RSAConference2019

San Francisco | March 4–8 | Moscone Center

BETTER.

SESSION ID: SPO3-W03

How to Evolve Threat Hunting by Using the MITRE ATT&CK Framework

Jared Myers

Sr. Threat Researcher
Carbon Black, Threat Analysis Unit
@jmyers36

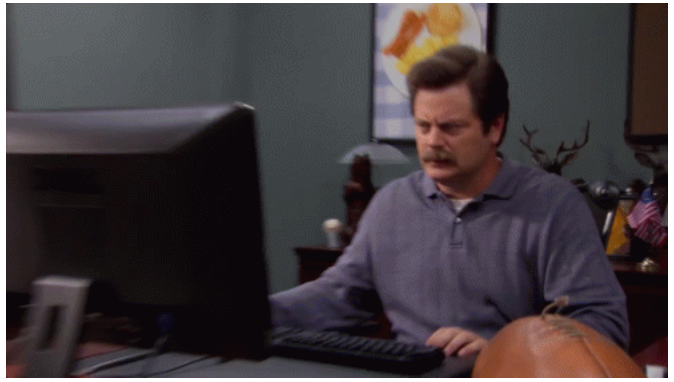
Agenda and whoami

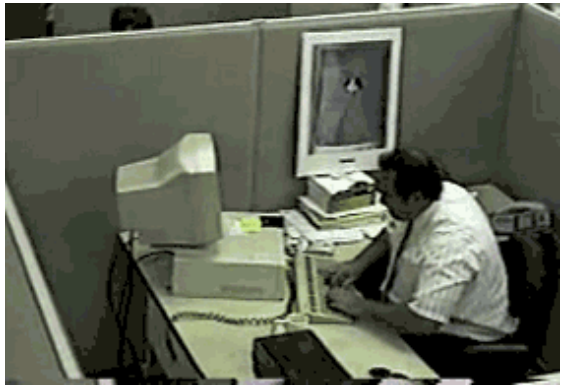
- Background of ATT&CK
- Case Study of ATT&CK in action
- MITRE ATT&CK Simulations
- Advanced Threat Hunting

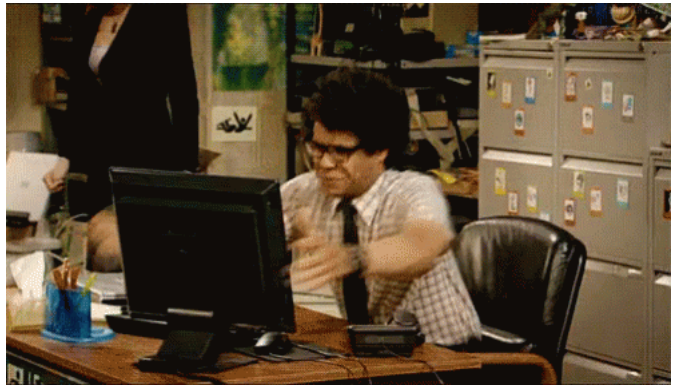
Feeding the Fire

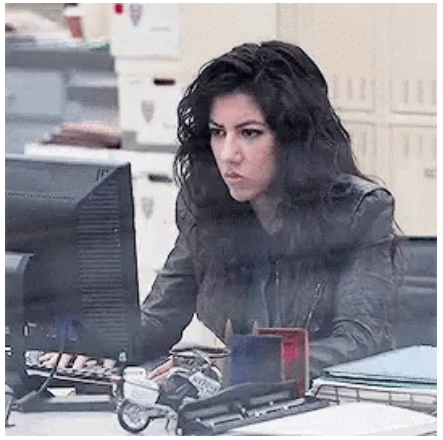
- Threat Hunting Objectives
  - Finding the unknown
  - While hunting for the characteristics and behaviors that are harder to automate you will continue to identify gaps
  - *How well are we doing at detecting documented adversary behavior?* -MITRE
  - And the cycle starts over again.

But they said to just do the ATT&CK...





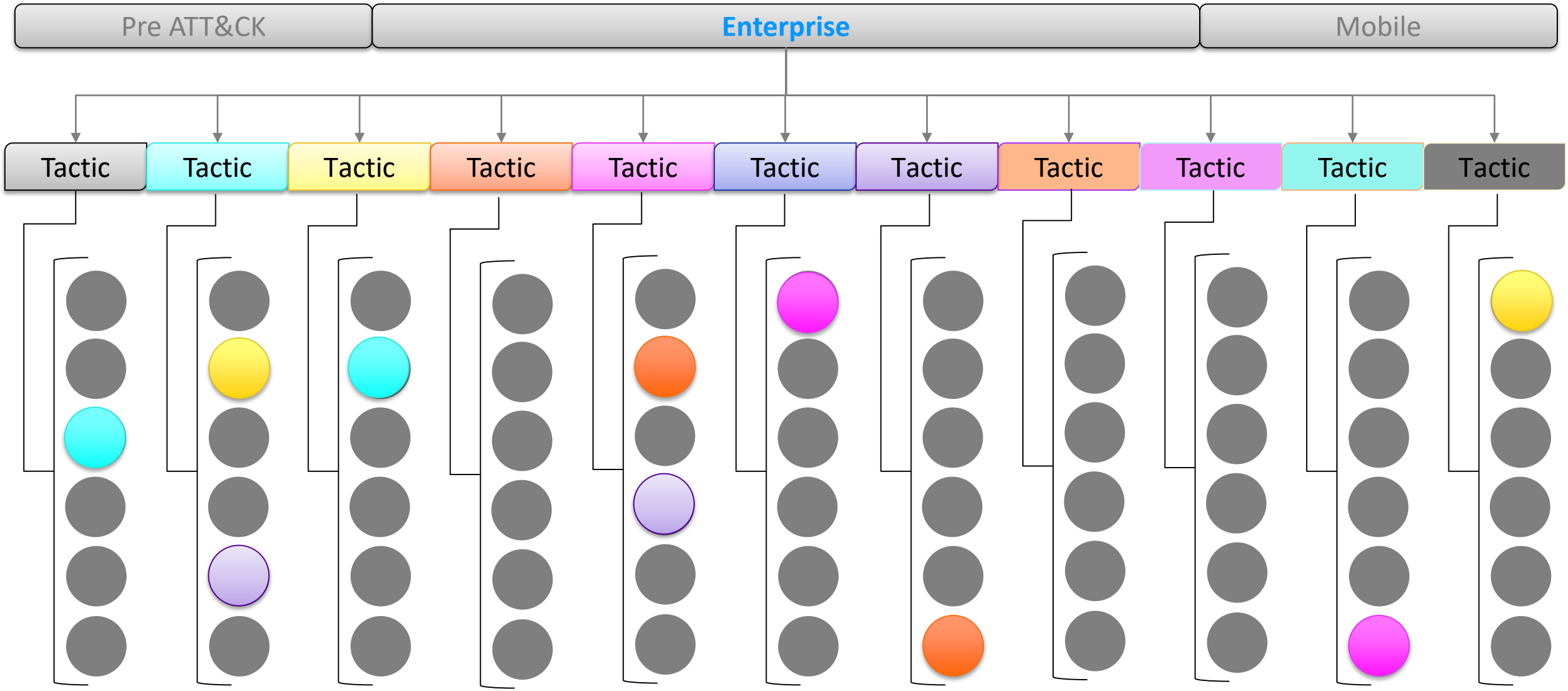




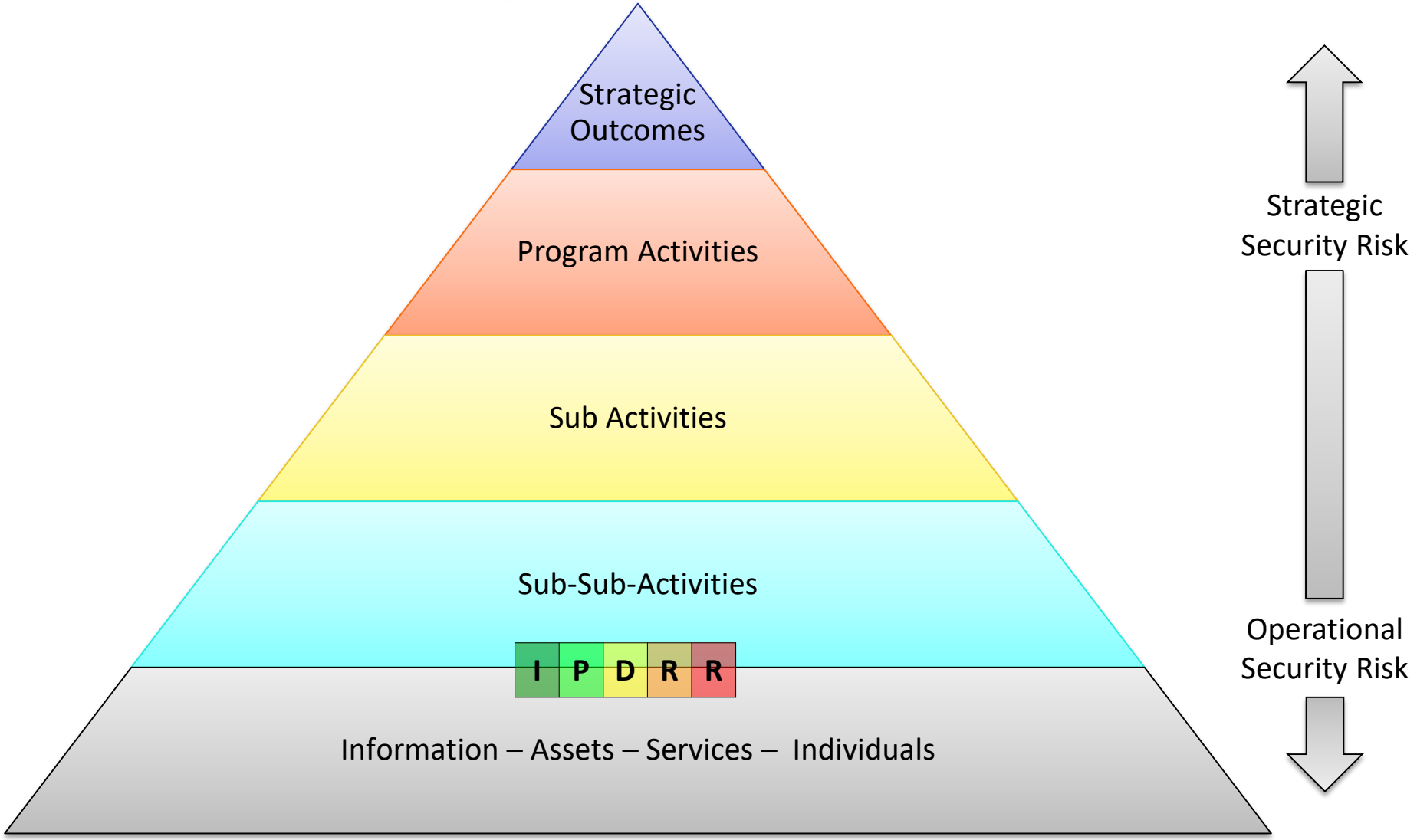
RSAConference2019

ATT&CK Background

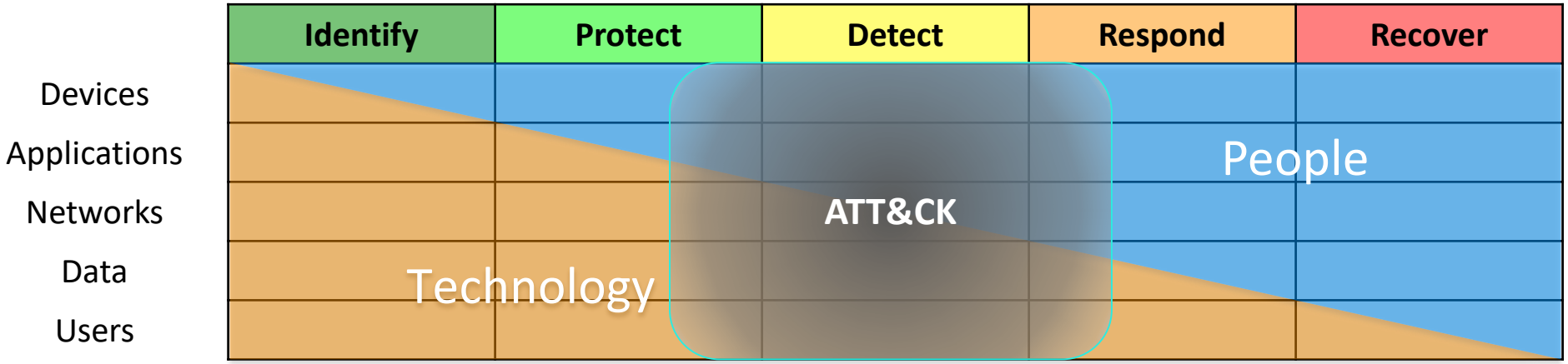
Quick ATT&CK Overview



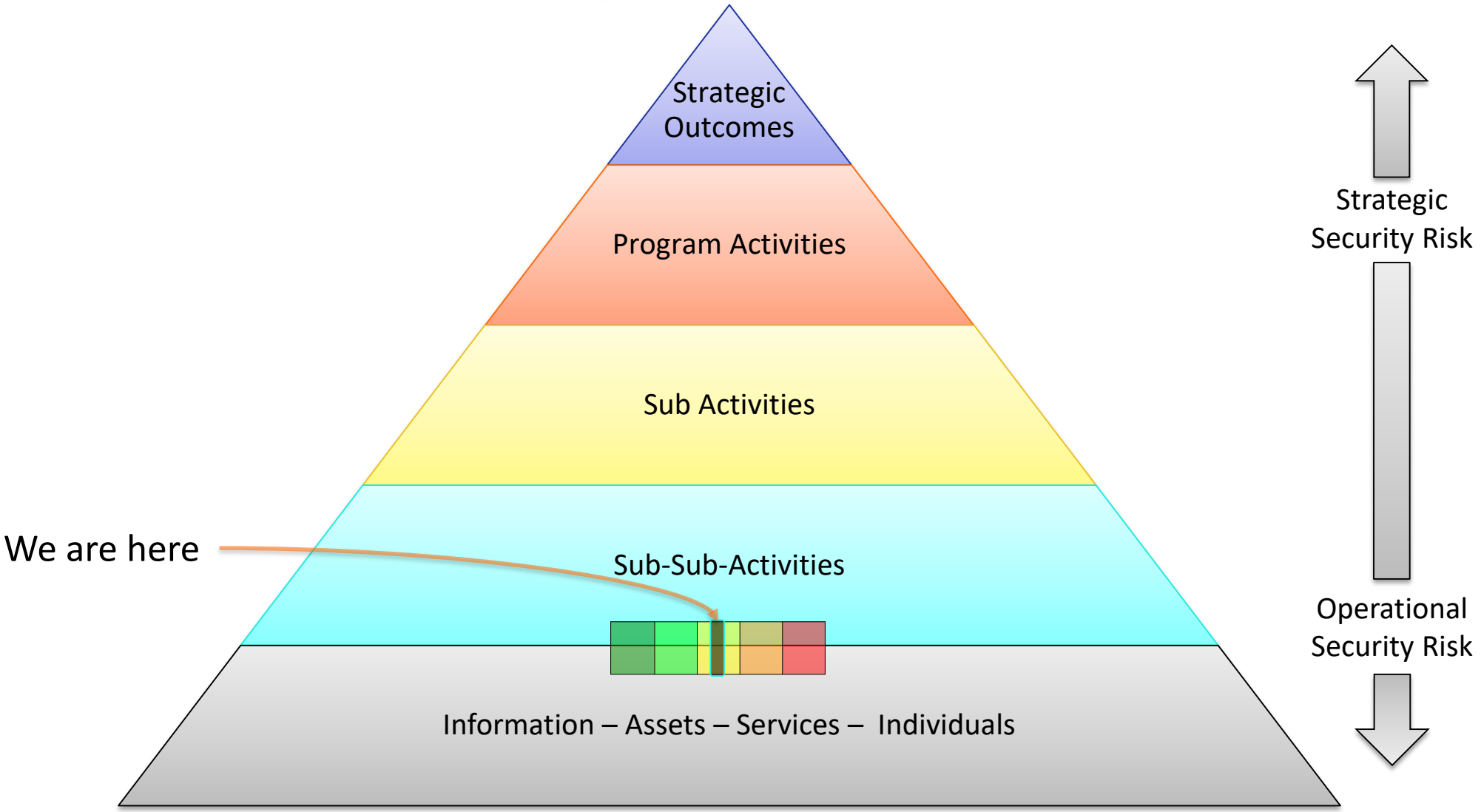
Where ATT&CK Fits



Where ATT&CK Fits



Where ATT&CK Fits



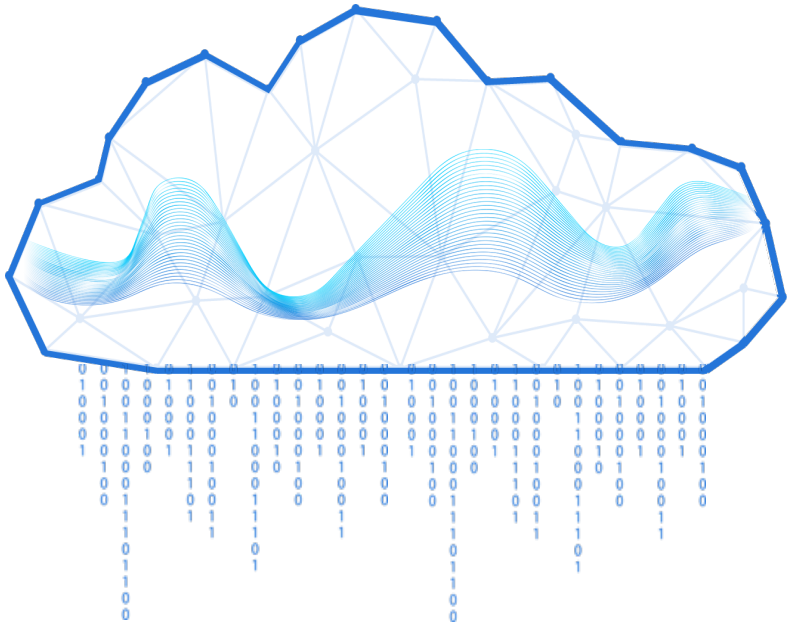
In perspective

MITRE ATT&CK is:

- *A common language that can be used to share intel based off of a standardized model*
- *A useful tool for measurement an understanding your visibility and gaps*
- *An approach to go beyond conventional IOCs*

In perspective

- MITRE ATT&CK is not:
  - *ATT&CK by itself is not intended to be a checkbox of risk assessment*
  - *The evaluation put out are not a single axis but rather a way to understand the Vendor's philosophy for detection*
  - *Not all techniques are equal*



In perspective

T1107

File Deletion

- Malware, tools, or other non-native files dropped or created on a system by an adversary may leave traces behind as to what was done within a network and how. Adversaries may remove these files over the course of an intrusion to keep their footprint low or remove them at the end as part of the post-intrusion cleanup process.

RSAConference2019

Threat Hunting

Threat Hunting after you lay your foundation

Easy vs Hard

- Why is this different
  - You should be able to leverage your tools or products to detect high fidelity alerts which you identified previously.
  - Your threat hunting should focus on the things that are not so easily detectable.

Threat Hunting

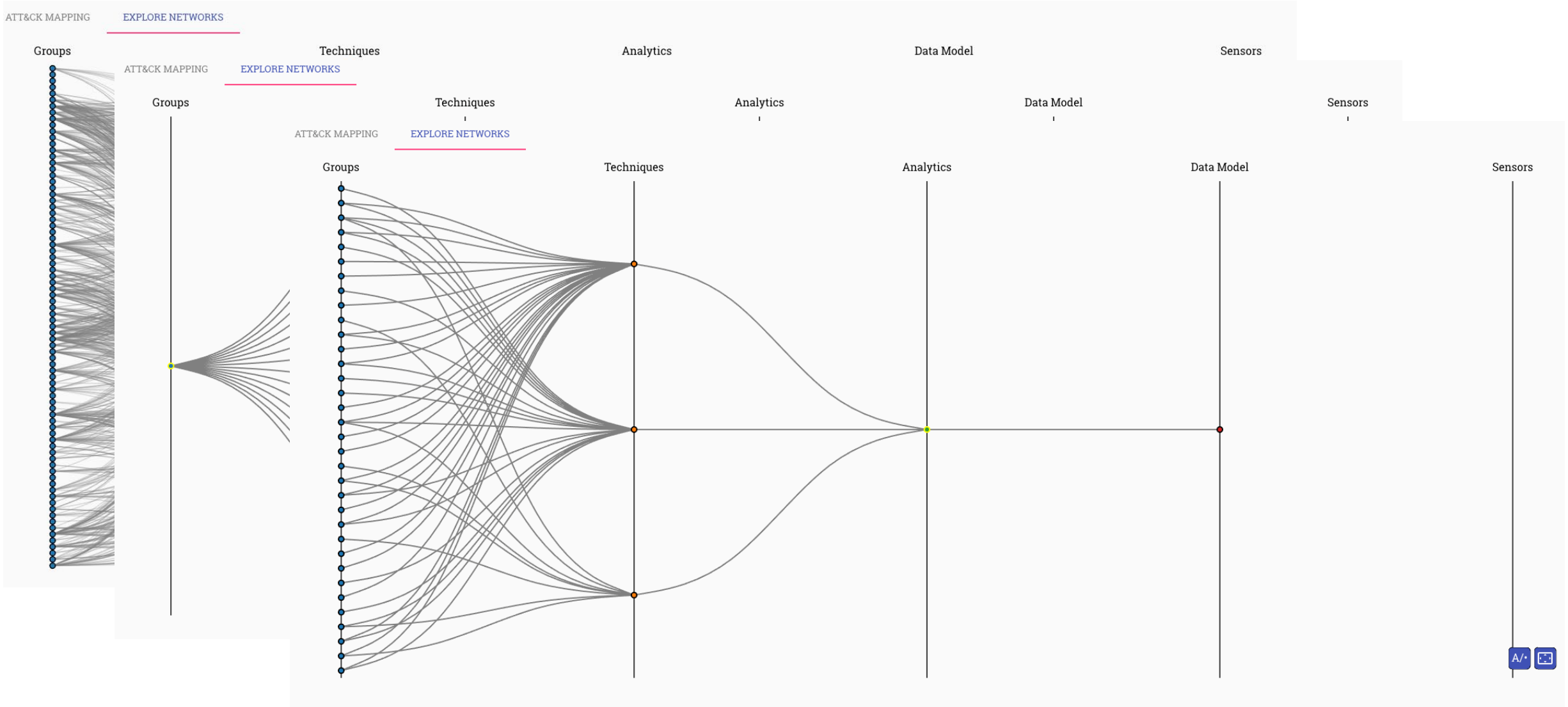
Hunting for Threats or Gaps

Same approach different goals

Going Broader

- Moving from specific Tactics or Techniques to emulation
- Live Action or Pen Test

Use Cases, Building a POV



RSAConference2019

Case Study

ATT&CK in action

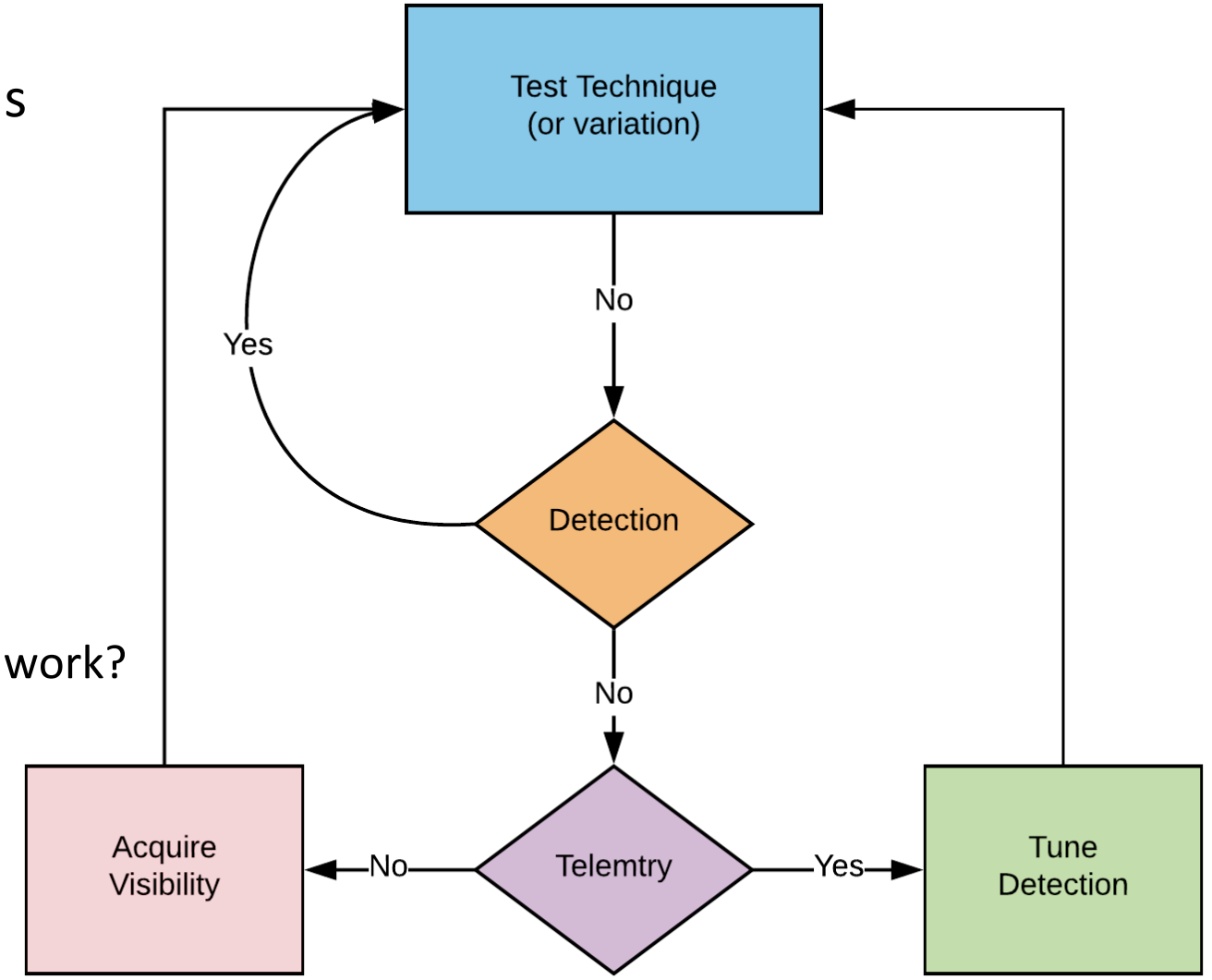
Use Cases, Start Small

Testing your production security controls

Aid in evaluation of new controls

Testing for <u>results</u>

- Is this thing on?
- Does the security operations system actually work?



LolBins, UAC Bypass, & Priv-Escs….Oh My

https://attack.mitre.org/wiki/Technique/T1191

- Adversary's are adapting tradecraft to less known execution techniques.
- What is this **CMSTP** binary and why is it making network connections?

- Is the binary signed?
- Does the binary ship in EVERY version of modern windows?
- Can the binary execute remote payloads?
- Does the binary allow auto-elevation of process execution?

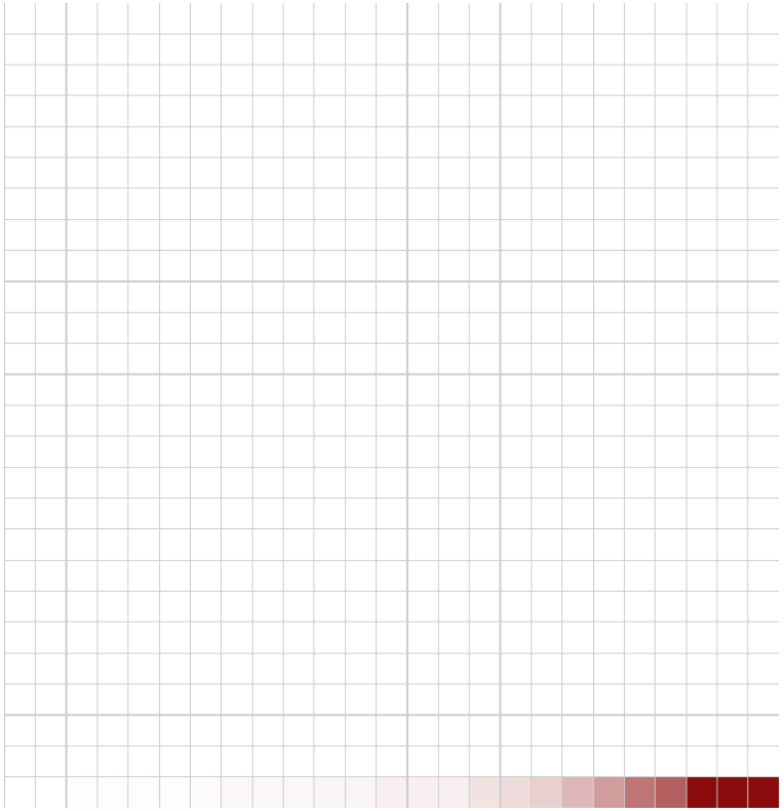
UAC Bypass and LOLBins

- Let's get familiar with the MITRE Wiki for T1191

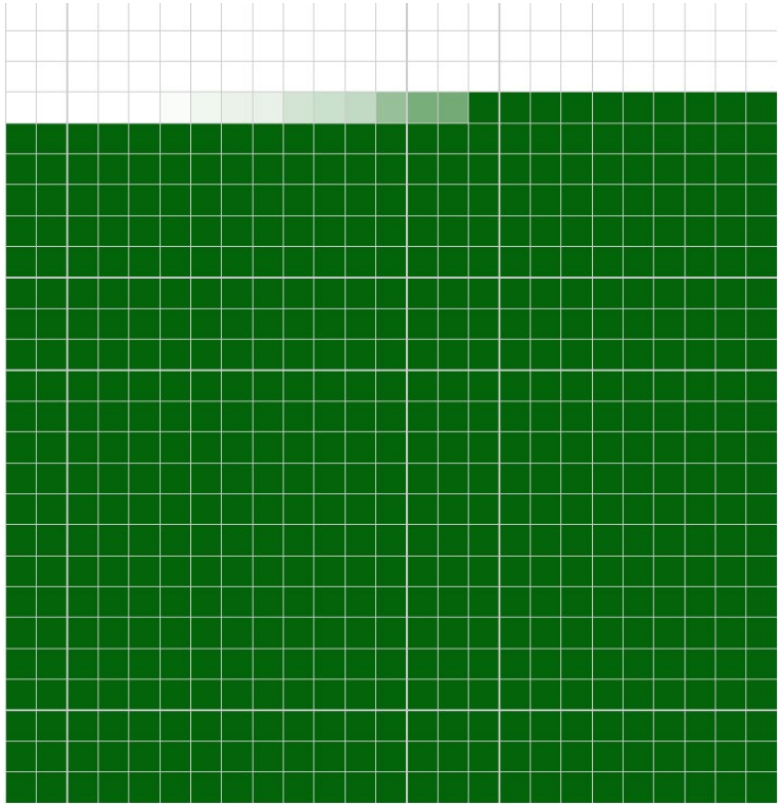
> *"Use process monitoring to detect and analyze the execution and arguments of CMSTP.exe. Compare recent invocations of CMSTP.exe with prior history of known good arguments and loaded files to determine anomalous and potentially adversarial activity."*

- How many times has this binary executed?
- Are there leading indicators of something malicious?
  - Making network connections?
  - Spawning child processes out of temp directories, command-interps, etc?
  - Child processes spawned from dllhost cmstp COM object?

How often is cmstp executed

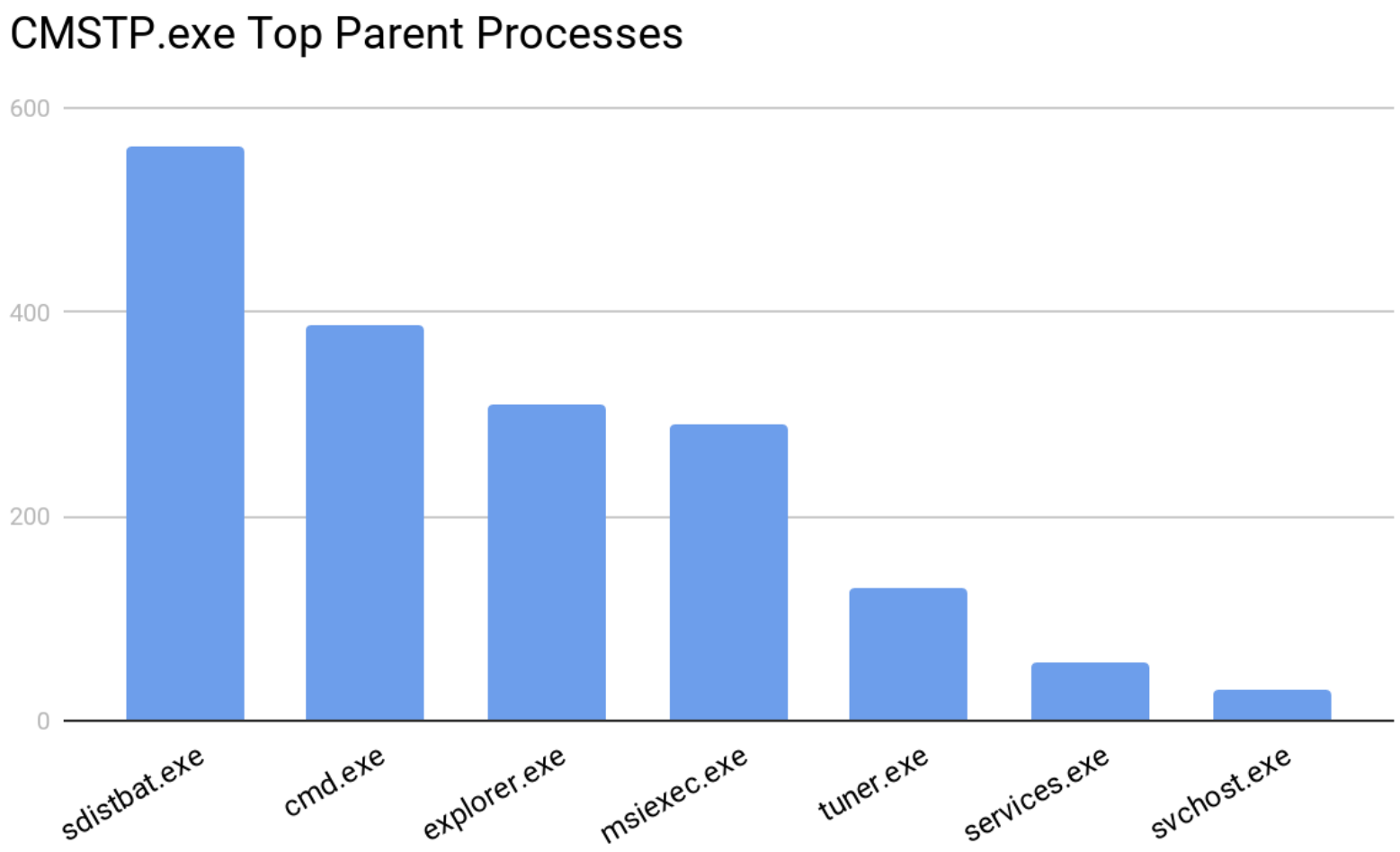


cmstp.exe



chrome.exe

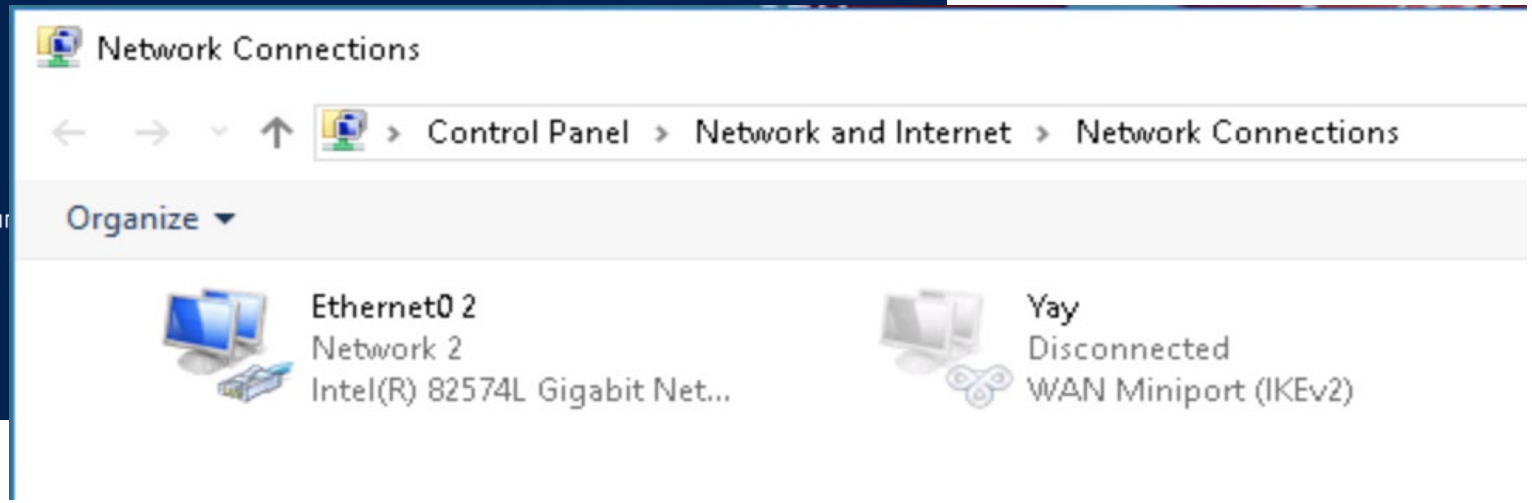
What are the most common parents



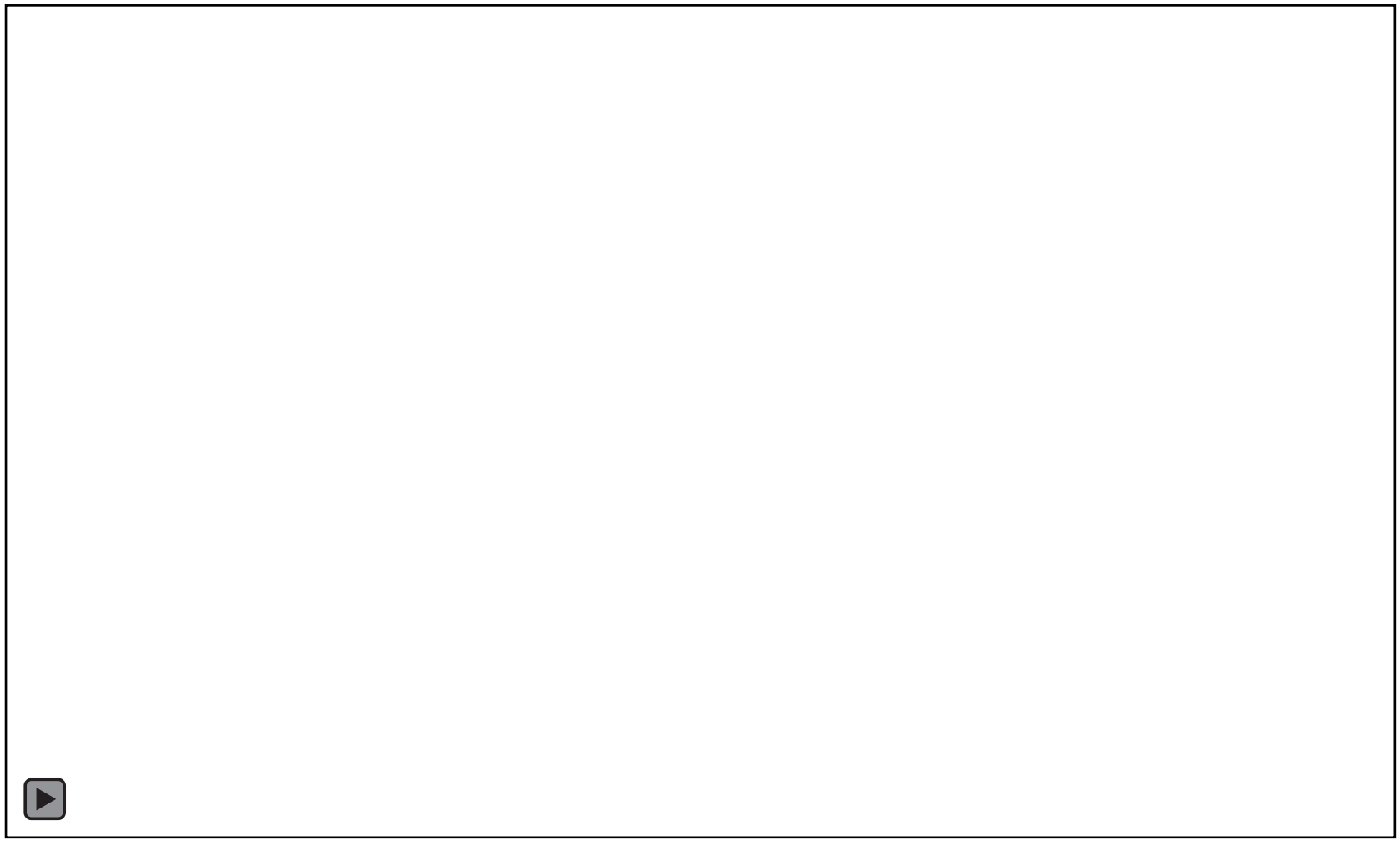
Leveraging Unit Testing Internally

- You don’t have to be a red teaming expert to test your security controls

```
PS C:\Users\tbrady\Desktop\atomic-red-team-master> $T1191 = Get-AtomicTechnique -Path .\atomics\T1191\T1191.yaml
PS C:\Users\tbrady\Desktop\atomic-red-team-master> cd .\atomics\T1191
PS C:\Users\tbrady\Desktop\atomic-red-team-master\atomics\T1191> Invoke-AtomicTest $T1191
[********BEGIN TEST*******]
CMSTP T1191
CMSTP Executing Remote Scriptlet
Adversaries may supply CMSTP.exe with INF files infected with malicious commands

Command Prompt:
 cmstp.exe /s T1191.inf

[********BEGIN TEST*******]
CMSTP T1191
CMSTP Executing UAC Bypass
Adversaries may invoke cmd.exe (or other malicious com
NF file

Command Prompt:
 cmstp.exe T1191_uacbypass.inf /au

[!!!!!!!!END TEST!!!!!!!!]
```

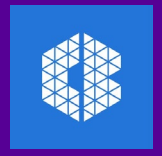


Automating Testing



RSAConference2019

Questions ?



@jmyers36
jmyers@carbonblack.com