Desjardins

Purple Team: From Silos to Heroes

Hackfest 14 - Resurection Edition

📅 2022-10-29

TTIC CYBER DEFENSE

Agenda

- Who we are
- Defining Purple Teaming
- Challenges with the current landscape
- Continuous Purple Teaming
  - Process
  - People
  - Techno
- Building a security posture
- The ultimate goal

> TL;DR ❤️ + 💙 = 💥🚀

TTIC CYBER DEFENSE

Bio: Martin Dubé

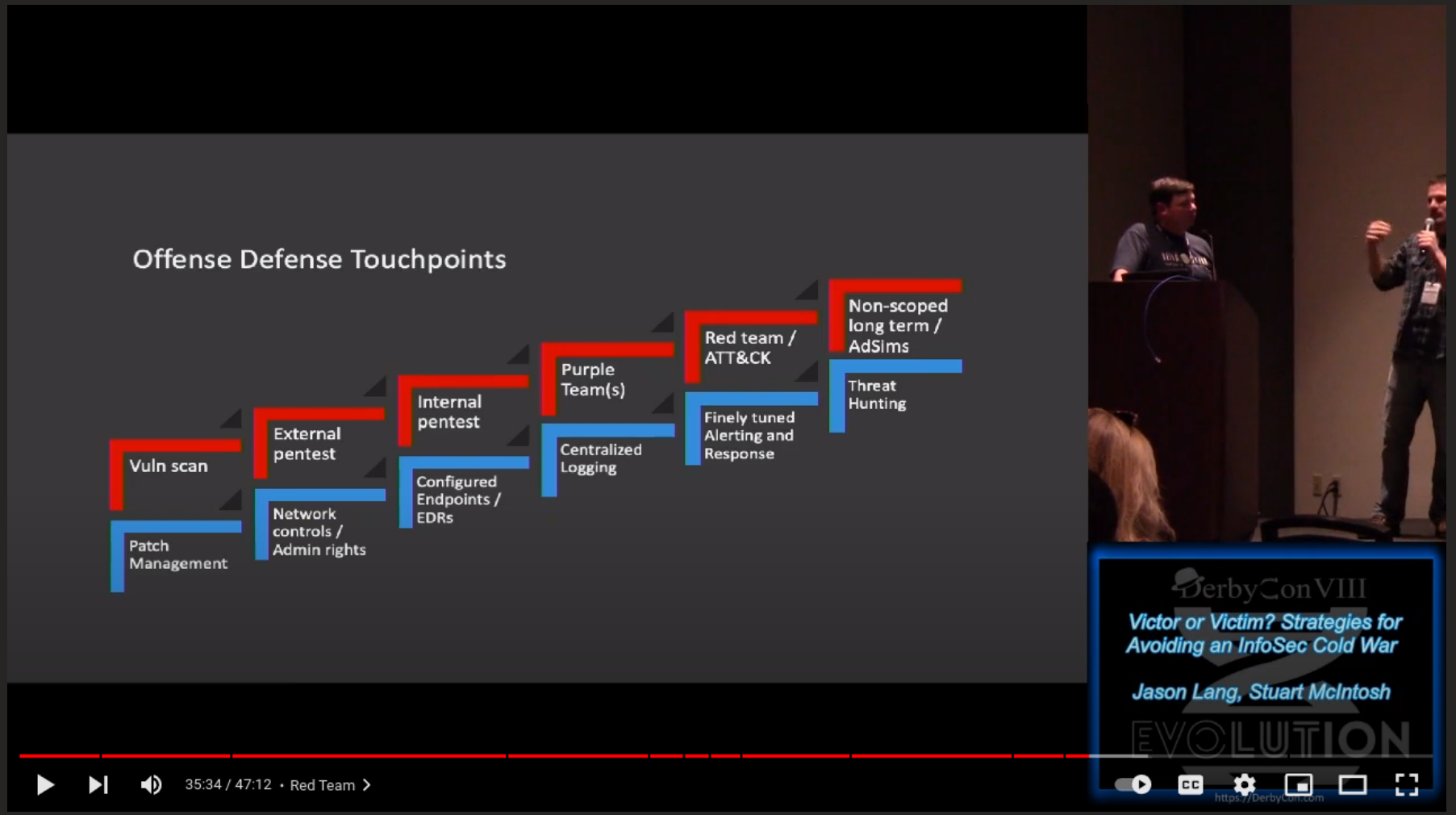
- Offensive Security Senior Manager 👔
  - Strive to improve Cyber-Security one meeting at a time 📅
  - Pentest, ROP, Red, AppSec, Threat Modeling
- Former HF board member and CTF Team Leader (2010-2015 + 2017)
- Former CTF Designer at NSEC (2018)
- Father of 2 👨‍👧‍👧, Woodworker 🪵, Runner 🏃
- May be found where there is:
  - Expresso 🍮
  - Whiskys 🥃
  - BBQ 🥩

Bio: Dany Lafrenière

- SOC Senior Manager 👔
- Master at agenda Tetris 🧩📅🧩
- Tierless SOC strong believer ♾️
- In love with a cat lover 🐱🐱🐱
- I eat chicken wings with a fork 🍴
- My favourite superhero is ... Forrest Gump!

TTIC CYBER DEFENSE

Inspiration for this talk



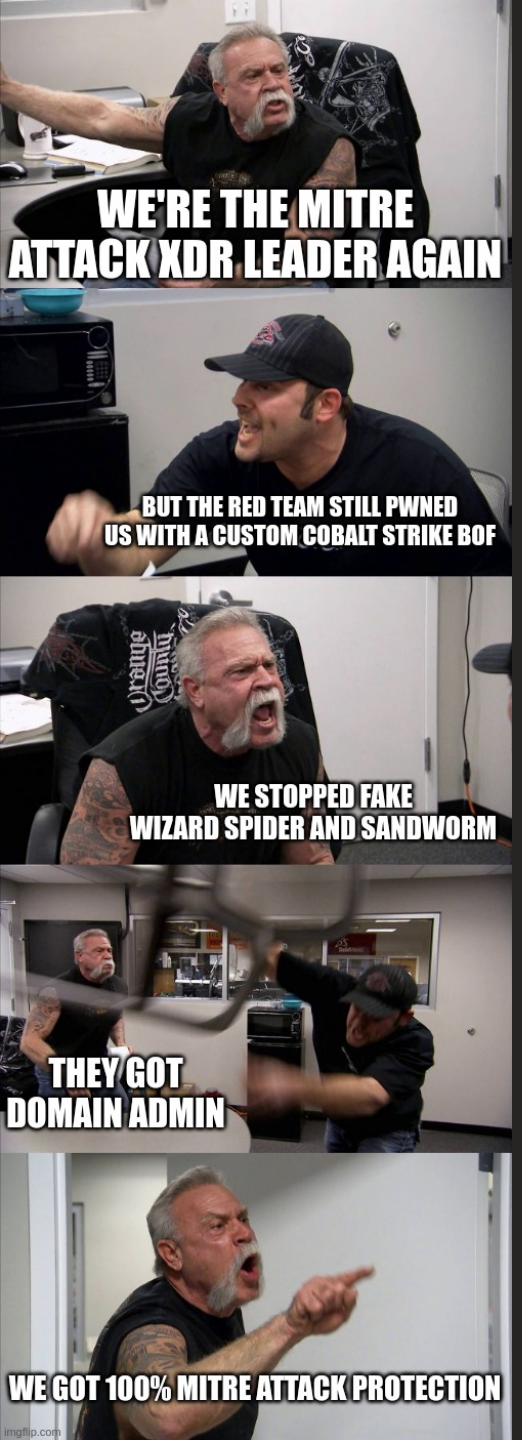
https://www.youtube.com/watch?v=9_cZ5xn-huc

Blue vs Purple vs Red (day-to-day)

Purple is a cooperative mindset between attackers and defenders working on the same side. As such, it should be thought of as a function rather than a dedicated team. ^1

Blue Team activities	Purple ~~Team~~ activities	Red Team activities
Goal: Defend	Goal: Improve posture	Goal: Test resiliency
Require: Autonomy	Require: Collaboration	Require: Incident (Surprise)
Velocity: High	Velocity: High	Velocity: Low
Analogy: Self-study	Analogy: Group study	Analogy: The exam

^1: https://danielmiessler.com/study/red-blue-purple-teams/



Challenges with current landscape

The typical project-based testing workflow is limited.

- Priorization is often only based on public data
- CVSS is *so* imperfect
- Reports require unnecessary time to write and consume
  - And they "expire" once delivered (snapshots)
- Reports hardly feed a security posture

Some security vendors are very optimistic.

> 100% Mitre Attack Protection 💪

Challenges with current landscape

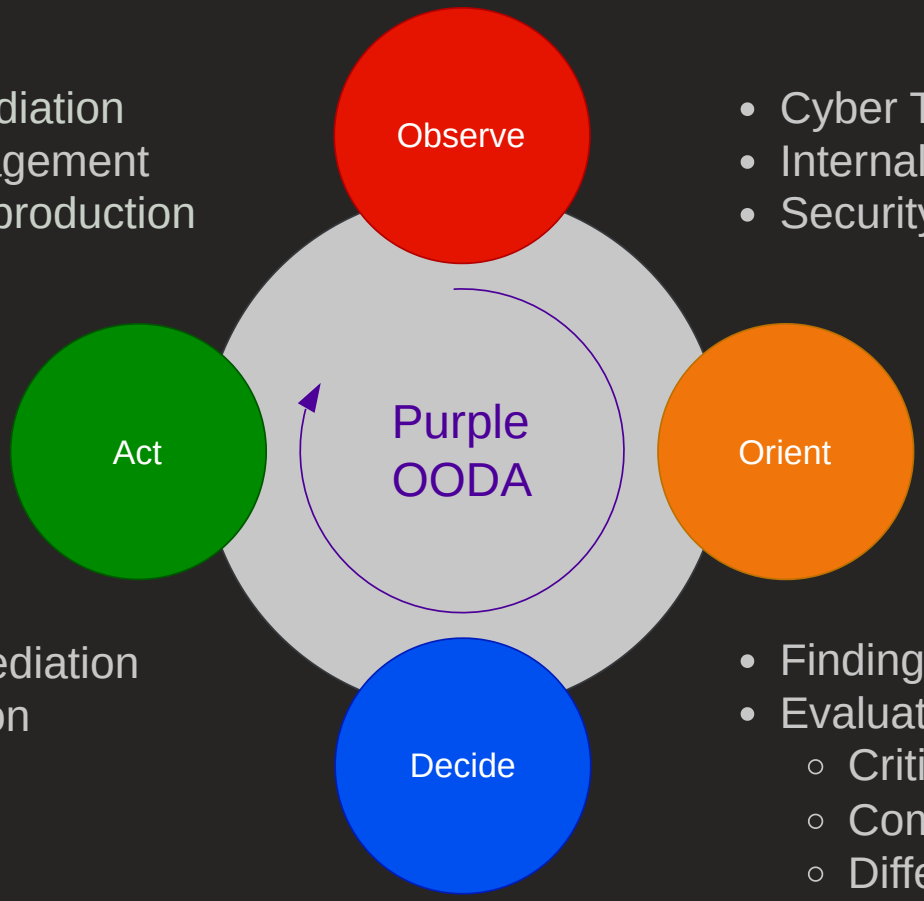
- Results are hard to consume
  - Blue team manager's point of view ... TL;DR
- Recommendations are easy
- Multiples goals and priorities with finite resources
  - ...the never-ending operational backlog and incident response

Continuous Purple Teaming

Process, People, Techno

Can Your Purple Team OODA Loop?

- Prepare remediation
- Change management
- Implement in production

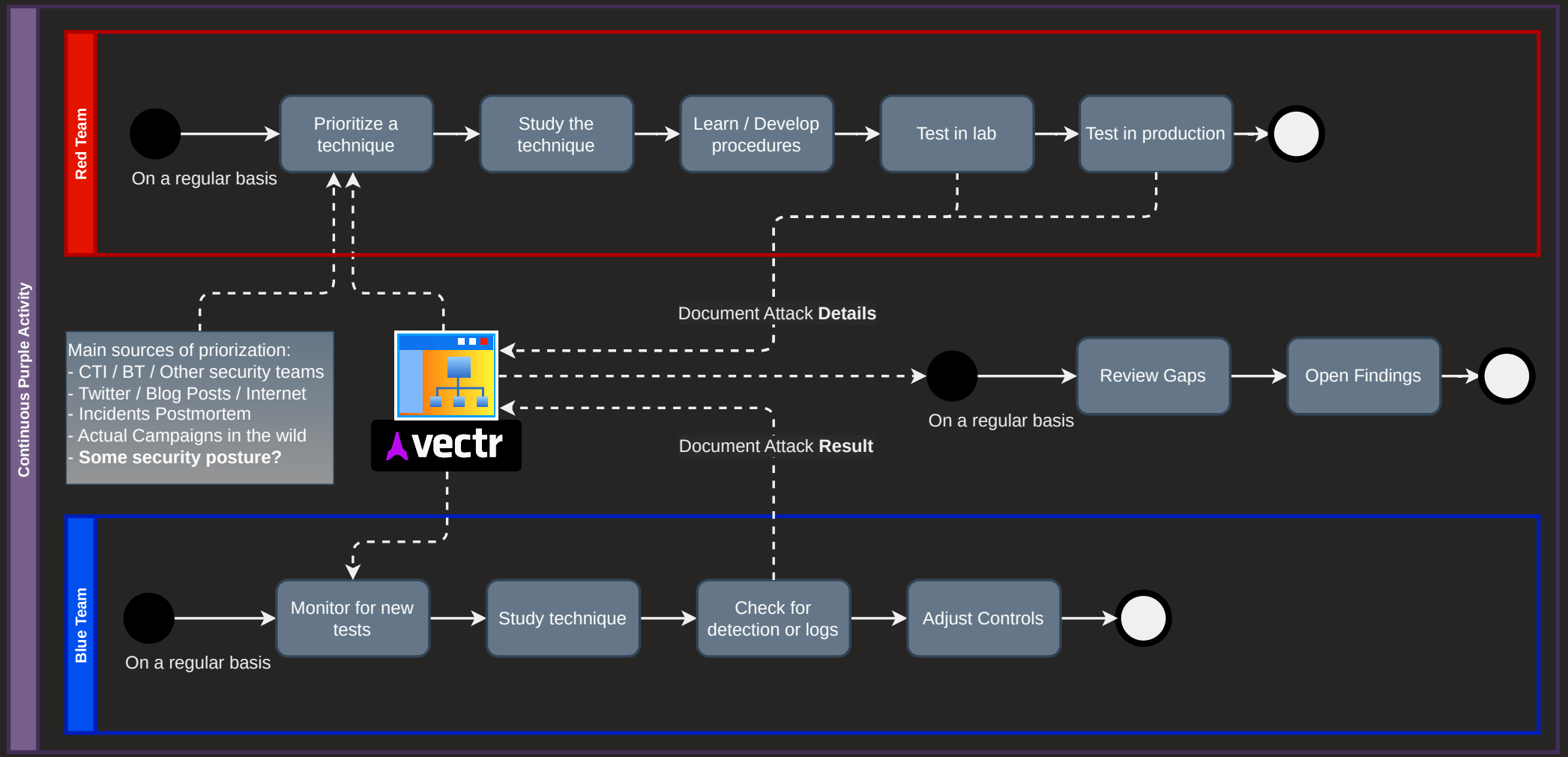


- Cyber Threat Intelligence
- Internal and external environment
- Security posture

- Prioritize remediation
  - Planification
  - Funding

- Findings and vulnerabilities
- Evaluate
  - Criticality
  - Complexity and efforts to remediate
  - Different options and partial remediation
- Risk assessment

How it looks on the field



Continuous Purple Teaming

Process, People, Techno

Manage your ego

- The foundational importance of trust in relationships
  - Consistency
  - Communication
  - **Time**
- Messages and actions from management is key
- The grass is always greener on the other side

Team or Teams?

What distinguishes a team from a group of people?

- The team has **a common goal**

A purple team is a *virtual* team, even though it is composed of multiple teams.

- One clear goal
- Autonomy
- Mastery

Continuous Purple Teaming

Process, People, Techno

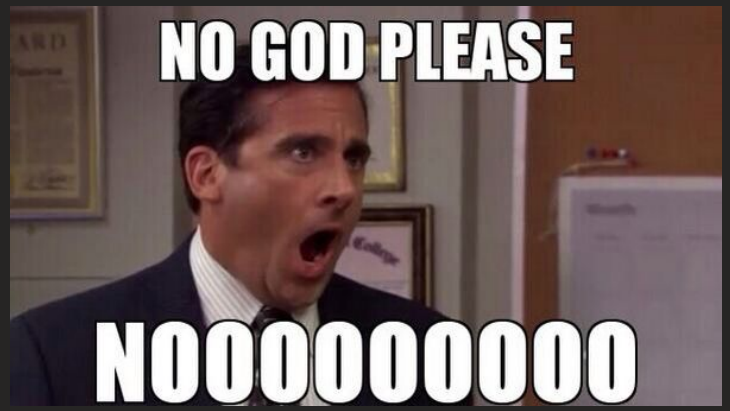
Principles

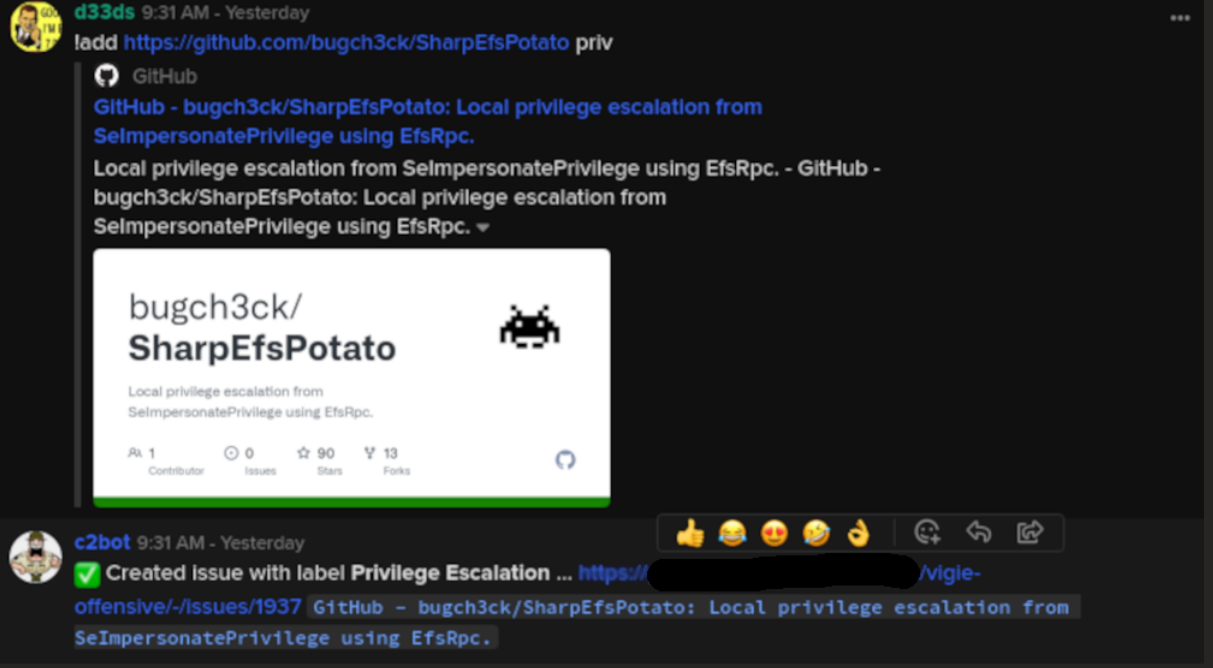
Do

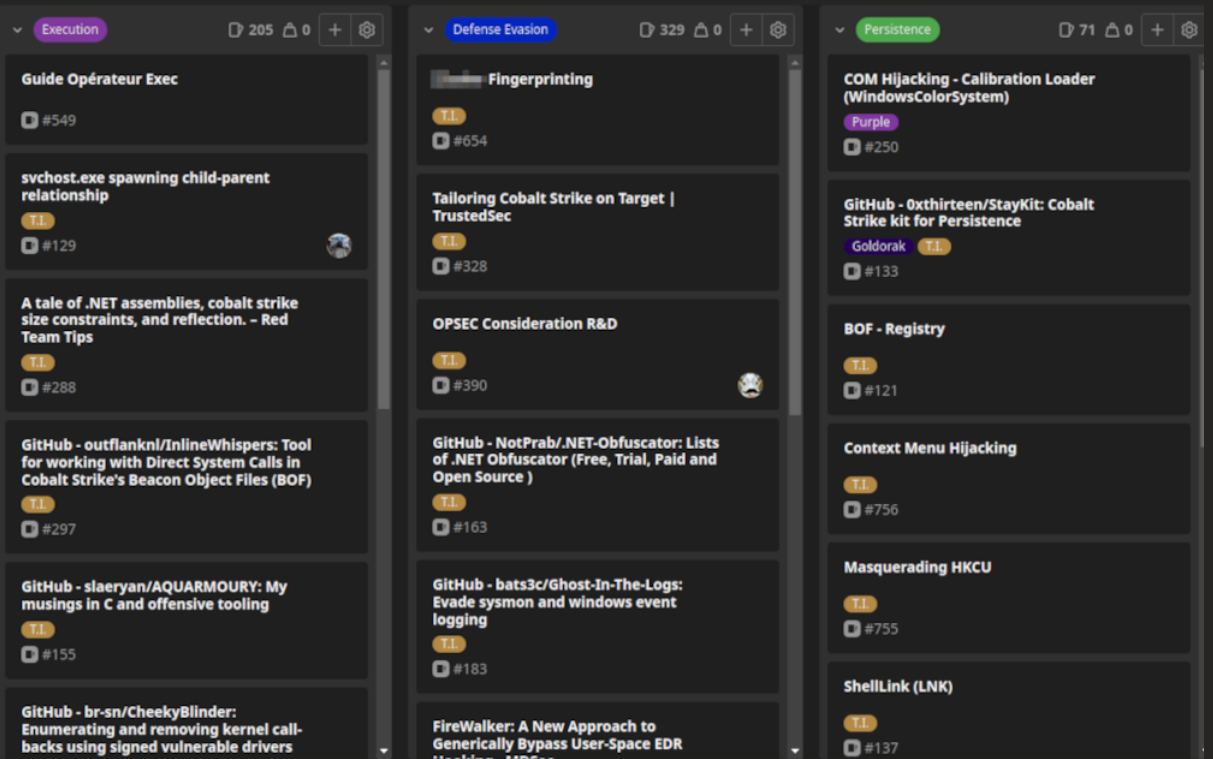
- Testing Environment
  - Run in production
  - Share to both teams ❤️💙
- Results Platform
  - Centralize results for all teams ❤️💙💛
  - APIs

Don't

- Write reports unless necessary
- Use Microsoft Office
  - Write results in Excel 🤮
  - Macros are not meant for continuous operations







Tradecraft Intelligence Platform

Intelligence Gathering is an everyday task.
Must be as lean as possible!

Prerequisite:

- Choose a ticketing system 🎟️
- Dev a bot 🤖

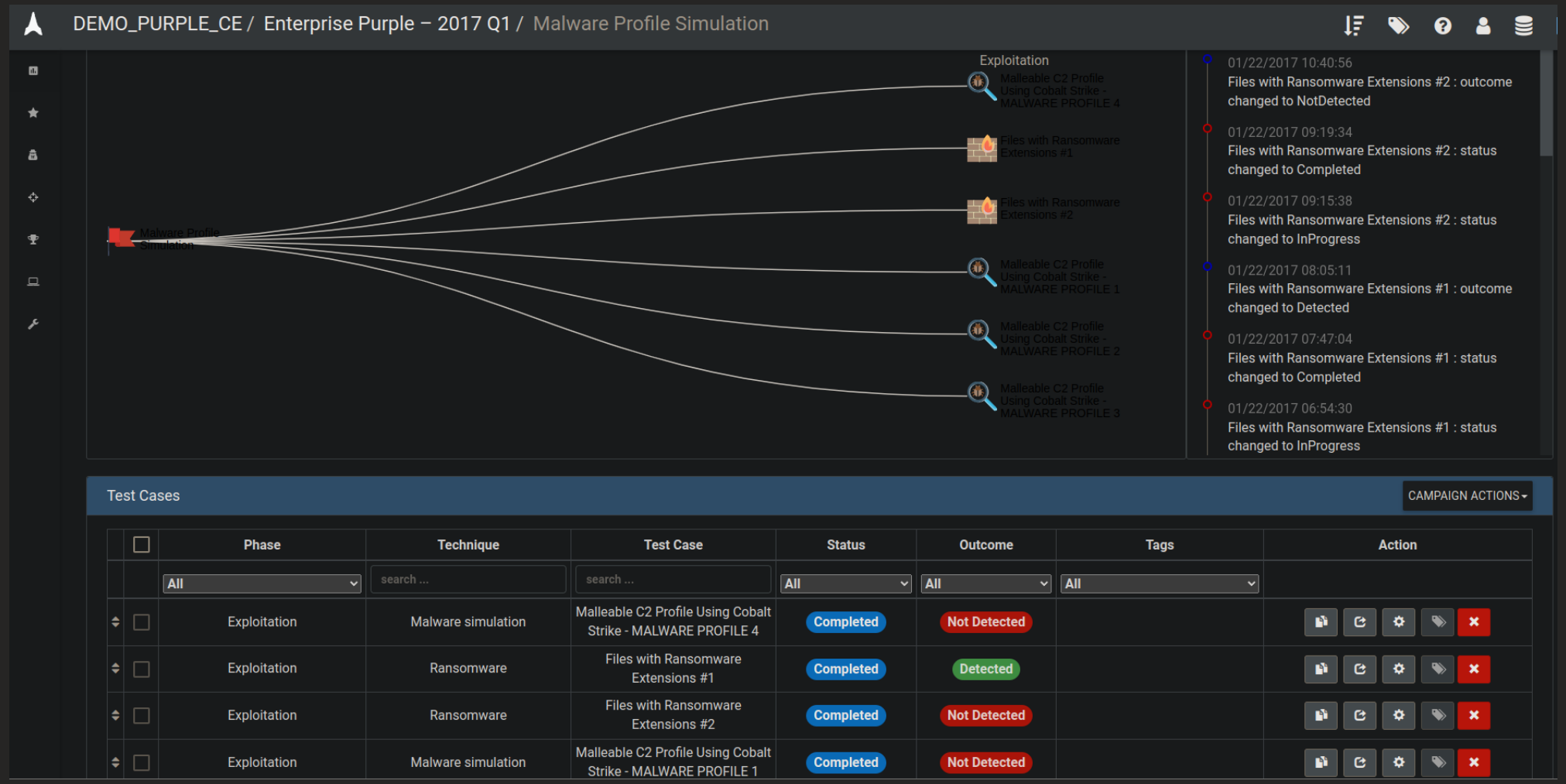
Then:

1. Discover attack procedures on twitter
2. Send them to the bot, specify the **Tactic**
3. The bot verify if it already exists
4. Append it to the pile 💩
5. Prioritize through Backlog Grooming

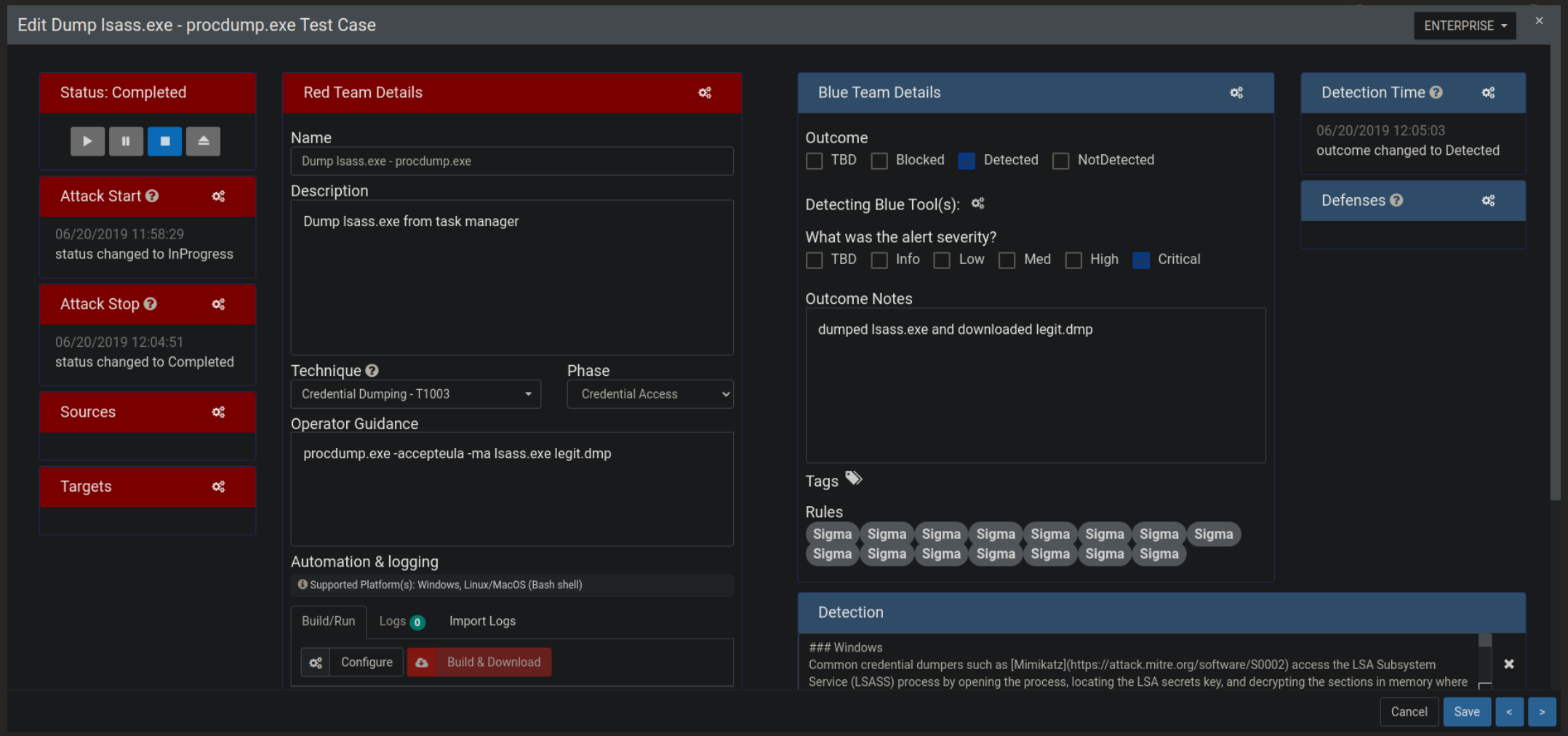
Testing Environment

- Unit Testing Tools
  - Great to quick start testing and automation
  - Many open source options
  - Can be hard to maintain ...
- Breach and Attack Simulation (BAS)
  - Feeds from up-to-date intel and TTPs
  - Great to automatically test if the controls or detection are working... or still working
  - Can be used to automate repeatable purple team tests

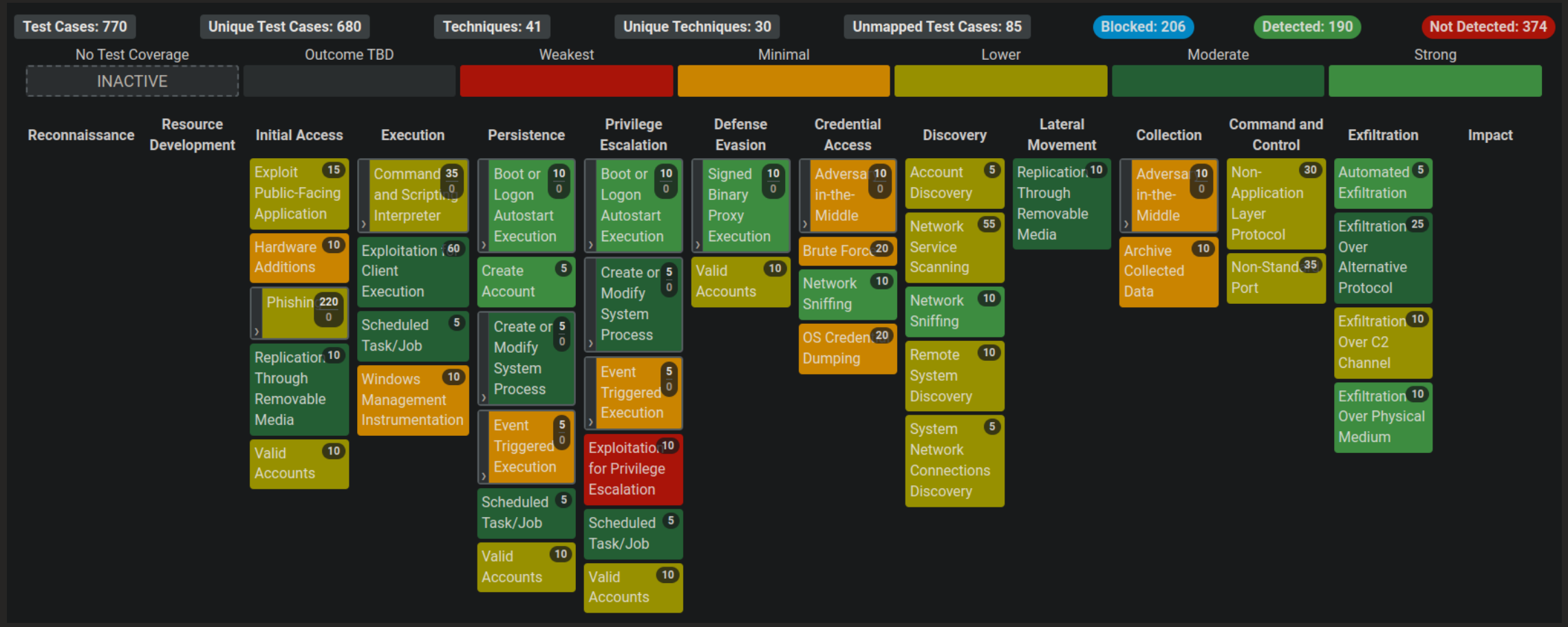
Results Platform - Vectr



Results Platform - Vectr

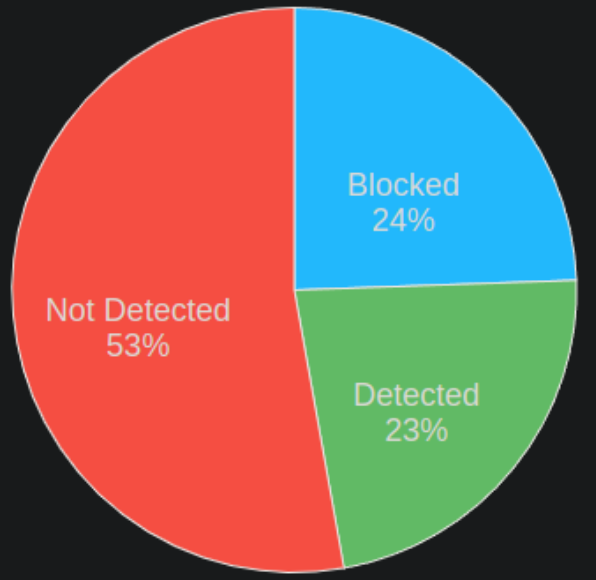


Results Platform - Vectr



Results Platform - Vectr

Campaigns Aggregated	105
Test Cases Completed:	765
Test Cases Passed:	361
Detected:	174
Blocked:	187
Test Cases Failed:	404
Not Detected:	404
Test Cases Not Completed:	0
To Be Determined:	0



Building a (*living*) security posture

What is our next best move?

The quest of building a living security posture

More challenges:

- How do we measure our progression?
- What is the baseline?
- How do we define "good enough"?
- How do we update it in real time?
- 🤯 What the hell is a security posture? 😵

The quest of building a living security posture

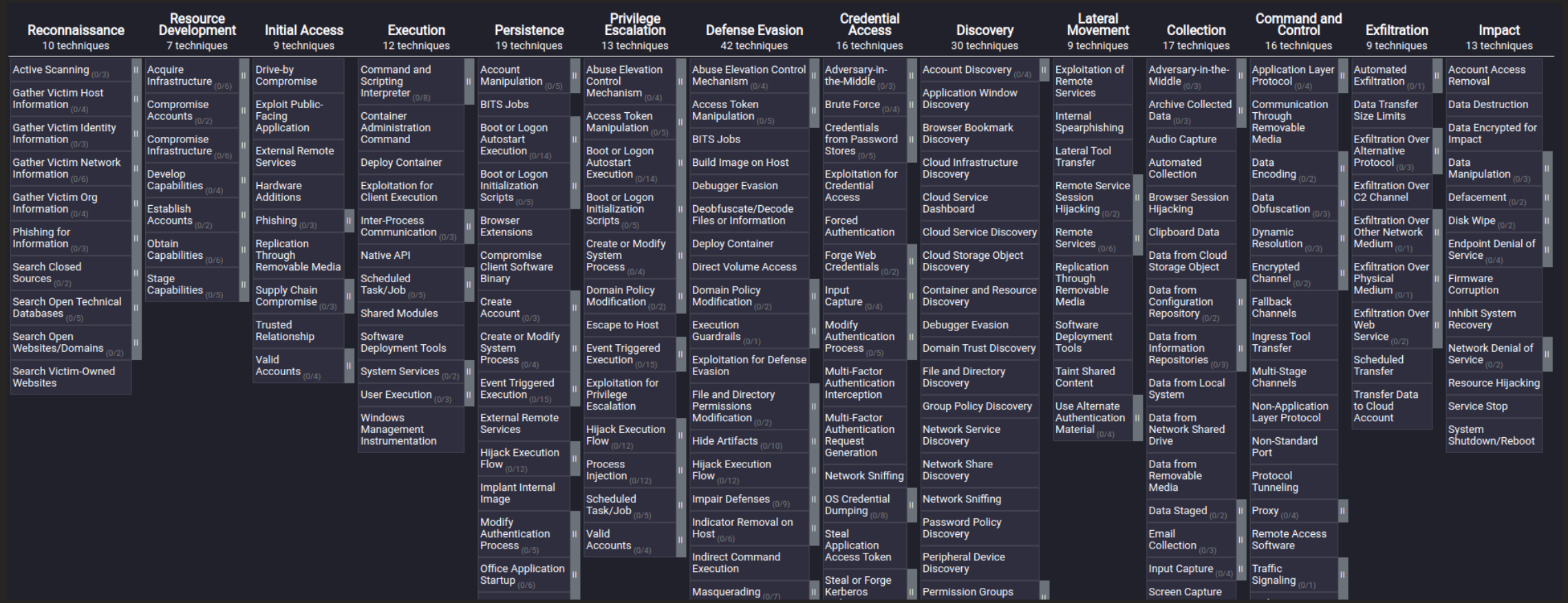
A **security posture** is an organization's overall cybersecurity strength and how well it can predict, prevent, detect and respond to ever-changing cyber threats. ^1

MVP

- Must be built from irrefutable data 💜
- Must fit a single page 🗎
- Quantitative over Qualitative
- Indicators with colours 🔴🟠🟡🟢
- Support "ever-changing cyber threats" 🦡
- Must quickly answer where we're **good** and where we're **bad**.

Solution: Use the Mitre ATT&CK Navigator *with a few hacks*.

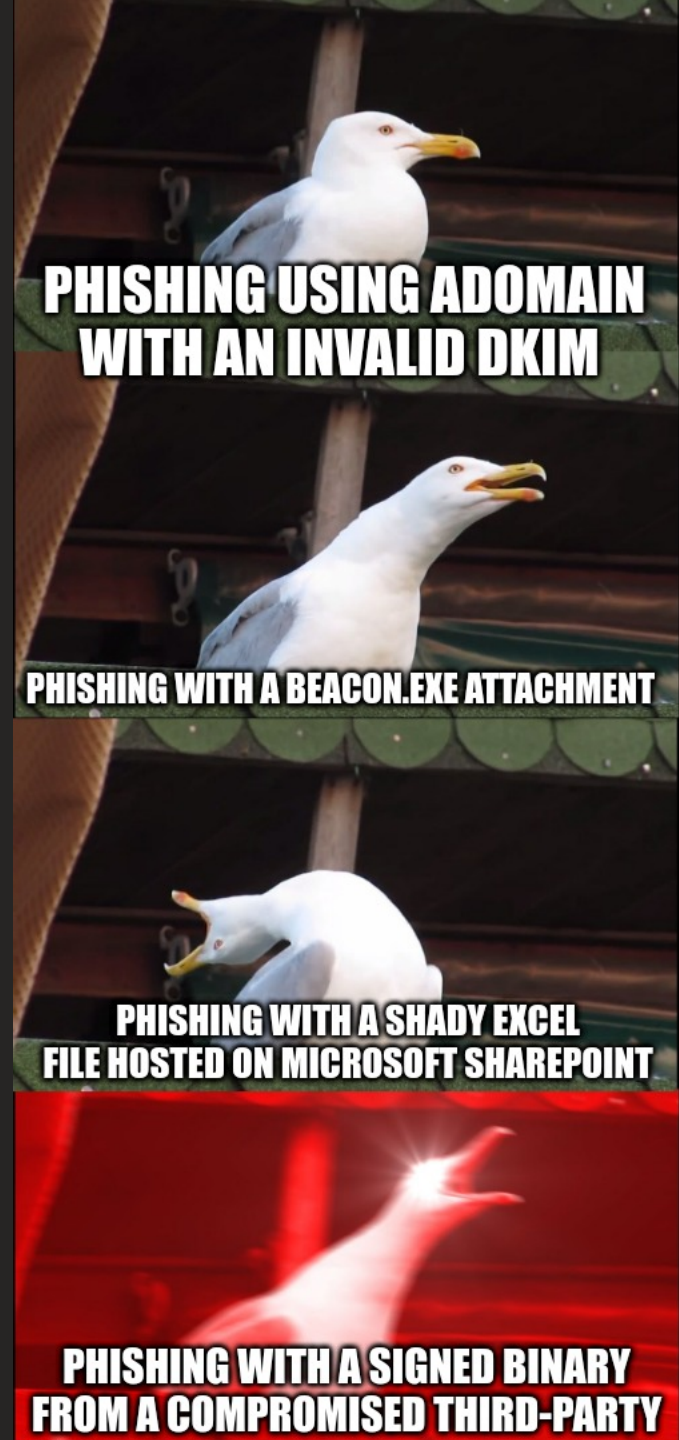
ATT&CK Navigator



ATT&CK Navigator - Select your Threat Groups

ATT&CK Navigator - Technique vs Procedure

- The technique is **what**
- The procedure is **how**
- For example, the technique **Phishing** can executed via:
  - A domain with an invalid DKIM
  - A domain with high reputation
  - A domain with low reputation
  - The organization's domain
  - All kind of attachments
  - Links
  - *At least 100 more procedures...*



For each procedure, we will define 3 fields

Result

The **scored** result of the attack during the purple team exercise.

- Blocked (3)
- Detected (2)
- Logged (1)
- Not Logged (0)

Expected result

The **scored** expected result of the attack during the purple team exercise.

- Blocked (3)
- Detected (2)
- Logged (1)
- Not Logged (0)

> Need to be realistic, otherwise the posture will just be red...

Sophistication level

The minimum sophistication level of the Threat Actor.

- Strategic (7)
- Innovator (6)
- Expert (5)
- Advanced (4)
- Intermediate (3)
- Minimal (2)
- None (1)

The sophistication level comes from STIX 2.1

Gaps

$$Gap = ExpectedResult - Result$$

An example with Phishing technique (T1566):

Procedure	Result	Expected result	Sophistication	Gap
Phishing using a domain with an invalid DKIM	Logged(1)	Blocked(3)	Minimal(2)	2
Phishing with an excel file hosted on Sharepoint	Logged(1)	Detected(2)	Intermediate(3)	1
Phishing with a signed binary from a compromised third-party	Logged(1)	Logged(1)	Expert(5)	0

Weighted Gaps

$$Gap' = Gap * Weight$$

We can push it even further by adding a **weight** dimension, which can be as simple as the **popularity of the attack technique** (not procedure). An example with several techniques

Procedure	Gap	Weight	Weighted Gap
Phishing using a domain with an invalid DKIM	2	7	**14**
Phishing with a signed binary from a compromised third-party	0	7	**0**
Hardware Additions via a Rubber Ducky	2	1	**2**

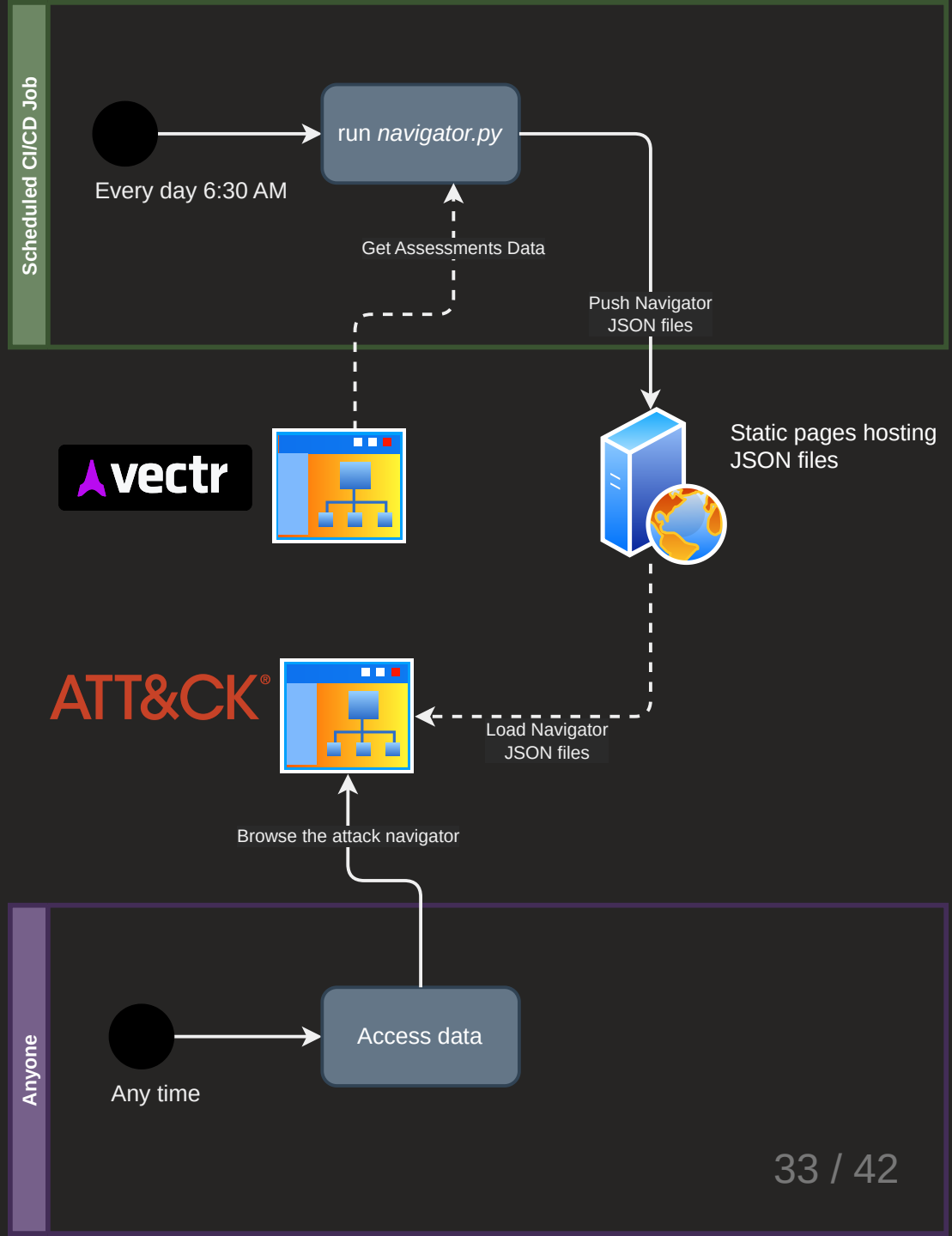
Add a pinch of CI/CD 👉

Every morning:

1. A scheduled job start
2. Data is pulled from Vectr
3. Several JSON files are generated
4. The files are uploaded on a static website

Any time:

- Navigate the navigator 😌



Security Posture - Gaps

Security Posture - Weighted Gaps (*Most important*)

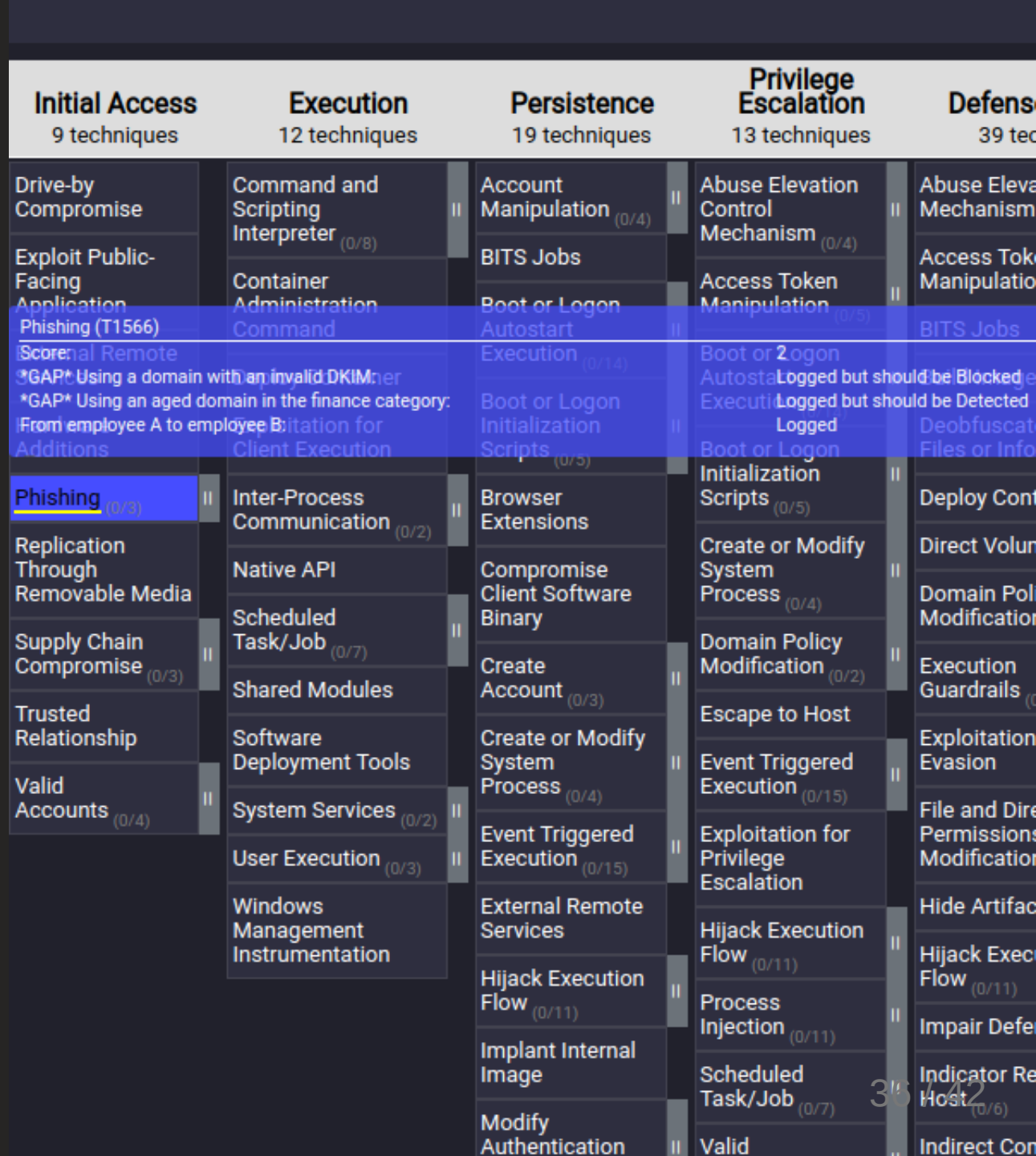
Where are our gaps?

Need to be able to answer the question quickly.

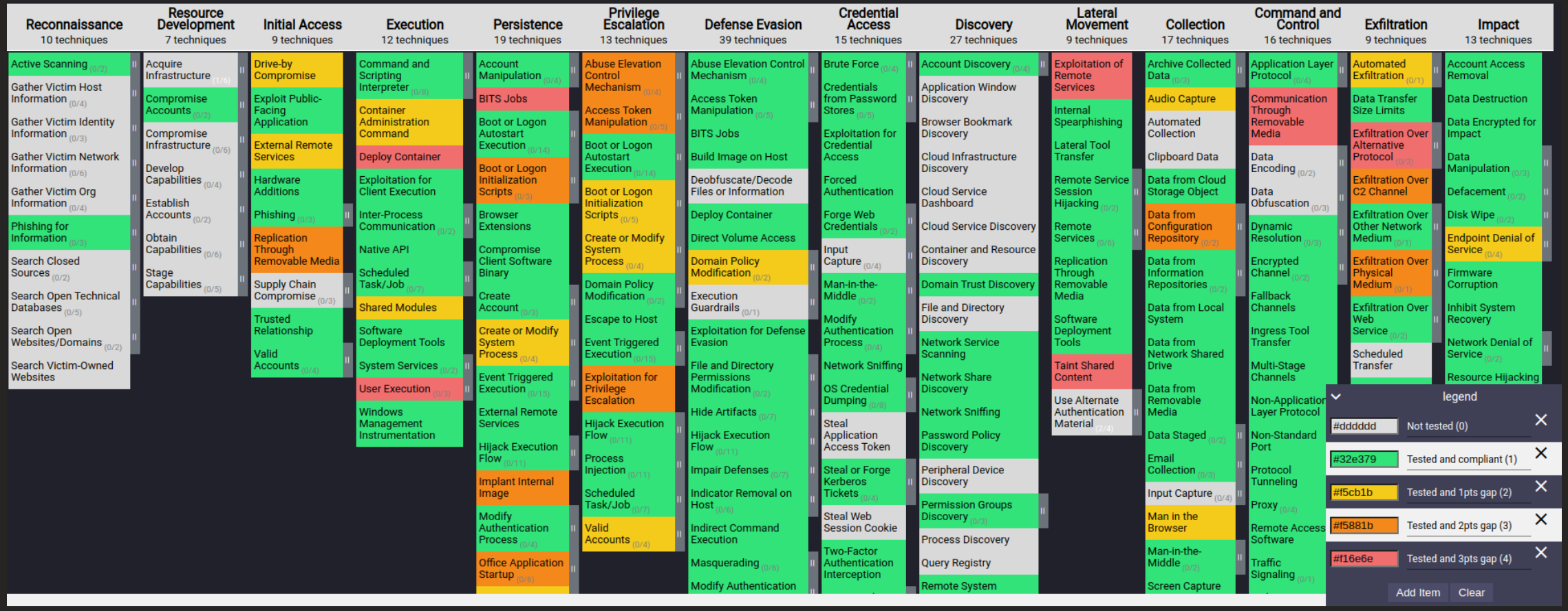
From quantitative to qualitative.

Solution: metadata field

How to: **Mouse over**



Security Posture - Gaps - `filter(sophistication=1)`



Security Posture - Gaps - `filter(sophistication=2)`

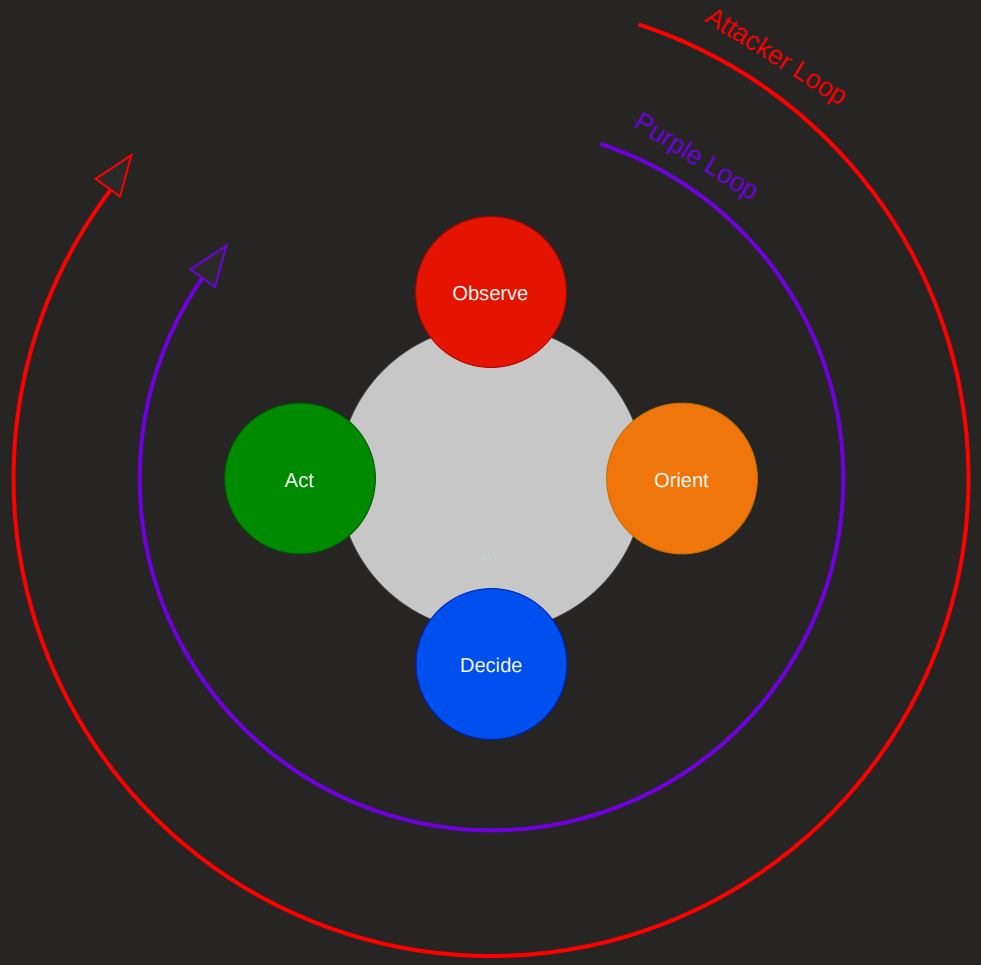
Security Posture - Gaps - `filter(sophistication=3)`

The ultimate goal

Improve the security posture!

The Shortest Loop Wins!

- Can you identify your gaps faster than the attacker?
- Can you adjust faster than your opponent?
- How can you disrupt their OODA Loop?



Thank you! 🤘 🙏 💜

We wish you an awesome HF14!

And the most important of all: Avoid Excel 😆

MITRE ATT&CK CYBER DEFENSE