MITRE ATT&CK® Roadmap

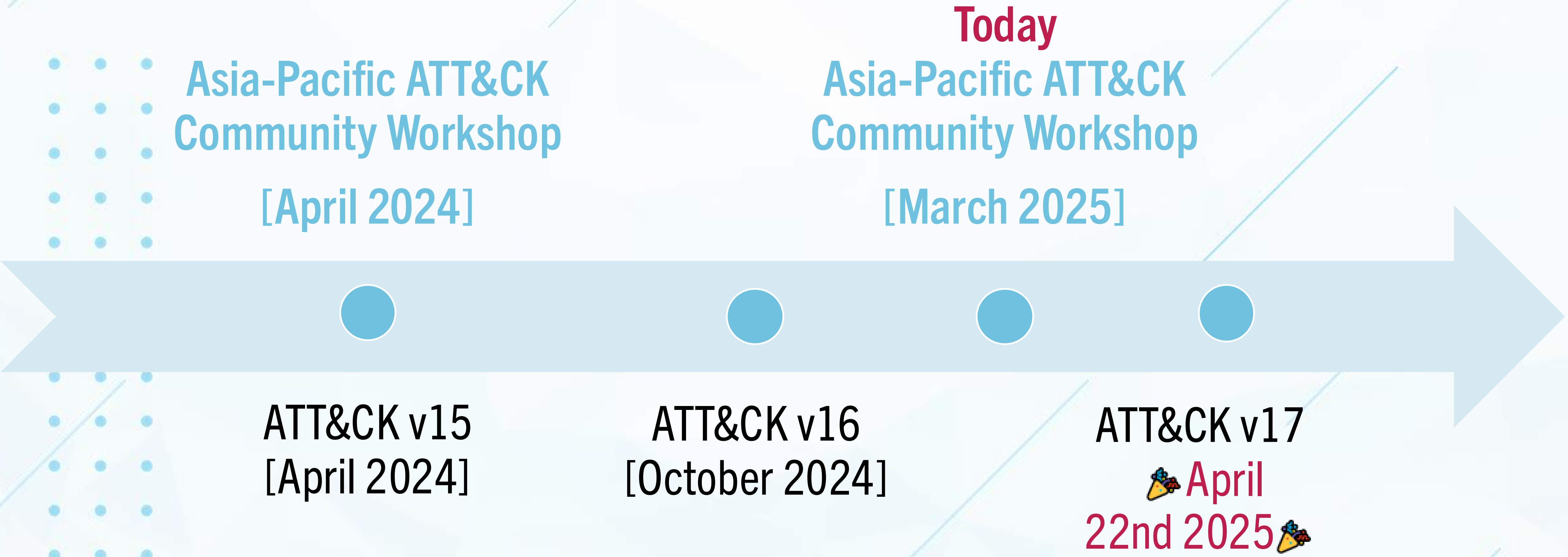
Lauren Lusty, ATT&CK Enterprise

ATT&CK Team

- Enterprise
- Network (Devices)
- Mac/Linux
- Defenses
- Threat Intel
- ICS
- Mobile
- Software Development
- Outreach

With support from 30+ MITRE staff

[You are here]



Today

Asia-Pacific ATT&CK Community Workshop

[April 2024]

Asia-Pacific ATT&CK Community Workshop

[March 2025]

ATT&CK v15
[April 2024]

ATT&CK v16
[October 2024]

ATT&CK v17
🎉April 22nd 2025🎉

ATT&CK v16 Highlights

Released October 31, 2024

ATT&CK v16 by the numbers

19
NEW
TECHNIQUES/
SUB-TECHNIQUES

11
NEW
GROUPS

6
NEW
CAMPAIGNS

34
NEW
SOFTWARE

231
NEW
ANALYTICS

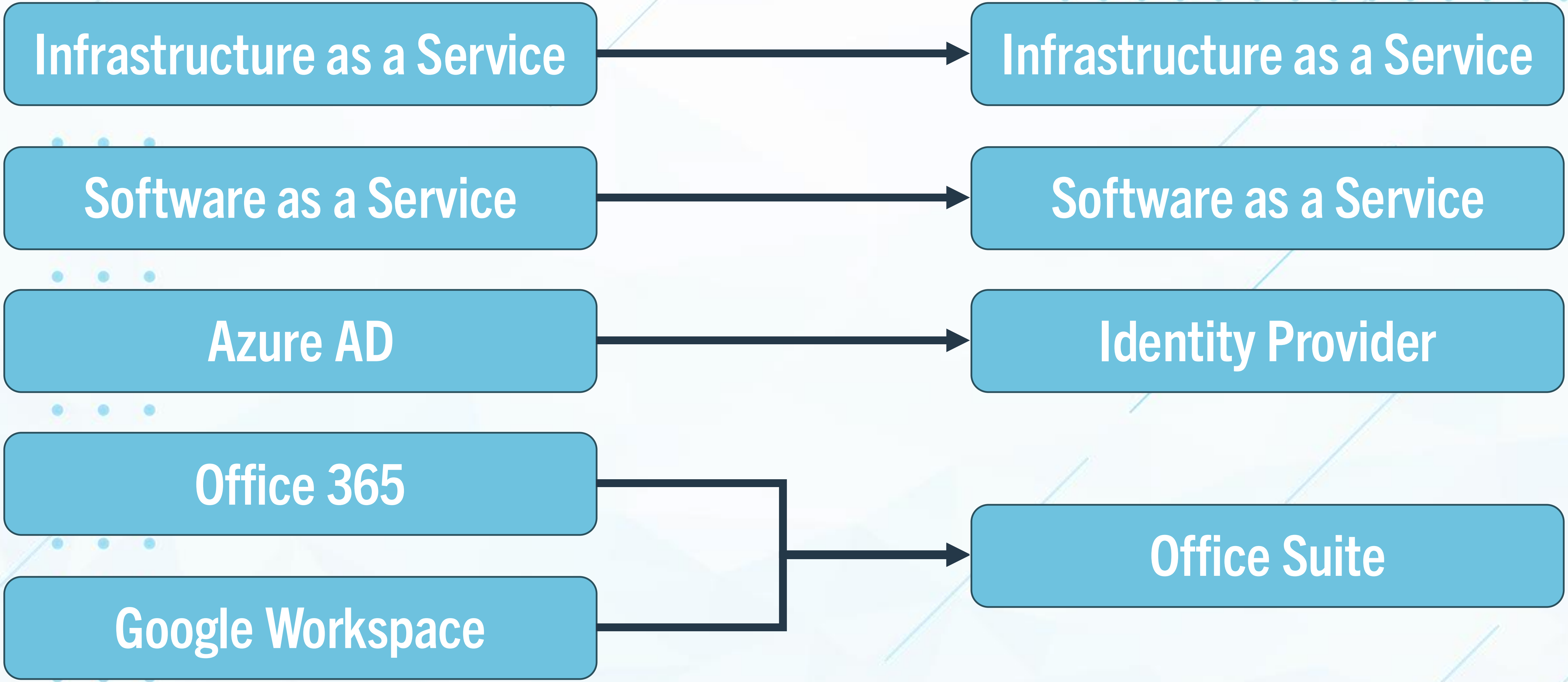
67
NAMED
CONTRIBUTORS

…and many many updates!

Cloud Platforms

- Infrastructure as a Service
- Software as a Service
- Azure AD
- Office 365
- Google Workspace

Cloud Platforms



Infrastructure as a Service → Infrastructure as a Service

Software as a Service → Software as a Service

Azure AD → Identity Provider

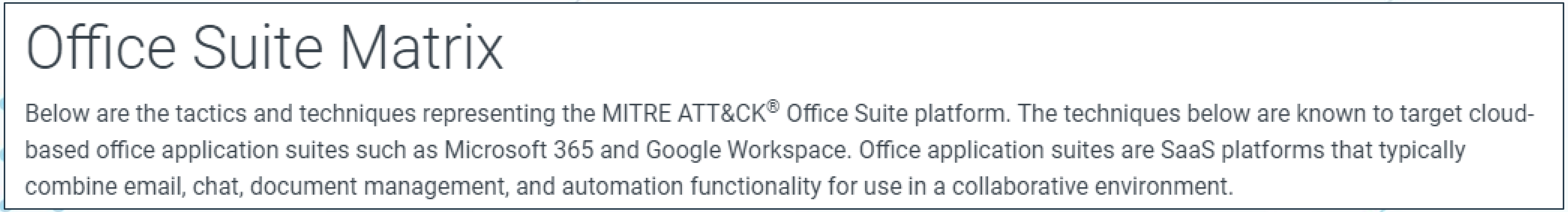
Office 365 → Office Suite

Google Workspace → Office Suite

Why?

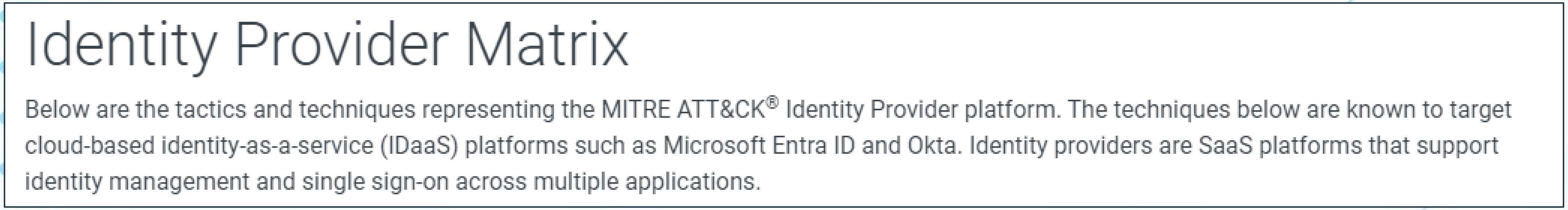
- There's more than one identity-as-a-service platform!
  - Okta
  - Ping Identity
  - JumpCloud
  - OneLogin
  - etc.
- Office 365 ≈ Google Workspace

Bonus: Updated Platform Descriptions



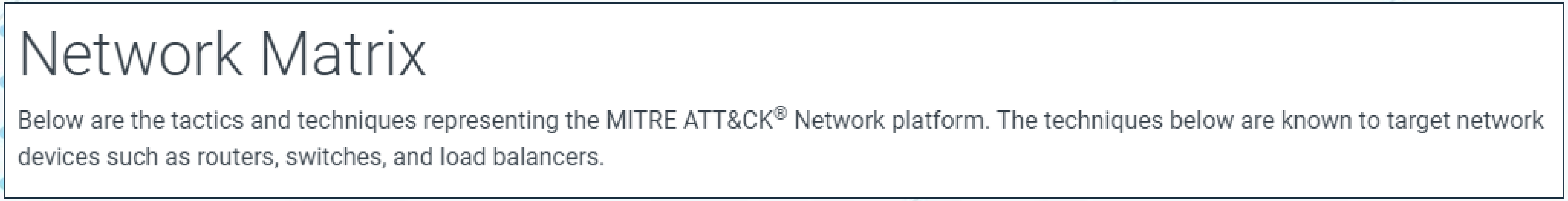
Office Suite Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Office Suite platform. The techniques below are known to target cloud-based office application suites such as Microsoft 365 and Google Workspace. Office application suites are SaaS platforms that typically combine email, chat, document management, and automation functionality for use in a collaborative environment.



Identity Provider Matrix

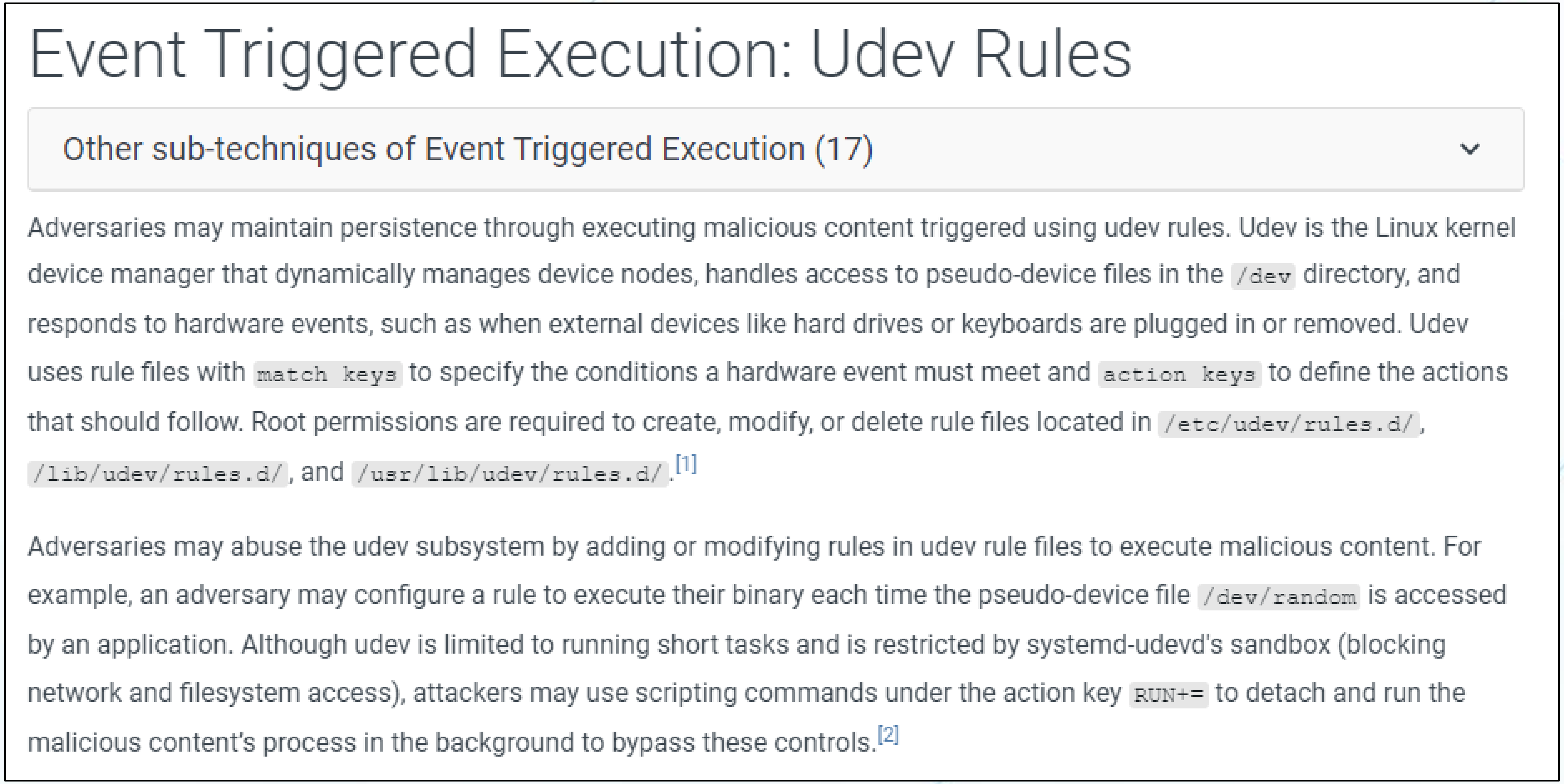
Below are the tactics and techniques representing the MITRE ATT&CK® Identity Provider platform. The techniques below are known to target cloud-based identity-as-a-service (IDaaS) platforms such as Microsoft Entra ID and Okta. Identity providers are SaaS platforms that support identity management and single sign-on across multiple applications.



Network Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Network platform. The techniques below are known to target network devices such as routers, switches, and load balancers.

V16 Updates: By popular demand



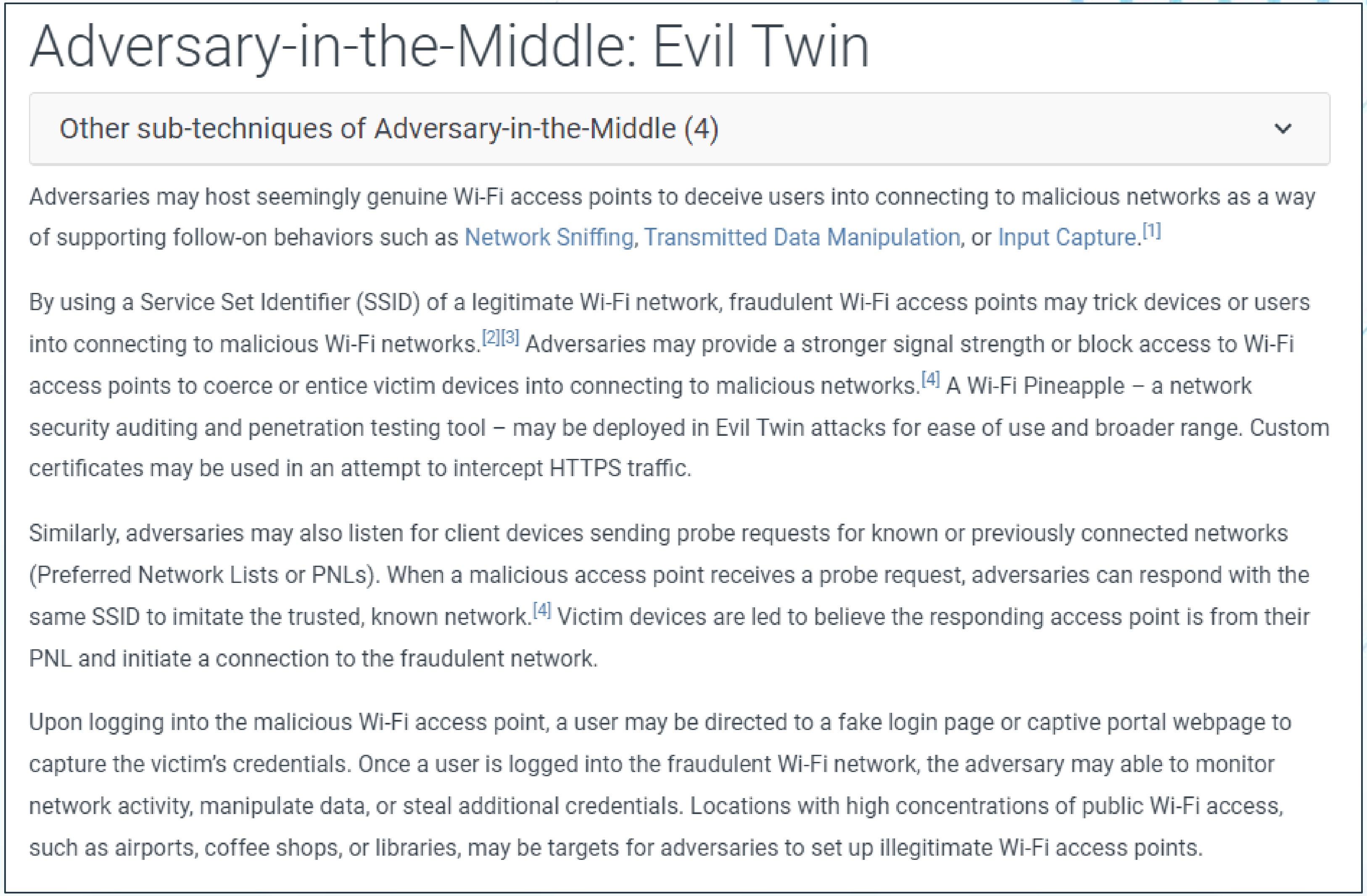
Event Triggered Execution: Udev Rules

Other sub-techniques of Event Triggered Execution (17) ⌄

Adversaries may maintain persistence through executing malicious content triggered using udev rules. Udev is the Linux kernel device manager that dynamically manages device nodes, handles access to pseudo-device files in the `/dev` directory, and responds to hardware events, such as when external devices like hard drives or keyboards are plugged in or removed. Udev uses rule files with `match keys` to specify the conditions a hardware event must meet and `action keys` to define the actions that should follow. Root permissions are required to create, modify, or delete rule files located in `/etc/udev/rules.d/`, `/lib/udev/rules.d/`, and `/usr/lib/udev/rules.d/`.[1]

Adversaries may abuse the udev subsystem by adding or modifying rules in udev rule files to execute malicious content. For example, an adversary may configure a rule to execute their binary each time the pseudo-device file `/dev/random` is accessed by an application. Although udev is limited to running short tasks and is restricted by systemd-udevd's sandbox (blocking network and filesystem access), attackers may use scripting commands under the action key `RUN+=` to detach and run the malicious content's process in the background to bypass these controls.[2]

V16 Updates: An Oldie but a Goodie



Adversary-in-the-Middle: Evil Twin

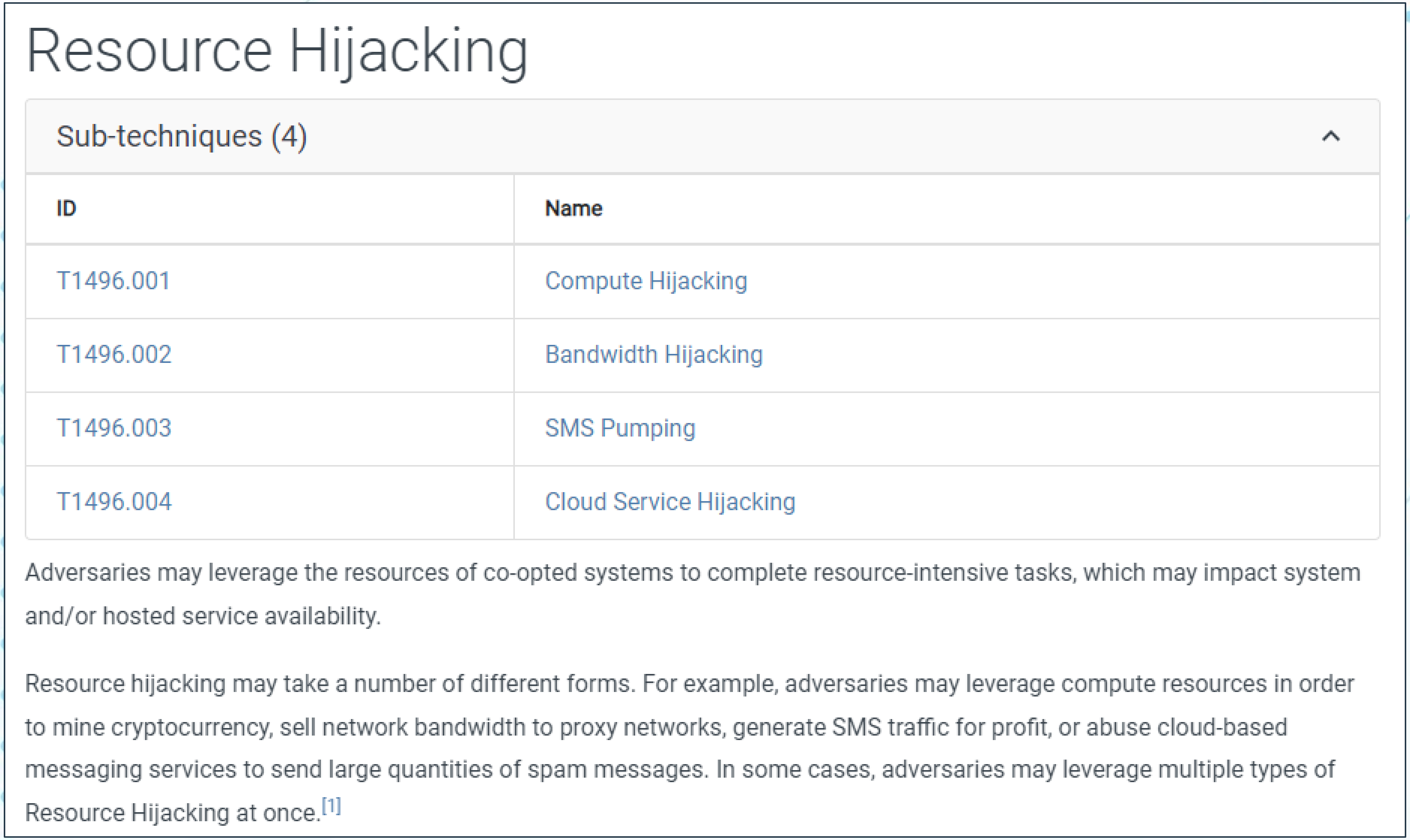
Adversaries may host seemingly genuine Wi-Fi access points to deceive users into connecting to malicious networks as a way of supporting follow-on behaviors such as Network Sniffing, Transmitted Data Manipulation, or Input Capture.[1]

By using a Service Set Identifier (SSID) of a legitimate Wi-Fi network, fraudulent Wi-Fi access points may trick devices or users into connecting to malicious Wi-Fi networks.[2][3] Adversaries may provide a stronger signal strength or block access to Wi-Fi access points to coerce or entice victim devices into connecting to malicious networks.[4] A Wi-Fi Pineapple – a network security auditing and penetration testing tool – may be deployed in Evil Twin attacks for ease of use and broader range. Custom certificates may be used in an attempt to intercept HTTPS traffic.

Similarly, adversaries may also listen for client devices sending probe requests for known or previously connected networks (Preferred Network Lists or PNLs). When a malicious access point receives a probe request, adversaries can respond with the same SSID to imitate the trusted, known network.[4] Victim devices are led to believe the responding access point is from their PNL and initiate a connection to the fraudulent network.

Upon logging into the malicious Wi-Fi access point, a user may be directed to a fake login page or captive portal webpage to capture the victim's credentials. Once a user is logged into the fraudulent Wi-Fi network, the adversary may able to monitor network activity, manipulate data, or steal additional credentials. Locations with high concentrations of public Wi-Fi access, such as airports, coffee shops, or libraries, may be targets for adversaries to set up illegitimate Wi-Fi access points.

V16 Updates: A Breakup…



Resource Hijacking

Sub-techniques (4)

ID	Name
T1496.001	Compute Hijacking
T1496.002	Bandwidth Hijacking
T1496.003	SMS Pumping
T1496.004	Cloud Service Hijacking

Adversaries may leverage the resources of co-opted systems to complete resource-intensive tasks, which may impact system and/or hosted service availability.

Resource hijacking may take a number of different forms. For example, adversaries may leverage compute resources in order to mine cryptocurrency, sell network bandwidth to proxy networks, generate SMS traffic for profit, or abuse cloud-based messaging services to send large quantities of spam messages. In some cases, adversaries may leverage multiple types of Resource Hijacking at once.[1]

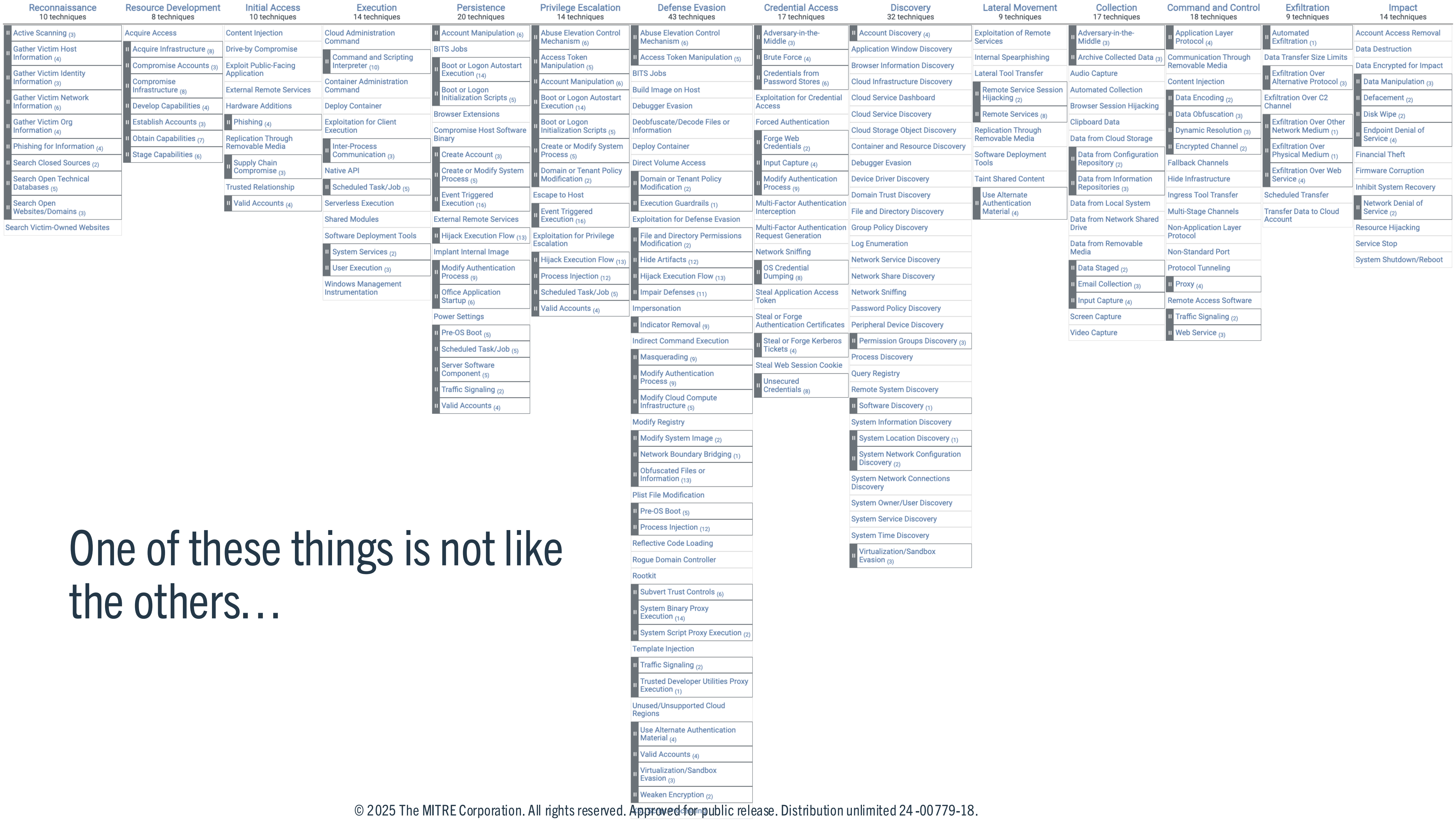
What next?

Content Updates

- Focus on Linux and Network
  - More content
  - More CTI
  - Fill in the gaps

Another Breakup?

One of these things is not like the others…



Reconnaissance
10 techniques

- Active Scanning (3)
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
- Gather Victim Network Information (6)
- 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

Resource Development
8 techniques

- Acquire Access
- Acquire Infrastructure (8)
- Compromise Accounts (3)
- Compromise Infrastructure (8)
- Develop Capabilities (4)
- Establish Accounts (3)
- Obtain Capabilities (7)
- Stage Capabilities (6)

Initial Access
10 techniques

- Content Injection
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (4)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)

Execution
14 techniques

- Cloud Administration Command
- Command and Scripting Interpreter (10)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (3)
- Native API
- Scheduled Task/Job (5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (2)
- User Execution (3)
- Windows Management Instrumentation

Persistence
20 techniques

- Account Manipulation (6)
- BITS Jobs
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Host Software Binary
- Create Account (3)
- Create or Modify System Process (5)
- Event Triggered Execution (16)
- External Remote Services
- Hijack Execution Flow (13)
- Implant Internal Image
- Modify Authentication Process (9)
- Office Application Startup (6)
- Power Settings
- Pre-OS Boot (5)
- Scheduled Task/Job (5)
- Server Software Component (5)
- Traffic Signaling (2)
- Valid Accounts (4)

Privilege Escalation
14 techniques

- Abuse Elevation Control Mechanism (6)
- Access Token Manipulation (5)
- Account Manipulation (6)
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (5)
- Domain or Tenant Policy Modification (2)
- Escape to Host
- Event Triggered Execution (16)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (13)
- Process Injection (12)
- Scheduled Task/Job (5)
- Valid Accounts (4)

Defense Evasion
43 techniques

- Abuse Elevation Control Mechanism (6)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain or Tenant Policy Modification (2)
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)
- Hide Artifacts (12)
- Hijack Execution Flow (13)
- Impair Defenses (11)
- Impersonation
- Indicator Removal (9)
- Indirect Command Execution
- Masquerading (9)
- Modify Authentication Process (9)
- Modify Cloud Compute Infrastructure (5)
- Modify Registry
- Modify System Image (2)
- Network Boundary Bridging (1)
- Obfuscated Files or Information (13)
- Plist File Modification
- Pre-OS Boot (5)
- Process Injection (12)
- Reflective Code Loading
- Rogue Domain Controller
- Rootkit
- Subvert Trust Controls (6)
- System Binary Proxy Execution (14)
- System Script Proxy Execution (2)
- Template Injection
- Traffic Signaling (2)
- Trusted Developer Utilities Proxy Execution (1)
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material (4)
- Valid Accounts (4)
- Virtualization/Sandbox Evasion (3)
- Weaken Encryption (2)
- XSL Script Processing

Credential Access
17 techniques

- Adversary-in-the-Middle (3)
- Brute Force (4)
- Credentials from Password Stores (6)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)
- Modify Authentication Process (9)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (8)
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets (4)
- Steal Web Session Cookie
- Unsecured Credentials (8)

Discovery
32 techniques

- 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
- Permission Groups Discovery (3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1)
- System Information Discovery
- System Location Discovery (1)
- System Network Configuration Discovery (2)
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion (3)

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (8)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (4)

Collection
17 techniques

- 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 (3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2)
- Email Collection (3)
- Input Capture (4)
- Screen Capture
- Video Capture

Command and Control
18 techniques

- Application Layer Protocol (4)
- Communication Through Removable Media
- Content Injection
- Data Encoding (2)
- Data Obfuscation (3)
- Dynamic Resolution (3)
- Encrypted Channel (2)
- Fallback Channels
- Hide Infrastructure
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (4)
- Remote Access Software
- Traffic Signaling (2)
- Web Service (3)

Exfiltration
9 techniques

- 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

Impact
14 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (3)
- 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

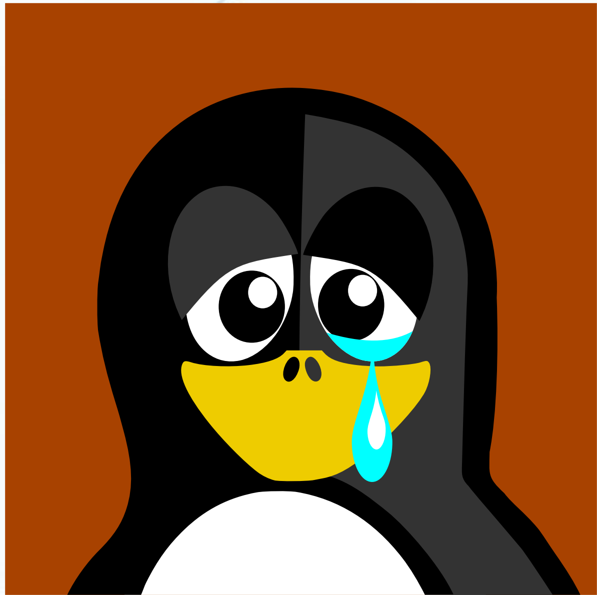
Another Breakup?

- Defense Evasion is really big
- Can we tear it apart?
    - Evading detections versus mitigations?

Linux

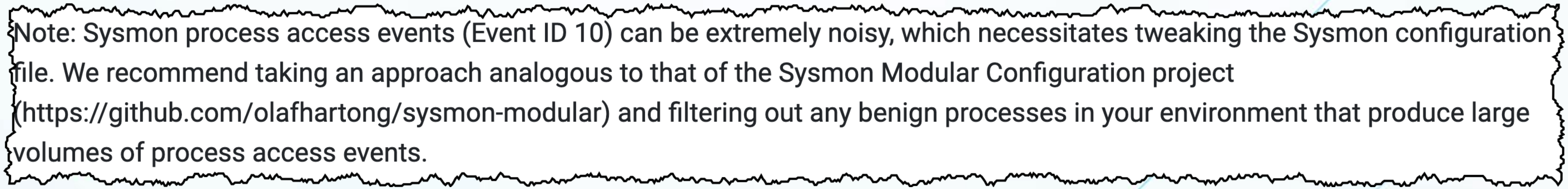
- We continue to have a tough time getting Linux data
- We've added to our Linux platform the past several releases
- It's used heavily in containers, cloud, embedded devices, network appliances, IoT, etc
- Many of you confirm that you're seeing Linux in incidents
- …And yet we still need a slide in here pleading for better Linux reporting

- Continues to be a focus area for us
  - Seeking better intelligence on Linux actor behaviors
  - Join us in #linux_attack on the MITRE ATT&CK Slack



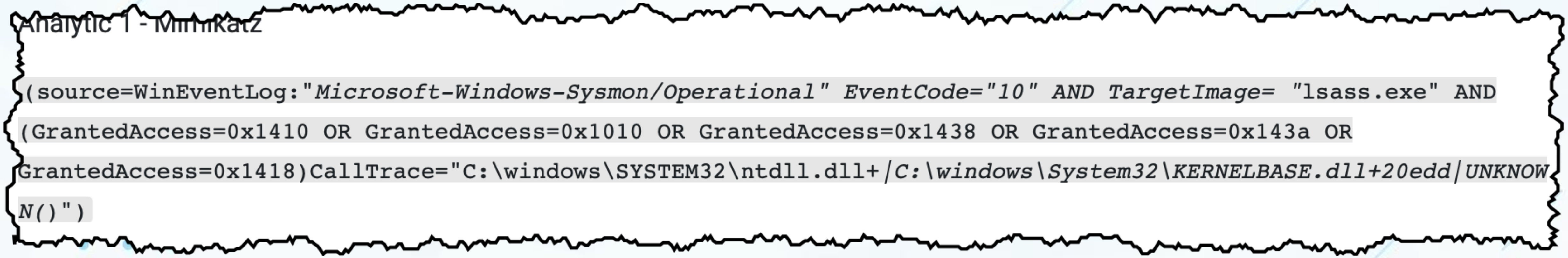
ATT&CK for Enterprise Detection Enhancements

- 100s of Techniques and Sub-Techniques updated
- More detailed notes describing the ins and outs of detection



Note: Sysmon process access events (Event ID 10) can be extremely noisy, which necessitates tweaking the Sysmon configuration file. We recommend taking an approach analogous to that of the Sysmon Modular Configuration project (https://github.com/olafhartong/sysmon-modular) and filtering out any benign processes in your environment that produce large volumes of process access events.

- 100s more analytics, developed in more directly usable formats

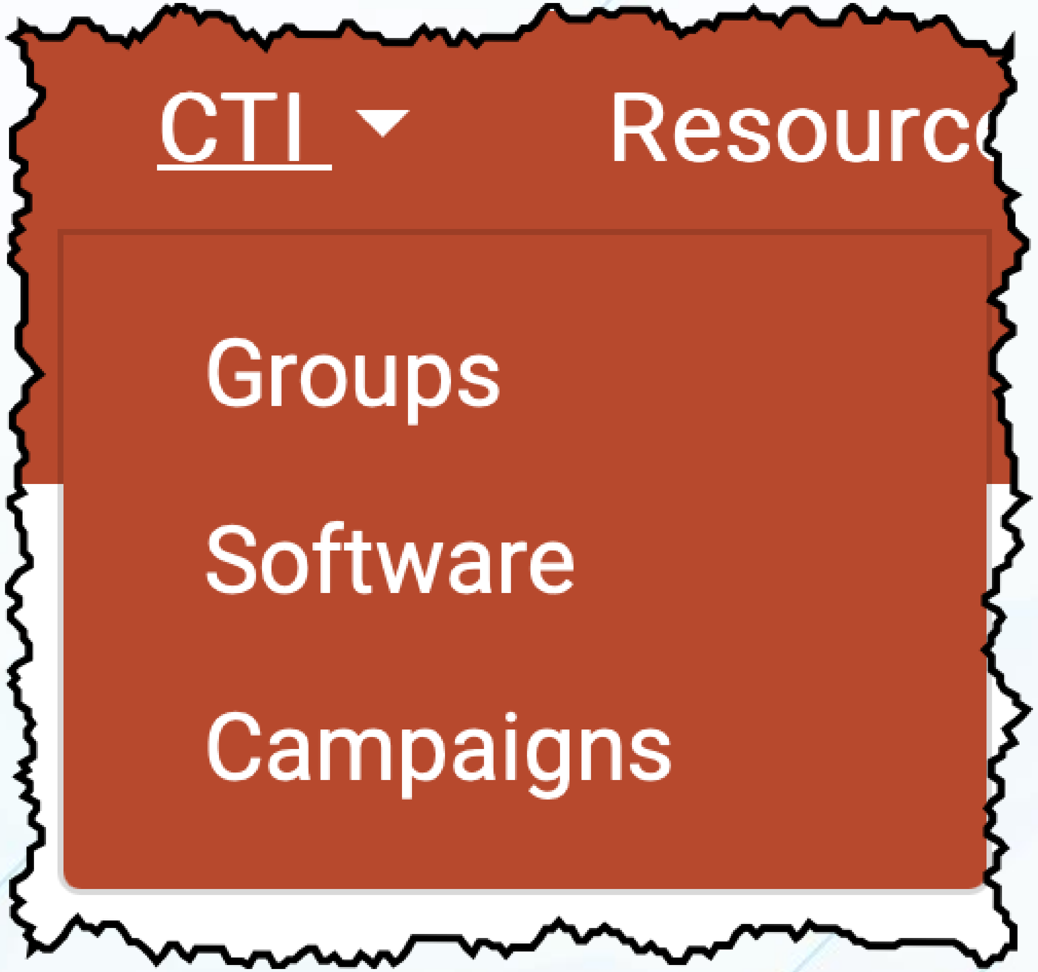


Analytic 1 - Mimikatz

```
(source=WinEventLog:"Microsoft-Windows-Sysmon/Operational" EventCode="10" AND TargetImage= "lsass.exe" AND
(GrantedAccess=0x1410 OR GrantedAccess=0x1010 OR GrantedAccess=0x1438 OR GrantedAccess=0x143a OR
GrantedAccess=0x1418)CallTrace="C:\windows\SYSTEM32\ntdll.dll+|C:\windows\System32\KERNELBASE.dll+20edd|UNKNOW
N()")
```

CTI

- Making sure we're capturing relevant groups
  - Keep up with state-directed threats
  - Continue to improve on crimeware
- Dealing with the flood of ransomware
- Better leverage campaigns

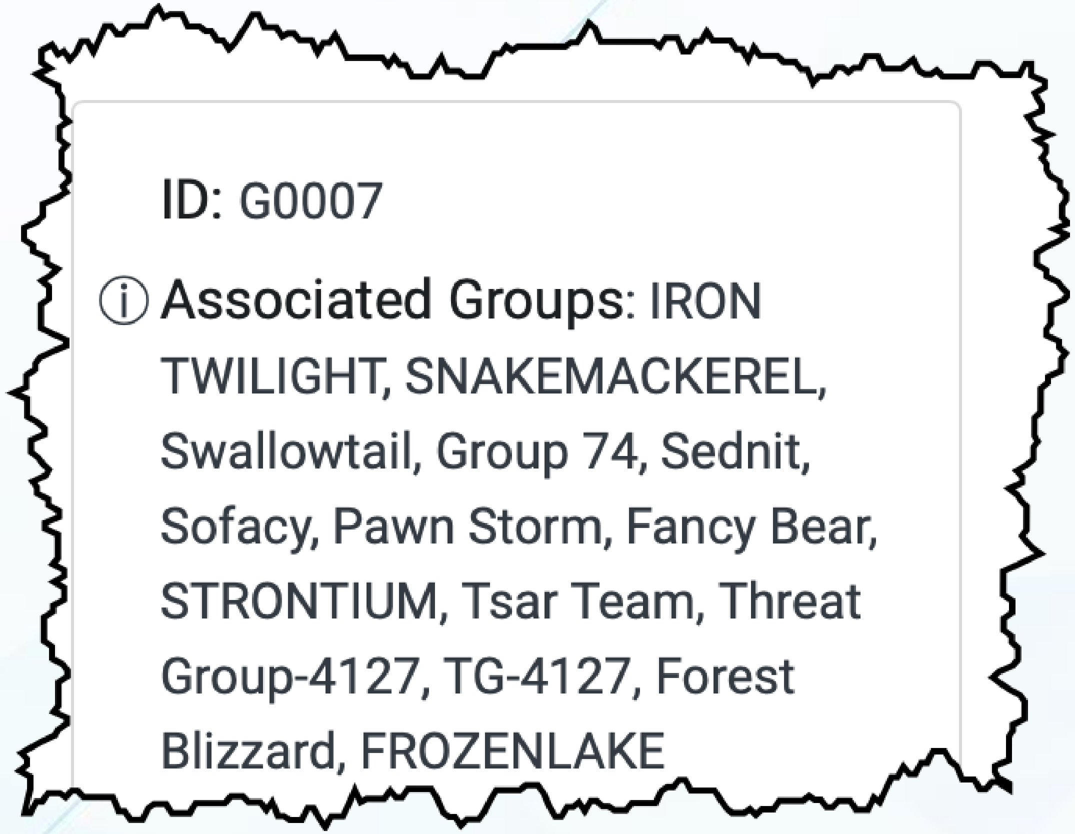


Group Names ?

APT28, IRON TWILIGHT, SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127, Forest Blizzard, FROZENLAKE

→

G0007?



ID: G0007

ⓘ Associated Groups: IRON TWILIGHT, SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127, Forest Blizzard, FROZENLAKE

ATT&CK for ICS and Mobile

- No new content in v16– Work has restarted for v17

- ATT&CK for ICS
  - 🎉 Joining the sub-technique party! 🎉
  - Asset coverage expansion
  - Improved defensive coverage

- ATT&CK for Mobile
  - Expansion into Reconnaissance and Resource Development Tactics
  - The return of telecom platform(s)?

Getting involved

ATT&CK Benefactor Program

- Opportunity for organizations to help sustain and advance ATT&CK
- Accepting charitable donations to be leveraged directly for ATT&CK
- Recognition on attack.mitre.org, CTID’s website, our social media, and at ATT&CKcon
- To learn about other benefits or to contact us visit https://bit.ly/ATBenif

TIDAL CYBER
THREAT-INFORMED DEFENSE

ZIMPERIUM®

SOC PRIME

Thank you! & more ways to get involved

- Social media – all major announcements to each
  - Bluesky @attack.mitre.org
  - LinkedIn https://www.linkedin.com/showcase/mitre-att&ck/
  - Slack https://bit.ly/ATTd

- Community contributions
  - attack@mitre.org
  - https://attack.mitre.org/resources/engage-with-attack/contribute/

- ATT&CKcon 6.0
  - October 14 & 15, 2025 at MITRE's McLean, VA campus and virtually online