HUNTABIL.IT

TIEIN THREATS TOGETHE R

YING THE TECHNIQUE INFERENCE
NE TO ENHANCE DETECTIONS

RAYMOND SCHIPPERS

INTRO RAYMOND

- CTO/CISO @ Huntabil.IT
- Previously Engineering Director - Cyber Defence @ Canva
- 15+ years in cyber defence and CTI roles

Graphics where generated by Leonardo.AI

INTRODUCTI SECURIT Y

In a galaxy close to all of us...
in a time no so distant...
We are here to understand our adversaries
and use our Jedi powers to predict their next moves

CYBE GALAXY R

ADVERSARIES

The threats we look to do battle with on a daily basis

TECHNIQUES

How our adversaries go about their deeds, the methods they use to attack us

JEDIS

We the defenders, fightings against evil naydoers

TECHNIQUE INFERENCE ENGINE

OUR JEDI POWER

Graph-based system taught to understand connections between TTPs

WHY USE TIE

CHALLENGE

Incomplete adversary reporting,

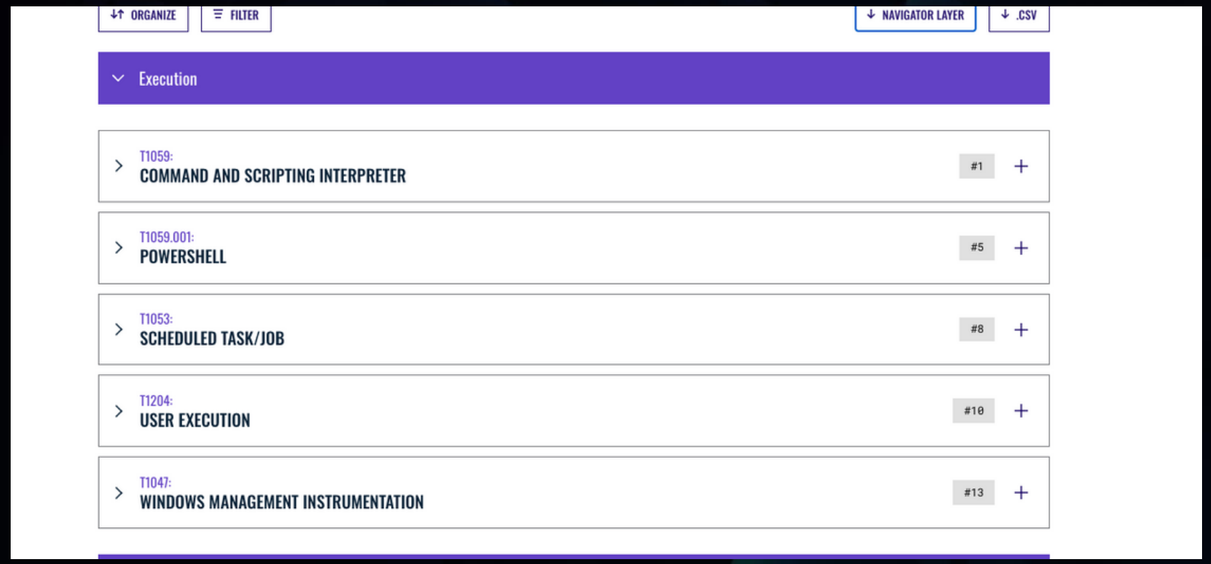
SOLUTION

Make predictions on likely TTPs to fill in the gaps.

EXAMPLE SCENARIO 1

Reports on the compromise of a peer in our industry.
We know actions on objective and some other details but we don’t know:

- How did they get in
- what are their possible lateral movement steps?
- What detections should we have?



DEMO SCENARIO 1

Add observed techniques

Then add techniques it returns to refine the model

When it makes sense, export the layer

DEMO
SCENARIO 1

The heatmap shows you confidence of the techniques used

WHY USE TIE

CHALLENGE

The need to create realistic possible adversary profiles based on a set of TTPs

SOLUTION

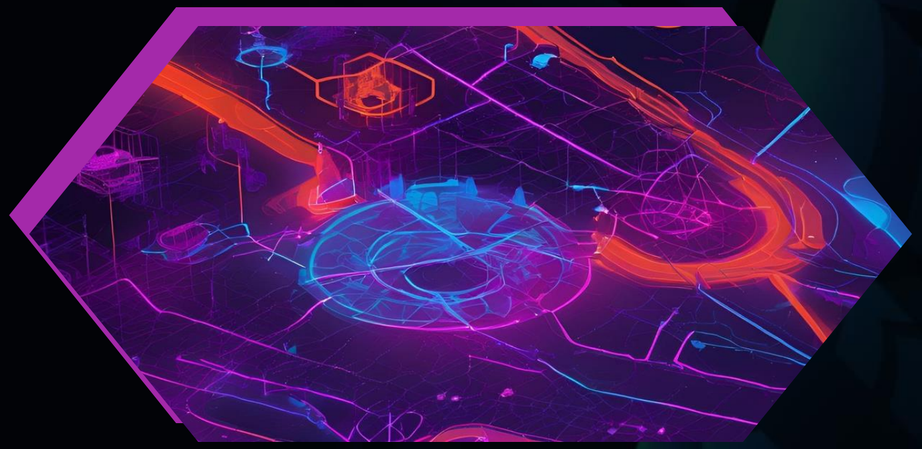
TIE lets you create highly probable adversaries based on known real world attacks

EXAMPLE SCENARIO 2

We need to simulate & creates detections for an adversary likely to steal data from a S3 bucket through stolen credentials.

TIE can help us create a likely adversary profile with TTPs

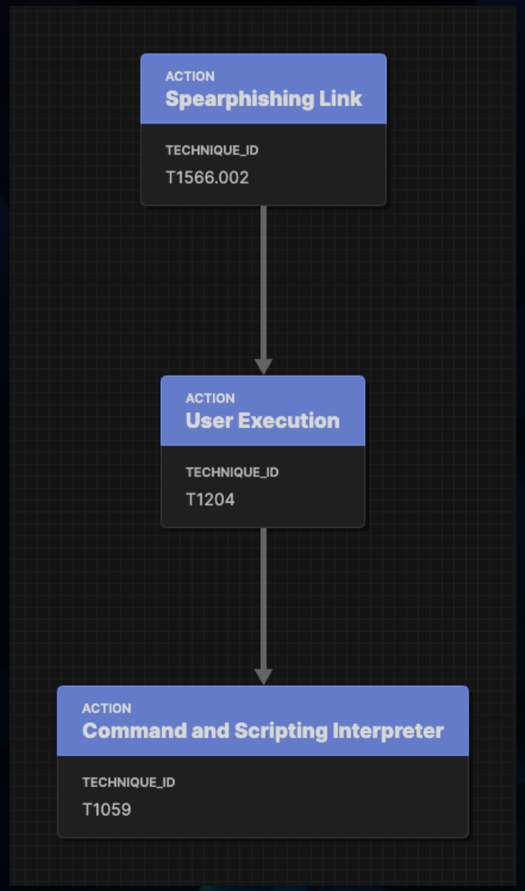
USING FORCE



BUILDING KNOWLEDGE

Feed into TTPs into the rest of the Threat informed defence cycle

- Help build adversary profiles
- Improve your adversary simulations and develop likely adversaries to simulate



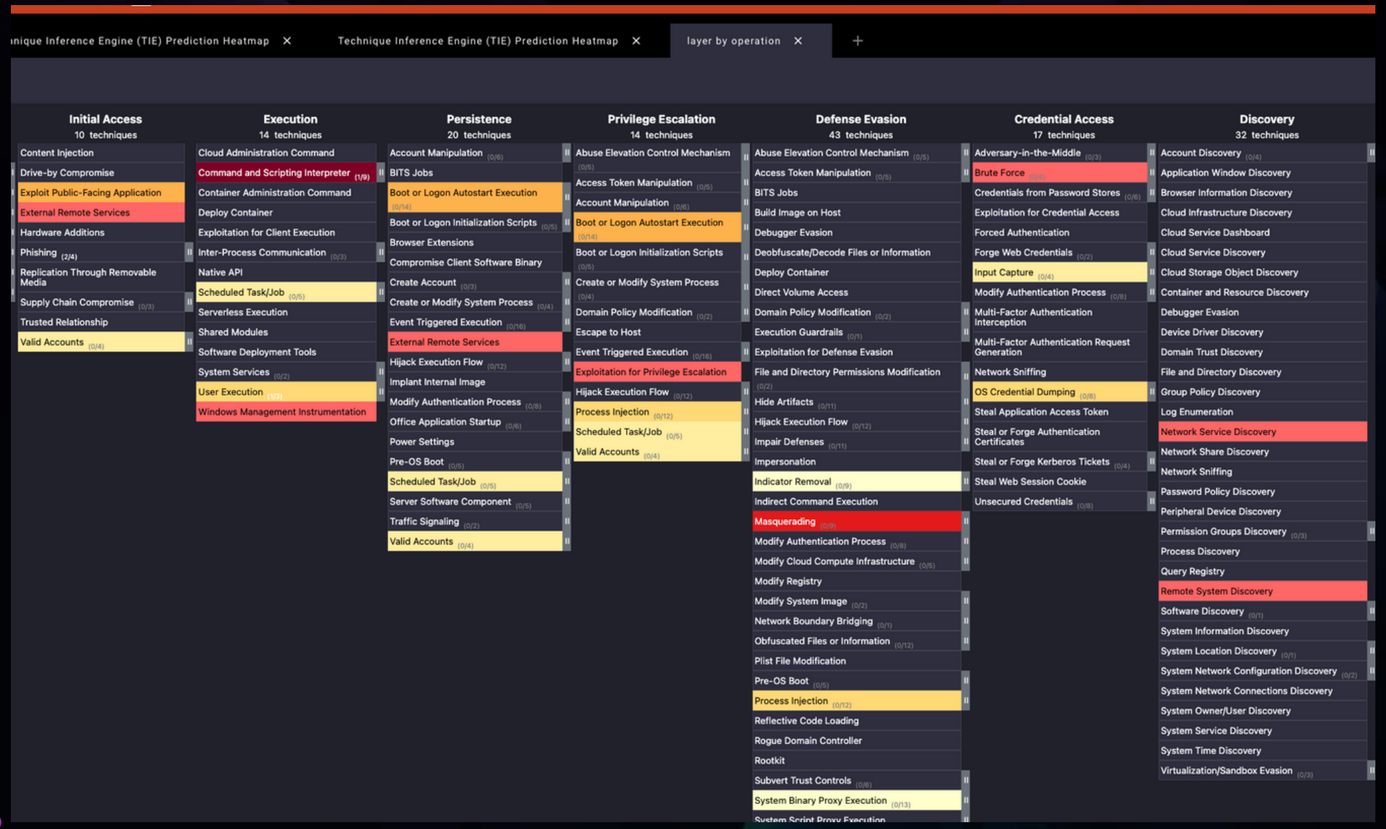
BUILDING KNOWLEDGE

What are our courses of action for these techniques

- Help build better ATT&CK Flows
- See common choke points

DETECTI REQUIREMENTS

- Build a comprehensive list of likely TTP
- Build attack flows
- Look for top-N detections
- Priortise based on the clusters
- Use Summiting the Pyramid to factor in resilience



DETECTION REQUIREMENTS

- Build your ATT&CK Layers
- Import them into navigator
- Add A+B+C etc
- Use the heatmap generated

DETECTI IDEAS

- Understand what is likely left of boom
- Build comprehensive understanding of post-compromise pre-impact TTPs
- Increase confidence of CTI based prioritisations

ADVERSAR SIMULATION

- Build more completed profiles
- Build potential profiles to simulate
- Help create attack flows
- Import into tools like OpenBAS

THE STRATEGY

- Leverage TIE to enhance CTI reporting
- Build profiles to simulate likely new adversaries
- Enhance your resilience and feed into the other great projects from MITRE

CHALLENG WITH TIE

- Uses ATT&CK V14
- Common techniques have been renumbered so dataset is..challenging
- You can’t select appropriate platforms
- Can’t export from TIE>ATT&CK Flow

TIEING IT TOGETHER

- As community let's contribute adversary knowledge
- Let's use our Jedi powers for good
- Join the defence alliance
- MITRE, how can we continue to improve the model as a community?
- MITRE: Let me select appropriate platforms

QUESTIONS?

THANKYOU

My LinkedIn

MITRE ATT&CK
Slack

LET'S NONE OF US ARE AS KNOWLEDGEABLE AS ALL OF US