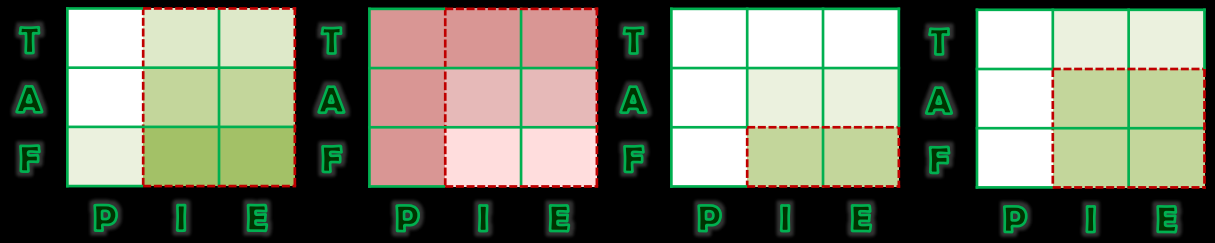
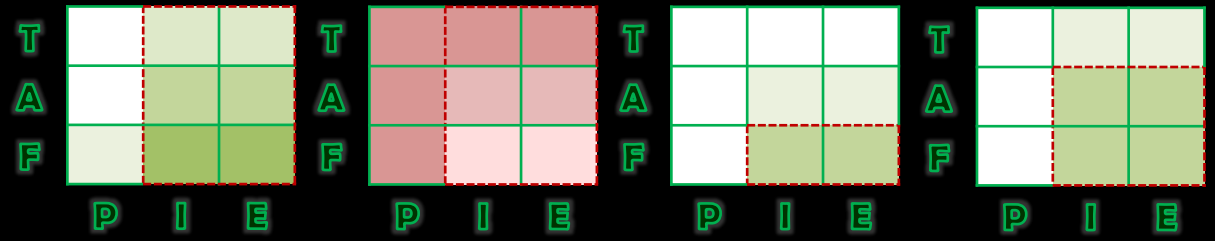


The Cyber Threat Intelligence Matrix



Alternative title:

Have your FAT PIE and eat it too...

About Me

>> Frode Hommedal

- Currently @ Telenor, Norway's biggest telco.
- Head of Incident Response and Security Analytics.
- Formerly @ NorCERT, the national CSIRT of Norway.

>> APT fighter and CSIRT modeler

- Roughly 10 years of CSIRT and SOC experience.
- Background from hardware and software development.
- Would very much like to help advance the infosec curriculum.

About this talk

>> «How can TI help IR?»

I was asked this by a friend and conference director earlier this year.

>> «Let me think about it...»

The CTI Matrix is the result of me pondering that question for a while, wanting to give a non-obvious answer. Warning: It's work in progress.

Warning!

>> This talk is about incident response

And specifically decision making regarding attacker eviction / “cleanup”.

>> This talk is for incident responders

But I hope it will be interesting no matter what kind of security work you do.

Definitions

>> Incident response:

I will be talking about responding to **high risk threat driven incidents** where you're fighting a motivated and mission driven attacker that has had a foothold within your infrastructure for a while.

>> Threat intelligence:

I will be using this about **evidence based knowledge** about your adversary, that your adversary would prefer to or benefit from keeping **secret**, and that is actionable or beneficial to decision making during incident response.

USENIX Enigma 2016 - NSA TAO Chief on Disrupting Nation State Hackers

USENIX Enigma Conference

Subscribe 2,569

88,813 views

Add to Share More 657 19

Press release quote

«We live in a time where the technological and geopolitical realities have made **covert digital infiltration of critical infrastructure** commonplace. Responding to such intrusions requires a lot of effort, and there will be a period during the response where you need to **observer, analyze and learn** before it is possible to take effective actions to successfully evict the attacker from your infrastructure.

But knowing whether you are **ready to evict an attacker** or not, and more importantly, ready to keep the attacker from re-entering your infra-structure at will, is difficult. This is why I started developing the Cyber Threat Intelligence Matrix, and it is for those kinds of situations I hope it can prove to be useful in the future.»

A challenging IR lesson

We've accepted that we need to observe and learn before we try to evict an attacker. But for how long?

When are we ready to take action?

Problem statement

How do we utilize threat intelligence to make informed decisions regarding attacker eviction during incident response?

Proposed solution

>> The Cyber Threat Intelligence Matrix

The model I will present during this talk, where we map out what we know about an adversary to better understand our readiness to evict them.

>> Making the complex accessible

Distilling complex knowledge into a simpler representation to promote an informed dialog and decision making process between analysts and mgmt.

Wanted end state

>> Less uncertainty regarding eviction

Using the CTI Matrix, we should be able to make the decision to evict an attacker with less uncertainty regarding our ability to keep them out.

>> Bigger potential for improved accuracy

Using the CTI Matrix, we should be able to improve our accuracy over time, reducing the uncertainty of our ability to keep them out even more.

Assertion

>> The goal of eviction isn't "cleanup"

Perhaps a bit counterintuitive, but I'll assert that the goal of evicting an attacker from your infrastructure isn't to clean up your network.

>> It's to reclaim control and deny re-entry

Evicting before you have control is pointless. But evicting before you can deny re-entry is almost equally pointless. That is a point that can be easy to miss.

Eviction is really the "easy" part.

It's denying your adversary re-entry that's "the crux".

If you can't deny re-entry you may be better off observing...

(...while covertly mitigating damage as best you can)

So when are you ready?

And who gets to decide?

(Probably crisis management)

(Which means a lot of KISSing)

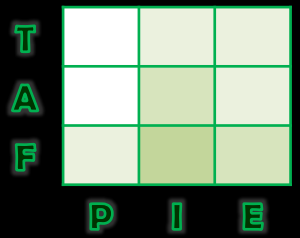
Because they neither want, need
nor understand your details.

Now, how can we aid this decision making process?

The CTI Matrix

CTI Matrix layout

FAT PIE



CTI Matrix layout

>> x-axis: Attack stages

Describes stages of an attack / intrusion.

>> y-axis: Depth of knowledge

Describes levels of knowledge, and the effectiveness of acting upon it.

CTI Matrix building blocks

>> x-axis: Attack stages

- The Cyber Kill Chain. (Mike Hutchins et al.)
- Cyber Attack Lifecycle. (Mandiant)
- (ATT&CK. (MITRE))

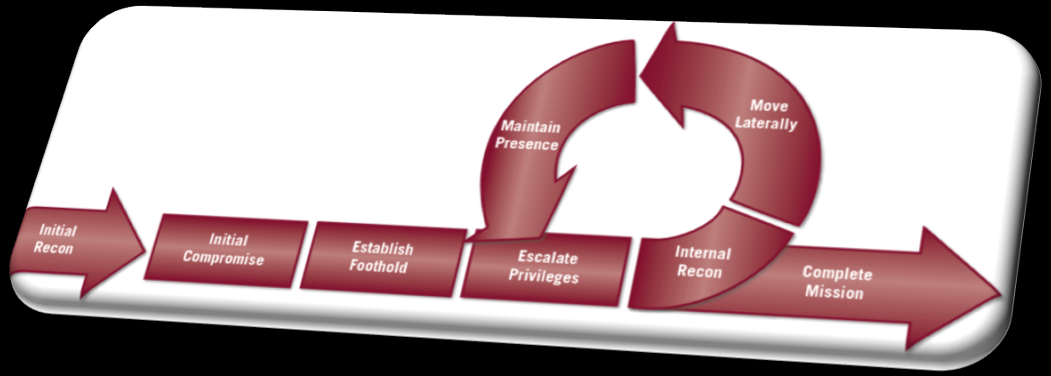
>> y-axis: Depth of knowledge

- The Pyramid of Pain. (David Bianco)
- Detection Maturity Level. (Ryan Stillions)
- («The Four Levels of War>>)
- (Strong correlation with countermeasure effectiveness)

The Cyber Kill Chain

Courtesy of Lockheed Martin

The Cyber Attack Life Cycle



Courtesy of Mandiant

The CTI Matrix

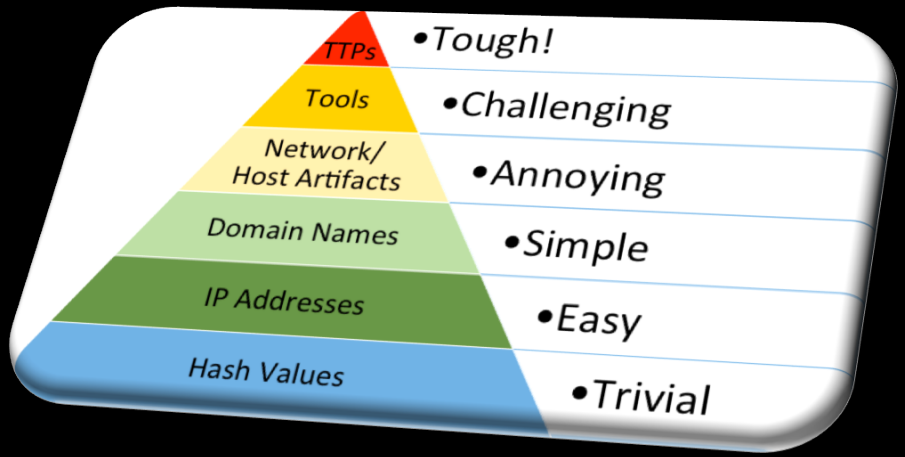
>> x-axis: Attack stages

Borrowing from the Cyber Kill Chain and similar models.

>> Simplified to 3 stages:

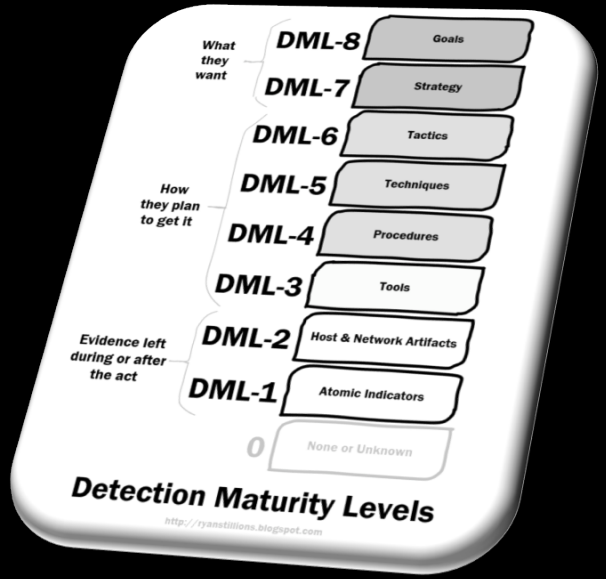
- **Preparation:** Stage 1 and 2 of KC. The attacker prepares the assault.
- **Intrusion:** Stage 3 to 5 of KC. The attacker tries to breach your defenses.
- **Execution:** Stage 6 and 7 of KC. The attacker operates in your infrastructure.

The Pyramid of Pain



Courtesy of David Bianco

Detection Maturity Level



Courtesy of Ryan Stillions

The CTI Matrix

>> y-axis : Level of knowledge

Borrowing from the Pyramid of Pain and Detection Maturity Levels etc.
Measures the level / quality of knowledge, and effectiveness when using it.

>> Simplified to 3 levels:

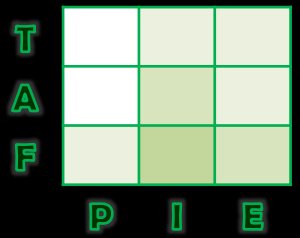
- **Footprint:** Specific traces of the attackers. PoP 1 to 4, DML 1 and 2.
- **Arsenal:** Your adversary's (technical) toolbox. PoP 5, DML 3.
- **Tradecraft:** The way your adversary operates. PoP 6, DML 4 to 6.

Inspiration

Courtesy of Devon Kerr

The CTI Matrix

So finally: The FAT PIE of CTI



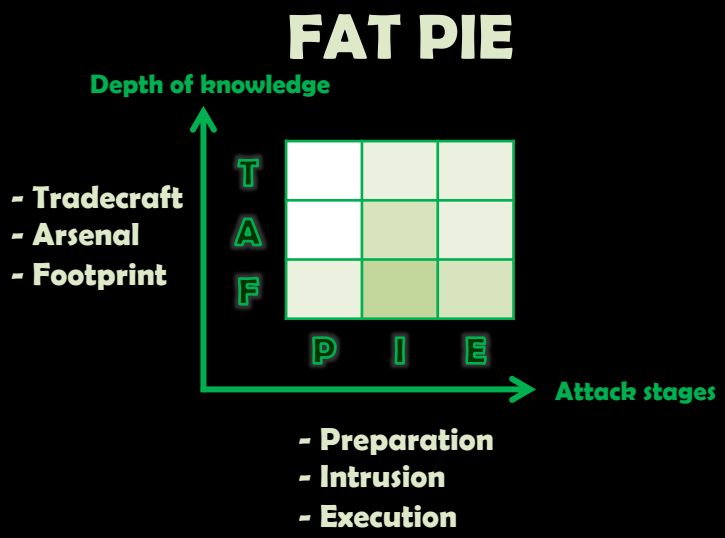
If you dare say *"but it says TAFPIE"*, I will h*t you.
I worked really hard for this backronyme...

Prerequisites

To populate the CTI Matrix you first need to classify your evidence using the more granular models.

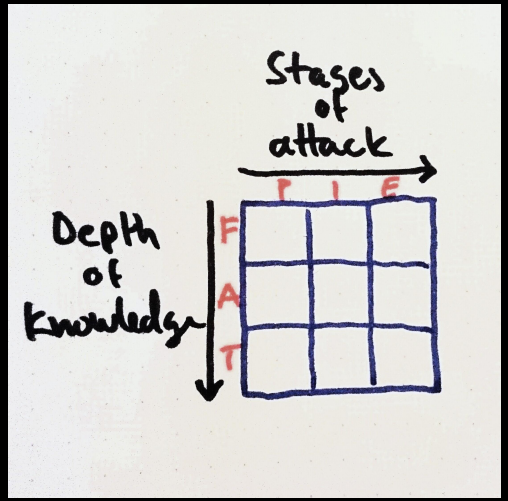
The CTI Matrix is not a replacement for those. It's using the output.

The CTI Matrix



DRAFT

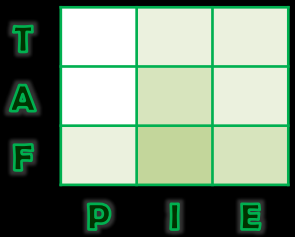
The CTI Matrix



The CTI Matrix

>> Classify findings from DFIR

- IMPORTANT: This is also threat intelligence.
- Remember that you need the A- and T-line too.
- If you can only fill the F-line, you're flying blind.



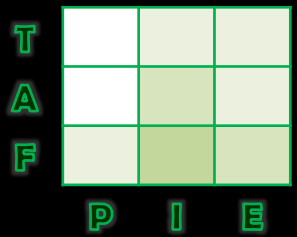
>> Classify findings from CTI

- Your own hunting in external sources.
- Intelligence shared from third parties.
- Only include that what you assess to be of high relevance.

The CTI Matrix

>> Assess your total knowledge

- What do you actually know?
- Do your DFIR findings differ from the CTI findings?
- Do you have obvious knowledge gaps?

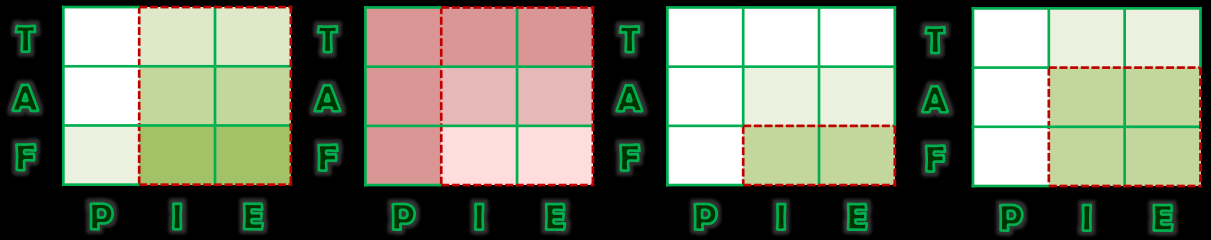


>> Assess your readiness to evict

- How much knowledge are you able to act upon to deny and evict?
- How much knowledge are you able to convert to re-entry prevention?
- How much knowledge are you able to convert to re-entry detection?

Using the CTI Matrix

Examples



Total knowledge

Knowledge gaps

Converted to prevention

Converted to detection

«Ready to evict the attacker?»

>> Must define ready

The CTI Matrix helps you do that. Or can at least guide your thinking.

>> Must measure progress towards "ready"

The CTI Matrix helps you do that as well. But not without hard work.

>> Should include resistance vs re-entry

Successful eviction should be measured against successful resistance to re-entry.

FIN

Thank you for your attendance and interest.

Destination Host Reachable

>> Questions and comments?

Ping me on twitter: @FrodeHommedal with #4SICS and/or #CTIM.

>> I would love feedback

I don't have all the answers, and the CTI Matrix is work in progress.

>> P.S. Good luck

The best of luck defending critical infrastructure. You're gonna need it.