The Cyber Threat Intelligence Matrix

— taking the attacker eviction red pill

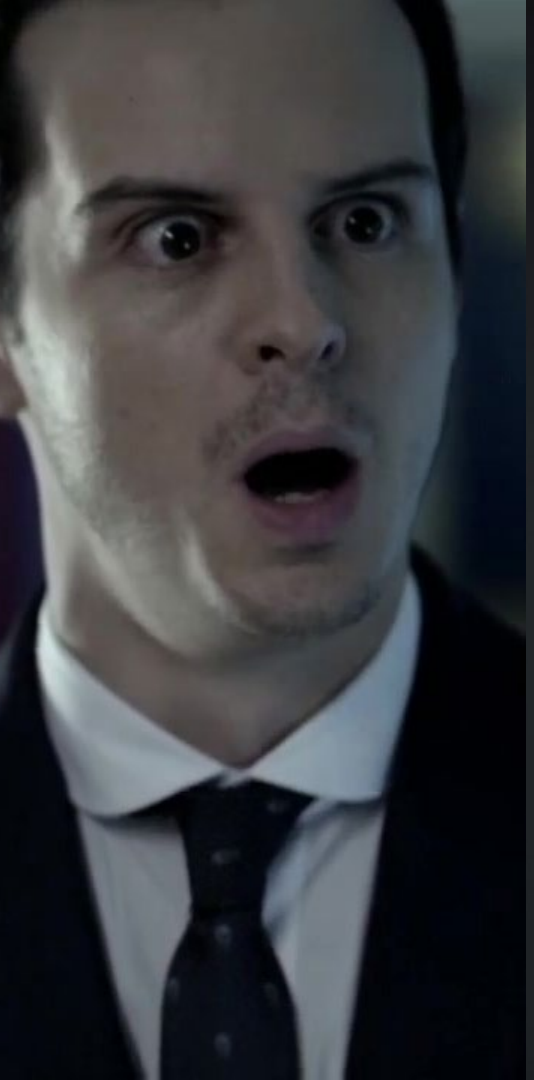
Frode Hommedal

Telenor CERT // @FrodeHommedal // #ACSC2017

This talk is about fighting APT

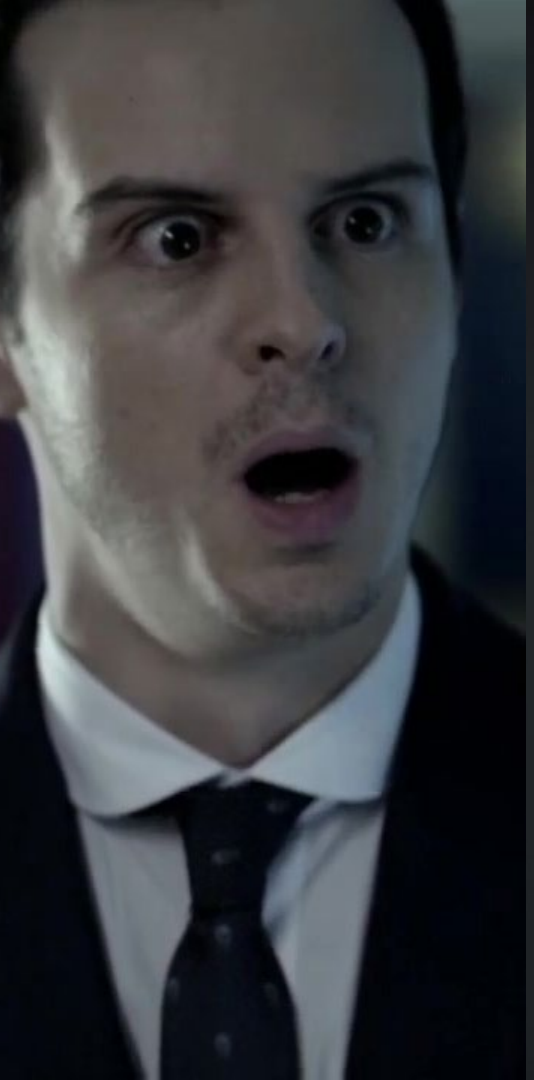
The aim is to help you be the one still standing.

But it will require that you own up to some hard truths.



When evicting a persistent attacker:

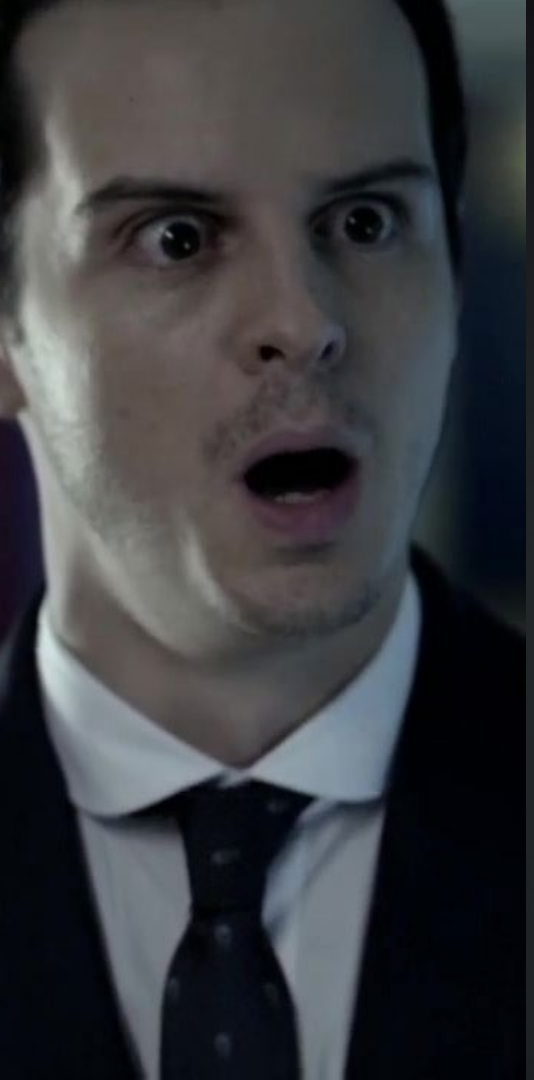
If you are 99% successful in closing down you attacker's access to you network, you will be exactly 0% successful in keeping them out.



When evicting a persistent attacker:

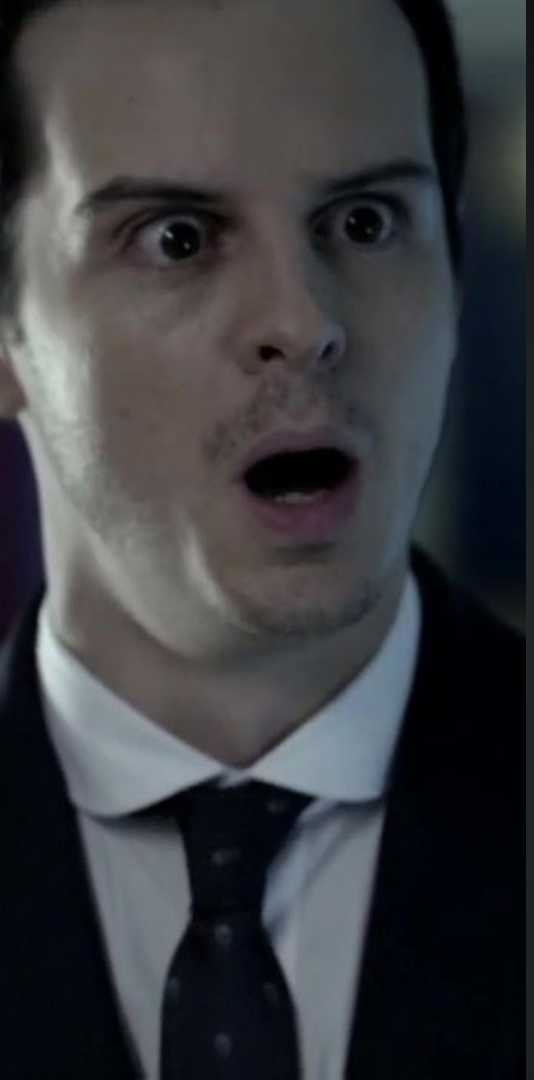
It's like removing cancer. You must get it all, or it will continue to spread.

80% isn't good enough…



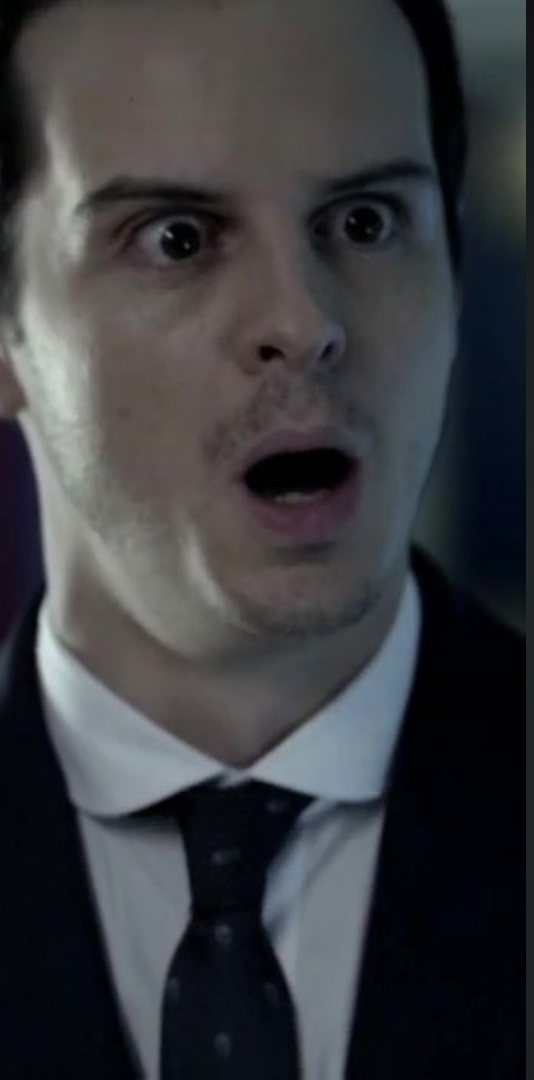
When evicting a persistent attacker:

If you fail, you waste a lot of time and resources and let your attacker learn and improve. That's not good…



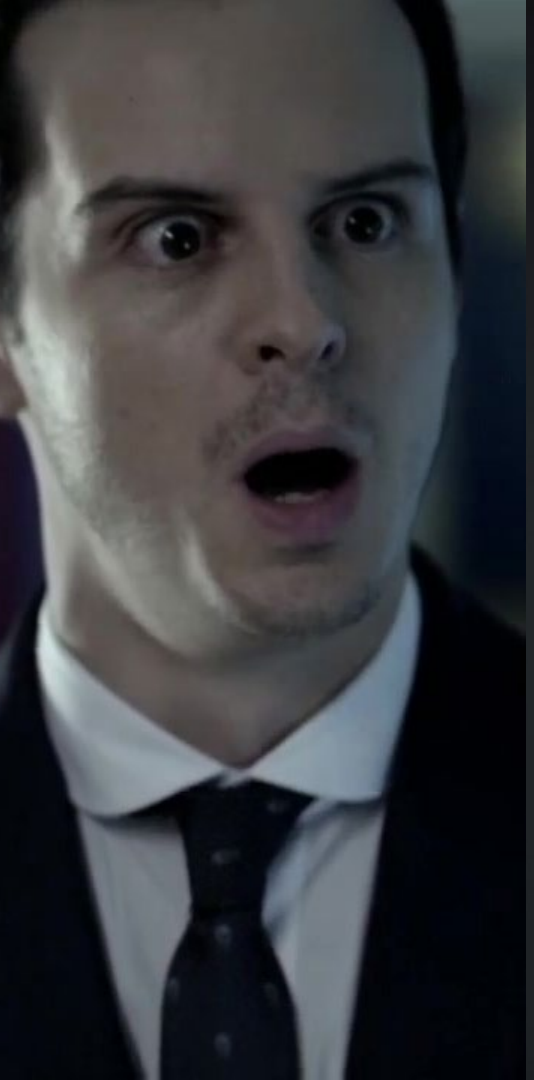
When evicting a persistent attacker:

"We have been at this long enough now" is not a very good argument to decide to evict a persistent attacker.



Knowledge gaps

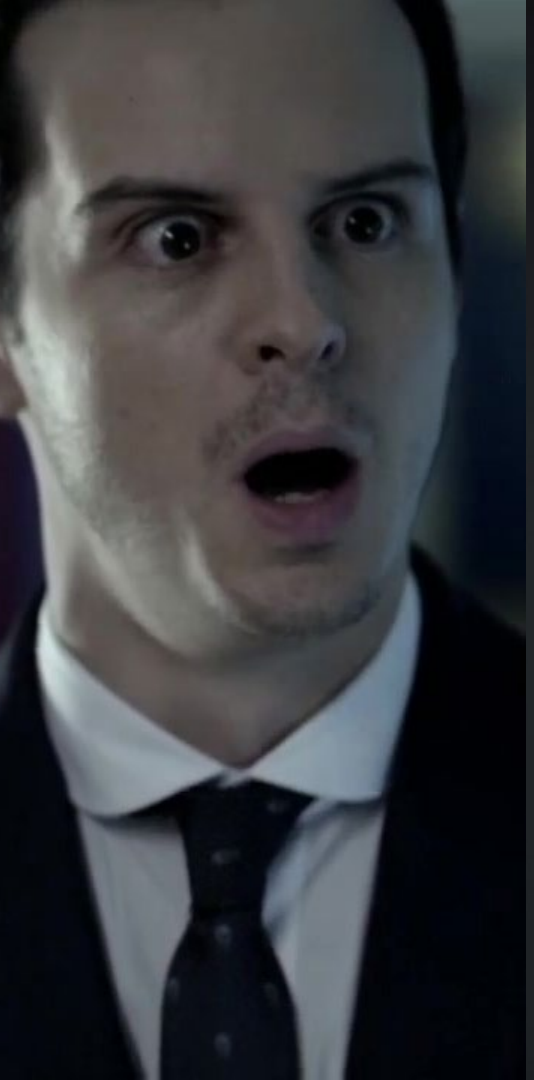
The attacker hide in your knowledge gaps. To succeed you need to find them and close them.



Closing the gaps

That is what the Cyber Threat Intelligence Matrix is about.

Helping you cl0sing those gaps, and knowing when you are ready to evict the attacker.



Assessing readiness

In addition you can use it to assess you readiness to act on your knowledge, come eviction day.

But first, let's spend a few slides on words and definitions

...

because words actually matter.

cyber cyber cyber

cyberspace cyber attacks
cyber threat intelligence
cyber defense cyber security
cyber cyber cyber cyber...

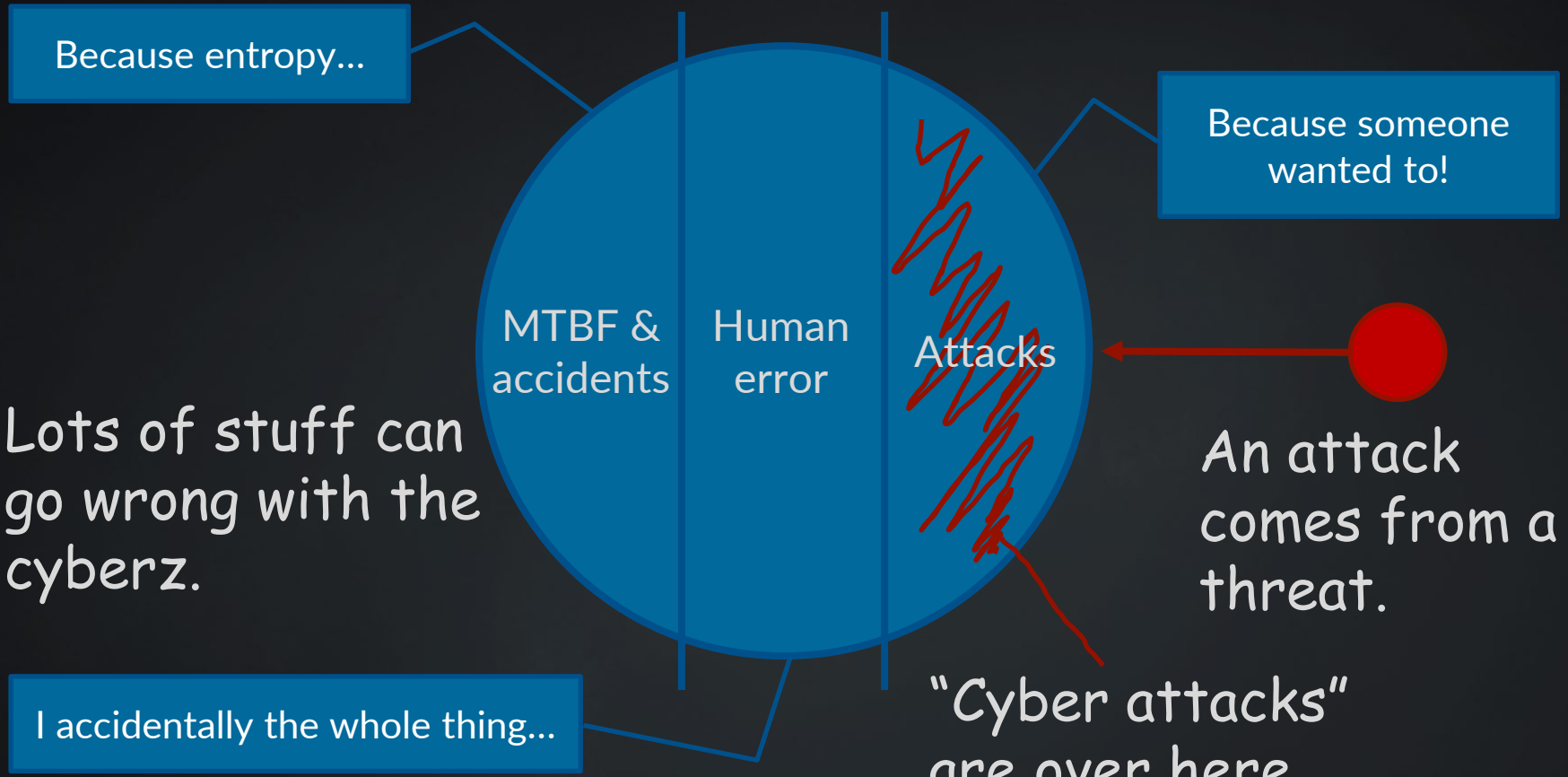
But cyber do mean something.

Cyberspace

The digital fabric that lets electronic devices, and through them, people, communicate and interoperate.

Cyber attack

People attacking people through manipulating electronic devices across this fabric, or by manipulating the very fabric itself.


Because entropy...
Because someone wanted to!
MTBF & accidents
Human error
Attacks
Lots of stuff can go wrong with the cyberz.
An attack comes from a threat.
I accidentally the whole thing...
"Cyber attacks" are over here.

Cyber threats

Some are more or less victim agnostic.

Example: Ransomware

Cyber threats

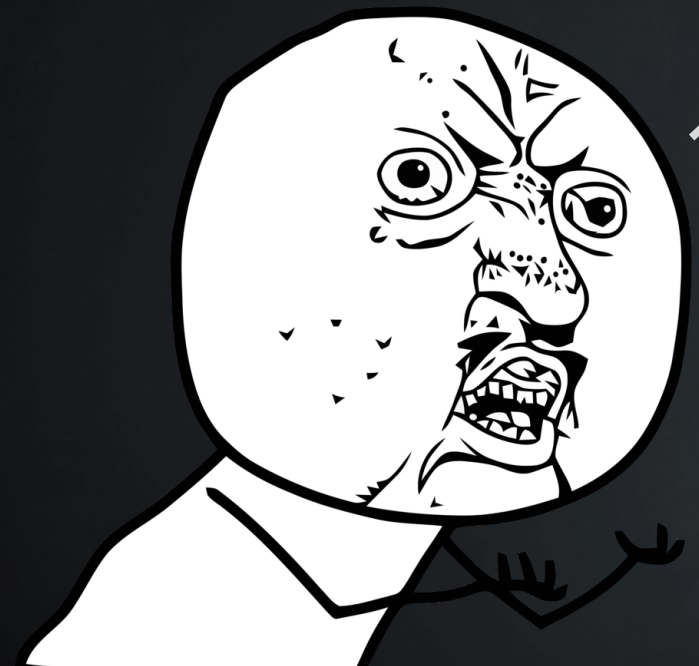
Others are significantly more targeted.

Example: APT

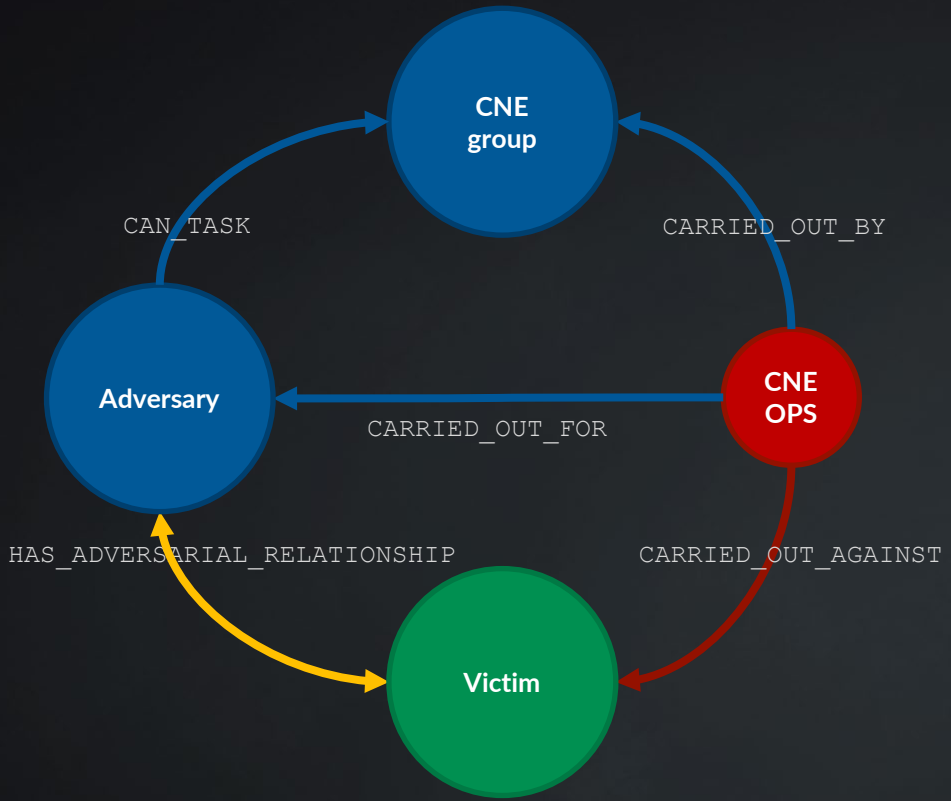
Cyber threats

Will reach you through the digital fabric of cyberspace and manipulate your komputarz to achive their goals, whatever they are.

Threats, Y U NO STOP?



For APT, an incident is an indication of some kind of adversarial relationship you're either in or relevant for.



Intelligence speak for "APT" is CNE.

It's carried out against a target, or if you like, a victim. E.g. you.

It's carried out by an attack group that specializes in this.

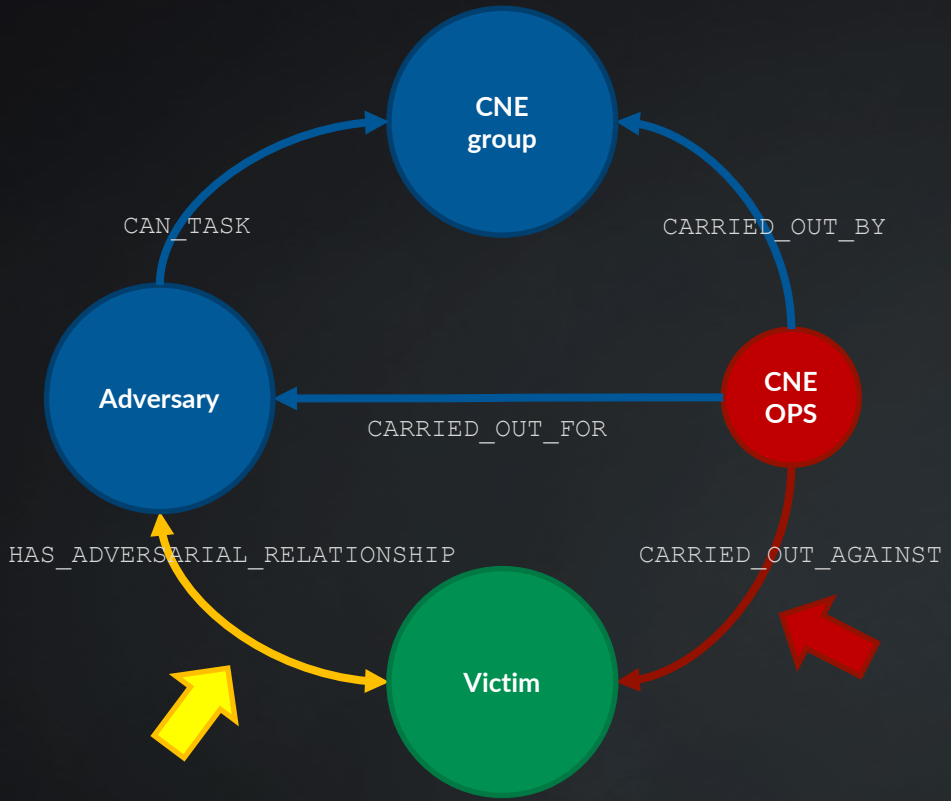
It's carried out on behalf of a customer.

It's this customer that is your adversary.

Cybersecurity

Defense against the digital dark arts of the attackers coming at you through cyberspace.

Defending against APT is like fighting Voldemort...



Cybersecurity is mostly preoccupied with defending here.

The Cyber Threat Intelligence Matrix is only concerned with (closing knowledge gaps on) this "flank".

But "business" should probably start worrying a bit more about how to defend this flank.

Cyber threat intelligence

Intelligence about threats carrying out cyber attacks!

So what is intelligence…?

Intelligence

Estimates of the secrets and mysteries clouding the intentions and capabilities of your adversaries.

Or here, their "attack groups".

Intelligence

The most important secret to uncover is your role in the adversarial relationship that is motivating the attacks

(Out of scope for the CTIM.)

Now that cyber threat intelligence should make sense to you, let's move on to the matrix and the knowledge gaps.

The CTI Matrix

and knowledge gaps

The CTI Matrix

or actually — of knowledge gaps

AV alert

You get an AV alert. AV found malware and put it in quarantine.

What are you knowledge gaps?

IDS alert

You get an IDS alert. The IDS says you probably have malware on a system.

What are you knowledge gaps?

China Chopper

You find a "china chopper" web shell on a web server.

What are you knowledge gaps?

"Kill chain" analysis

Any piece of evidence you get, will almost always lead to other things you should analyze.

Keep track of those.

“Kill chain” analysis

What happened before this?

What happened after?

Recon
Weaponize
Deliver
Exploit
Malware
C&C
Execute

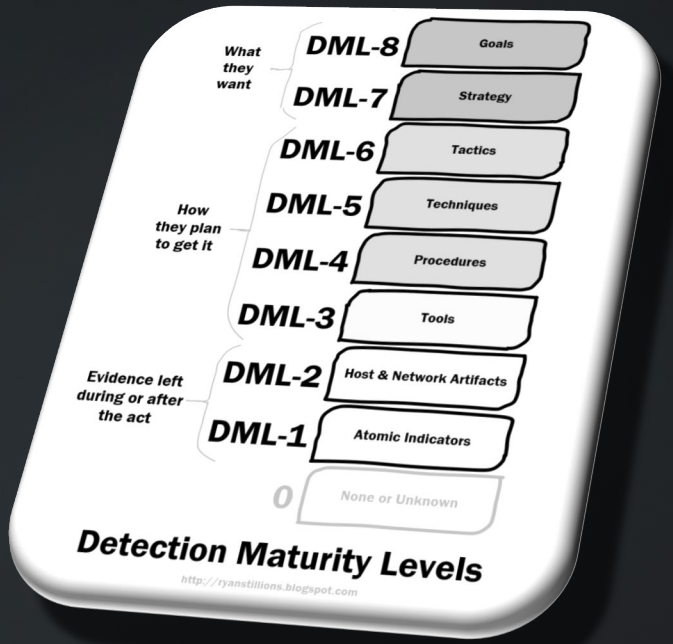
"DML" and "PoP"

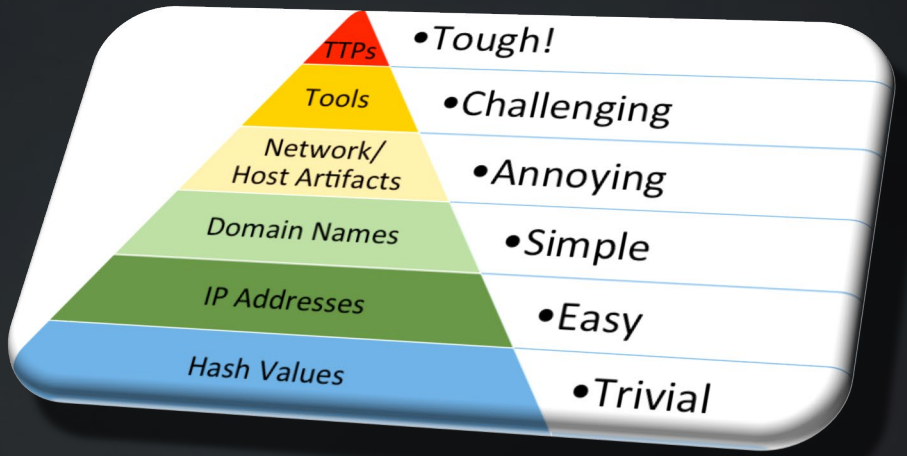
Detection Maturity Level

Ryan Stillions

Pyramid of Pain

David Bianco


What they want
DML-8
Goals
DML-7
Strategy
How they plan to get it
DML-6
Tactics
DML-5
Techniques
DML-4
Procedures
DML-3
Tools
Evidence left during or after the act
DML-2
Host & Network Artifacts
DML-1
Atomic Indicators
0
None or Unknown
Detection Maturity Levels
http://ryanstillions.blogspot.com


TTPs
Tools
Network/
Host Artifacts
Domain Names
IP Addresses
Hash Values
•Tough!
•Challenging
•Annoying
•Simple
•Easy
•Trivial

"DML" and "PoP"

You must also try to learn more about the artefact you are analyzing than where it fits in the "kill chain".

"DML" and "PoP"

How was this made?

How is it used?

What is this for?

"DML" and "PoP"

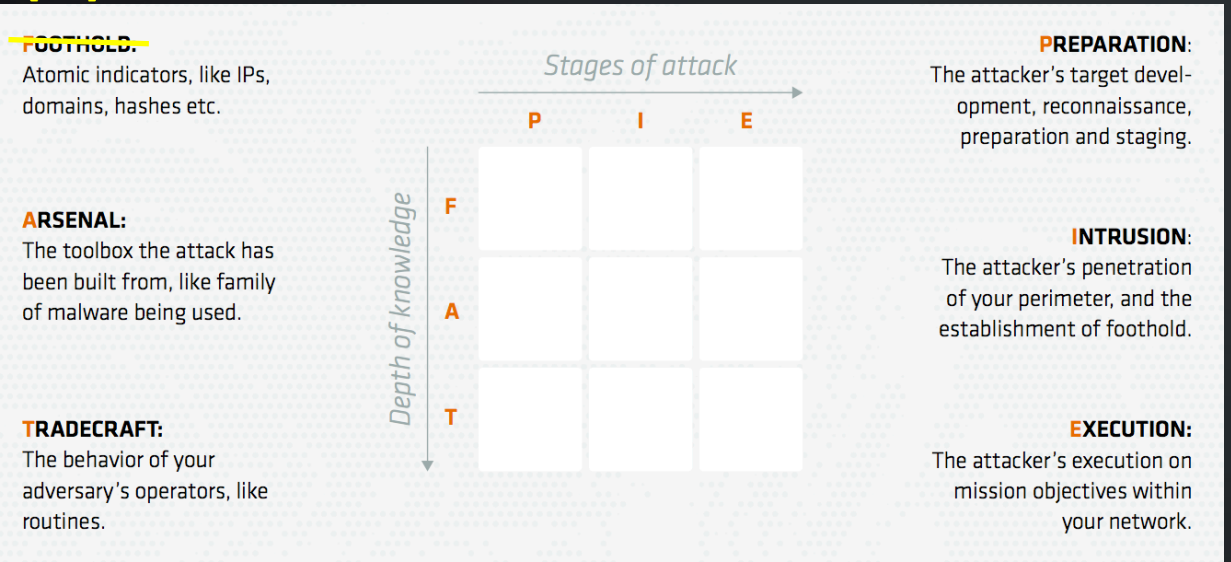
How dangerous is this for me?

How can I prevent and detect it, even if it changes a bit?

Can I detect the same thing being done with another tool?

The Cyber Threat Intelligence Matrix is basically a simplified combination of the "kill chain" and "DML" / "PoP".

[SIC] FOOTPRINT



You use it to map different types of knowledge of different stages of an attack.

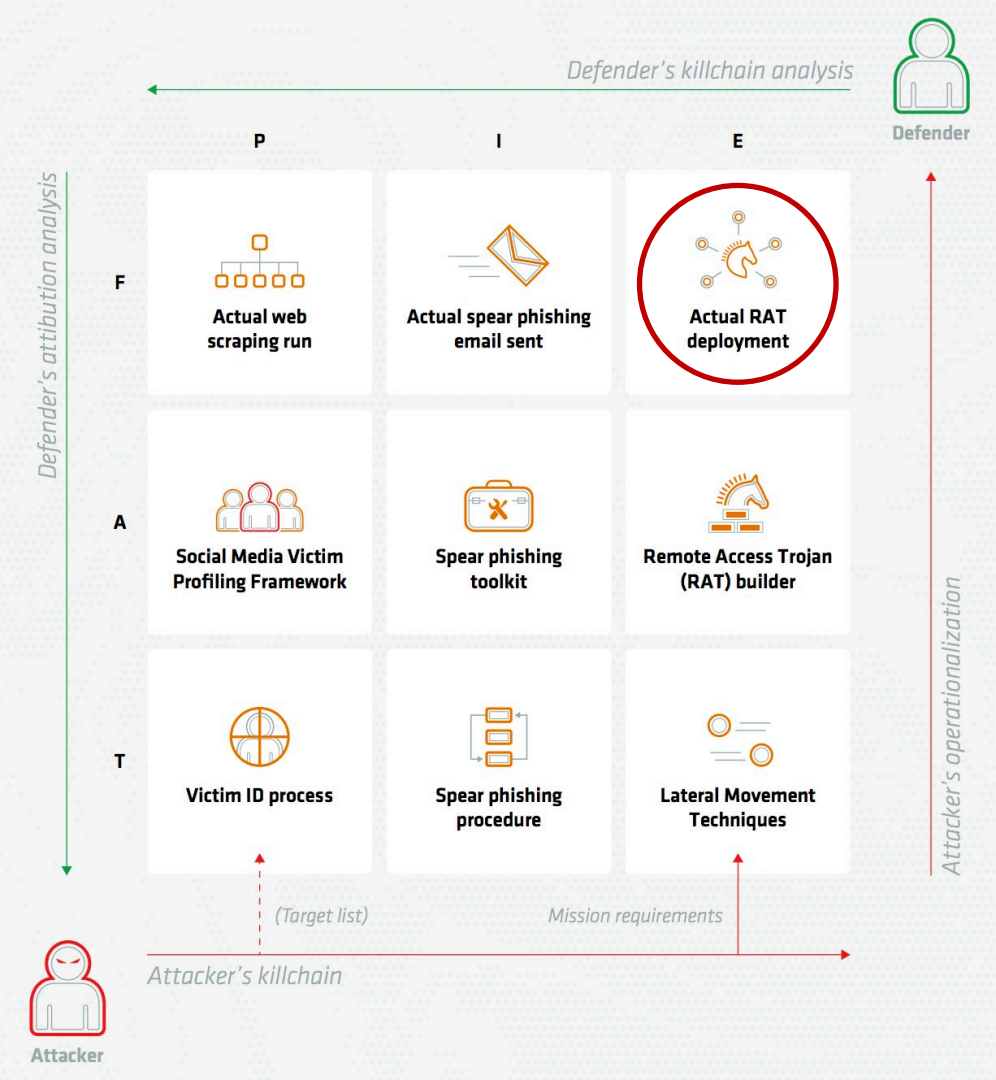
It requires a proper "kill chain analysis", and a good understanding of the "DML" / "PoP", and disciplined tagging and categorization of findings using e.g. MITRE ATT&CK.

You will create four matrices where you map:

1. your own findings from your incident;
2. intel from other sources and incidents;
3. your ability to convert what you know about the attacker to prevention;
4. and your ability to convert what you know to detection — facing re-entry attempts.

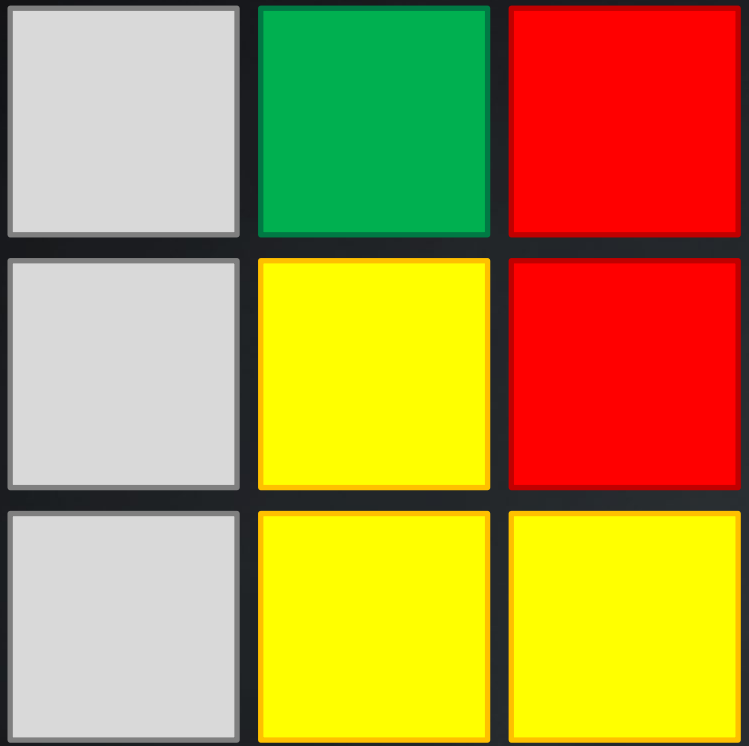
Be very aware of diffs… Diffs are indicators of either knowledge gaps, or your inability to act on what you know.

Both are enemies of successful eviction.

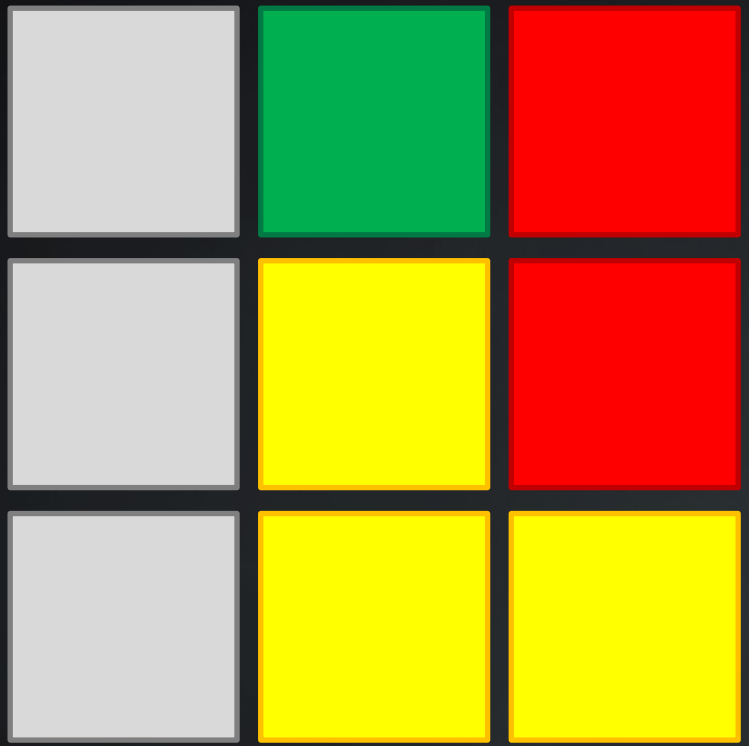


Example:

Map concrete evidence to the matrix, and hash out what else you should be able to either find evidence for or make inferences about.

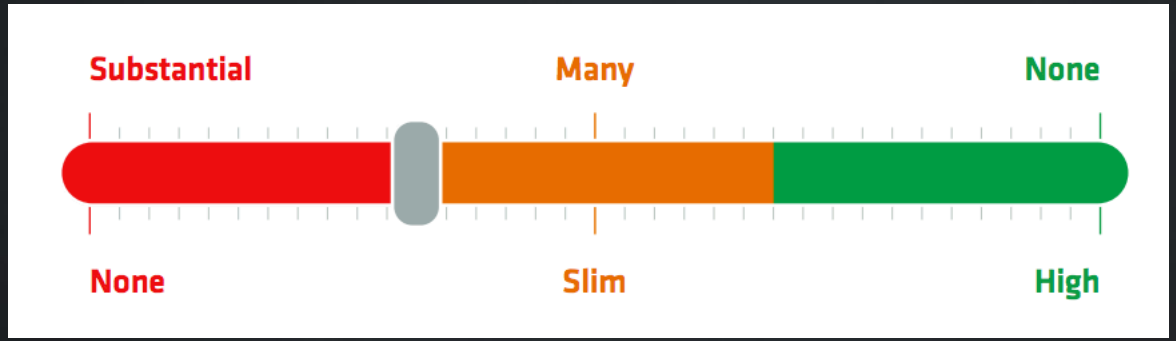


By using your own list of unanswered questions and the diff to the intel matrix, you can start figuring out if you have critical knowledge gaps in your analysis.

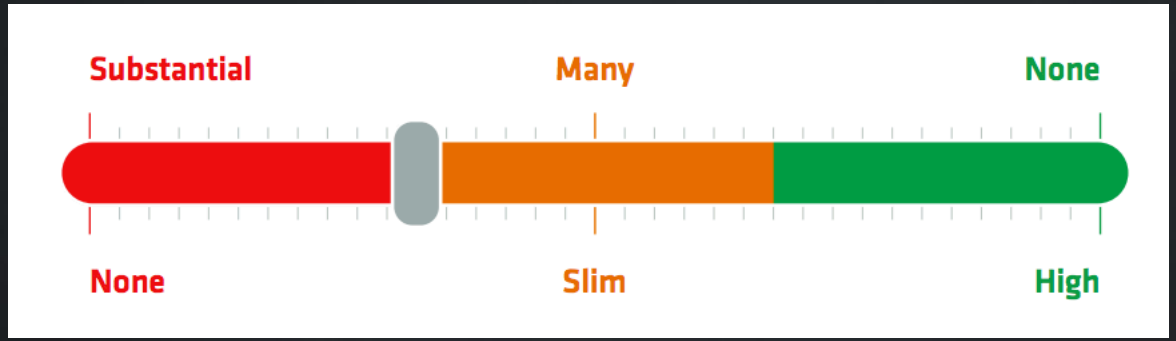


By diffing what you know with your ability to act on it, you can gauge your readiness to actually pull off successful eviction, and your ability to deny subsequent re-entry.

If you can prove that you have substantial knowledge gaps, your chances of a successful eviction is slim to none.



The same applies if you are unable to convert critical intelligence into prevention and detection.



The graphical 3x3 risk-like matrix is a visual aid you can bring to crisis management when discussing eviction, and advice them based on your assessment of success.

You arrived at your assessment using a more structured approach and they can reach a decision in a more informed manner.

#WINNING

Thank you.