Look Mum No Hands!

AUTOMATION IN THREAT INTELLIGENCE

Agenda

01

Why Automate Threat Intelligence

- The Pyramid of Pain

02

Getting Started

- Prioritisation
- Integrations

03

Common Use Cases

- Enrichment
- Alerting
- Active Detection & Enforcement
- Ticketing

04

To Infinity & Beyond The Common Use Cases

- Vulnerability Prioritisation
- Mapping TTPs To Courses of Action
- Tracking Adversary Behaviour

05

What Next?

whoami

- Tim Peters (imp0st3r)
- Threat Intelligence Engineer
- Security Nerd
- Gadget Aficionado
- DJ & Music Producer
- Faux Pa
- Yells At Clouds A Lot!

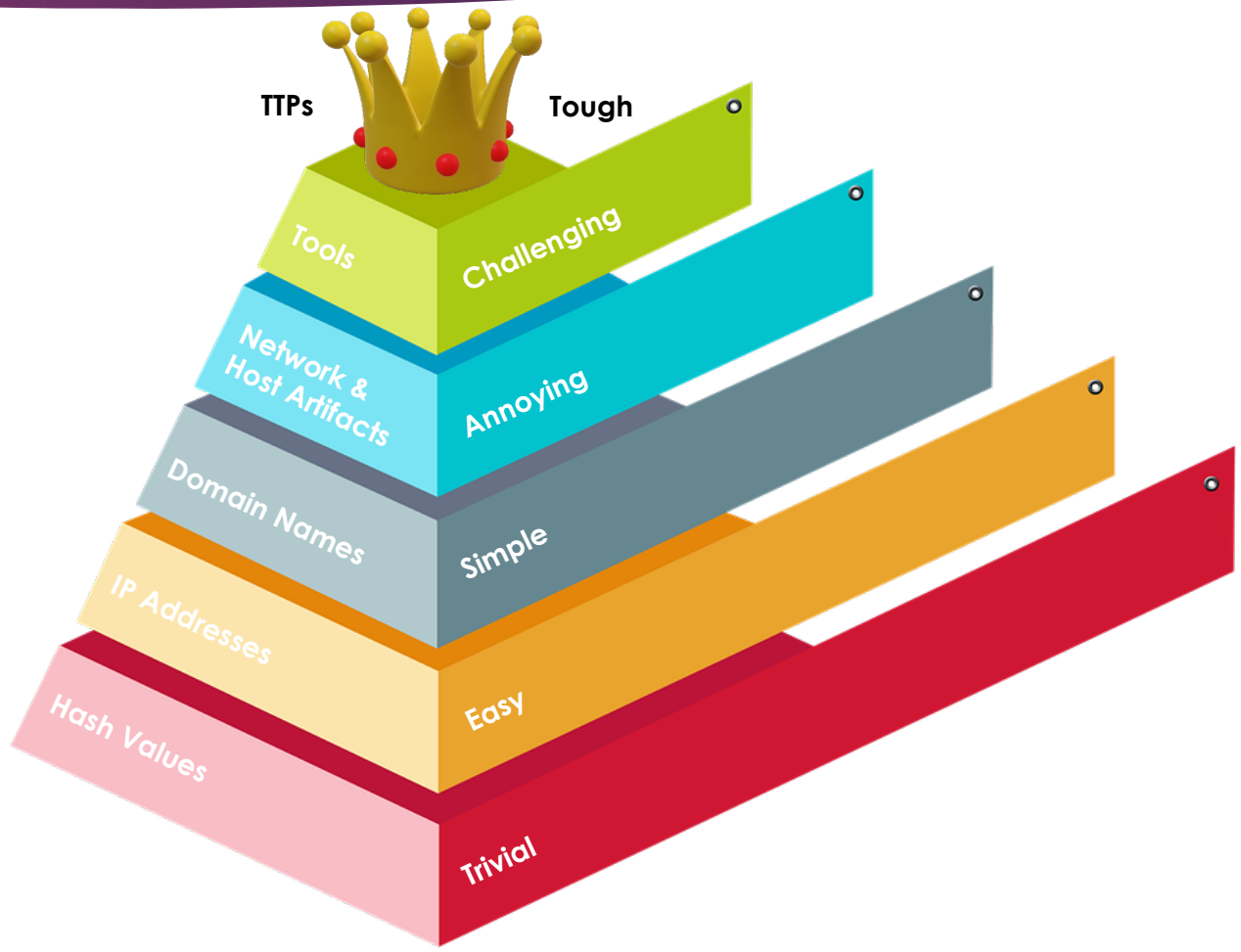
Web: https://imp0st3r.com
GitHub: https://github.com/Panz05

Not all Threat Intel is created equal.

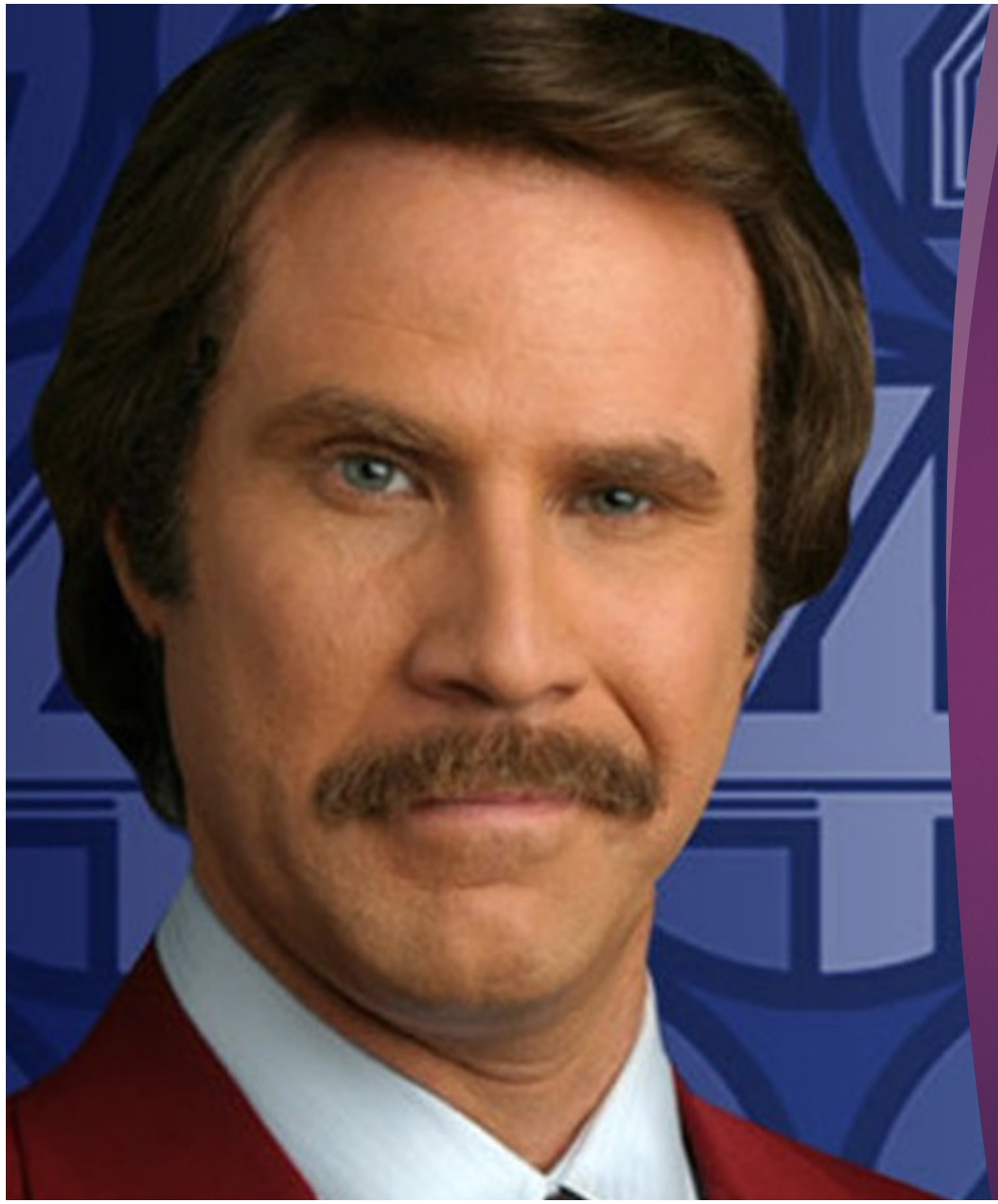
Why Automate Threat Intelligence?

The Pyramid of Pain

- Hard to make sense of data without context.
- Automate the bottom layers to allow time to focus on higher, more challenging layers.
- What value is the threat intel providing.
- Bringing together external threat intel with internal threat intel.
- Connecting the dots.



Getting Started



I don't know how to put this but, Threat Intel is kind of a big deal.

Prioritisation

Why Prioritise Threat Intelligence.

- Not all threat intelligence is equal.
- IoCs are mostly noise.
- What is relevant to you and what isn't.
  - Technical limitations with product IoC volumes.
- A lot of data with little to no context.
  - Too Many False Positives.
  - Low Accuracy.
  - Low Confidence.
- Greater focus on threats that are important to your organisation.

How To Prioritise Threat Intelligence.

- Map your threat profile to the threat intelligence.
  - What context does the threat intelligence have that you can map your threat profile to.
  - Map your intelligence requirements to align to collection, enrichment, prioritisation and dissemination.
- Score the threat intelligence to align with your threat profile and risk appetite.
  - Reduces false positives.
  - Improved accuracy.
  - Higher confidence in the data.

A higher score will indicate that the threat intelligence is more actionable

Integrations

Why Integrate:

- Threat Intelligence can bridge the gap and enhance detection capabilities of existing investments.
- Decrease time to detection and response.
- Visibility of potential compromise.
- Match what is happening outside to what is happening inside.
- Threat Intelligence can be used by other teams to gain additional context.
- Pro-actively block threats.

Threat Intelligence Platforms should Integrate With Your:

- SIEM
- SOAR
- EDR/XDR
- Firewall (IDS/IPS)
- Vulnerability Management
- Ticketing System
- Sandbox
- And more…

Integrations Should Be Bi-Directional Wherever Possible (To Facilitate Internal Intel Collection)

Common Use Cases

Enrichment

Enrich to gain further context.

- Enrich data in bulk.
  - Only send prioritised data to be enriched.
    - Helps to control API query limits on enrichment sources.
  - Use the additional context to further enhance your scoring.
- Enrich in multiple places.
  - Not all threat intelligence is equal.
- Enrich With Internal Intelligence Sources.
  - SPAM Email Submissions.
  - Sandbox Detonation Results.

Alerting

Automated alerts of prioritised data.

- Know when something has happened.
  - Is there a new alert from the SIEM or EDR/XDR that requires further investigation.
  - Know when a tracked adversary has changed their behaviour.
- Aid SoC Analysts.
  - Provide context alongside triggered IoCs to help speed up triage.
- Aid Vulnerability Management Team.
  - Provide context when a vulnerability has been exploited in the wild.

Active Detection & Enforcement

Proactively send IoCs to downstream tools.

- Only send prioritised data to EDR/XDR. (There is a limit on the number of objects they can store)
  - Bi-directional Integration between the TIP & EDR/XDR to close the feedback loop.
  - Send IoCs to pro-actively block.
  - Automate IoC Sweeps.
- Only send prioritised data to the SIEM.
  - There is only so much data a SIEM can handle before it grinds to a halt.
  - The SIEM should send alerts back to the TIP when a detection has been made so an investigation can commence.
  - Retrospectively hunt for IoCs.
- Only send prioritised data to the firewall (IDS/IPS).
  - Proactively block IPs and FQDNs.
  - Don't send everything as you will block legitimate traffic.

Ticketing

Automate the creation of tickets from the Threat Intelligence Platform.

- Speed up response times by:
  - Providing the context needed for the analyst to perform the required task.
- Track the lifecycle of a security incidents in a single system rather than multiple systems.
  - Automated ticket creation makes life so much easier.
- Easier To Collaborate With Other Teams.
  - SoC, Red Team etc. can all have visibility of the ticket and provide input.
- Bi-directional integration can show the value threat intelligence provides.
  - Metric of how many tickets were created, how many were closed as false positive, true positive etc.

To Infinity & Beyond The Common Use Cases

170,524 Vulnerabilities, all CVSS 10.0

Vulnerability Prioritisation

Which Vulnerability do you patch first?

- Identify the vulnerabilities that are applicable to your organisation.
  - Use this to score the vulnerabilities. The higher the score the more applicable it is to your organisation.
- Use Threat Intelligence to identify if:
  - Is there an exploit available?
  - Is the vulnerability actively being exploited?
  - Search for evidence if there is an attempt to leverage a vulnerability.
  - Who is exploiting (or seeking an exploit), and are they likely to target you?
- Integrate the Threat Intelligence platform with your vulnerability management tool.
  - Match the highest scoring vulnerabilities to your internal assets.
  - Identify the criticality of the assets to give you a prioritised list of assets to patch.

Mapping TTPs To Courses of Action

Map the TTP's an adversary is using to the courses of action.

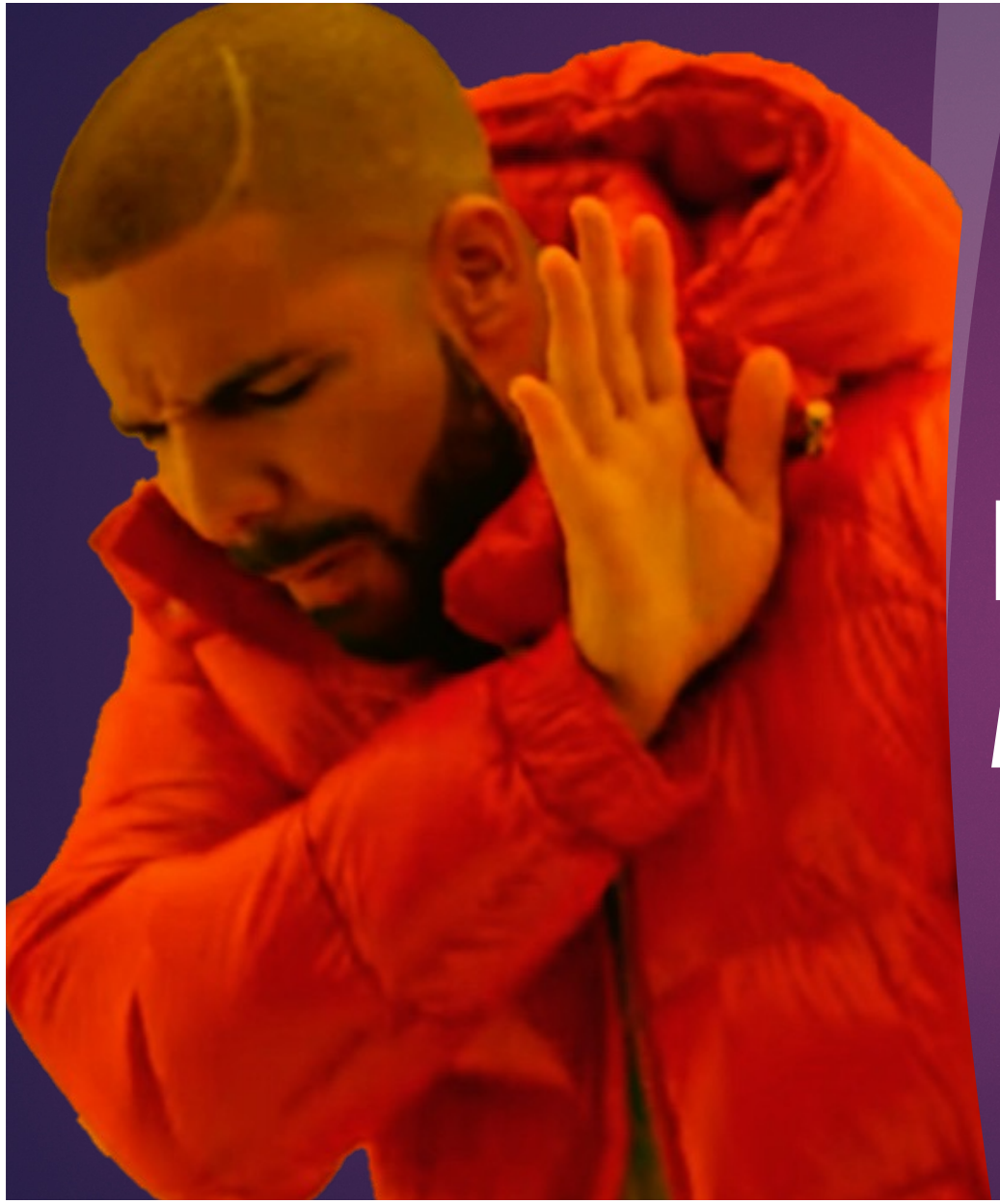
- Set up automated alerting when changes occur.
- Validate the courses of action have been implemented to identify gaps.
  - Red Teams can use the courses of action to determine if the organisation can detect, withstand and neutralise an attack.
- Correlate all TTPs with corresponding courses of action used by adversaries.
  - What are the most common TTPs used by adversaries.
  - Match the courses of actions to the TTPs and validate.

Tracking Adversary Behaviour

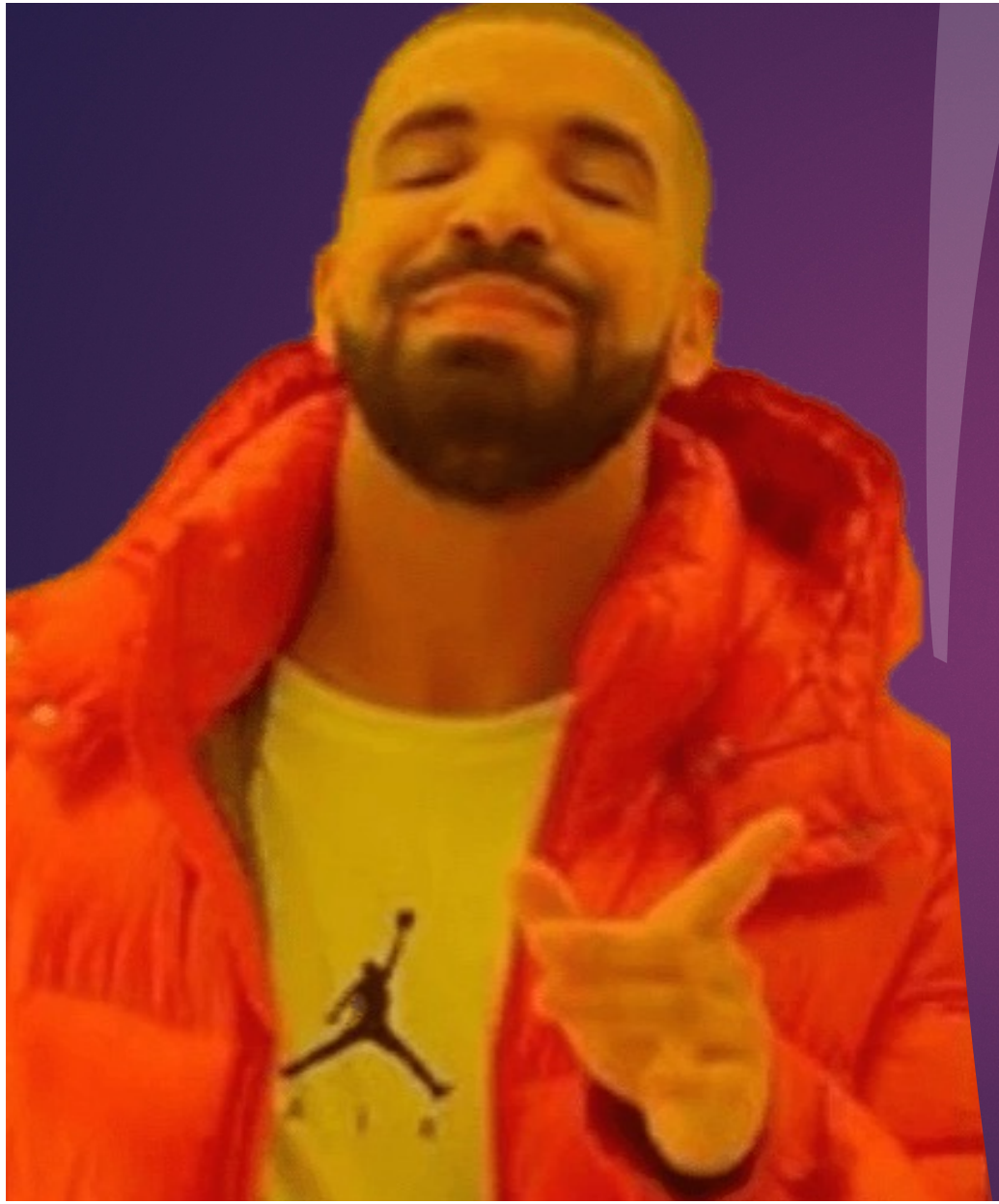
Set up automated alerts if the adversaries you are tracking have changed their behaviour.

- Adversary has been found to:
  - Use new TTPs.
  - Using new malware.
  - Newly discovered indicators.
  - Exploiting a vulnerability.
  - Using new tools.
  - Targeting new industries.
  - Targeting new regions/countries.

What Next?



Doing All The Work Manually.



Automating It All.

More Room For Activities

Questions?

Thank You!

CTI User Group YouTube Channel

YouTube: @cti-user-group