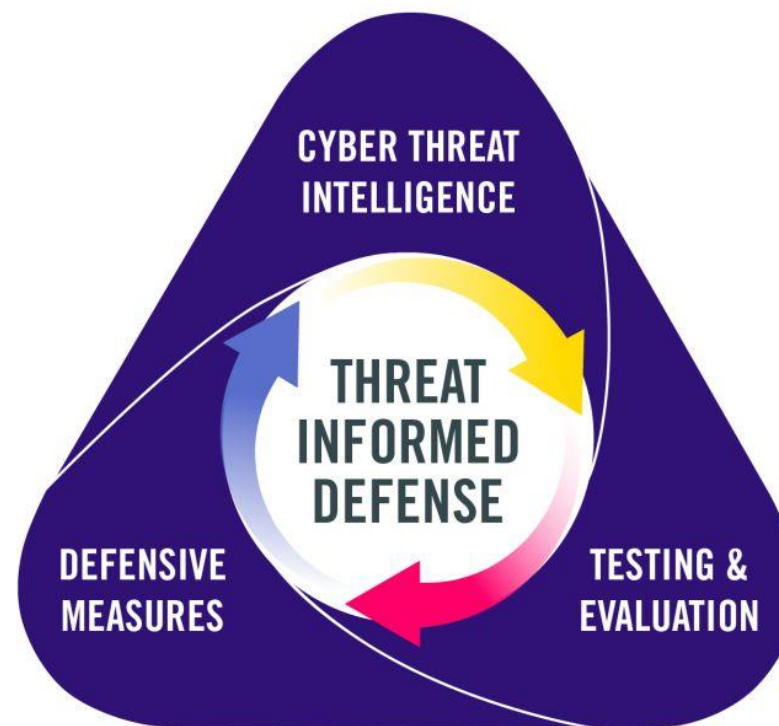


MITRE | ATT&CK®



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.

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

Pillar 01: Defensive Measures

Matrices (Technological Categories)

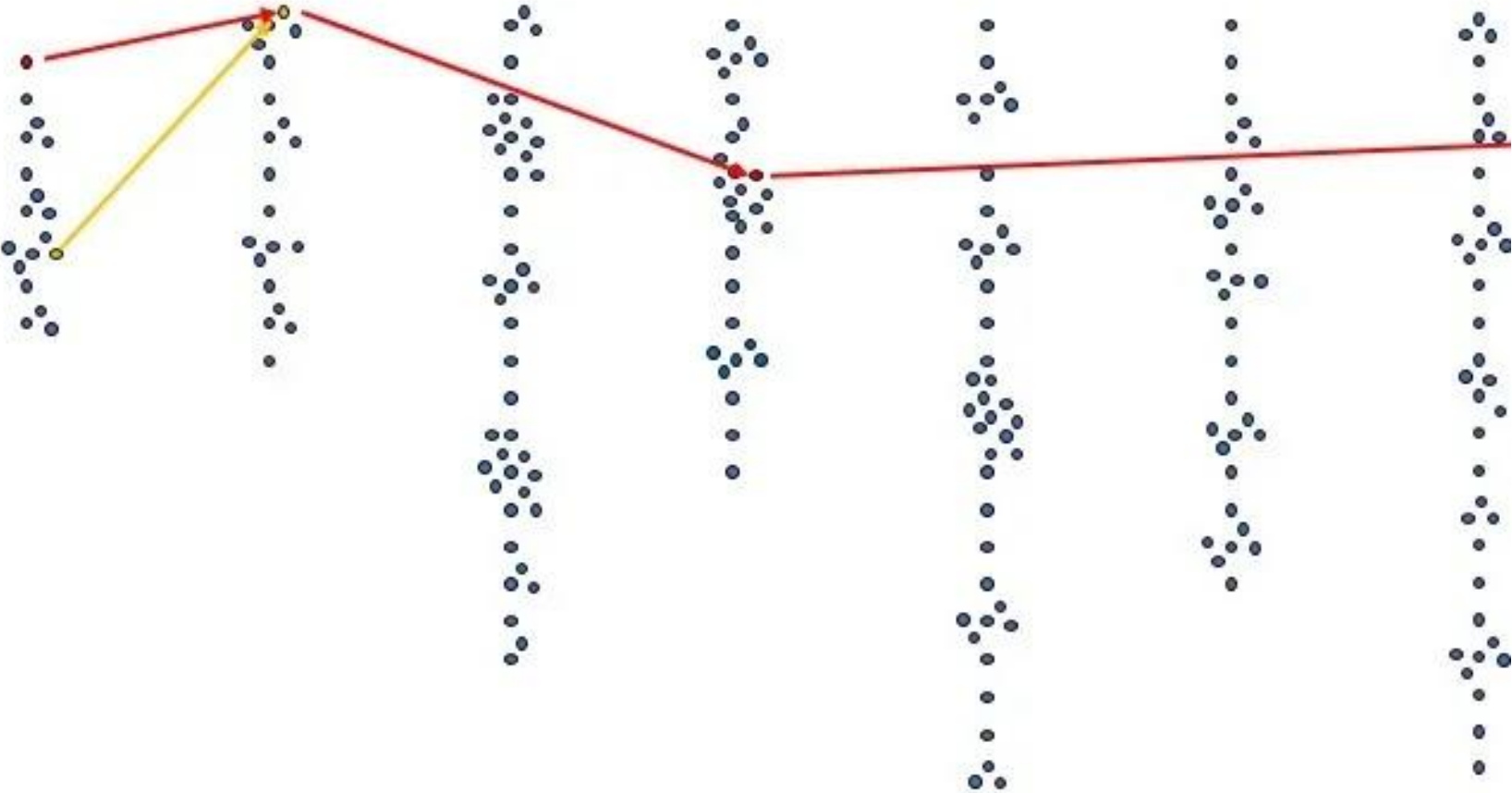
- Enterprise Matrix : 14 Tactics & 234 Techniques
- Mobile Matrix
- ICS Matrix

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

MITRE ATT&CK Matrix for Enterprises

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 Autostart Scripts (5)	Boot or Logon Initialization Scripts (5)	Debugger Evasion	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)	Deobfuscate/Decode Files or Information	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)	Deploy Container	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)	Direct Volume Access	Input Capture (4)	Cloud Storage Object Discovery	Data from Cloud Storage	Data from Configuration Repository (2)	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 (11)	Domain Policy Modification (2)	Modify Authentication Process (8)	Container and Resource Discovery	Data from Information Repositories (3)	Software Deployment Tools	Fallback Channels	Scheduled Transfer	Financial Theft
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Escape to Host	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	Debugger Evasion	Data from Local System	Taint Shared Content	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	File and Directory Permissions Modification (2)	Multi-Factor Authentication Request Generation	Device Driver Discovery	Data from Network Shared Drive	Use Alternate Authentication Material (4)	Multi-Stage Channels	Resource Hijacking	Inhibit System Recovery
			Software Deployment Tools	External Remote Services	Hijack Execution Flow (12)	Hide Artifacts (11)	Network Sniffing	File and Directory Discovery	Data from Removable Media		Non-Application Layer Protocol	Service Stop	Network Denial of Service (2)
			System Services (2)	Hijack Execution Flow (12)	Impersonation	Hijack Execution Flow (12)	OS Credential Dumping (8)	Group Policy Discovery	Data from Shared Drive		Non-Standard Port	System Shutdown/Reboot	
			User Execution (3)	Implant Internal Image	Indicator Removal (9)	Impair Defenses (11)	Steal Application Access Token	Log Enumeration	Data from Shared Drive		Protocol Tunneling		
			Windows Management Instrumentation	Modify Authentication Process (8)	Indirect Command Execution	Impersonation	Steal or Forge Authentication Certificates	Network Service Discovery	Data from Shared Drive		Proxy (4)		
				Office Application Startup (4)	Masquerading (9)	Impersonation	Modify Authentication Process (8)	Network Share Discovery	Data from Shared Drive		Remote Access Software		
				Power Settings	Power Settings	Masquerading (9)	Steal or Forge Authentication Certificates	Network Sniffing	Data from Shared Drive		Traffic Signaling (2)		
						Masquerading (9)	Steal or Forge Authentication Certificates	Password Policy Discovery	Data from Shared Drive				
						Masquerading (9)	Steal or Forge Authentication Certificates	Peripheral Device Discovery	Data from Shared Drive				

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.

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 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 [1]	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

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

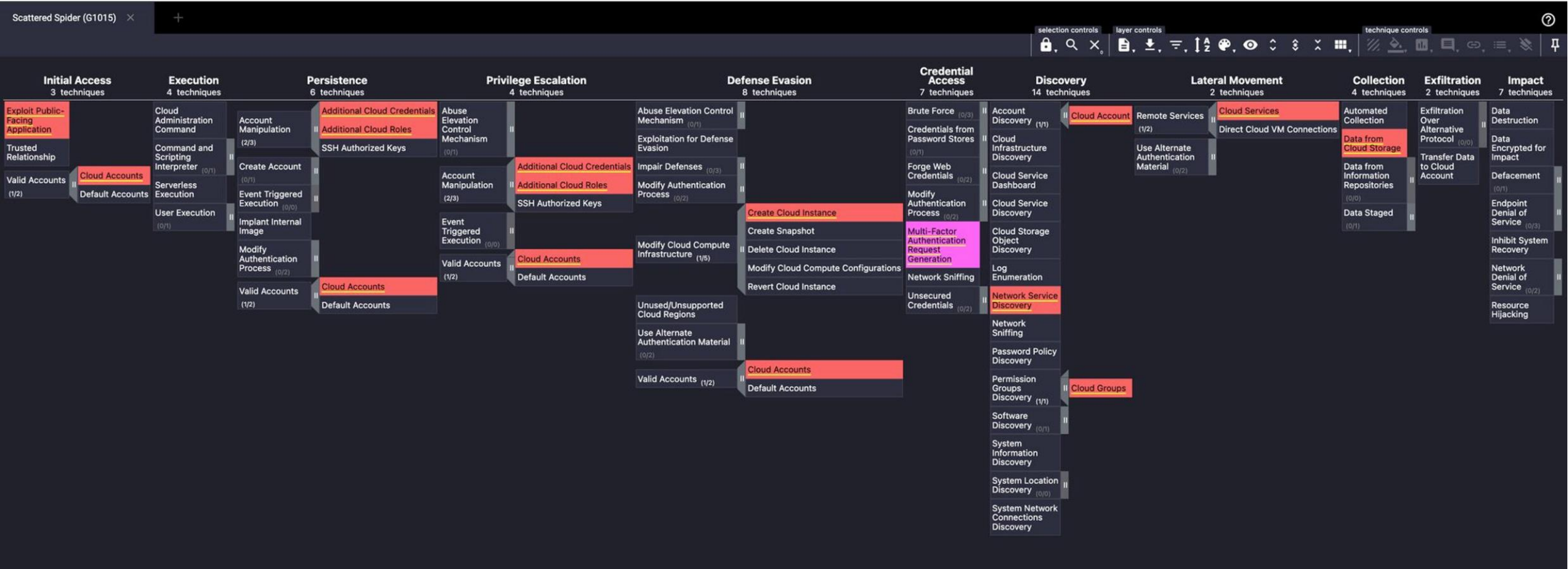
SUMMARY

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.

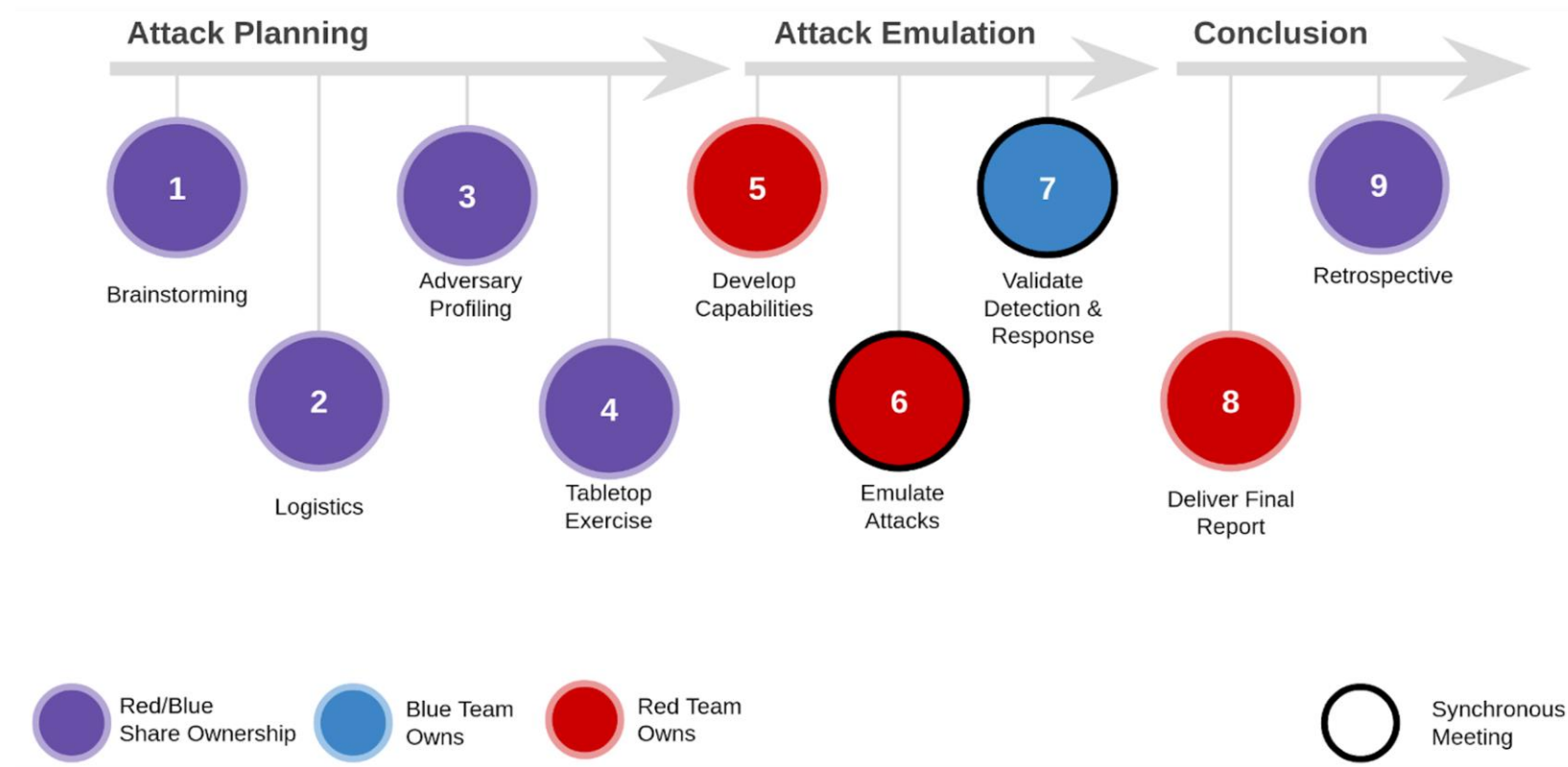


Why Adversary Emulation ?

- 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 ?



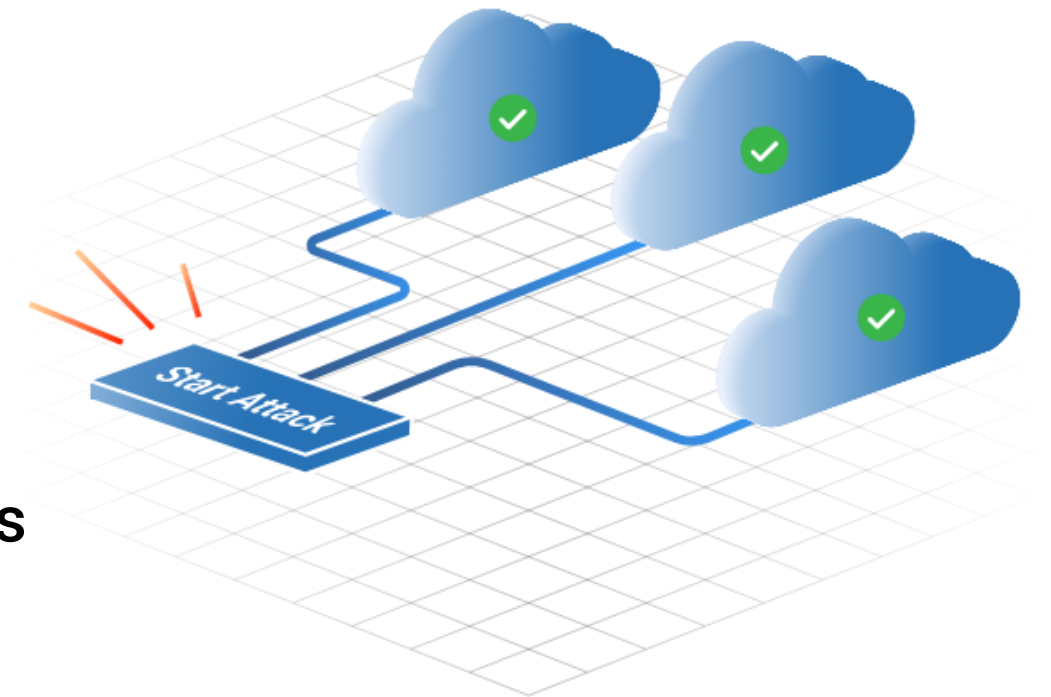
Adversary Emulation Workflow



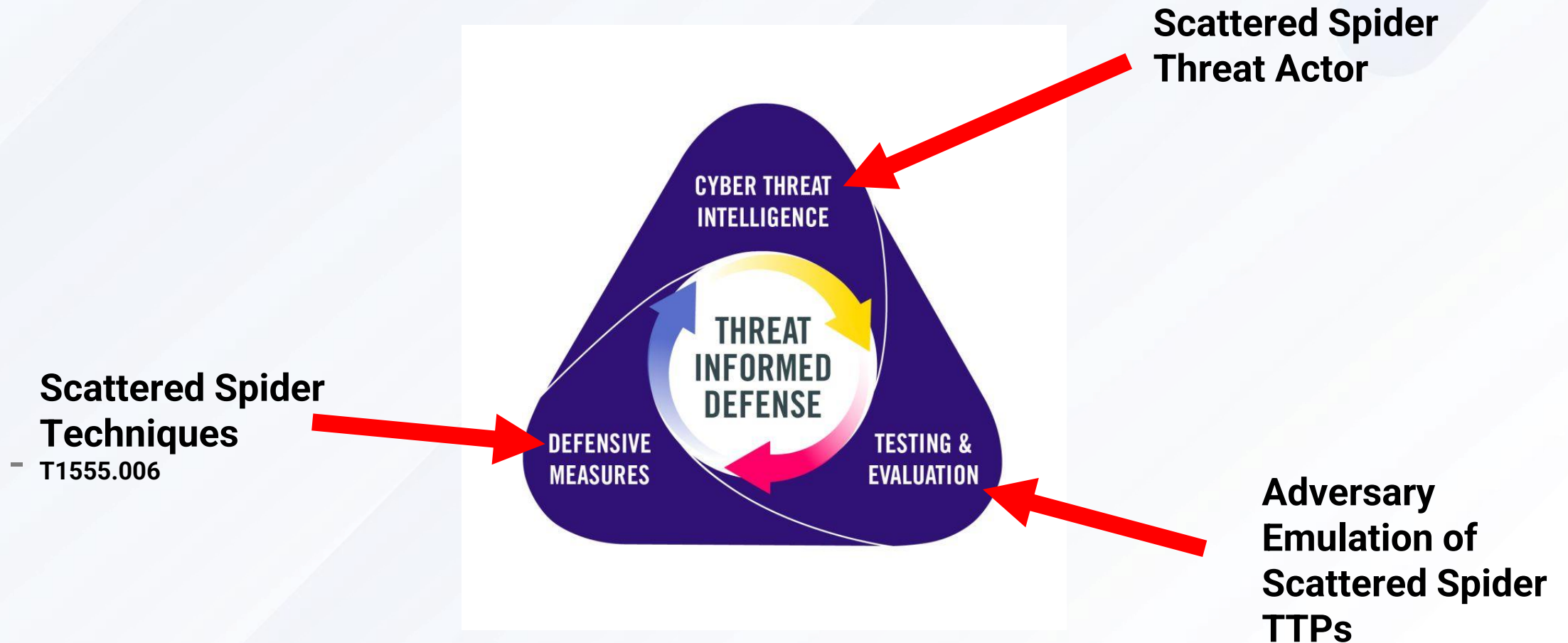
GitLab Security team's Attack Emulation Workflow

Cloud Attack Emulation – Adversary Emulation for the Cloud

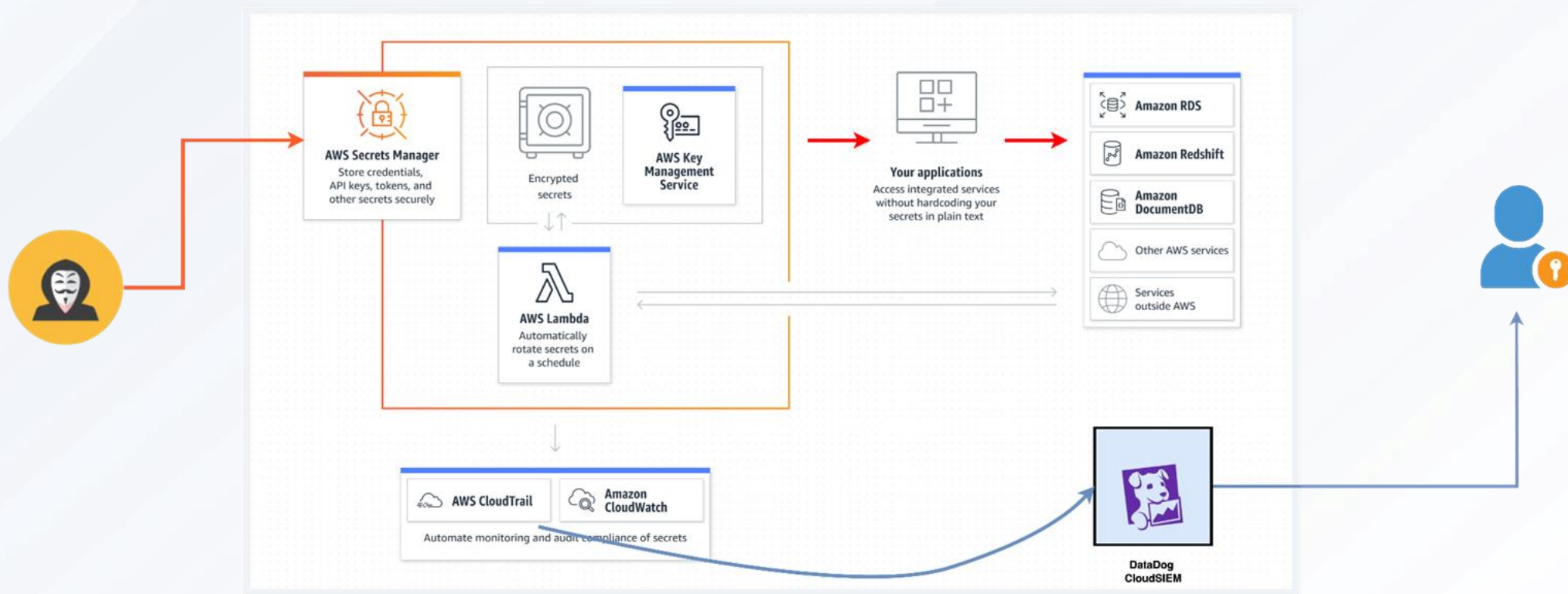
- Adversary emulation for the cloud.
- Efficient of mimicking of real-world threats that target cloud-native infrastructure.
- Cloud attack emulation is designed to address cloud-specific challenges.



Example Use-Case: Validating Threat Actors



Credential from Password Stores: Cloud Secrets Management Stores



Emulating the Attack

Cloud Attack Emulation 

Security Score:  aws 977267032707 

Attack Report is ready. [Success | View Report](#)

← Attack Emulation / Attack Region: EU (Frankfurt)

Attack Actions Attack Scenarios

Search by attack name, AWS services and category

- Malicious EC2 Enumeration EC2
- New IAM User IAM
- Degrade Password Policy IAM
- KMS Key Deletion KMS
- Suspend GuardDuty GuardDuty
- Disable S3 Logging S3
- Public S3 Bucket S3

Attack Steps

Start Attack

Malicious Secrets Retrieval Secrets Mgr

Malicious Batch Secret Retrieval Secrets Mgr

Finish Attack

GetBatchSecretValue API executed via this attack

Attack Summary Attack Reports

Malicious Batch Secret Retrieval [SUCCESS](#) 3.2s

ATT&CK Tactic: Credential Access ATT&CK Technique: Credentials from Password Stores

Attack Steps	Attack Remediation	Attack Evidence
- 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. - Retrieving secret values.		

[View Attack Report](#)

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