Getting Started With Threat Intelligence

WITHIN THE MICROSOFT ECOSYSTEM

Agenda

01

Why Use Threat Intelligence

- The Pyramid of Pain

02

Getting Started

- Microsoft Sentinel & Microsoft Defender XDR

03

Common Use Cases

- Enrichment
- Alerting
- Active Detection & Enforcement

04

Do I Need A TIP?

- When To Implement A TIP
- Open Source vs. Commercial TIP

05

What Next?

whoami

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

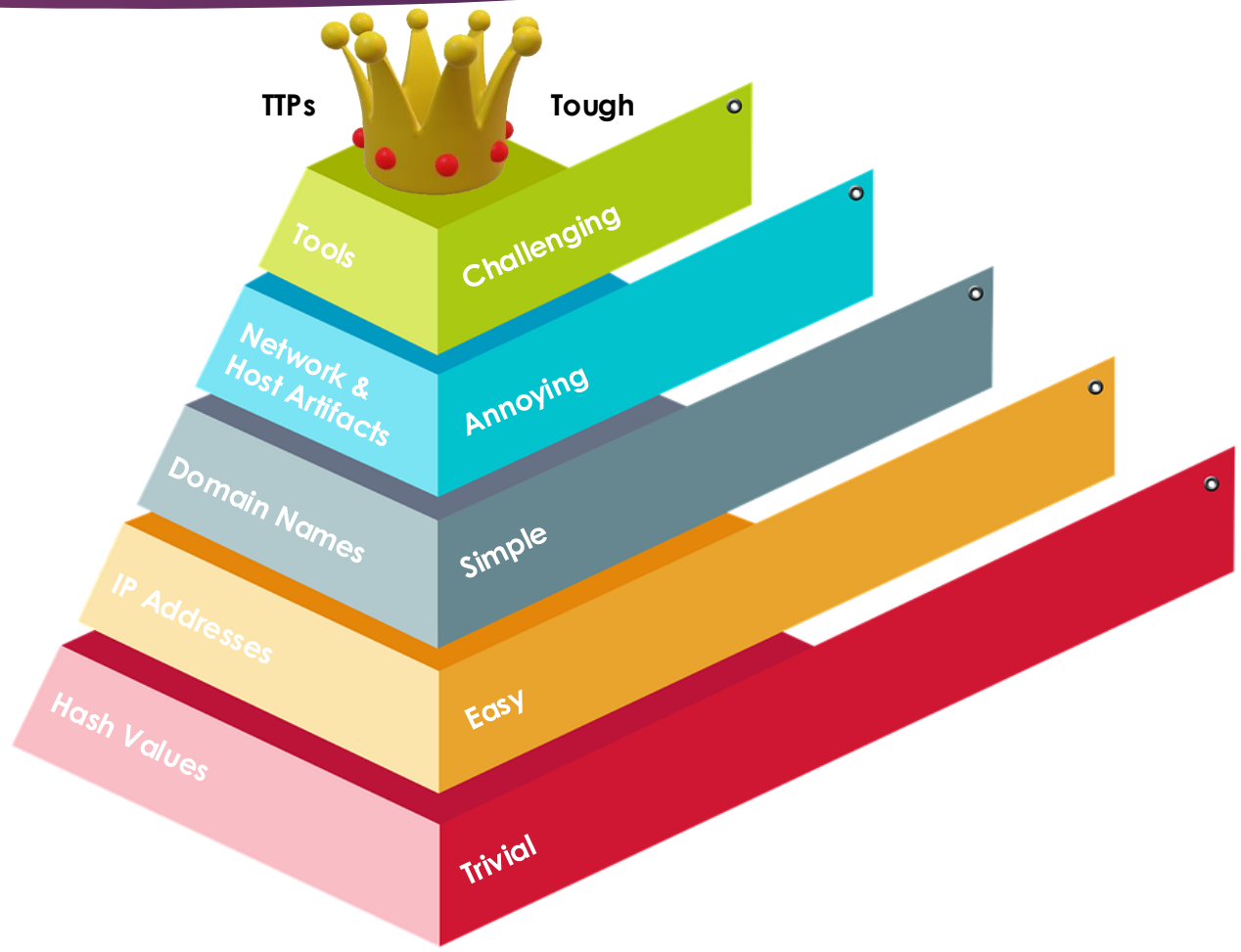
Web: https://imp0st3r.com
GitHub: https://github.com/Panz05

Not all Threat Intel is created equal.

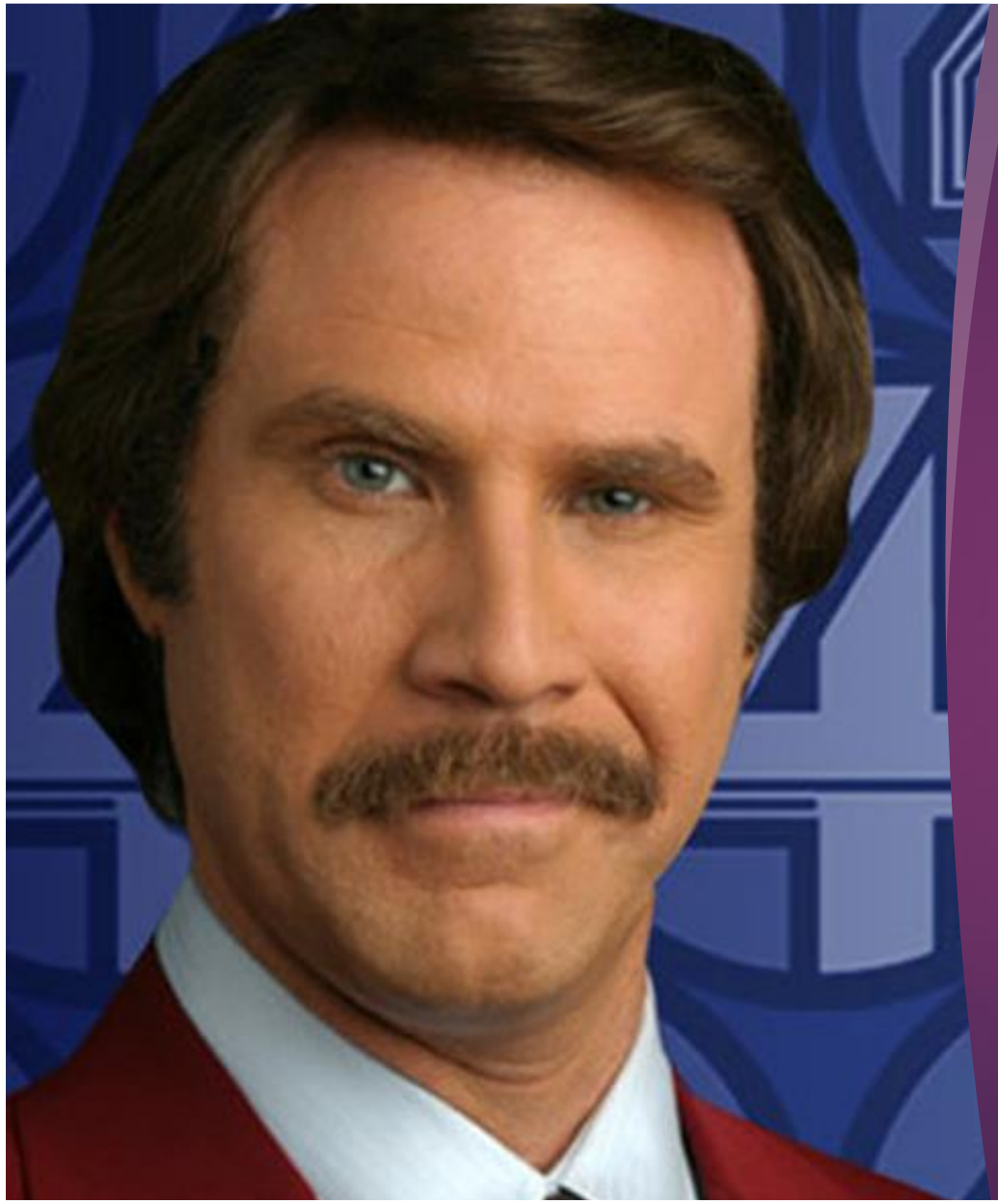
Why Use Threat Intelligence?

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.

Microsoft Sentinel & Defender XDR

Microsoft provides its own CTI (Free & Paid Subscription).

Ingest additional sources (CTIS) either via API or TAXII.

Create rules to utilize the CTI you are collecting.

A lot of data with little to no context.

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 prioritisation.
- Enrich in multiple places.
  - Not all threat intelligence is equal.
- Enrich With Internal Intelligence Sources.
  - SPAM Email Submissions.
  - Sandbox Detonation Results.

Alerting

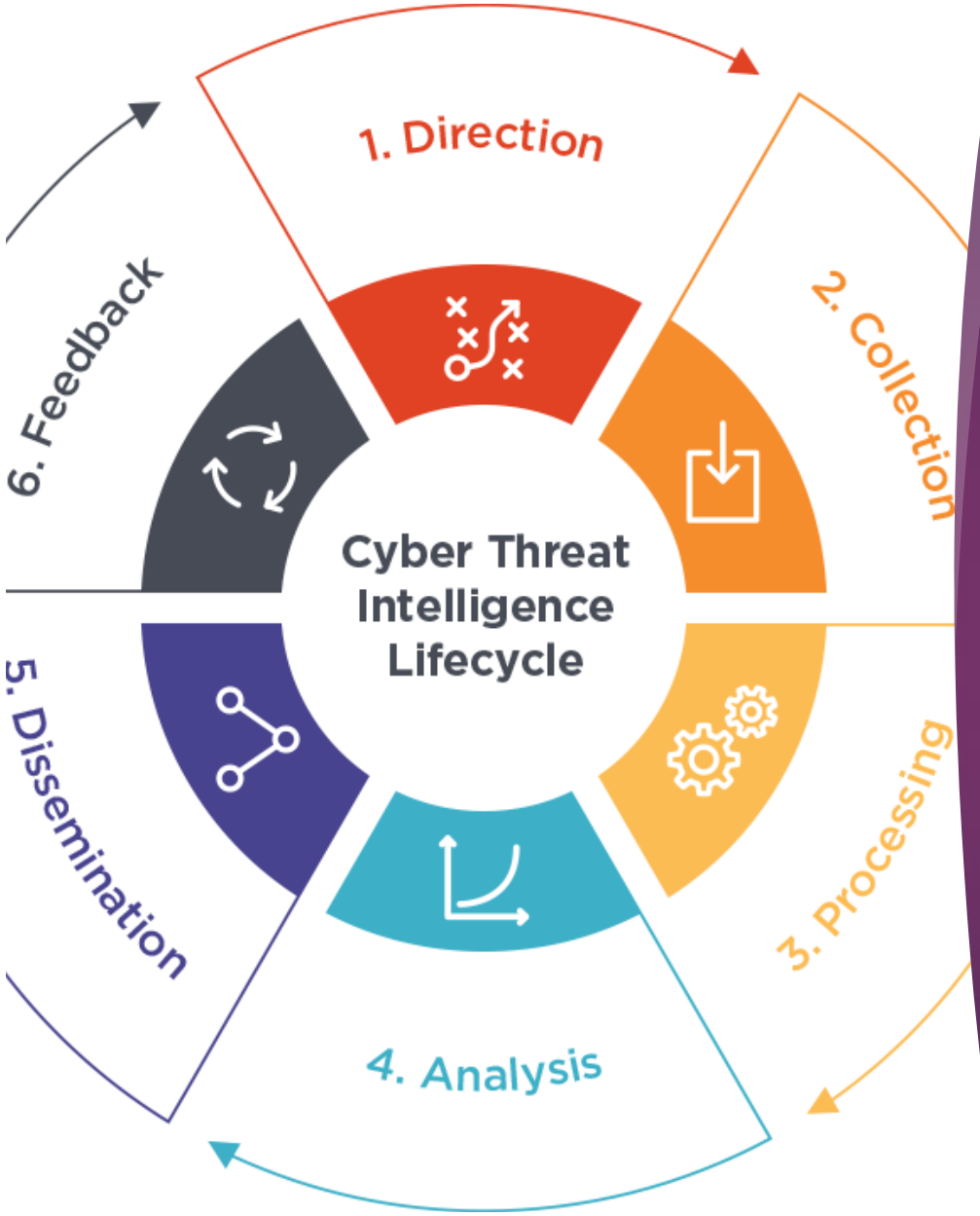
Automated alerts of prioritised data.

- 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.

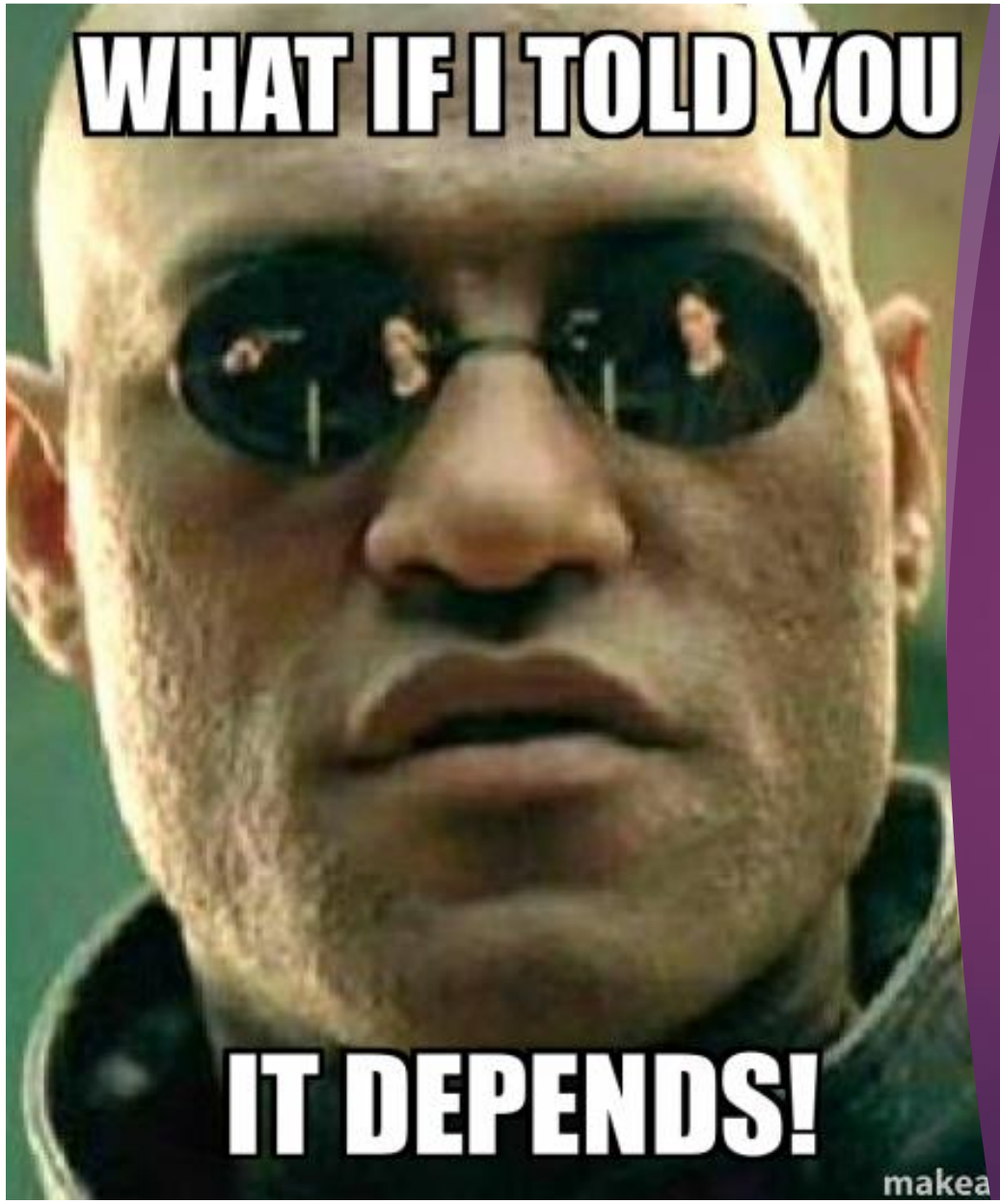
Active Detection & Enforcement

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 can block legitimate traffic.



Do I Need A TIP?



When To Implement A TIP.

Benefits Of A TIP

Central repository for all CTI.

Not all threat intelligence is equal.

Ingest multiple threat feeds (OSINT & Commercial)

- Aggregate
- Deduplicate
- Correlate
- Prioritise
- Transform

Prioritise what is relevant to you and what isn't.

- IoC's are mostly noise
- Technical limitations with product IoC volumes.

Gain Context & Insights.

- Reduce False Positives.
- Eliminate Alert Fatigue.
- Higher Confidence, Higher Fidelity.

Greater focus on threats that are important to your organisation.

Integrate faster with more Security Tools

Prioritisation

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.

- Improved accuracy.
- Gain insights on relevant threats quickly & efficiently.

Reduce False Positives.

- Eliminate Alert Fatigue.
- Higher Confidence, Higher Fidelity.

Greater focus on threats that are important to your organisation.

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.

Open-Source vs. Commercial TIPs

What's The Difference

Open-Source TIP.

- DIY installation.
- DIY management & updates.
- Community Support.
- DIY build and maintain integrations.
- Limited options.
- Free but not free.

Commercial TIP.

- Out of the box configuration.
- Constantly updated and managed.
- Vendor support.
- Vendor builds and maintains integrations.
- Spoilt for choice.
- Not free.

If you have the capacity or resources, you can start with open-source TIP otherwise invest in a commercial TIP.

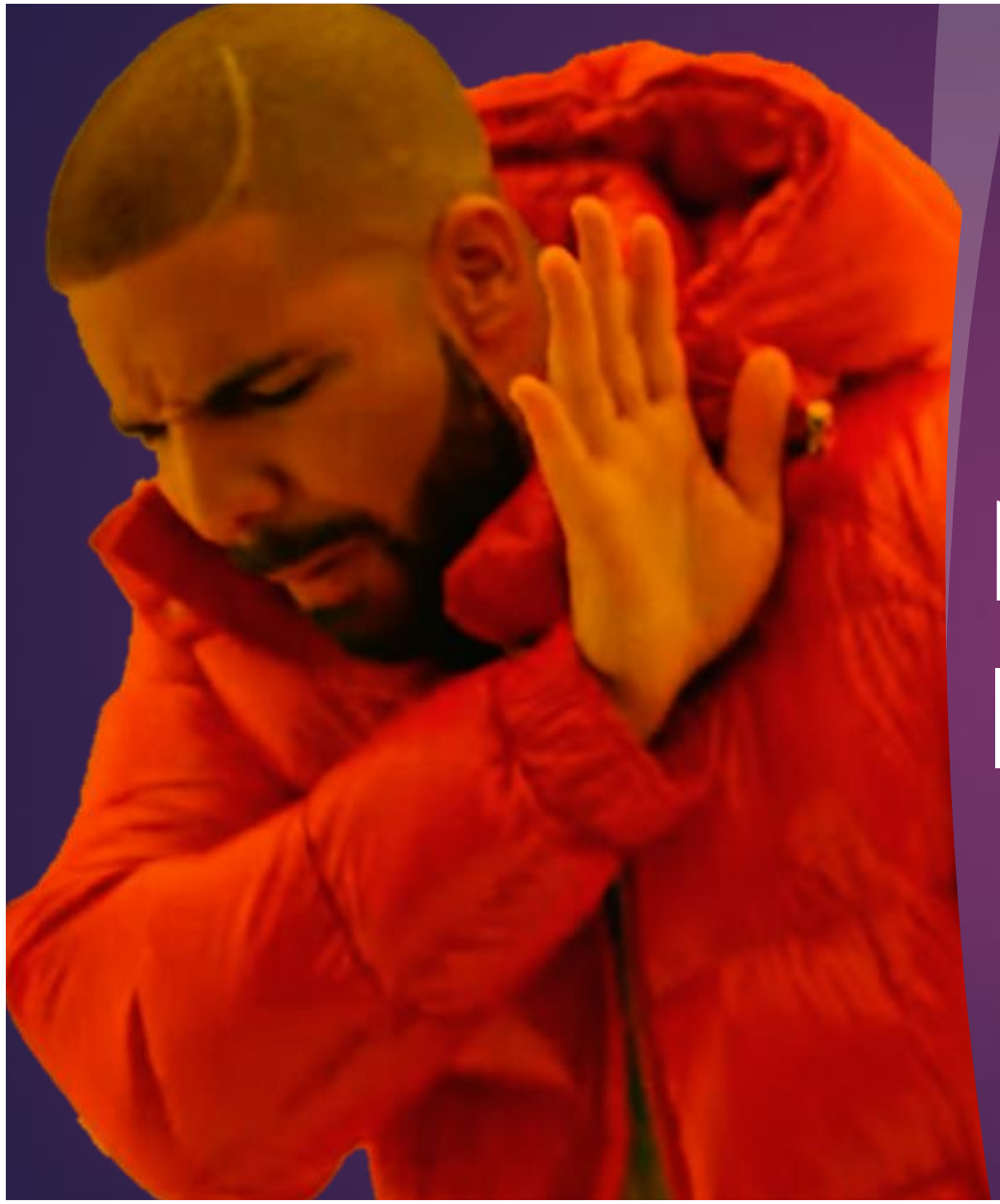
Integrations

Threat Intelligence Platforms should Integrate With Your:

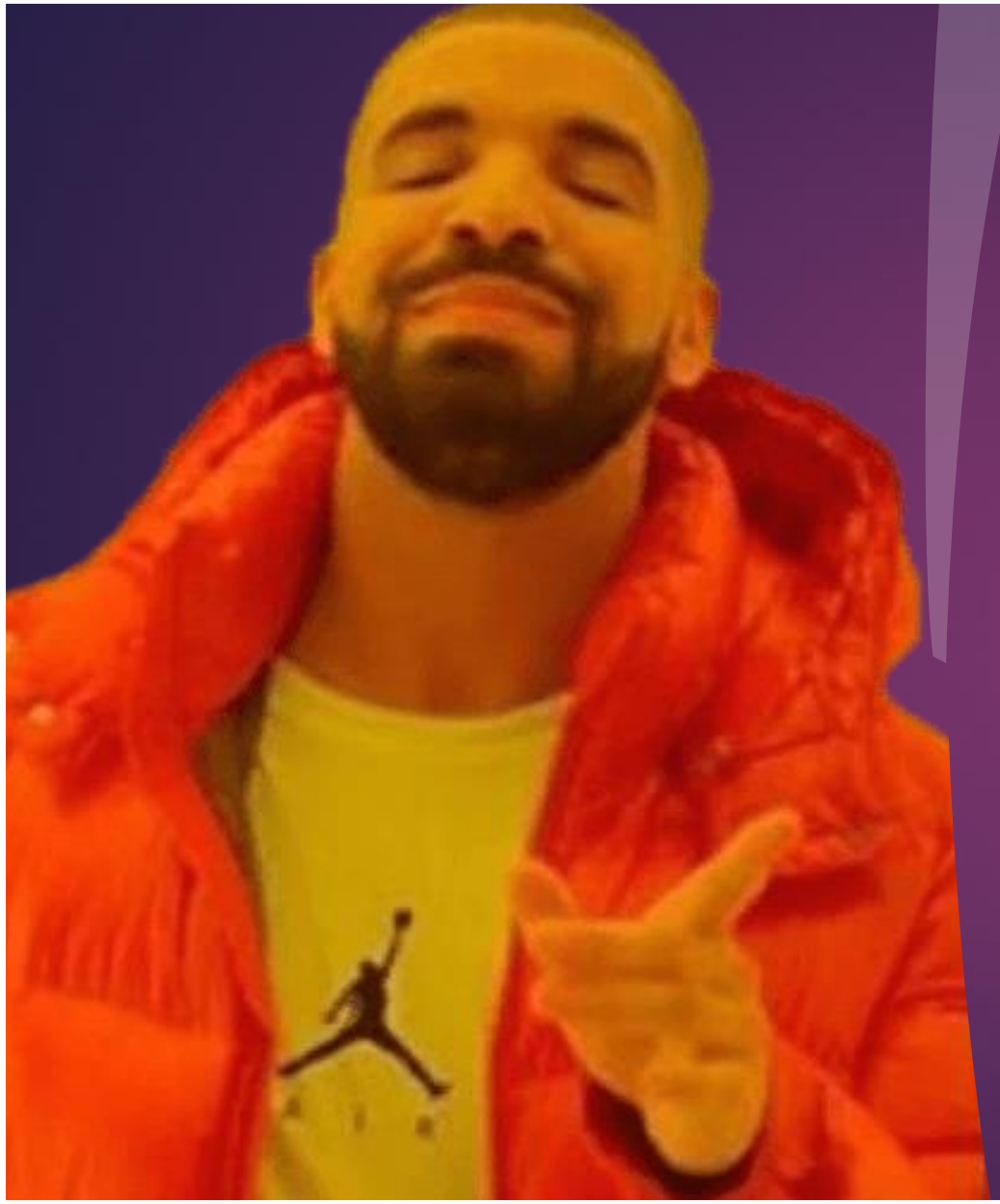
- SIEM
- SOAR
- EDR/XDR
- Firewall (IDS/IPS)
- Vulnerability Management
- Ticketing System
- Sandbox
- And more…

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

What Next?



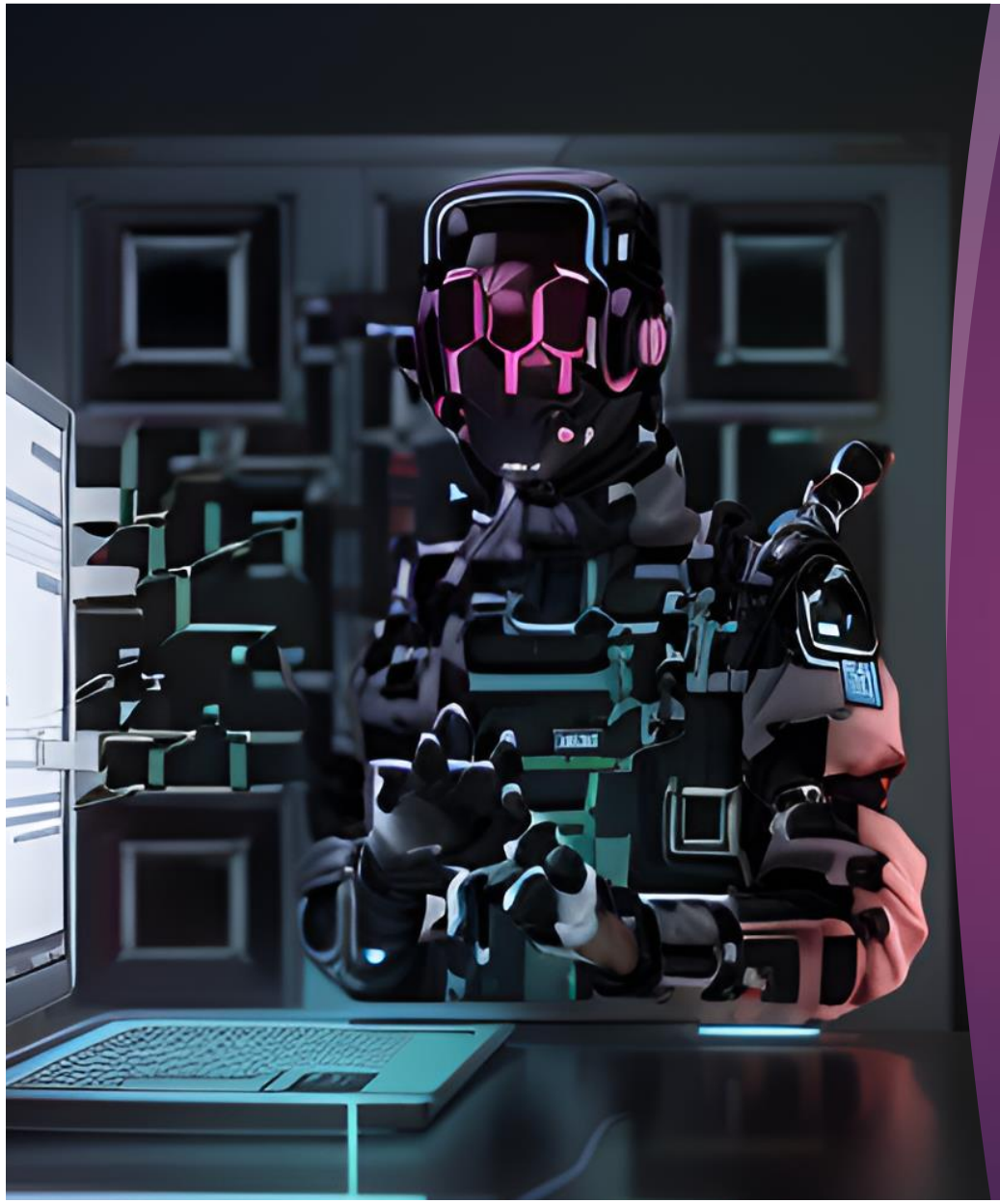
Not Using Threat Intelligence.



Gaining Insights From Threat Intelligence.

Questions?

Thank You!



CTI User Group YouTube Channel

YouTube: @cti-user-group