THE CTI CLOUD CONTEXT DILEMMA

Evaluating and building CTI for the Cloud

Neil Thacker, CISO EMEA @ Netskope
nthacker@netskope.com
@nt_hacker

$WHOAMI

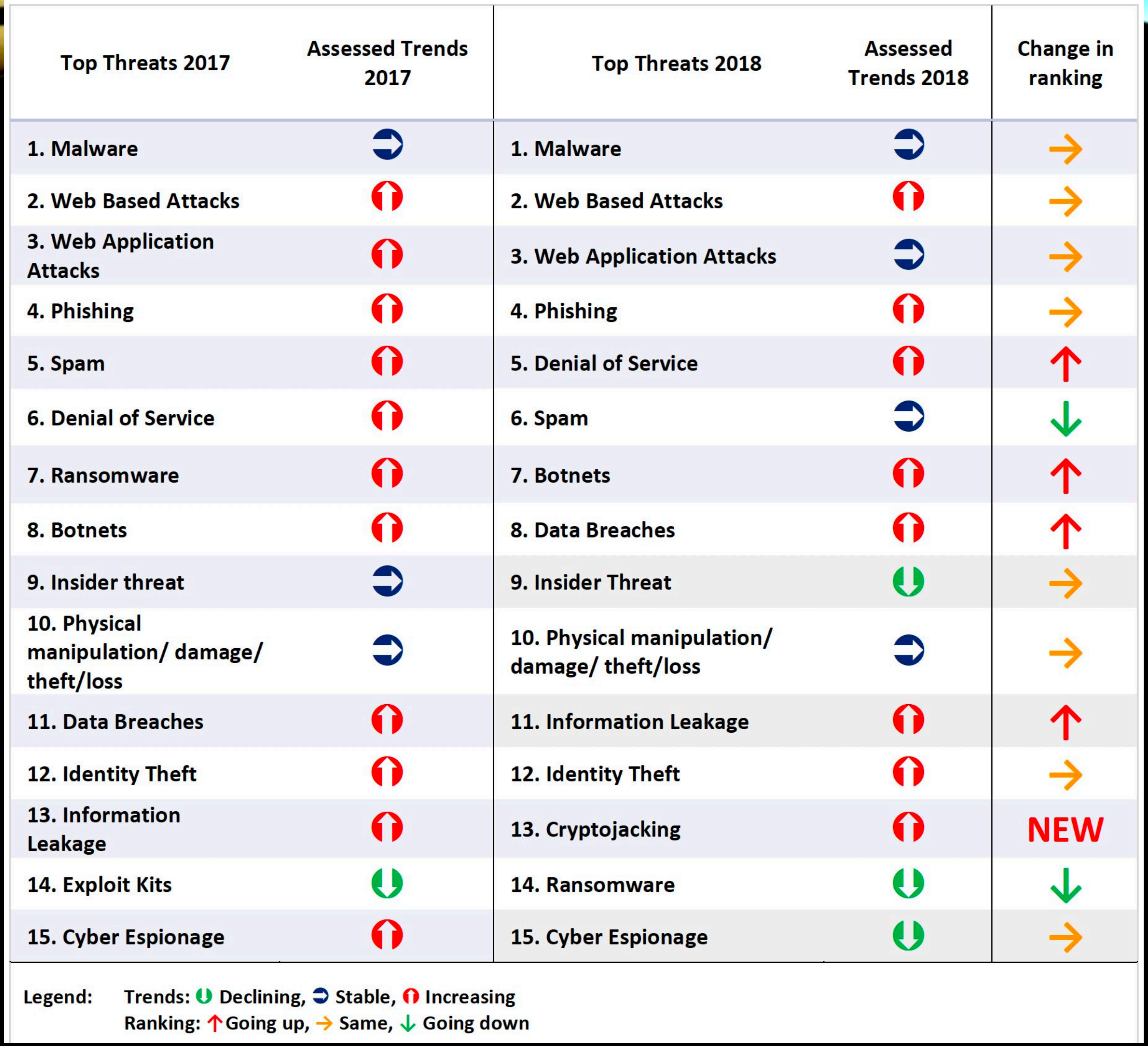
- 20 years experience in Information Security, Threat protection & Data protection
- Swiss Re, Deutsche Bank, Camelot, Websense, Netskope
- CISSP, CIPP/E, CEH

- Co-founder Security Advisor Alliance (CISO non-profit)
- Advisory Board member to CSA EMEA
- Advisory Board member to NeuroCyber
- ENISA Threat Landscape Stakeholder

AGENDA

- ENISA THREAT LANDSCAPE (for CLOUD)
- MITRE ATT&CK CLOUD MATRIX
- 3 CASE STUDIES (TTPs)
  - EXPLOITING IAM PERMISSIONS (GCP)
  - EXPLOITING TEMP CREDS (AWS)
  - SLUB COVERT C2 & DATA EXFIL
- CONCLUSION – Q&A

- Top 3 threats remain unchanged
- Web attacks are also Cloud attacks
- Top 3 threats used in common kill-chain/attack loop
- Cryptojacking entry primarily due to IaaS and browser plug-in
- New 2019/2020 report will be issued in Feb/March 2020



Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	⇨	1. Malware	⇨	→
2. Web Based Attacks	⇧	2. Web Based Attacks	⇧	→
3. Web Application Attacks	⇧	3. Web Application Attacks	⇨	→
4. Phishing	⇧	4. Phishing	⇧	→
5. Spam	⇧	5. Denial of Service	⇧	↑
6. Denial of Service	⇧	6. Spam	⇨	↓
7. Ransomware	⇧	7. Botnets	⇧	↑
8. Botnets	⇧	8. Data Breaches	⇧	↑
9. Insider threat	⇨	9. Insider Threat	⇩	→
10. Physical manipulation/ damage/ theft/loss	⇨	10. Physical manipulation/ damage/ theft/loss	⇨	→
11. Data Breaches	⇧	11. Information Leakage	⇧	↑
12. Identity Theft	⇧	12. Identity Theft	⇧	→
13. Information Leakage	⇧	13. Cryptojacking	⇧	NEW
14. Exploit Kits	⇩	14. Ransomware	⇩	↓
15. Cyber Espionage	⇧	15. Cyber Espionage	⇩	→

Legend: Trends: ⇩ Declining, ⇨ Stable, ⇧ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

ENISA THREAT LANDSCAPE 2018/2019

- "Researchers suggest that web-application attacks often result in larger data breaches. **Not surprisingly, cloud infrastructure seems to be the most attractive target for malicious actors**"

- "The average cost of a cybersecurity breach increased 6.4% in 2018. Notably, the average size of a data breach is typically amplified by 2.2%. **Third-party involvement and extensive cloud migration at the time of a breach increases the cost."**

- "**Cryptojacking hits cloud's high-powered resources.** Cryptojacking is one of the major issues found in cloud environments. The recent incident with cryptojacking activity in the cloud environments of Tesla, Aviva, Gemalto and LA Times are indicative of the trend. Moreover, cloud threats also include cryptomining via Docker and Kubernetes as well as hacked serverless functions."

enisa

netskope

MITRE ATT&CK

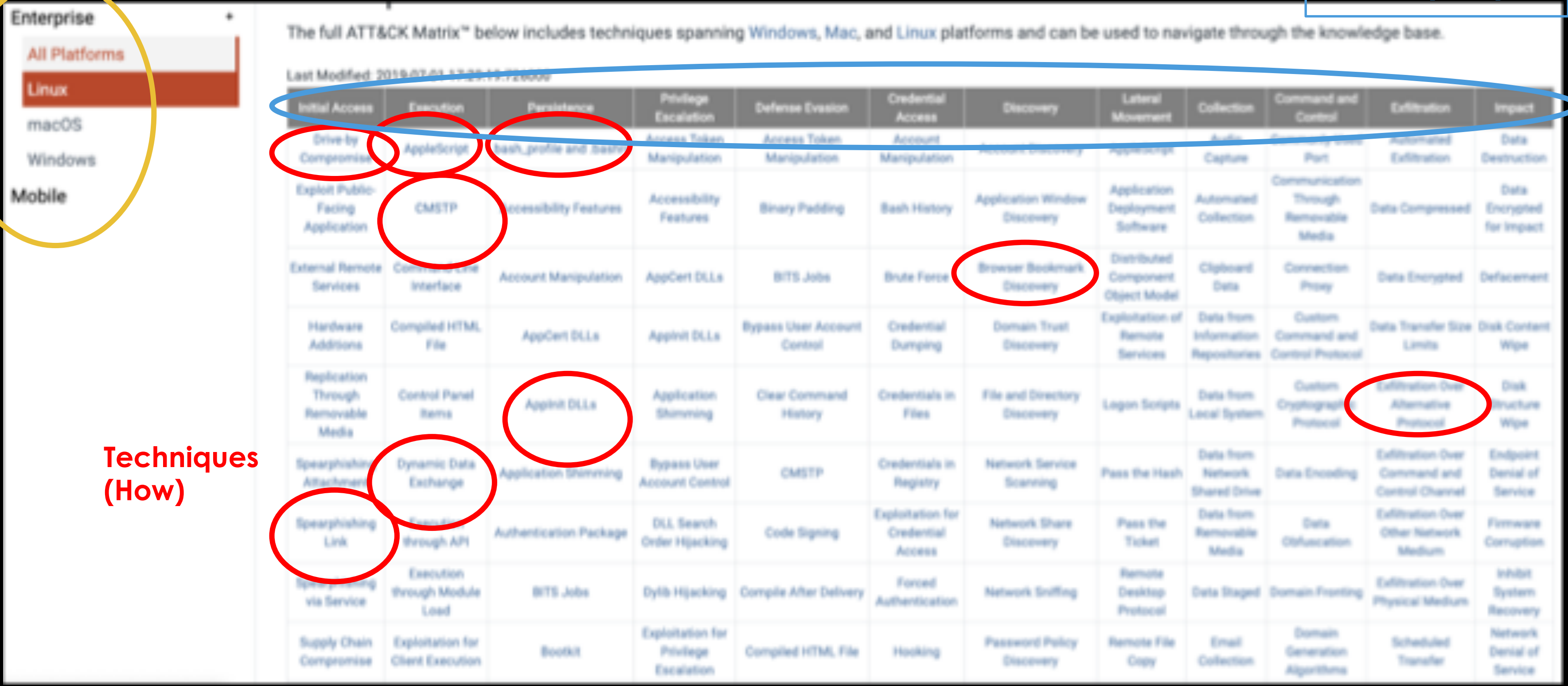
MITRE ATT&CK™ is a knowledge base of adversary tactics and techniques based on real-world observations. It is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

The MITRE ATT&CK framework is a structured model for understanding and analyzing the behavior (the tactics and techniques) of adversaries (i.e. actor groups and malware) and their attacks, as well as procedures to detect and mitigate such attacks.

MITRE ATT&CK MATRIX (NOTE: NO CLOUD DOMAIN 8TH OCT 2019)

Domains

Tactics (Why)



- Enterprise
  - All Platforms
  - Linux
  - macOS
  - Windows
- Mobile

The full ATT&CK Matrix™ below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the knowledge base.

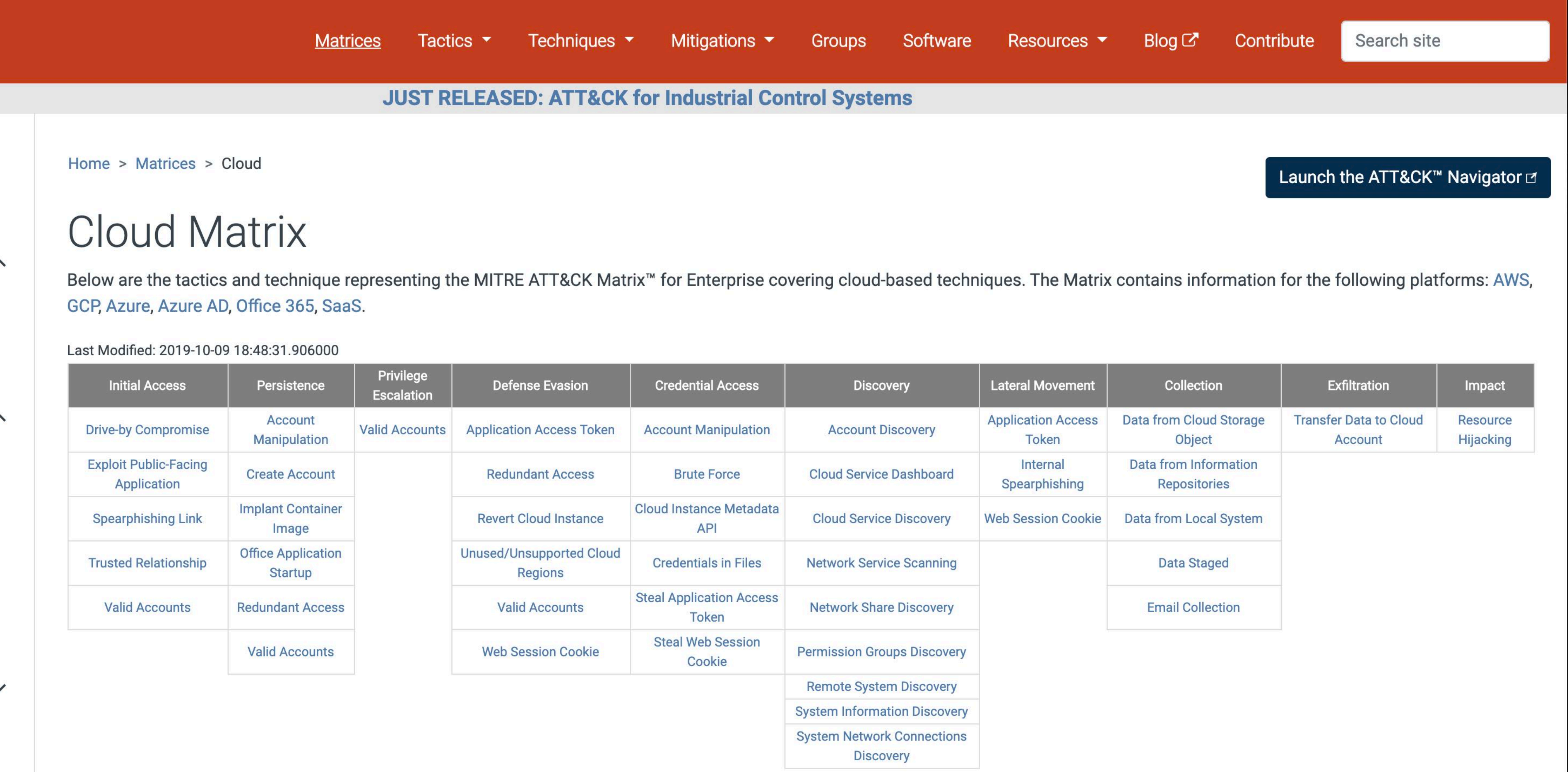
Last Modified: 2019-07-01 17:23:19.726000

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service

Techniques (How)

Source: https://attack.mitre.org/matrices/enterprise/

2020 © Netskope Inc. All rights reserved.



JUST RELEASED: ATT&CK for Industrial Control Systems

Home > Matrices > Cloud

Cloud Matrix

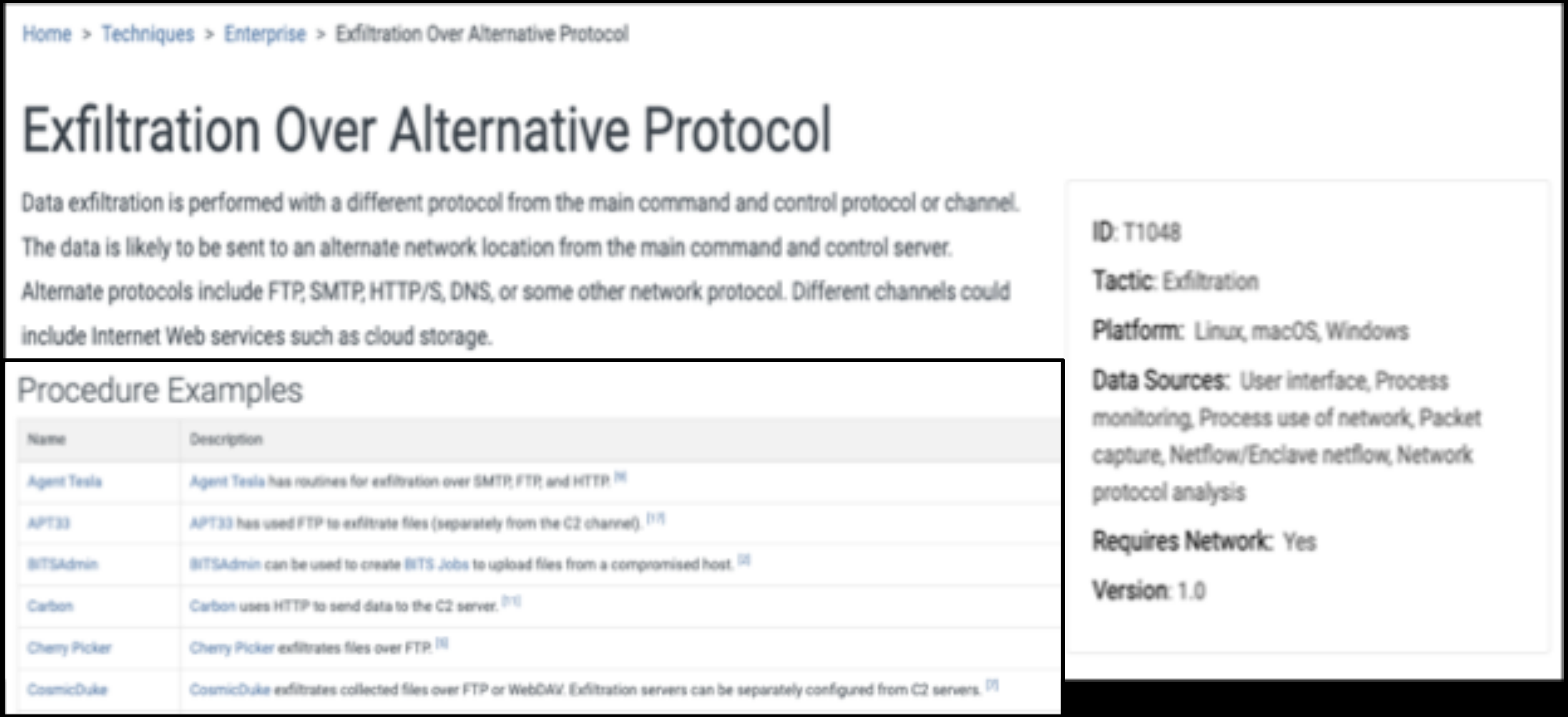
Below are the tactics and technique representing the MITRE ATT&CK Matrix™ for Enterprise covering cloud-based techniques. The Matrix contains information for the following platforms: AWS, GCP, Azure, Azure AD, Office 365, SaaS.

Last Modified: 2019-10-09 18:48:31.906000

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
Drive-by Compromise	Account Manipulation	Valid Accounts	Application Access Token	Account Manipulation	Account Discovery	Application Access Token	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Exploit Public-Facing Application	Create Account		Redundant Access	Brute Force	Cloud Service Dashboard	Internal Spearphishing	Data from Information Repositories		
Spearphishing Link	Implant Container Image		Revert Cloud Instance	Cloud Instance Metadata API	Cloud Service Discovery	Web Session Cookie	Data from Local System		
Trusted Relationship	Office Application Startup		Unused/Unsupported Cloud Regions	Credentials in Files	Network Service Scanning		Data Staged		
Valid Accounts	Redundant Access		Valid Accounts	Steal Application Access Token	Network Share Discovery		Email Collection		
	Valid Accounts		Web Session Cookie	Steal Web Session Cookie	Permission Groups Discovery				
					Remote System Discovery				
					System Information Discovery				
					System Network Connections Discovery				

Source: https://attack.mitre.org/matrices/enterprise/cloud/

DATA EXFILTRATION



Home > Techniques > Enterprise > Exfiltration Over Alternative Protocol

Exfiltration Over Alternative Protocol

Data exfiltration is performed with a different protocol from the main command and control protocol or channel. The data is likely to be sent to an alternate network location from the main command and control server. Alternate protocols include FTP, SMTP, HTTP/S, DNS, or some other network protocol. Different channels could include Internet Web services such as cloud storage.

Procedure Examples

Name	Description
Agent Tesla	Agent Tesla has routines for exfiltration over SMTP, FTP, and HTTP. [9]
APT33	APT33 has used FTP to exfiltrate files (separately from the C2 channel). [17]
BITSAdmin	BITSAdmin can be used to create BITS Jobs to upload files from a compromised host. [2]
Carbon	Carbon uses HTTP to send data to the C2 server. [11]
Cherry Picker	Cherry Picker exfiltrates files over FTP. [6]
CosmicDuke	CosmicDuke exfiltrates collected files over FTP or WebDAV. Exfiltration servers can be separately configured from C2 servers. [7]

ID: T1048

Tactic: Exfiltration

Platform: Linux, macOS, Windows

Data Sources: User interface, Process monitoring, Process use of network, Packet capture, Netflow/Enclave netflow, Network protocol analysis

Requires Network: Yes

Version: 1.0

- >85% of org web traffic (by volume) is going to Cloud applications (SaaS, IaaS etc)
- HTTPS, DNS still common egress channels for exfil. FTP, SMTP becoming less common
- Increase in use of SaaS for C2 & exfil through API

CASE STUDIES

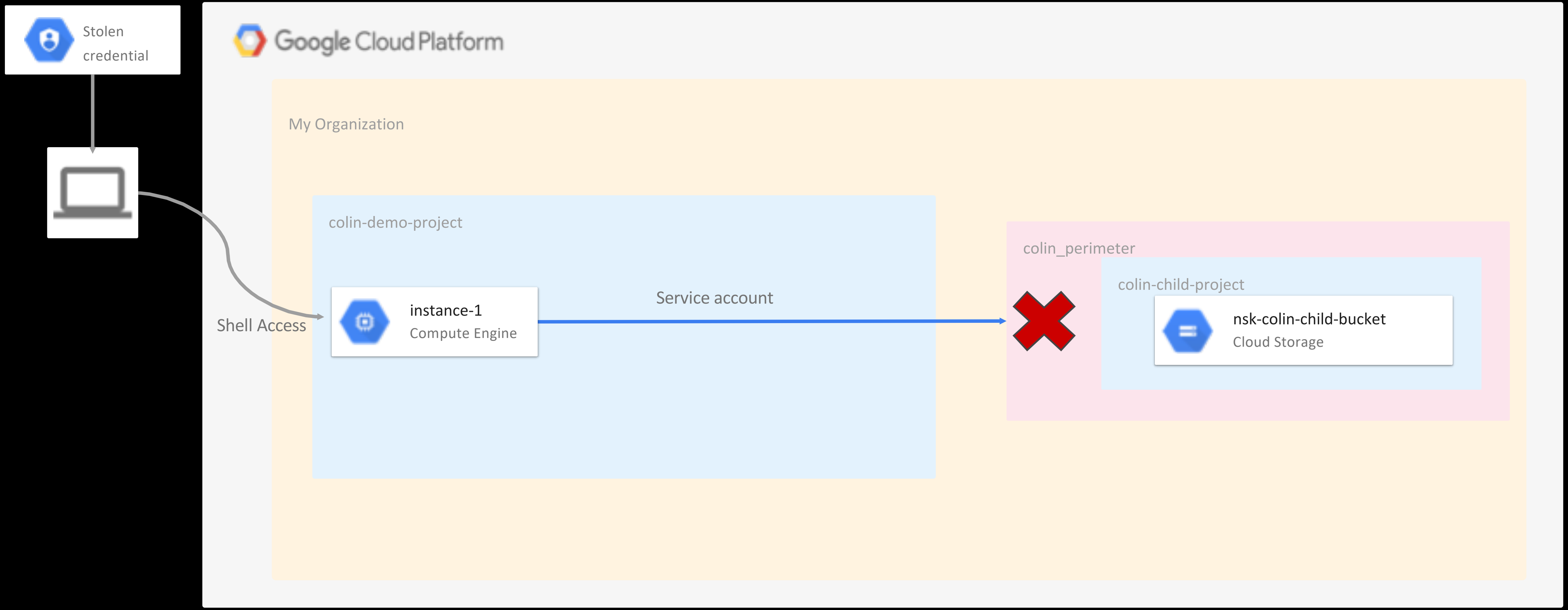
Deeper analysis and better insights on CTI measures for:

1. Exploiting IAM Permissions in GCP
2. Exploiting Temporary Credentials in AWS
3. SLUB TTP

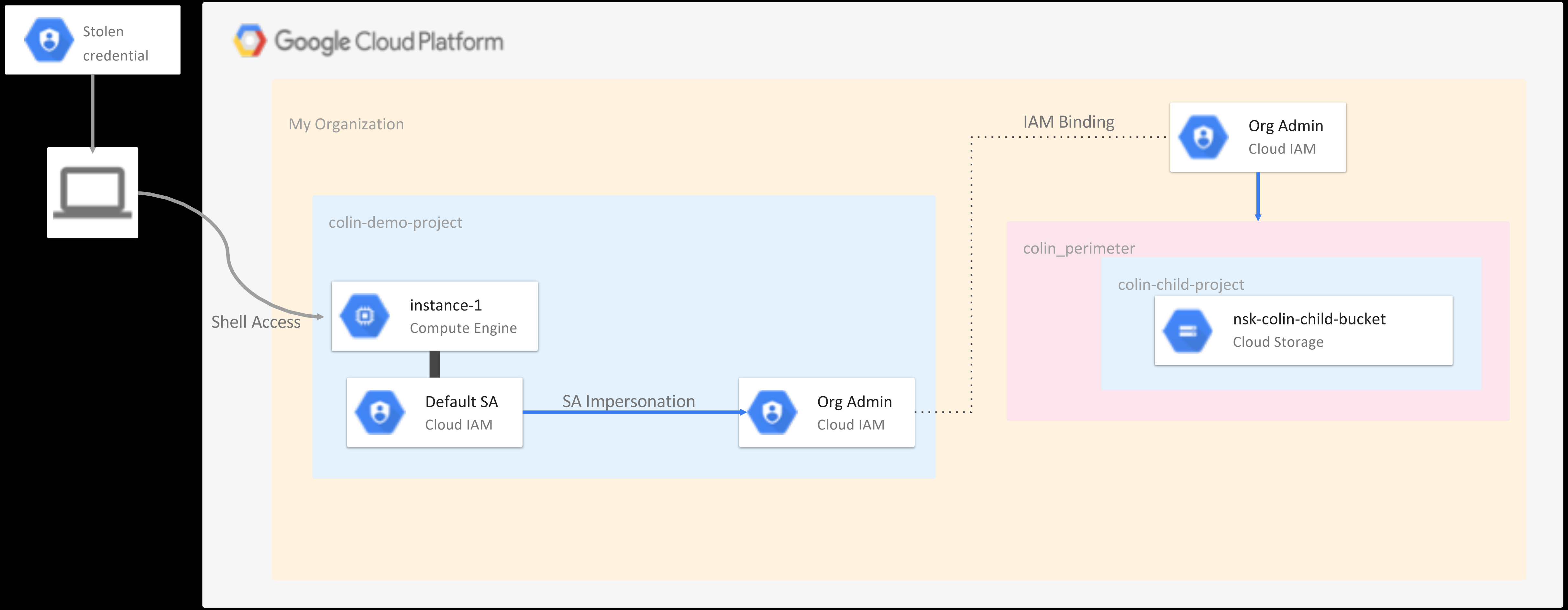
EXPLOITING IAM PERMISSIONS IN GCP

- Colin Estep, Netskope Threat Research Labs
- Netskope Field Summary
- Netskope Blog Post
- DEF CON Presentation (Aug 2019)

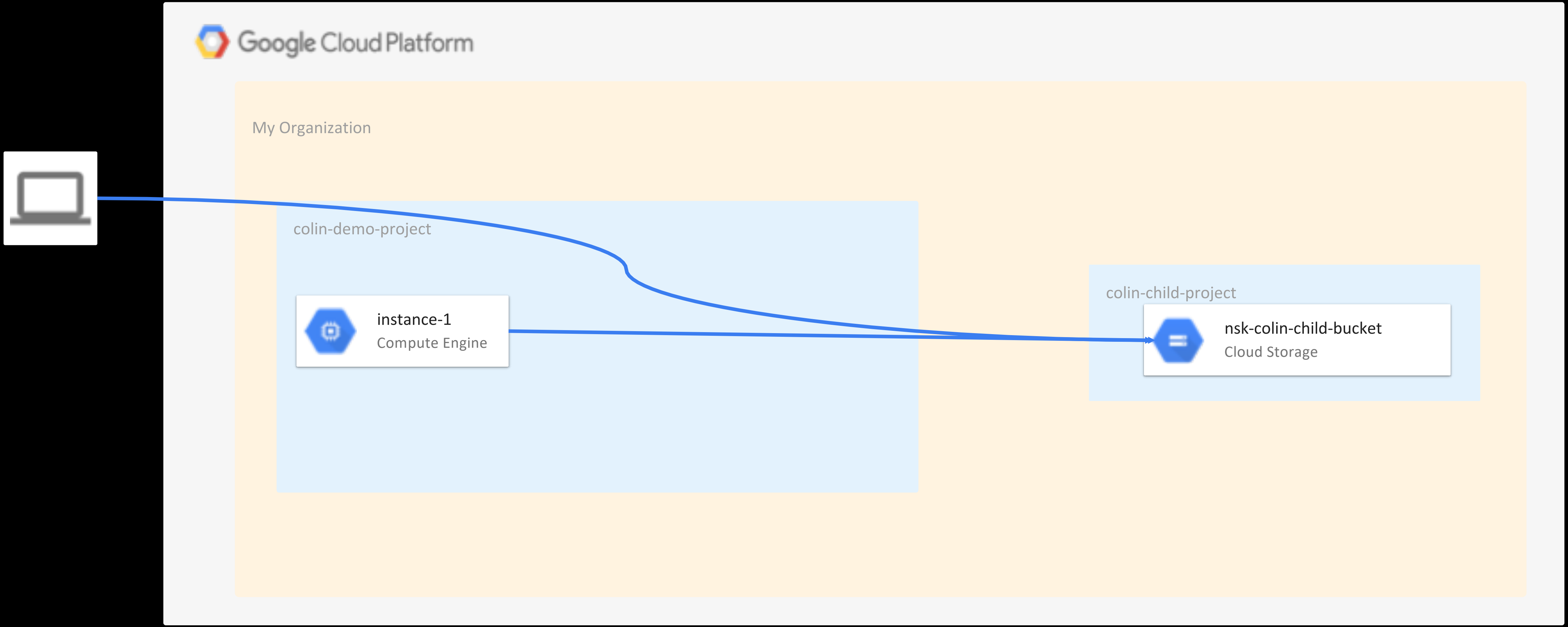
VPC SERVICE CONTROL PROTECTS AGAINST DATA EXFIL



COMPROMISED CREDENTIAL -> COMPROMISED INSTANCE -> DEFAULT SERVICE ACCOUNT BOUND TO ORGANIZATION -> PRIVILEGE ESCALATION / LATERAL



DISABLE OF VPC SERVICE CONTROL -> DATA EXFILTRATION FROM INTERNET



MITRE ATT&CK ANALYSIS

Credential Access (Credentials in Files)

- Exposed SA key (credential) that has not been expired. Also without any MFA or other context.

Initial Access (Valid Accounts)

- Publicly exposed workload accessed from unknown IP space (successful SSH)

Discovery (Account Discovery)

- Publicly exposed workload has been given a default service account, which is not recommended.
- Publicly exposed workload has been given a service account with too much privilege
- Publicly exposed workload has been given a service account with a primitive role
- Project level bindings for a service account user results in the ability to find any other SA in that project.

Privilege Escalation (Sudo)

- Using a service account for administrative tasks at the Organization level in GCP
- Administrative service account resides in the same project as publicly exposed workloads.
- Project level bindings for a service account user results in the ability to authenticate as any other service account in that project.

Execution (User Execution)

- Tearing down of an organization-level security control without any MFA or other context.

Exfiltration (Automated Exfiltration)

- Security control changes have opened exposure of sensitive data in a bucket.

MITRE ATT&CK ANALYSIS

Checks

- SSH is allowed from 0.0.0.0/0 using a service account (OS Login)
  [SSH authentication was allowed from any IP address, based on cloud identity credentials (not SSH keys).]
- Default Compute Engine service account used on publicly exposed workload with full scopes
  [A cloud identity credential was assigned to a publicly exposed workload had no scope limitations, so its full capabilities would be allowed.]
- A service account with a primitive role is associated to a publicly exposed workload. [An over privileged cloud identity credential associated with a workload exposed to the Internet.]
- A service account with a primitive role is associated to a publicly exposed workload AND that service account has project level binding with "service account user" permissions
  [An over privileged cloud identity credential associated with a workload exposed to the Internet, which was given the ability to assume other cloud identities.]
- An organization-level administrative service account has been authenticated from a publicly exposed workload
  [An administrator-level cloud identity authenticated from a workload exposed to the Internet.]
- A VPC Service Perimeter was removed, which protected a bucket. Now, data from that bucket is downloaded to an IP address outside of the organization
  [A cloud perimeter control was removed, followed by data access from an unknown IP address.]

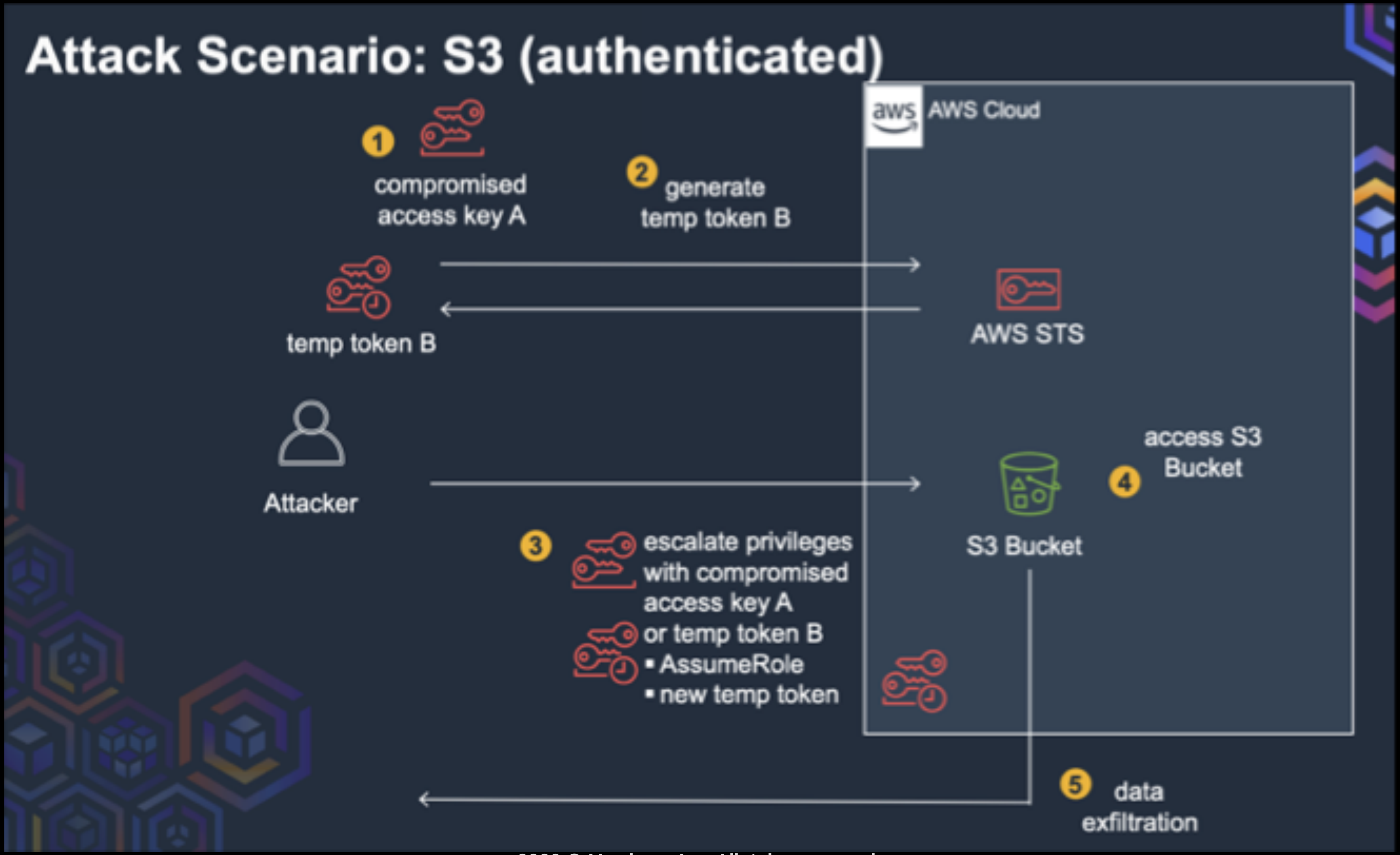
* additional checks from ATT&CK-based analysis

* generalized checks

EXPLOITING AWS TEMPORARY CREDENTIALS

- Jenko Hwong, Netskope Threat Research Labs
- Netskope Field Summary
- Netskope Blog Post
- DEF CON Presentation (Aug 2019)

TEMPORARY CREDENTIALS -> PERSISTENCE/DEFENSE EVASION -> PRIVILEGE ESCALATION -> DATA EXFIL



ORIGINAL TAKEAWAYS

Prevention

- Lockdown access keys(aws:sourceIp or aws:sourceVpc[1]/MFA)
- isolate temp token usage in separate accounts
- service-only IAMUsers in separate accounts
- minimal privileges for AssumeRole and PassRole

Detection

- alert on GetSessionToken
- alert on temp tokens (ASIA*)
- harden CloudTrail/CloudWatch/SIEM
- AWS Config (IAM,Lambda)

Mitigation/Remediation

- review/revise remediation playbook
- do not use GetSessionToken, use AssumeRole
- maybe don't use temp tokens at all…permanent access keys
- use revoke active sessions for role(aws:TokenIssueTime[1])
- create/test a recovery plan from compromised temp tokens
- AWS Config (IAM,Lambda)

Provisioning/Inventory

- track temp tokens that are created in a datastore
- use wrapper code for custom apps that need temp tokens
- for AWS-generated tokens (IoT, AssumeRole) have to parse logs

MITRE ATT&CK ANALYSIS OF TEMPORARY CREDENTIAL TECHNIQUES

MATRICES

PRE-ATT&CK

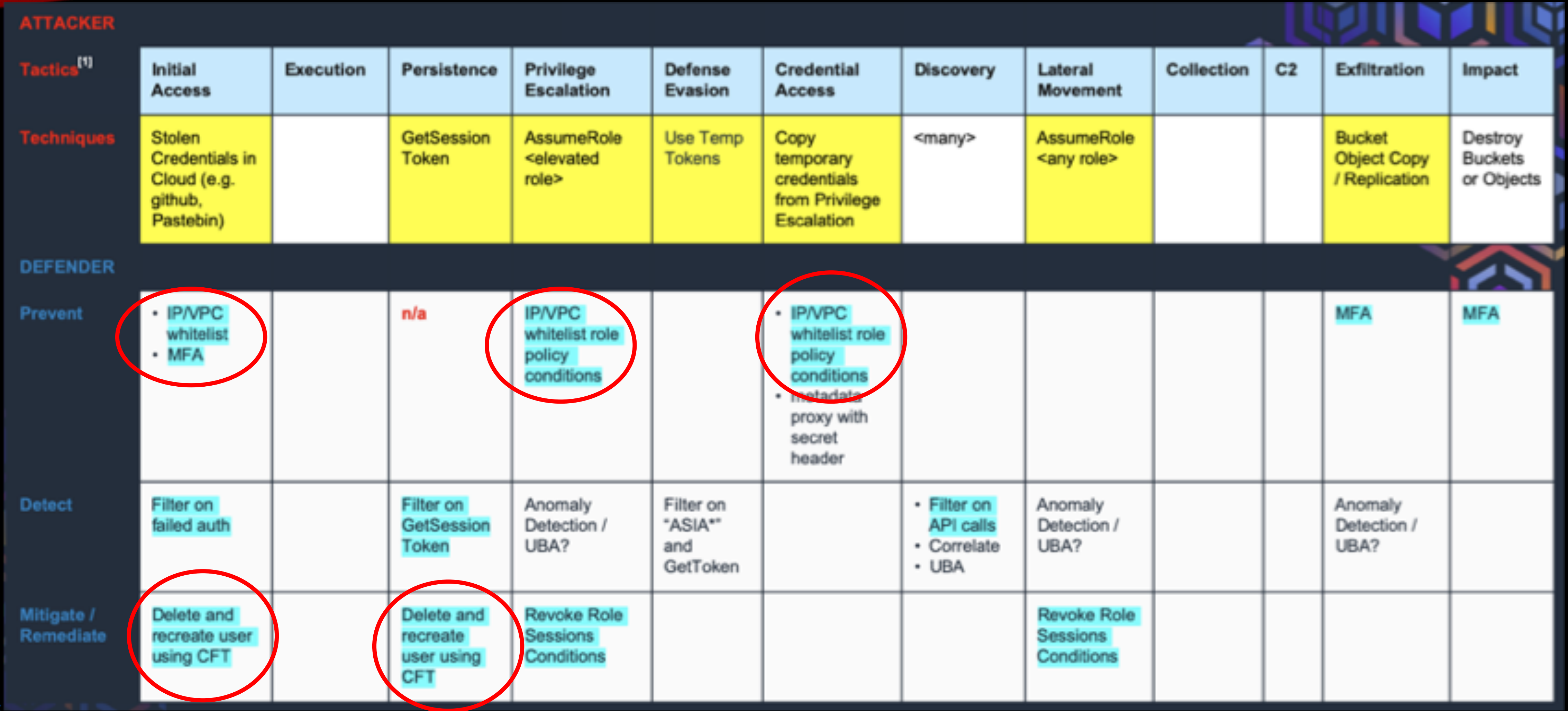
Enterprise
- All Platforms
- Linux
- macOS
- Windows

Mobile

Cloud
- IaaS
  - AWS
  - Azure
  - GCP
- SaaS
  - Office365
  - DropBox

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
API Keys in Source Code	Serverless Functions	Serverless Functions	Assume Role	Disable Logging	Copy temporary credentials from PE	User Enumeration	Run Compute Instance	Data from Cloud Storage	Commonly Used Port	Bucket Object Copy / Replication	Destroy Buckets
Brute Force	Compute Instance Compromise	Persistent Compute Volumes	Pass Role	Delete Logs		Group Enumeration	Assume Role		Bucket Objects	File.io	Destroy Compute Instance Disks
Stolen Credentials	Compute Resource Creation	Versioned Policies	Modify Policies	Modify Logs		Role/Policy Enumeration	Remote Services		Slack		Destroy Backups
Cloud Service Trust Abuse		Get Temporary Token	Snapshot Restore	Disable Alerts		Account Identification			Twitter		
S3 Bucket Subdomain Takeover		Cloud User Backdoor	Set default policy	Use older versions of policies		Compute Instance Enumeration			Gist		
		Auto Resource Regen	Create new policy	Use older versions of code		Bucket Enumeration					
		Use EC2 temp creds	Create new access key	Auto Resource Regen		Credential Report Download					

STRUCTURED ANALYSIS OF PREVENTION, DETECTION, MITIGATION PROCEDURES



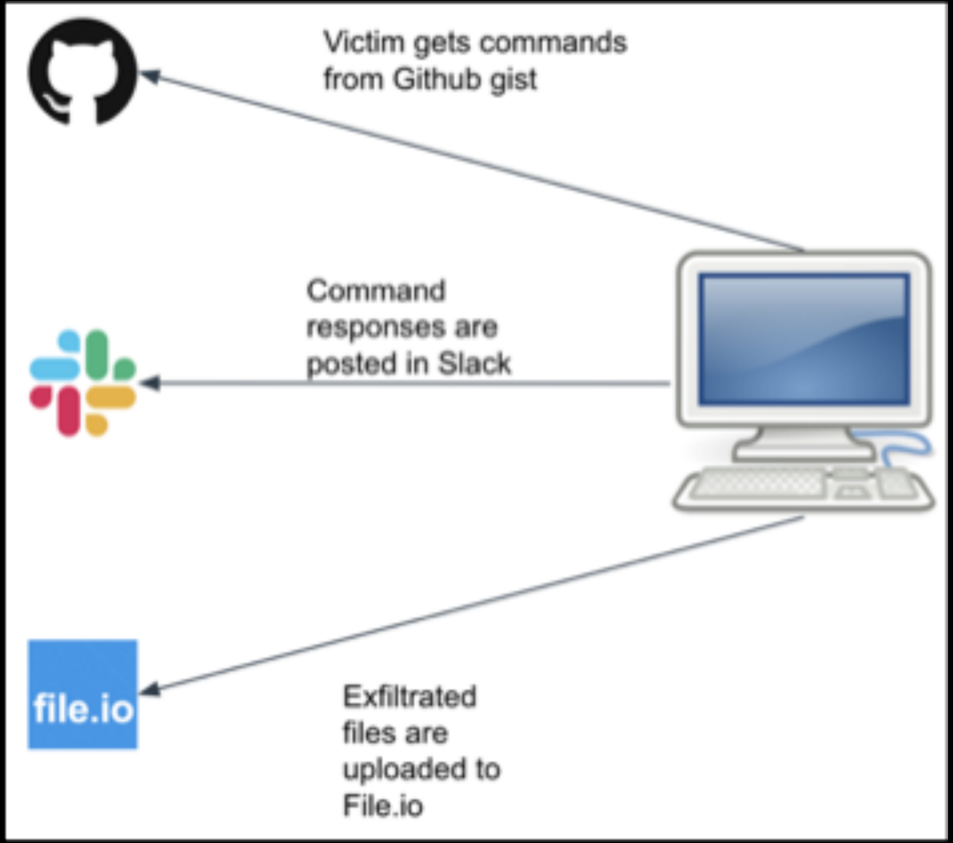
ATTACKER

Tactics[1]	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	C2	Exfiltration	Impact
Techniques	Stolen Credentials in Cloud (e.g. github, Pastebin)		GetSession Token	AssumeRole <elevated role>	Use Temp Tokens	Copy temporary credentials from Privilege Escalation	<many>	AssumeRole <any role>			Bucket Object Copy / Replication	Destroy Buckets or Objects
DEFENDER												
Prevent	• IP/VPC whitelist • MFA		n/a	IP/VPC whitelist role policy conditions		• IP/VPC whitelist role policy conditions • metadata proxy with secret header					MFA	MFA
Detect	Filter on failed auth		Filter on GetSession Token	Anomaly Detection / UBA?	Filter on "ASIA*" and GetToken		• Filter on API calls • Correlate • UBA	Anomaly Detection / UBA?			Anomaly Detection / UBA?	
Mitigate / Remediate	Delete and recreate user using CFT		Delete and recreate user using CFT	Revoke Role Sessions Conditions				Revoke Role Sessions Conditions				

SLUB: COVERT CLOUD C2 & DATA EXFIL

- Erick Galinkin, Netskope Threat Research Labs
- Netskope Field Summary
- Netskope Blog Post
- DEF CON Presentation (Aug 2019)

SOPHISTICATED MALWARE UTILIZING MULTIPLE SAAS APPLICATIONS FOR CNC AND DATA EXFIL


Victim gets commands from Github gist
Command responses are posted in Slack
file.io
Exfiltrated files are uploaded to File.io

Challenges

- Focusing on single SaaS technique leads to high false positive rate
- Multi-channel behavioral approach required
- Correlation of events from trusted Cloud apps

MITRE ATT&CK ANALYSIS

MATRICES

ATT&CK

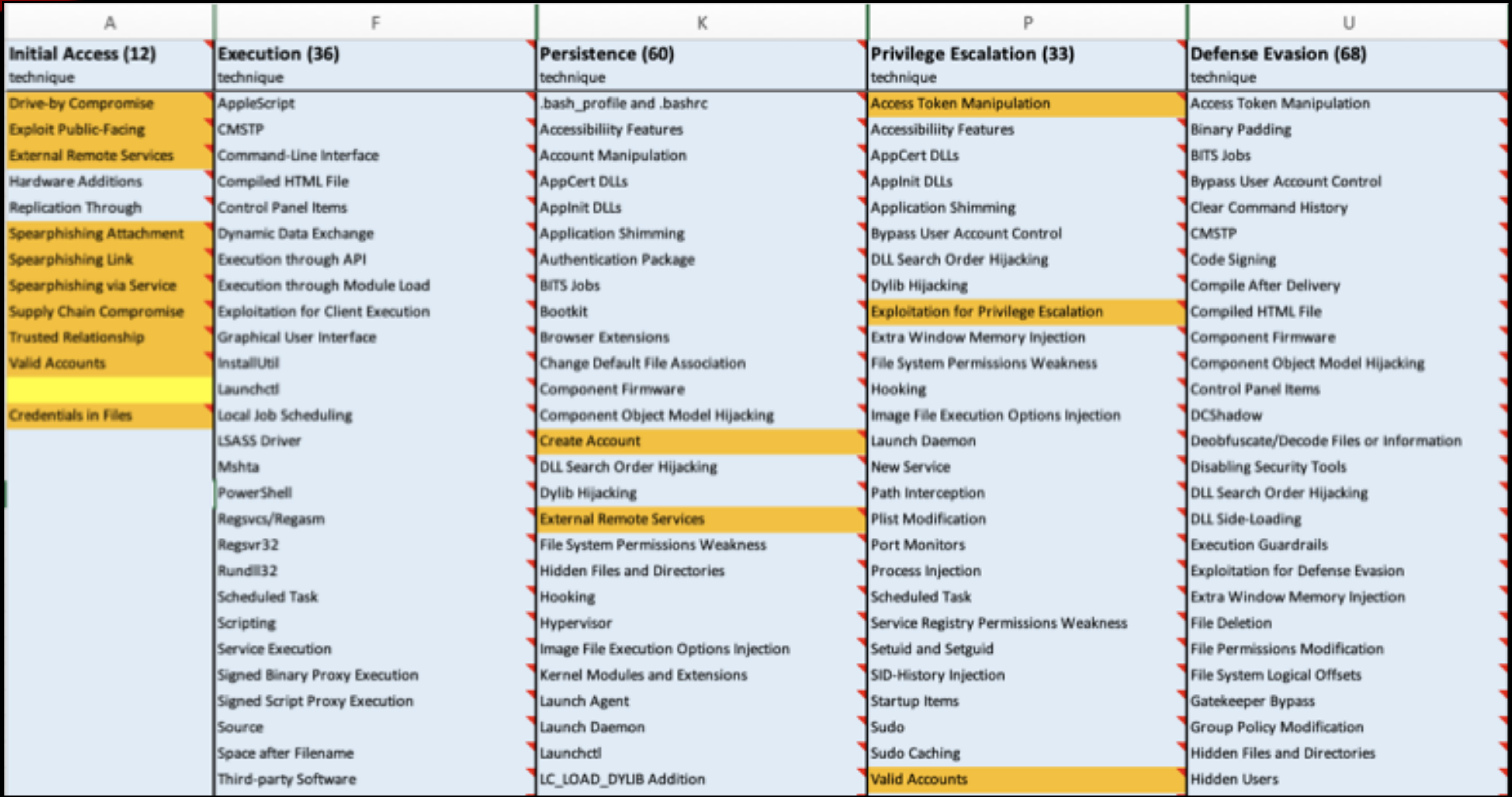
Enterprise
- All Platforms
- Linux
- macOS
- Windows

Mobile

Cloud
- IaaS
  - AWS
  - Azure
  - GCP
- SaaS
  - Office365
  - DropBox

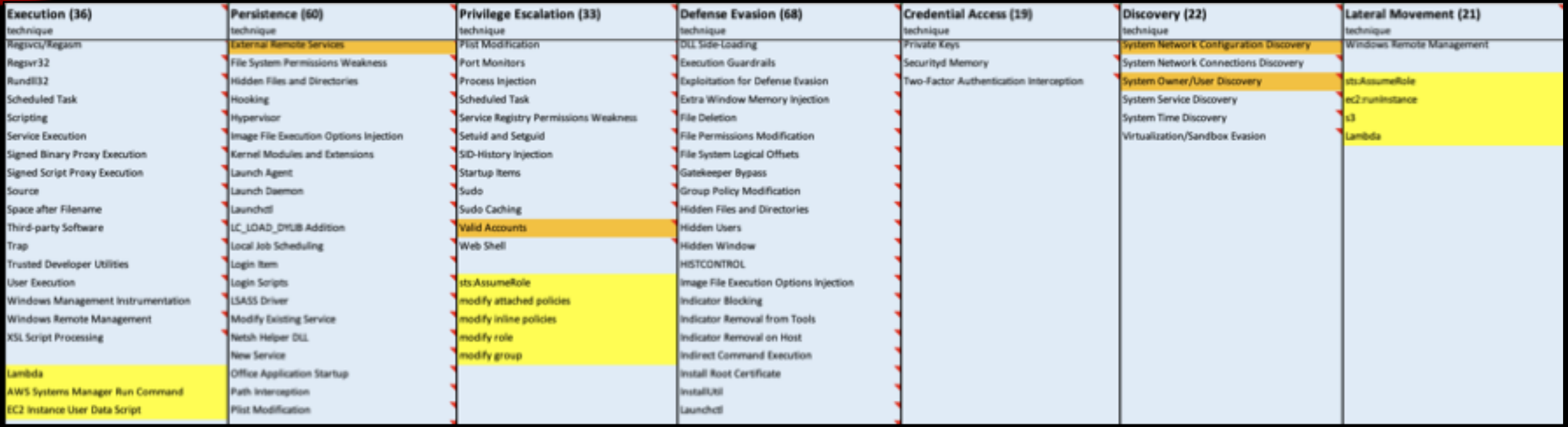
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
API Keys in Source Code	Serverless Functions	Serverless Functions	Assume Role	Disable Logging	Copy temporary credentials from PE	User Enumeration	Run Compute Instance	Data from Cloud Storage	Commonly Used Port	Bucket Object Copy / Replication	Destroy Buckets
Brute Force	Compute Instance Compromise	Persistent Compute Volumes	Pass Role	Delete Logs		Group Enumeration	Assume Role		Bucket Objects	File.io	Destroy Compute Instance Disks
Stolen Credentials	Compute Resource Creation	Versioned Policies	Modify Policies	Modify Logs		Role/Policy Enumeration	Remote Services		Slack		Destroy Backups
Cloud Service Trust Abuse		Get Temporary Token	Snapshot Restore	Disable Alerts		Account Identification			Twitter		
S3 Bucket Subdomain Takeover		Cloud User Backdoor	Set default policy	Use older versions of policies		Compute Instance Enumeration			Gist		
		Auto Resource Regen	Create new policy	Use older versions of code		Bucket Enumeration					
		Use EC2 temp creds	Create new access key	Auto Resource Regen		Credential Report Download					

TAXONOMY: START WITH EXISTING ATT&CK TECHNIQUES AND ID CLOUD-APPLICABLE TECHNIQUES



A	F	K	P	U
Initial Access (12)	**Execution (36)**	**Persistence (60)**	**Privilege Escalation (33)**	**Defense Evasion (68)**
technique	technique	technique	technique	technique
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation
Exploit Public-Facing	CMSTP	Accessibiliity Features	Accessibiliity Features	Binary Padding
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control
Replication Through	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking
	Launchctl	Component Firmware	Hooking	Control Panel Items
Credentials in Files	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information
	Mshta	DLL Search Order Hijacking	New Service	Disabling Security Tools
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection
	Scripting	Hypervisor	Service Registry Permissions Weakness	File Deletion
	Service Execution	Image File Execution Options Injection	Setuid and Setguid	File Permissions Modification
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	File System Logical Offsets
	Signed Script Proxy Execution	Launch Agent	Startup Items	Gatekeeper Bypass
	Source	Launch Daemon	Sudo	Group Policy Modification
	Space after Filename	Launchctl	Sudo Caching	Hidden Files and Directories
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Hidden Users

TAXONOMY: IDENTIFY/ADD NEW CLOUD TECHNIQUES



Execution (36)	Persistence (60)	Privilege Escalation (33)	Defense Evasion (68)	Credential Access (19)	Discovery (22)	Lateral Movement (21)
technique	technique	technique	technique	technique	technique	technique
Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management
Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery	
Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery	sts:AssumeRole
Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection		System Service Discovery	ec2:runInstance
Scripting	Hypervisor	Service Registry Permissions Weakness	File Deletion		System Time Discovery	s3
Service Execution	Image File Execution Options Injection	Setuid and Setguid	File Permissions Modification		Virtualization/Sandbox Evasion	Lambda
Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	File System Logical Offsets			
Signed Script Proxy Execution	Launch Agent	Startup Items	Gatekeeper Bypass			
Source	Launch Daemon	Sudo	Group Policy Modification			
Space after Filename	Launchctl	Sudo Caching	Hidden Files and Directories			
Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Hidden Users			
Trap	Local Job Scheduling	Web Shell	Hidden Window			
Trusted Developer Utilities	Login Item		HISTCONTROL			
User Execution	Login Scripts	sts:AssumeRole	Image File Execution Options Injection			
Windows Management Instrumentation	LSASS Driver	modify attached policies	Indicator Blocking			
Windows Remote Management	Modify Existing Service	modify inline policies	Indicator Removal from Tools			
XSL Script Processing	Netsh Helper DLL	modify role	Indicator Removal on Host			
	New Service	modify group	Indirect Command Execution			
Lambda	Office Application Startup		Install Root Certificate			
AWS Systems Manager Run Command	Path Interception		InstallUtil			
EC2 Instance User Data Script	Plist Modification		Launchctl			

HOW DOES NETSKOPE SUPPORT MITRE ATT&CK?

Netskope is working with MITRE to contribute content to MITRE ATT&CK, helping to describe cloud-specific threats and the techniques used within the cloud by today’s adversaries.

Content focuses not only on unique cloud threat vectors but also on prescriptive guidance for prevention, detection, and mitigation. Specifically, Netskope contributes content in 3 areas:

- submissions on cloud threat techniques
- prescriptive guidance on prevention, detection, mitigation
- cloud classification / taxonomy

enisa

netskope

CONCLUSION

- Consider updating your CTI data sources for Cloud including updating credential access TTP
- Consider API as a primary attack vector and SaaS as a C2 and data exfiltration method
- Review/Revisit MITRE ATT&CK CLOUD MATRIX. Support building new models based on new TTP
- RSS feed - https://www.netskope.com/resources/netskope-threat-research-labs
- Consider educating the next generation on Cybersecurity, CTI…and Cloud

THE CTI CLOUD CONTEXT DILEMMA

Evaluating and building CTI for the Cloud

Neil Thacker, CISO EMEA @ Netskope

nthacker@netskope.com

@nt_hacker