Taking the Attacker Eviction

RED PILL

Taking the Attacker Eviction

RED PILL

Or how to structure your thinking when countering

espionage

and

sabotage

from

"APT"

This talk will focus on the

eviction

of a

mission driven

and well organized

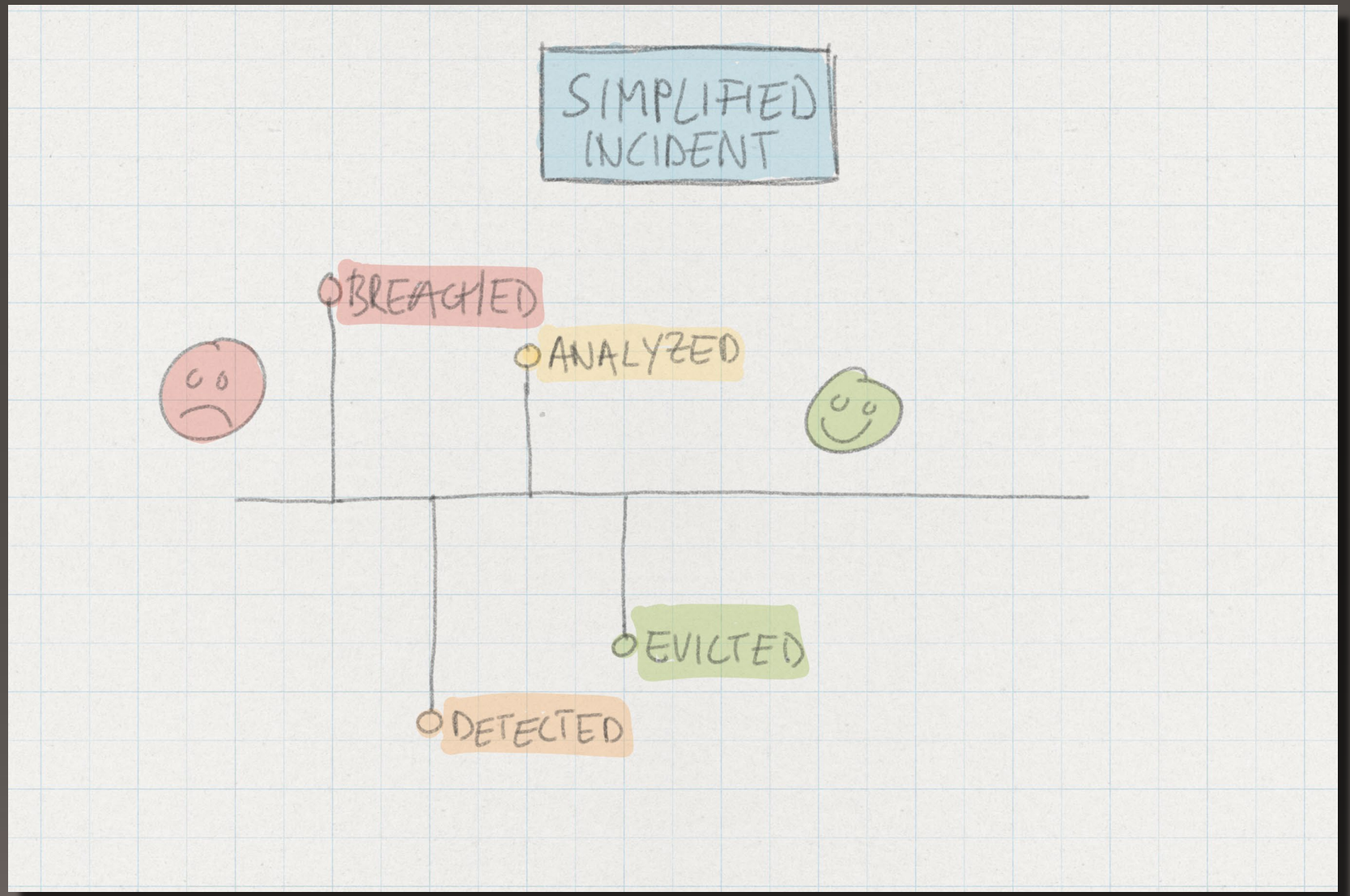
adversary

Incident Response

PICERL:
Prepare
Identify
Contain
Eradicate
Recover
Lessons Learned

NIST:
Preparation
Detect & Analyze
Contain & Eradicate & Recover
Post Incident Activities

Bottom Line:
Eventually you will try to get the attacker off your network

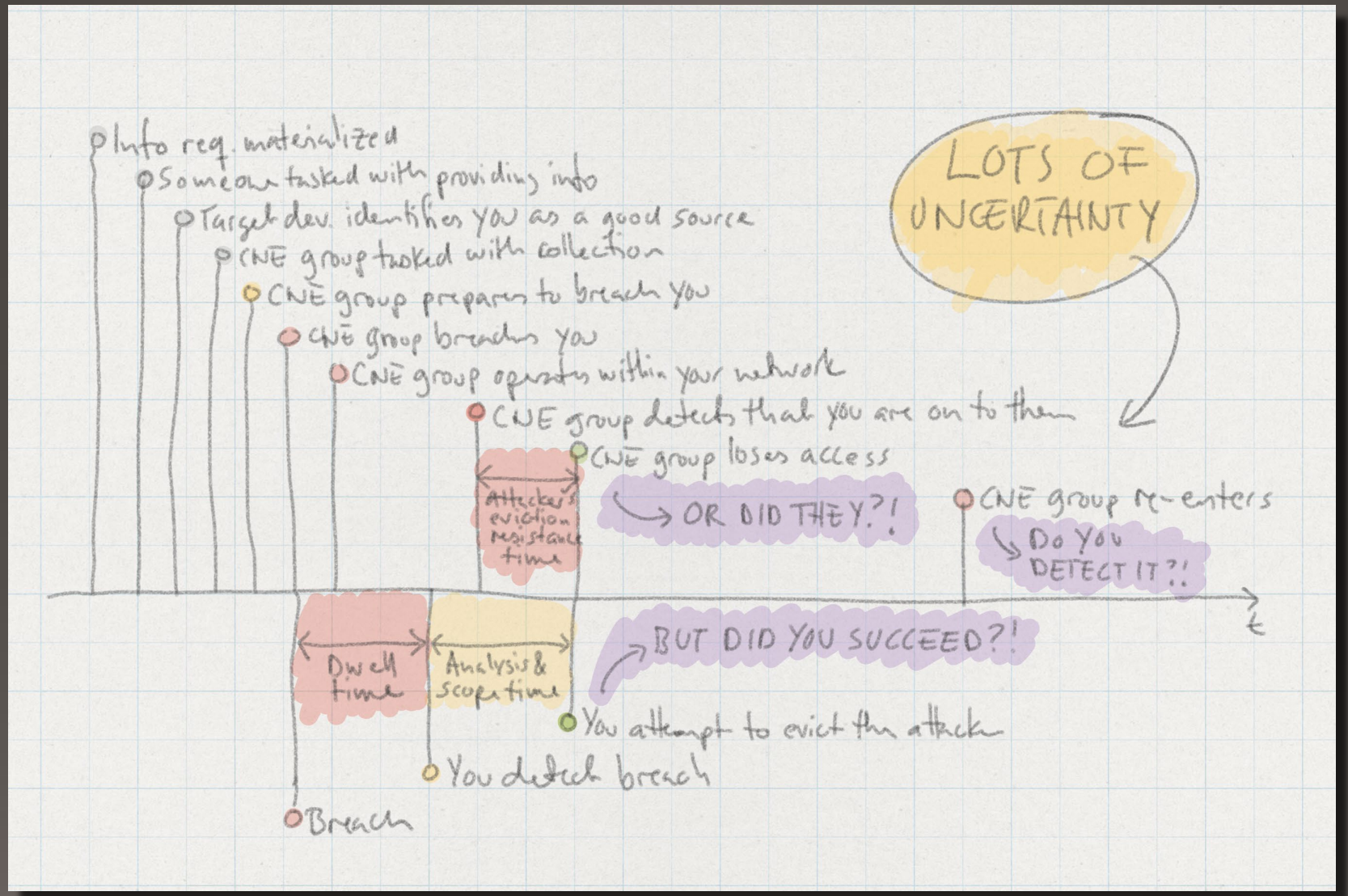


Incident Response

PICERL:
Prepare
Identify
Contain
Eradicate
Recover
Lessons Learned

NIST:
Preparation
Detect & Analyze
Contain & Eradicate & Recover
Post Incident Activities

Bottom Line:
Eventually you will try to get the attacker off your network



Turns out there's a lot of

uncertainty

to deal with when

responding

to a targeted and advanced

"APT breach"

Incident Response

when facing an APT threat

Best Practice:
Scope before you start responding.

Common Misstep:
Acting too soon, giving your adversary time to adapt.

Incident Response

when facing an APT threat

Best Practice:

Scope before you start responding.

Common Misstep:

Acting too soon, giving your adversary time to adapt.

COMMON MISSTEPS

Common missteps an organization can make when first responding

MITIGATING THE AFFECTED SYSTEMS TOO EARLY

- Can cause the loss of volatile data such as memory and other host based artifacts
- Adversary will notice and change TTPs

TOUCHING ADVERSARY INFRASTRUCTURE (PINGING, NSLOOKUP, BROWSING, ETC)

- These actions can tip off the adversary that they have been detected

PREEMPTIVELY BLOCKING ADVERSARY INFRASTRUCTURE

- Network infrastructure is fairly inexpensive. Adversary can easily change to new C2 and you will lose visibility of their activity.

PREEMPTIVE PASSWORD RESETS

- Adversary likely has multiple credentials – or worse owns your entire AD
- Adversary will use other credentials, create new credentials, or forge tickets

Password

* * * *

FAILURE TO PRESERVE OR COLLECT CRITICAL LOG DATA

- Learn what log types would be critical to an investigation in your organization.
- Collect and retain these logs for at least 1 year.

It turns out

"acting too soon"

is a thing when responding to an

APT threat

If you want to respond
effectively you need to

reduce the uncertainty

and understand when it's the right time

to act

But first some

APT patterns

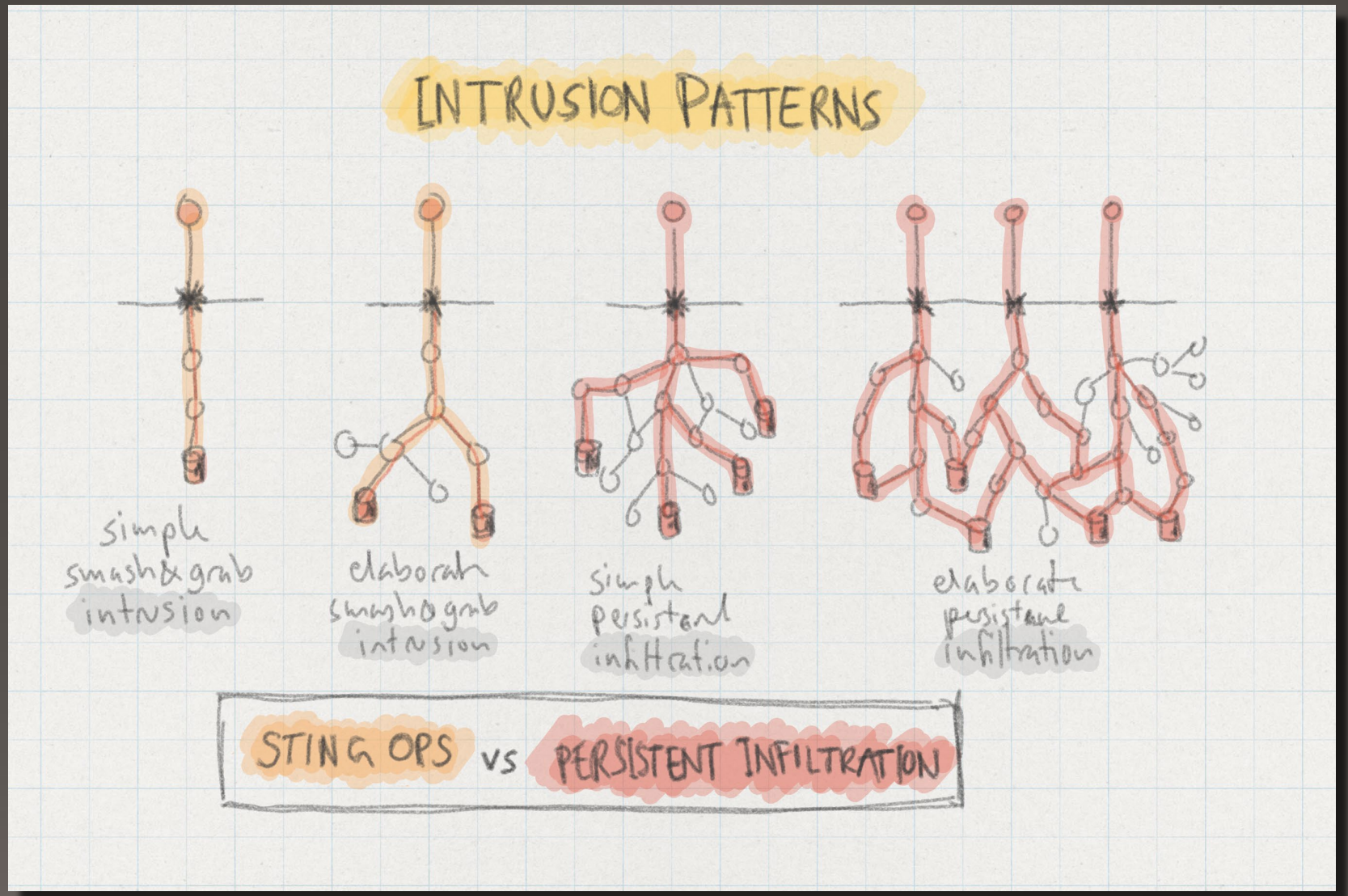
Intrusion Patterns

of APT threats

Sting Operation:
Also called "smash and grab". A direct attack to get a specific piece of information.

Persistent Infiltration:
A long running campaign against you, where your adversary will gain and sustain unauthorized access to your infrastructure for a long period of time.

Response:
When responding, you should take into consideration what kind of pattern you are seeing.



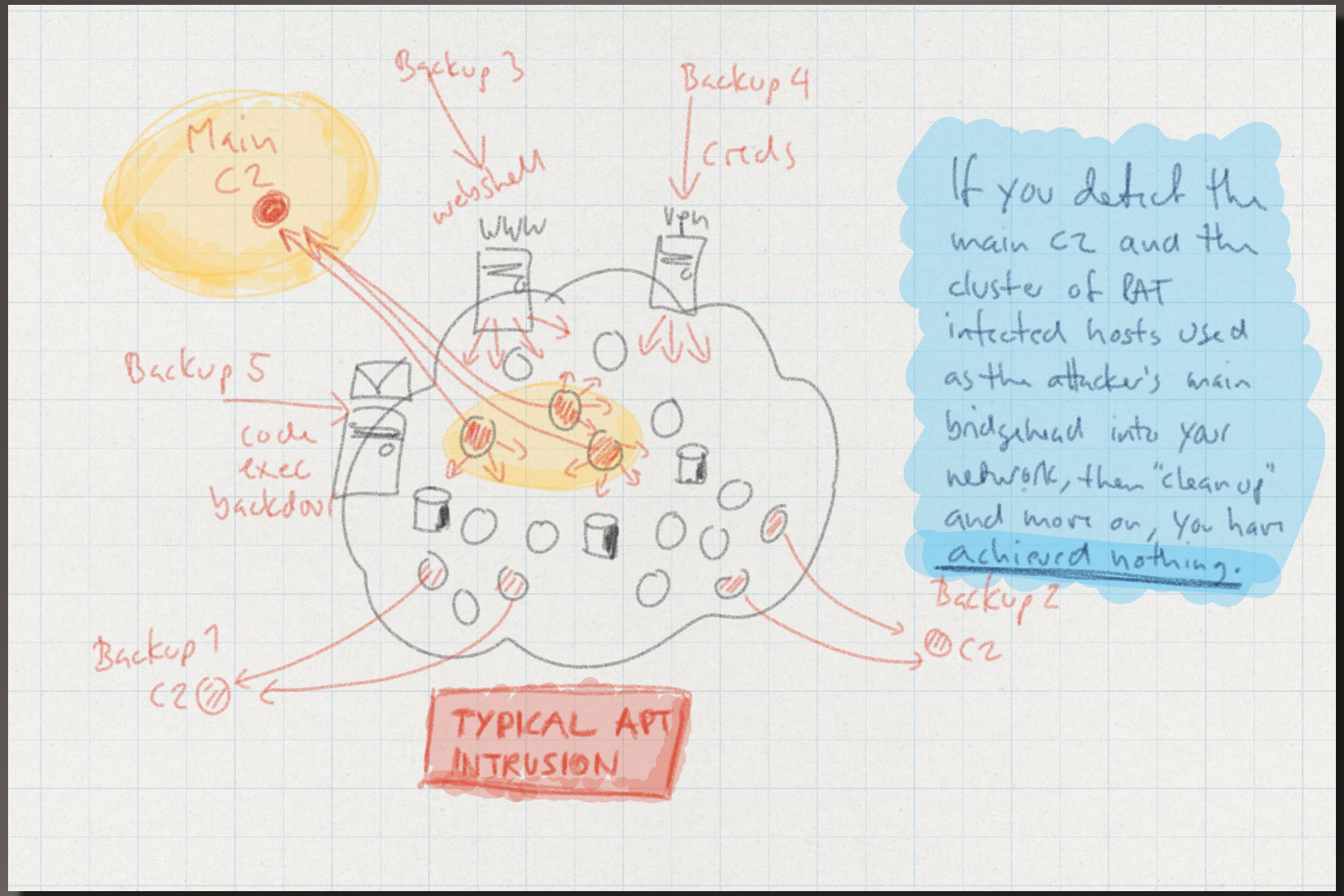
Intrusion Patterns

of APT threats

Sting Operation:
Also called "smash and grab". A direct attack to get a specific piece of information.

Persistent Infiltration:
A long running campaign against you, where your adversary will gain and sustain unauthorized access to your infrastructure for a long period of time.

Response:
When responding, you should take into consideration what kind of pattern you are seeing.



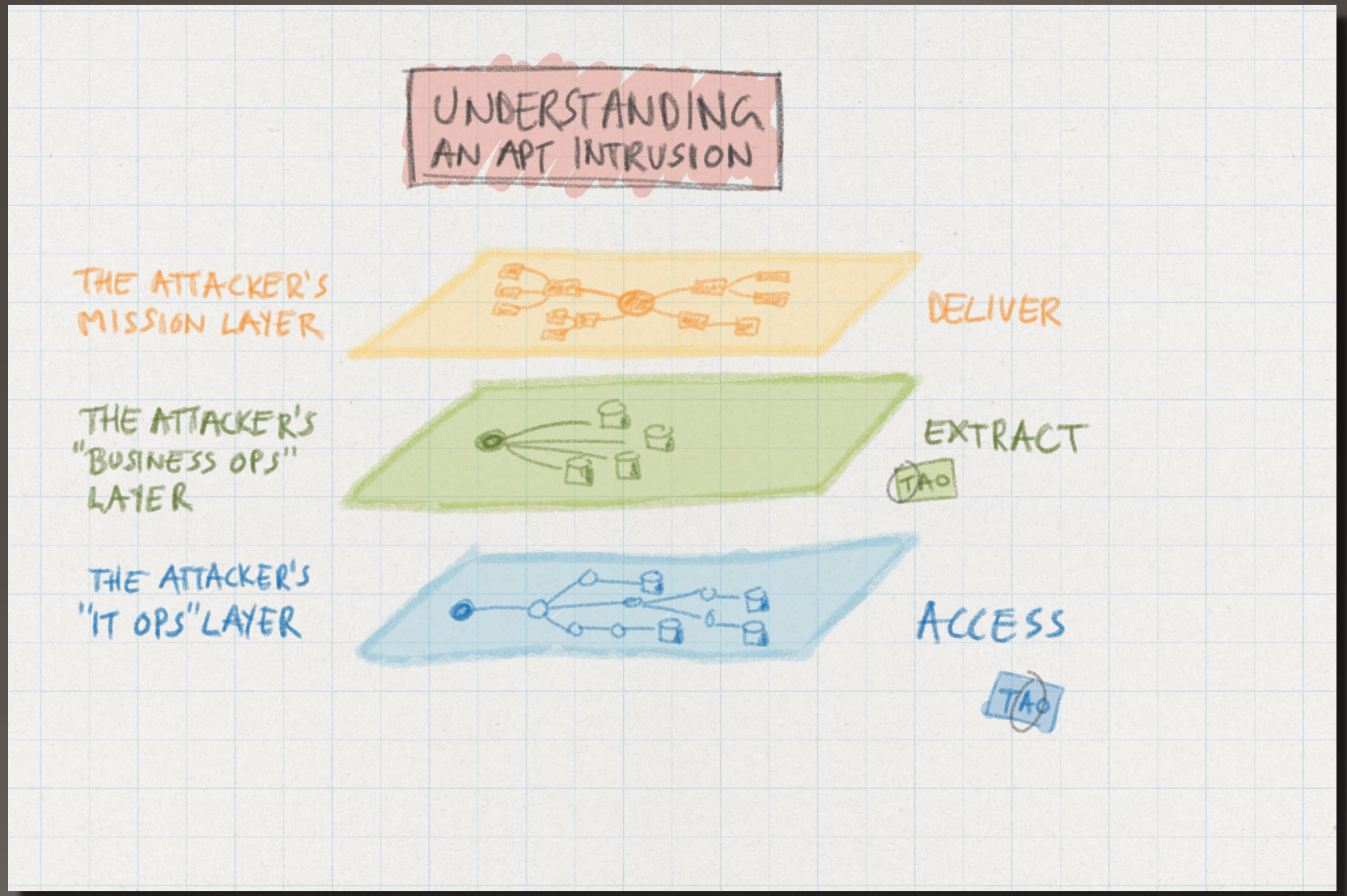
The Structure

of an APT infiltration

Access:
An APT infiltration is all about access. They work a lot to gain and sustain access.

Extract:
The purpose of gaining access is to find and extract useful information (or abuse your infrastructure).

Deliver:
All of this is done to deliver on goals set for the attacker's mission.



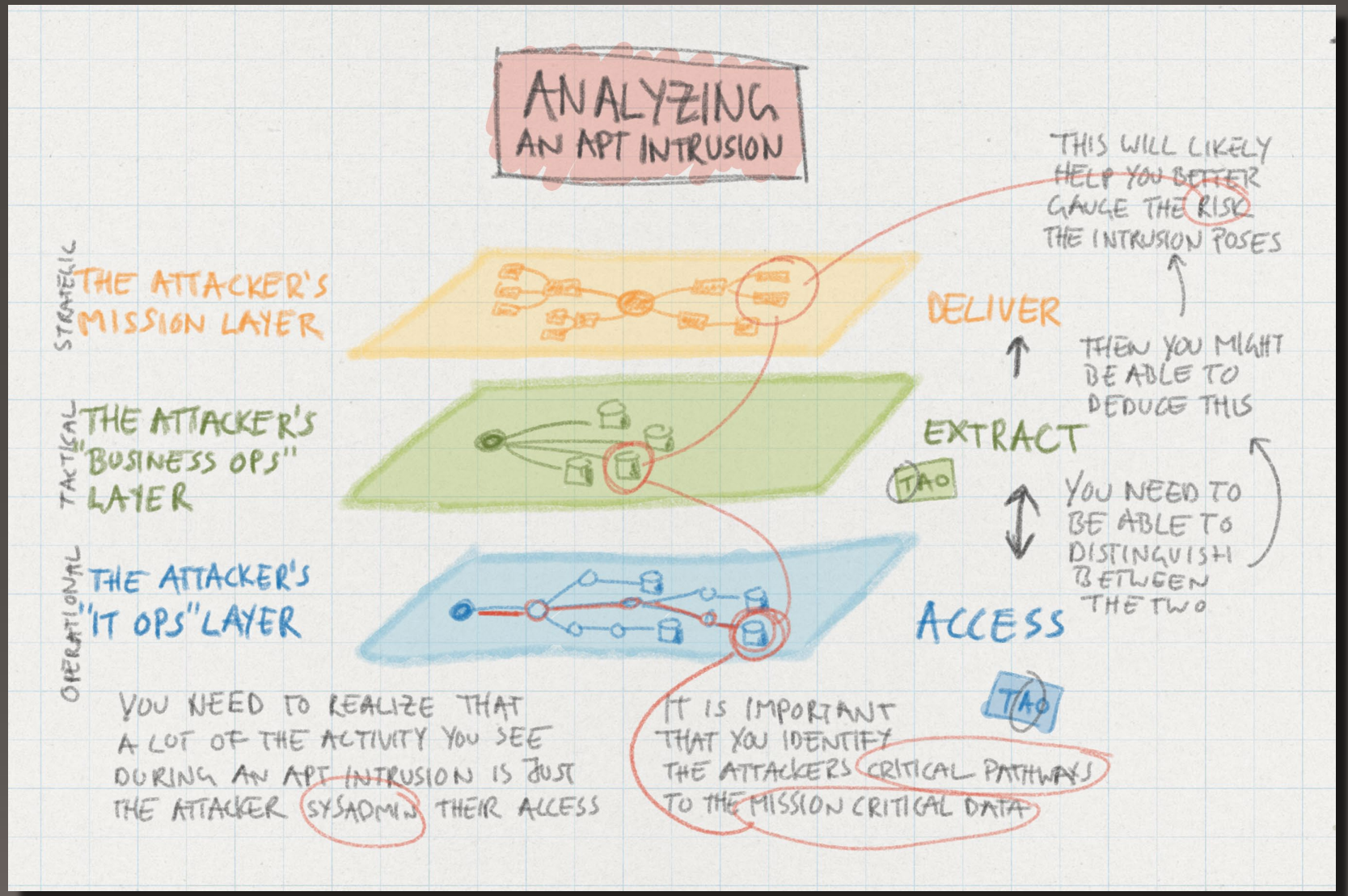
The Structure

of an APT infiltration

Access:
An APT infiltration is all about access. They work a lot to gain and sustain access.

Extract:
The purpose of gaining access is to find and extract useful information (or abuse your infrastructure).

Deliver:
All of this is done to deliver on goals set for the attacker's mission.



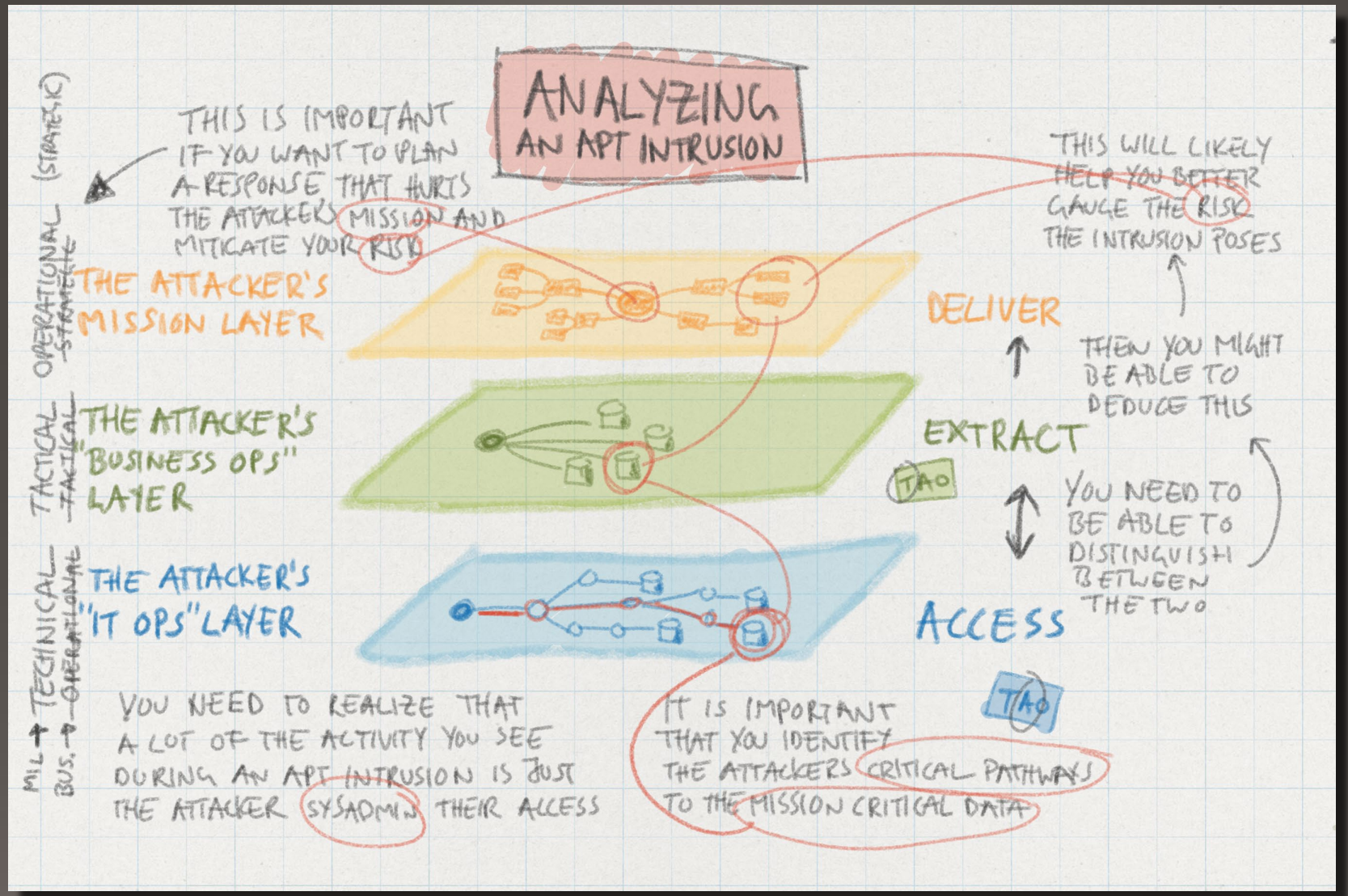
The Structure

of an APT infiltration

Access:
An APT infiltration is all about access. They work a lot to gain and sustain access.

Extract:
The purpose of gaining access is to find and extract useful information (or abuse your infrastructure).

Deliver:
All of this is done to deliver on goals set for the attacker's mission.



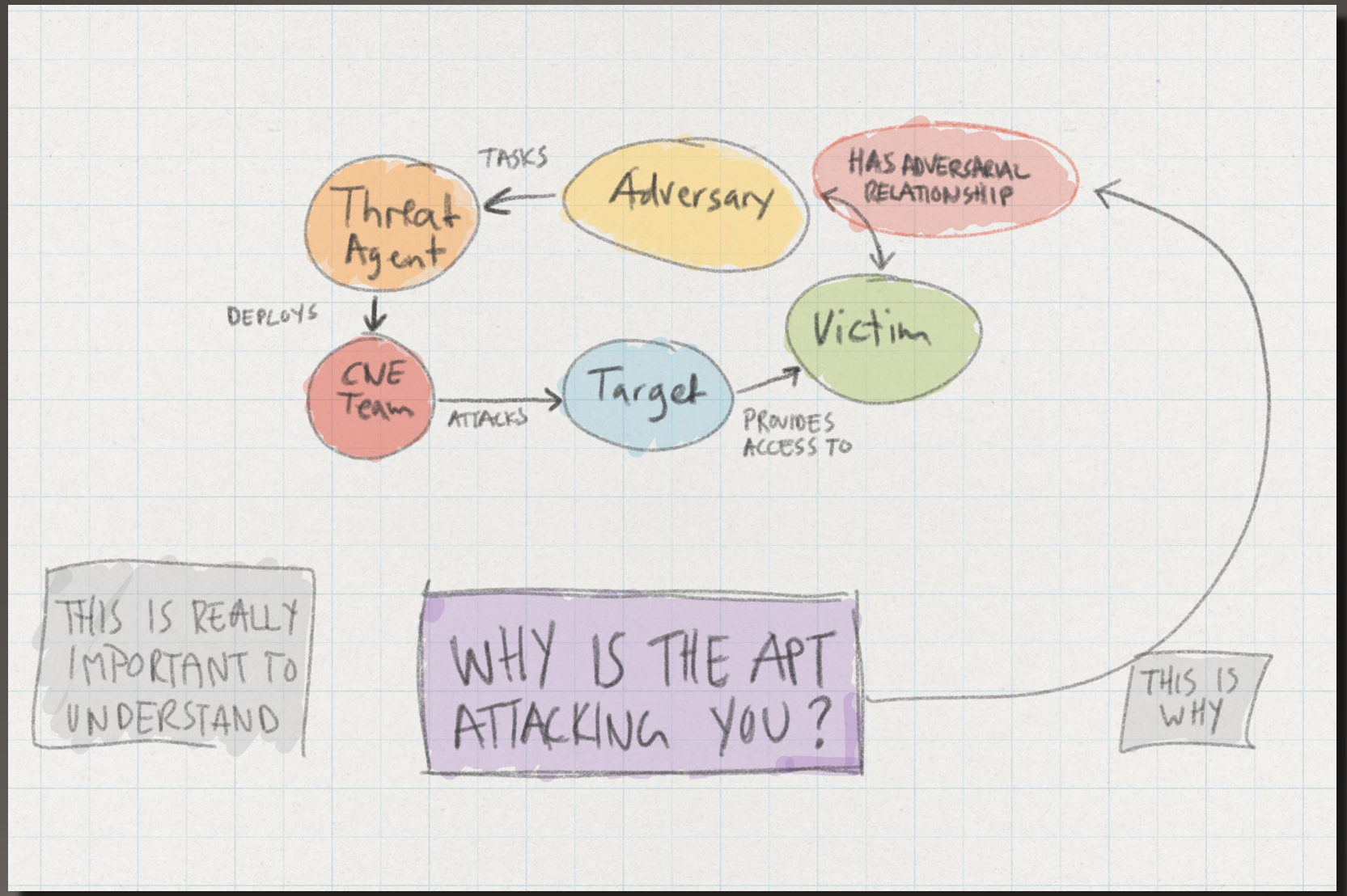
Why you are targeted

by an APT attack team

Adversarial Relationship:
For you to ever be targeted by an APT attack team you must be relevant for some kind of adversarial relationship.

Provide Access:
And you must provide access to something that will help the offensive party gain an advantage in that relationship.

Collection:
What you are observing though is only the collection part of a much bigger process.



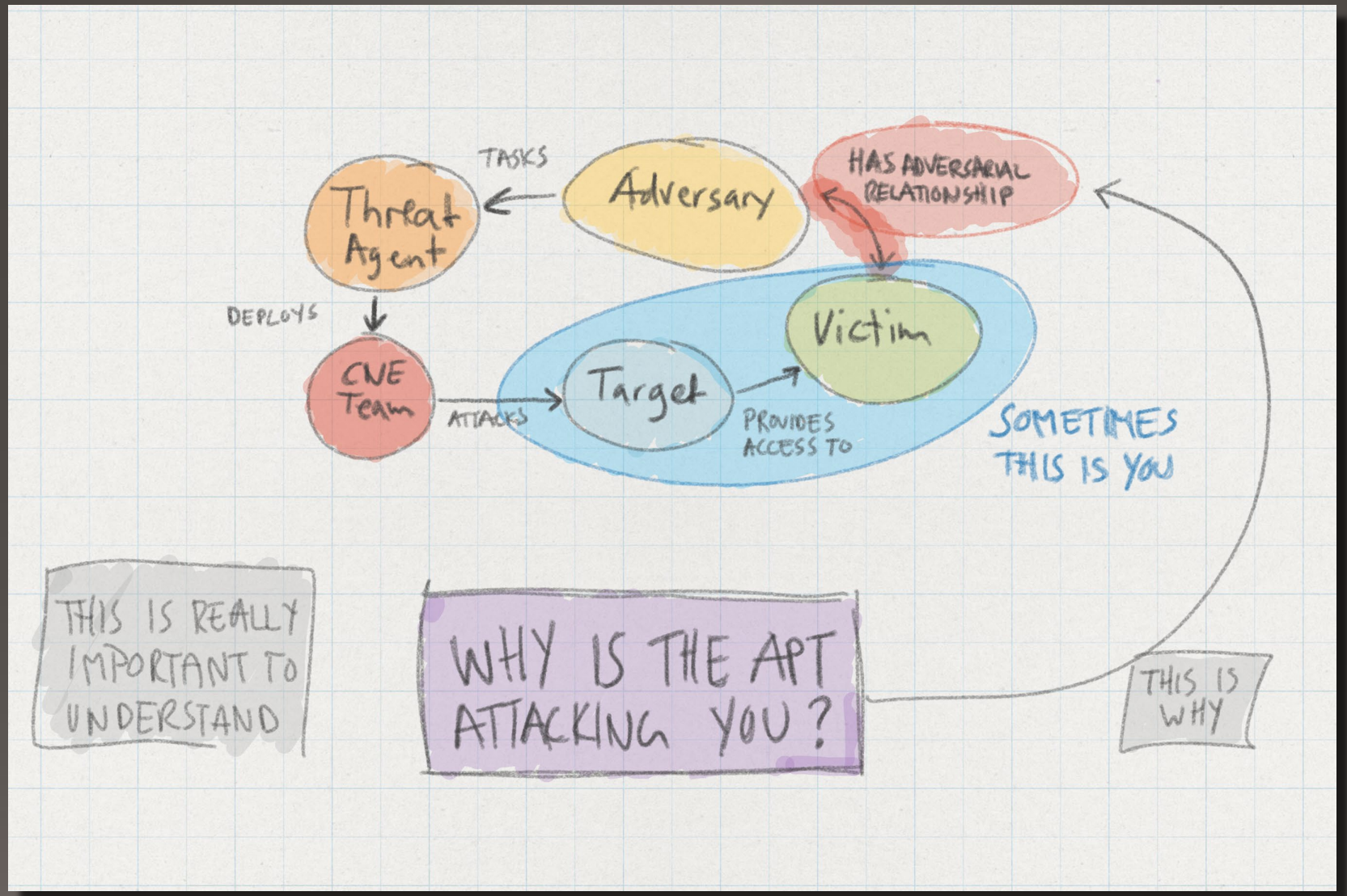
Why you are targeted

by an APT attack team

Adversarial Relationship:
For you to ever be targeted by an APT attack team you must be relevant for some kind of adversarial relationship.

Provide Access:
And you must provide access to something that will help the offensive party gain an advantage in that relationship.

Collection:
What you are observing though is only the collection part of a much bigger process.



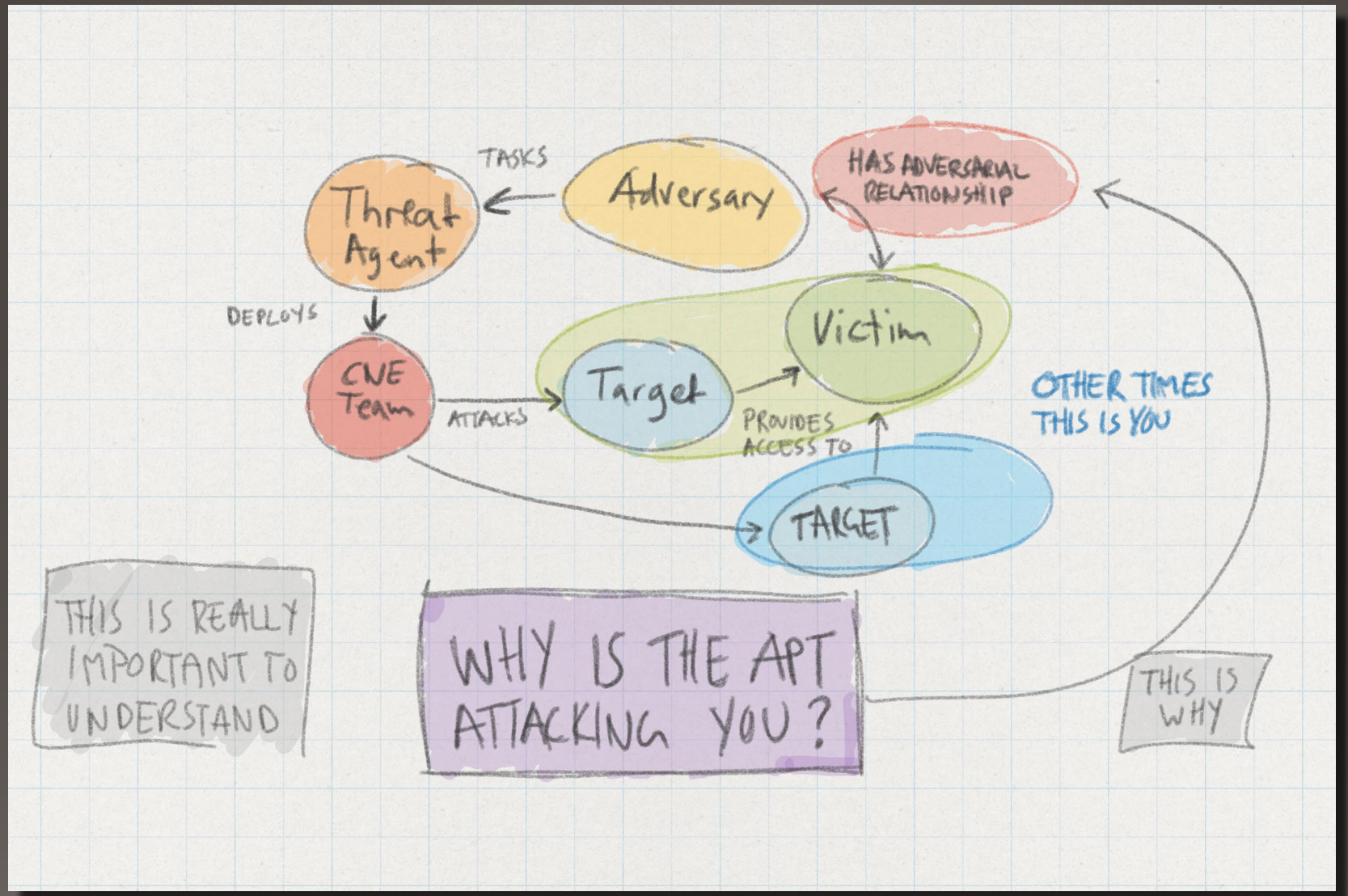
Why you are targeted

by an APT attack team

Adversarial Relationship:
For you to ever be targeted by an APT attack team you must be relevant for some kind of adversarial relationship.

Provide Access:
And you must provide access to something that will help the offensive party gain an advantage in that relationship.

Collection:
What you are observing though is only the collection part of a much bigger process.



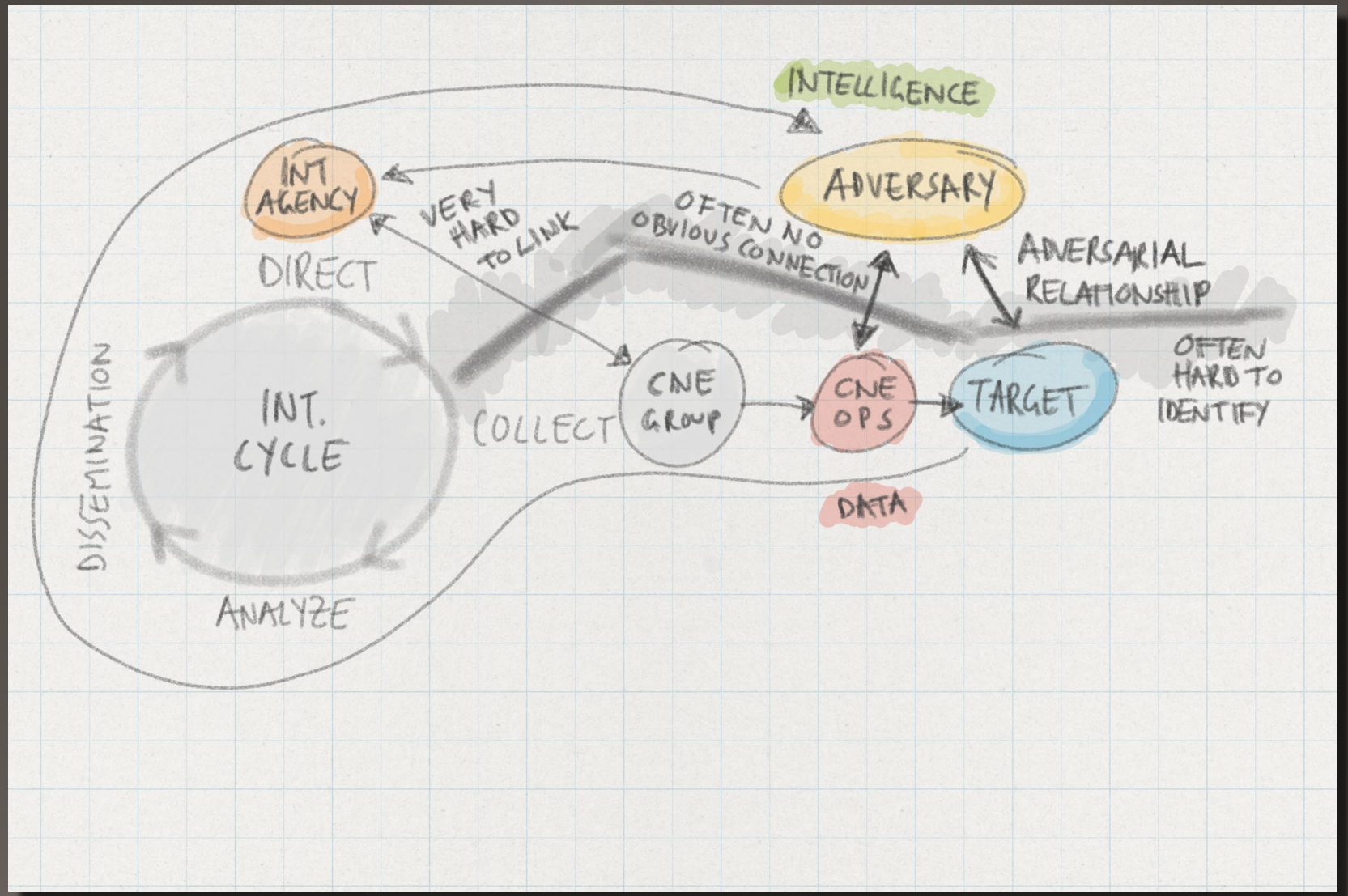
Why you are targeted

by an APT attack team

Adversarial Relationship:
For you to ever be targeted by an APT attack team you must be relevant for some kind of adversarial relationship.

Provide Access:
And you must provide access to something that will help the offensive party gain an advantage in that relationship.

Collection:
What you are observing though is only the collection part of a much bigger process.



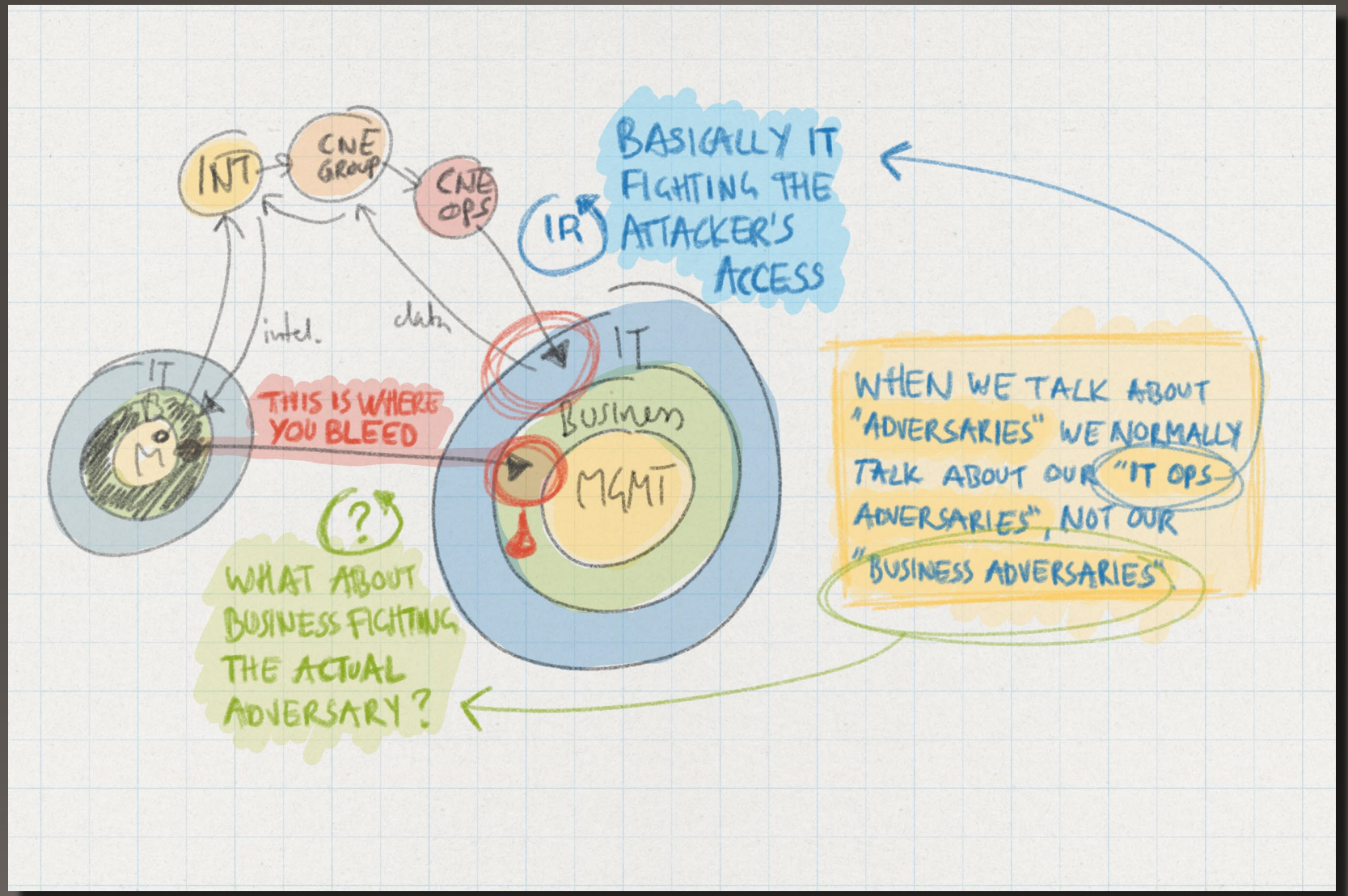
Why you are targeted

by an APT attack team

Adversarial Relationship:
For you to ever be targeted by an APT attack team you must be relevant for some kind of adversarial relationship.

Providing Access:
And you must provide access to something that will help the offensive party gain an advantage in that relationship.

Observing Collection:
What you are observing though is only the collection part of a much bigger process.



The IR and eviction process should not really be about

evicting the attackers

but rather

keeping them out

and preventing them from effortlessly re-entering

It also shouldn't be about

cleaning networks

but rather

mitigating risk

as effectively as possible

And sometimes this actually means leaving your

network compromised

while covertly containing the

most important risks

by using what you learn from the attackers

So how do we

make that decision?

By structured analytical thinking using

analytical models

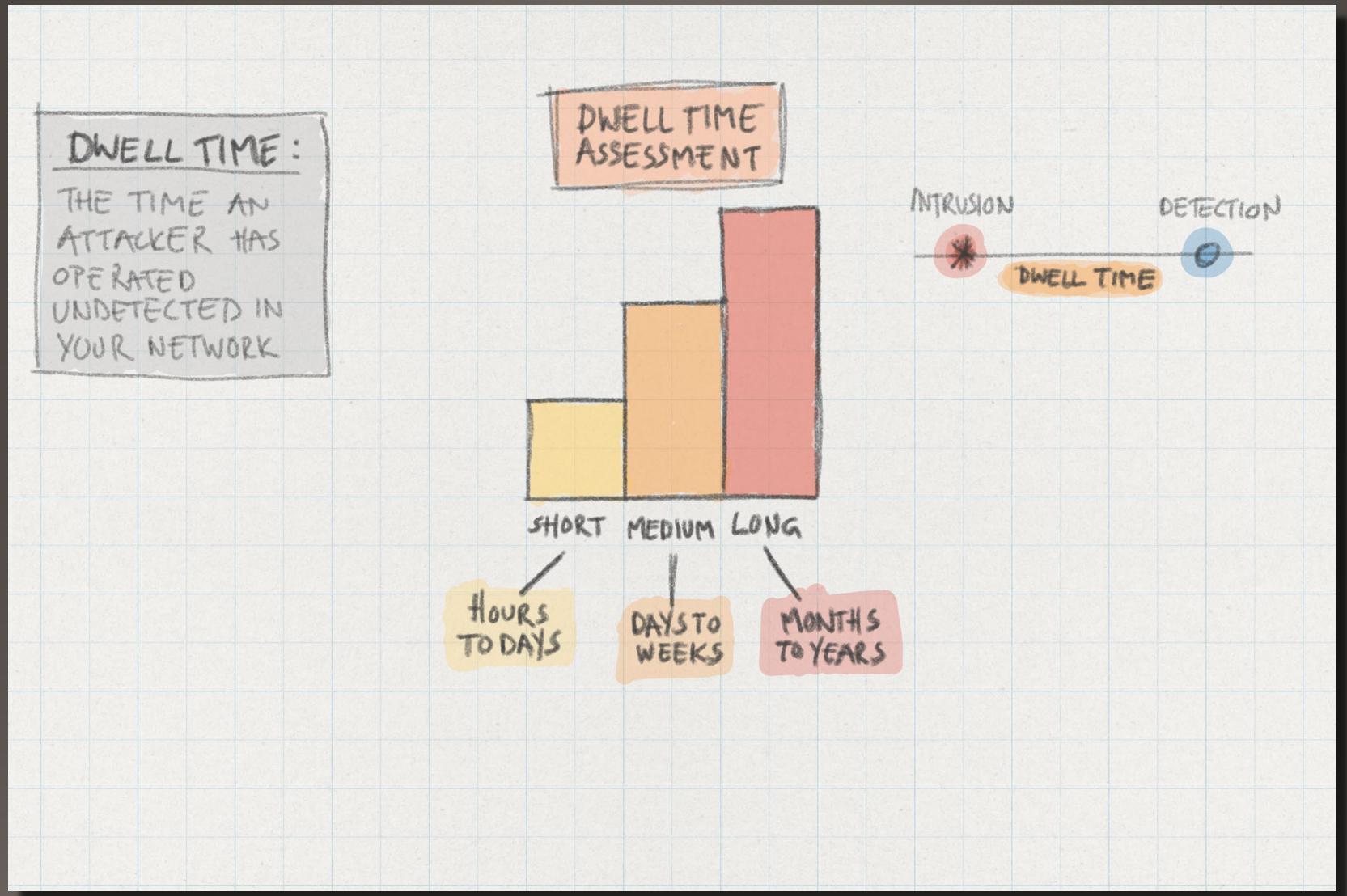
Dwell Time

The time an attacker has stayed undetected in your network.

Short:
Hours to day. Good changes of catching up with the attacker.

Medium:
Days to weeks. You may catch up if you have a capable and enabled team.

Long:
Months to years. Depending on the attacker your chances are in all fairness pretty slim without a full purge or migration.



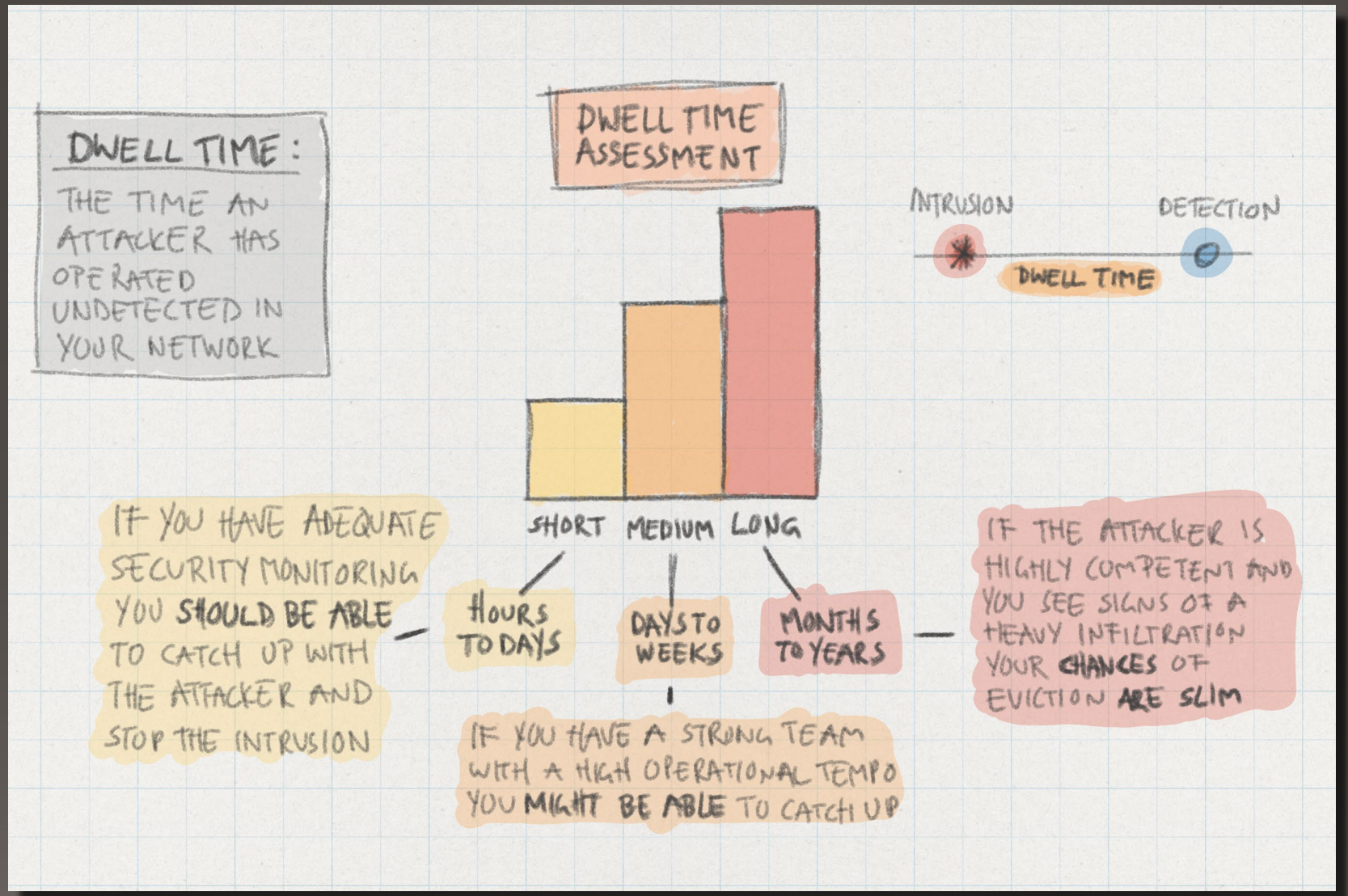
Dwell Time

The time an attacker has stayed undetected in your network.

Short:
Hours to day. Good changes of catching up with the attacker.

Medium:
Days to weeks. You may catch up if you have a capable and enabled team.

Long:
Months to years. Depending on the attacker your chances are in all fairness pretty slim without a full purge or migration.



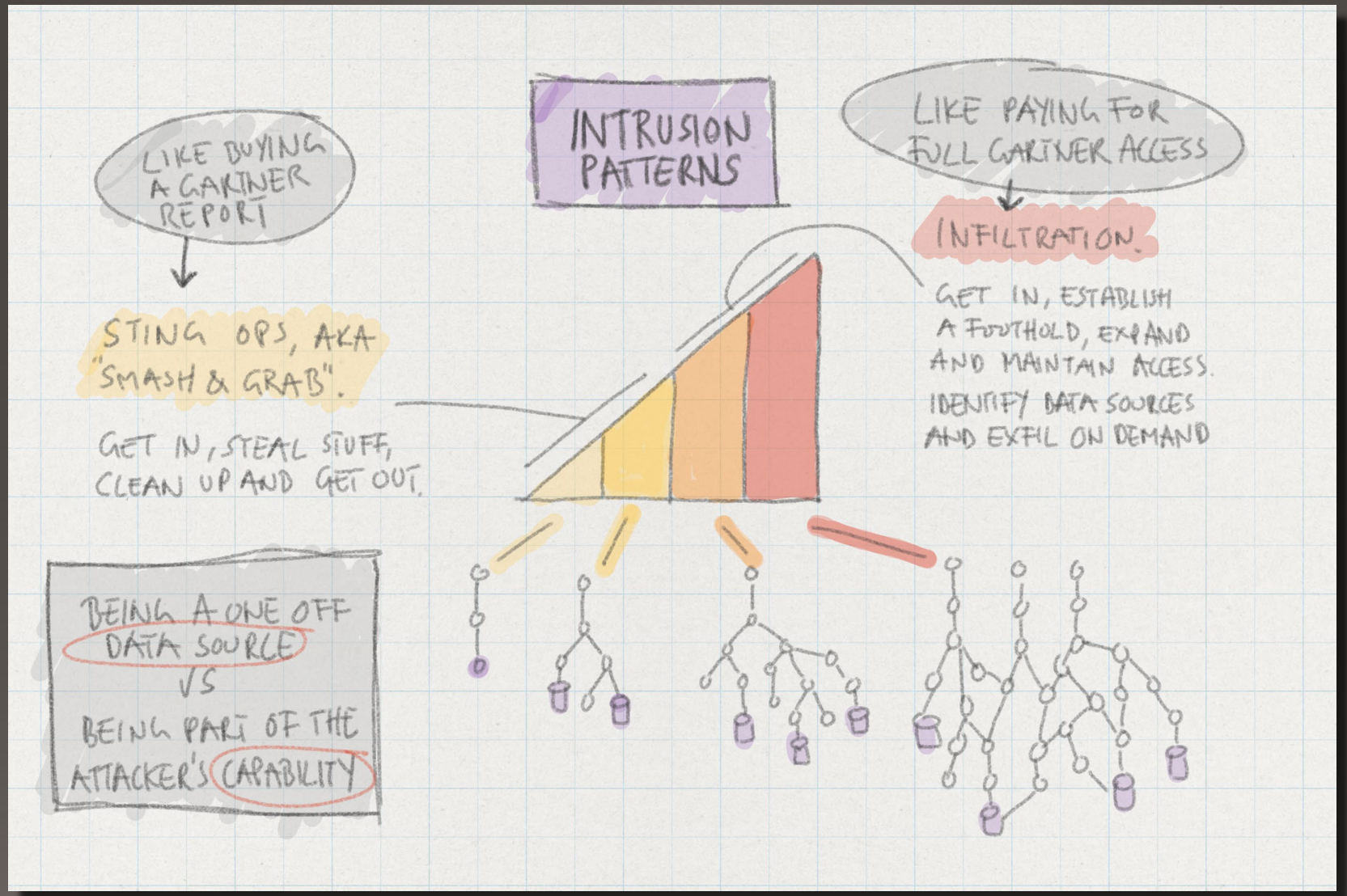
Intrusion Patterns

of APT threats

Sting Operation:
Also called "smash and grab". A direct attack to get a specific piece of information.

Persistent Infiltration:
A long running campaign against you, where your adversary will gain and sustain unauthorized access to your infrastructure for a long period of time.

Response:
When responding, you should take into consideration what kind of pattern you are seeing.



The Threat Type Matrix

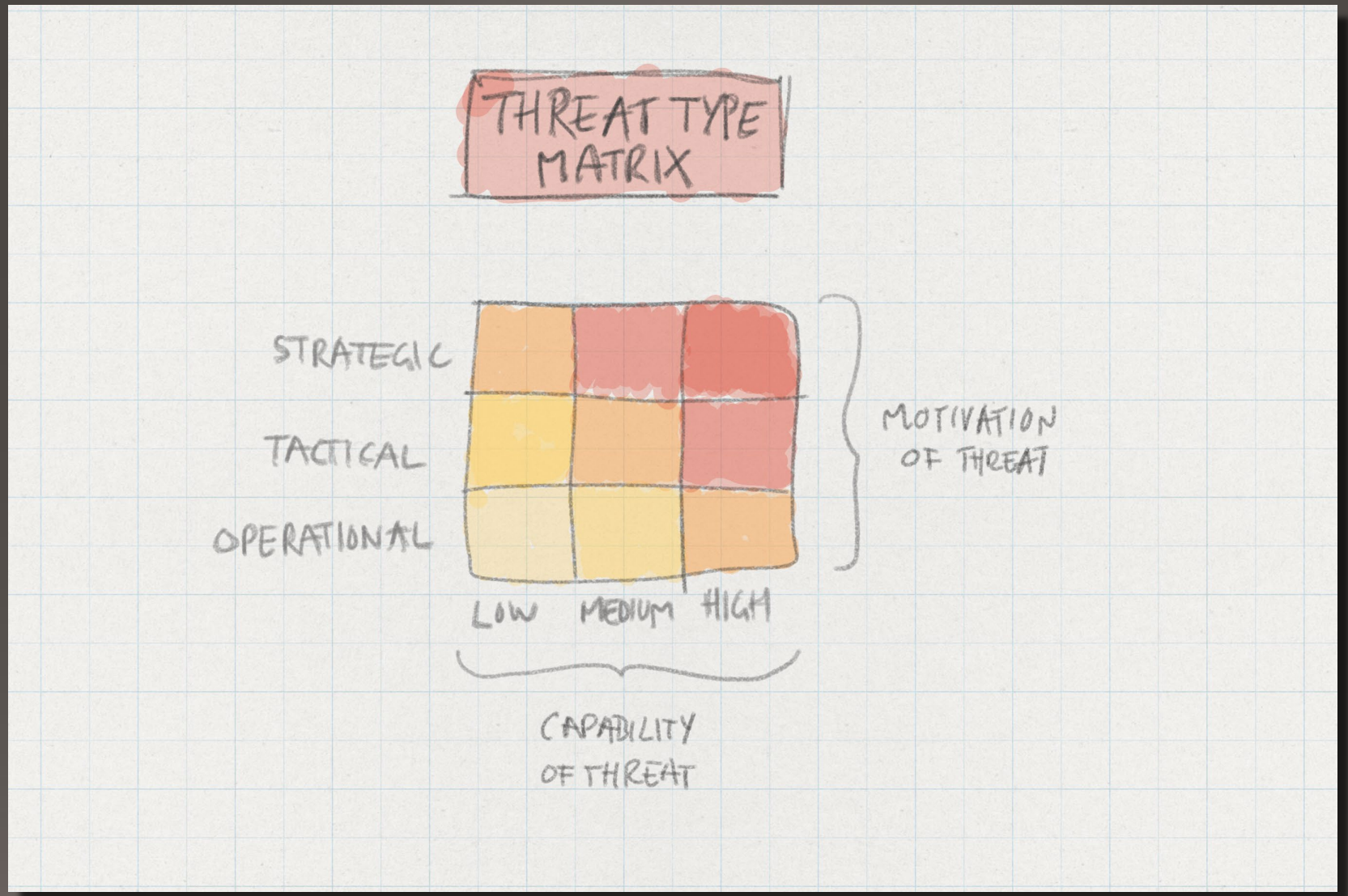
Threat Type:
Strategic | Tactical | Operational

Capability:
Low | Medium | High

Strategic:
You are a high priority and long term target for your adversary

Tactical:
You are a short/medium term target for a specific reason

Operational:
You are a target because the attacker wants infrastructure



The Threat Type Matrix

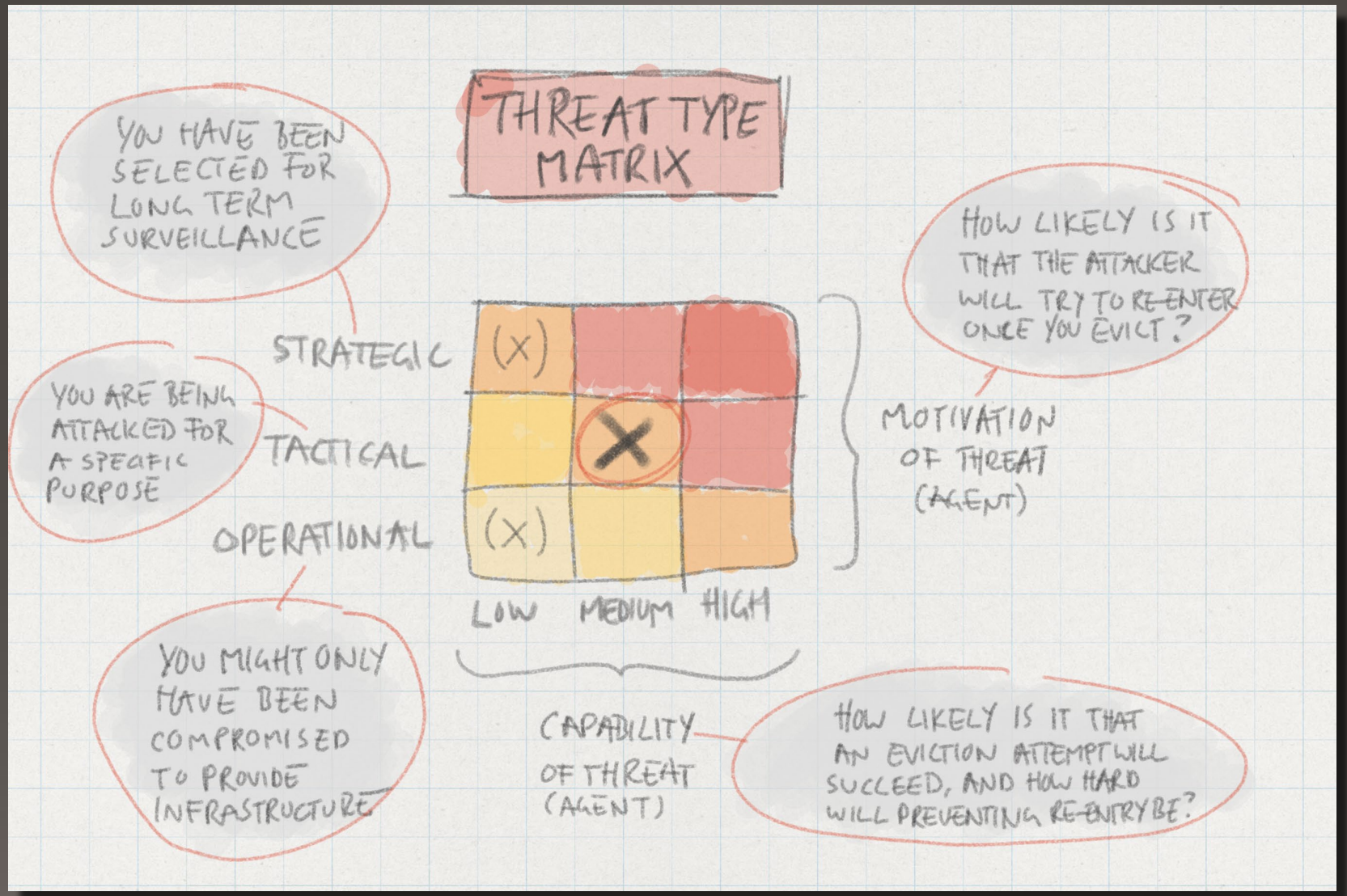
Threat Type:
Strategic | Tactical | Operational

Capability:
Low | Medium | High

Strategic:
You are a high priority and long term target for your adversary

Tactical:
You are a short/medium term target for a specific reason

Operational:
You are a target because the attacker wants infrastructure



The Threat Type Matrix

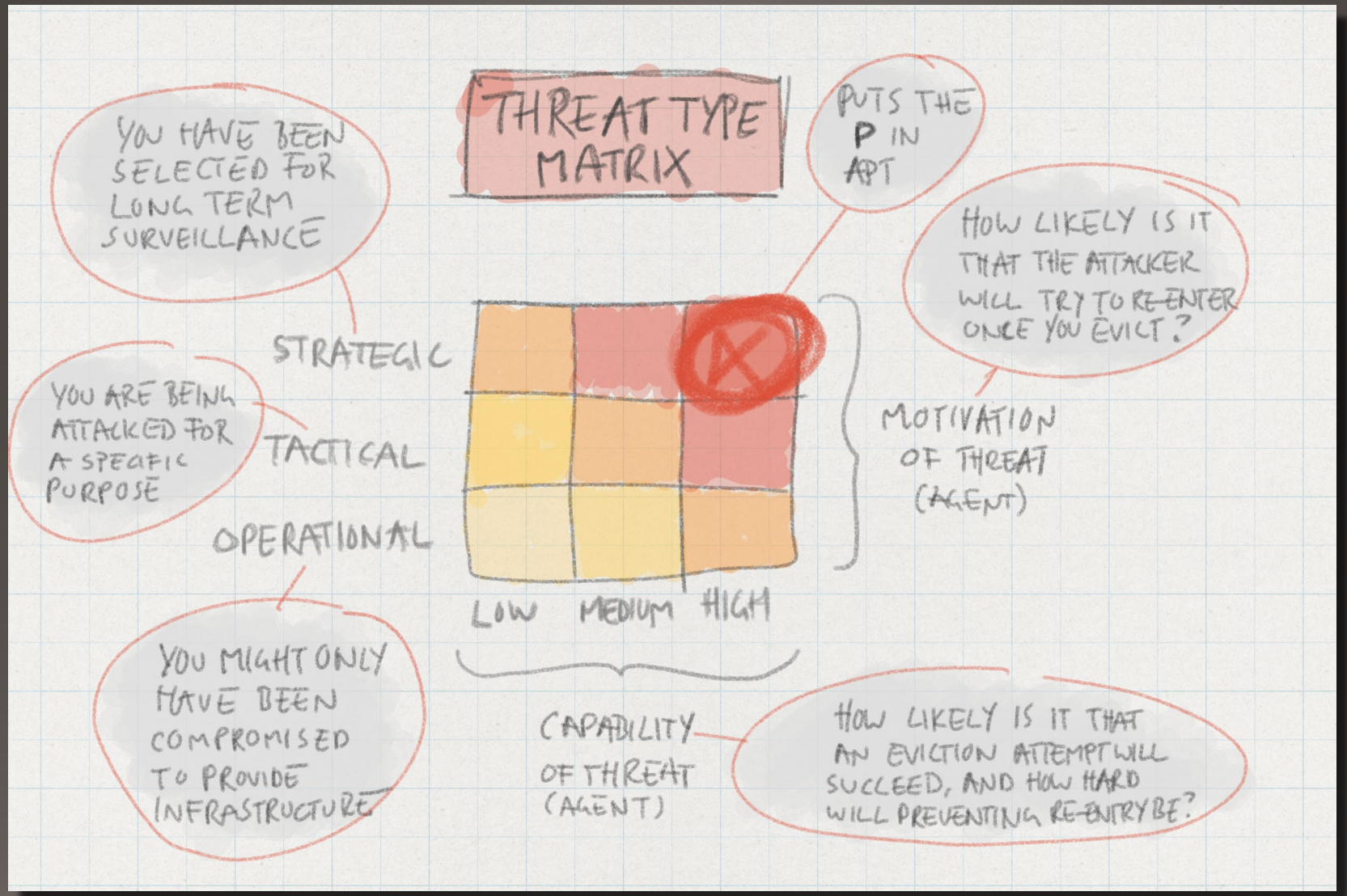
Threat Type:
Strategic | Tactical | Operational

Capability:
Low | Medium | High

Strategic:
You are a high priority and long term target for your adversary

Tactical:
You are a short/medium term target for a specific reason

Operational:
You are a target because the attacker wants infrastructure



The Risk Type Matrix

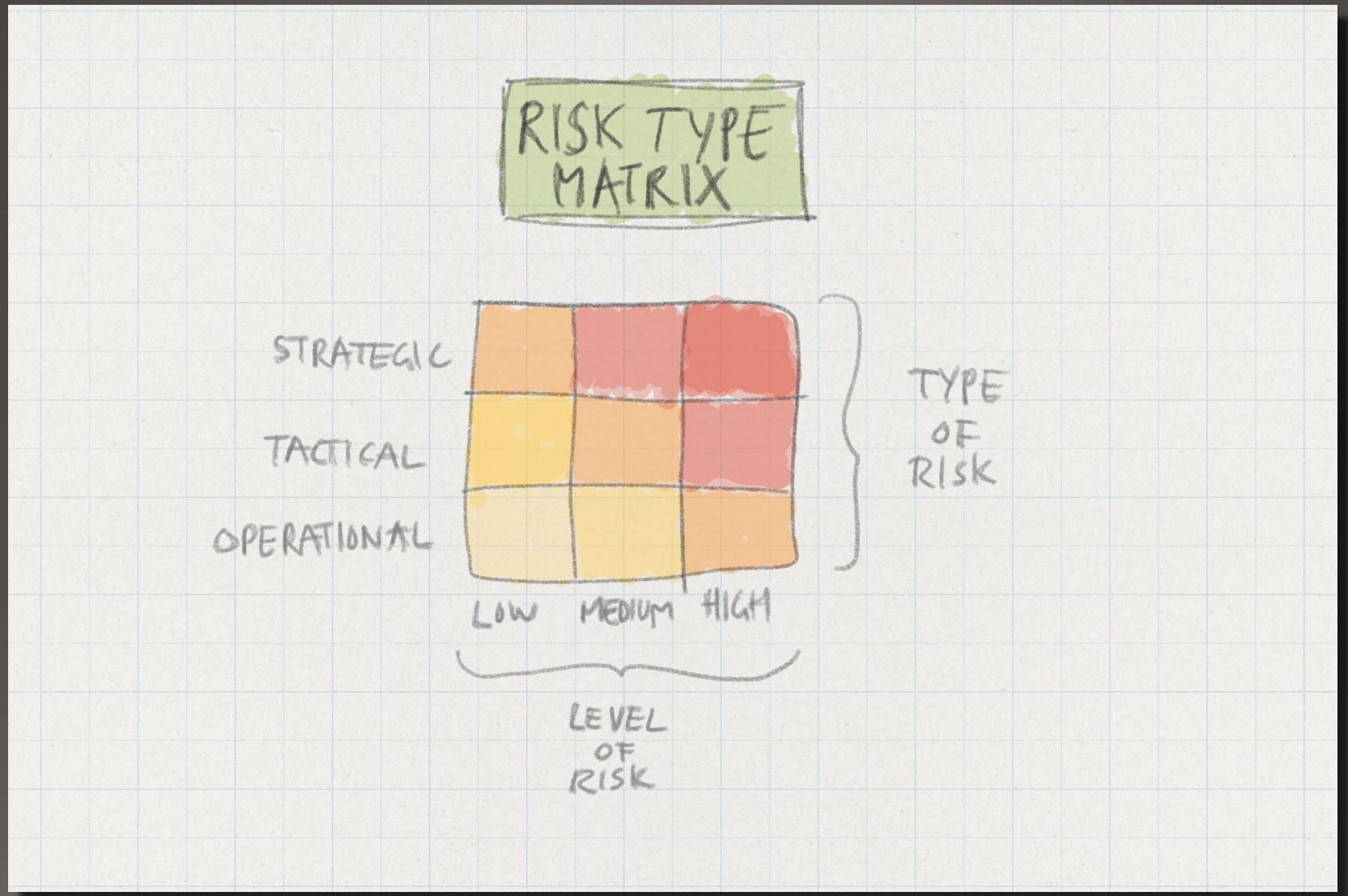
Risk Type:
Strategic | Tactical | Operational

Impact:
Low | Medium | High

Strategic:
Affects your org's long term strategic goals

Tactical:
Affects your org's current and near future execution

Operational:
Affects your org's (IT) operation



The Risk Type Matrix

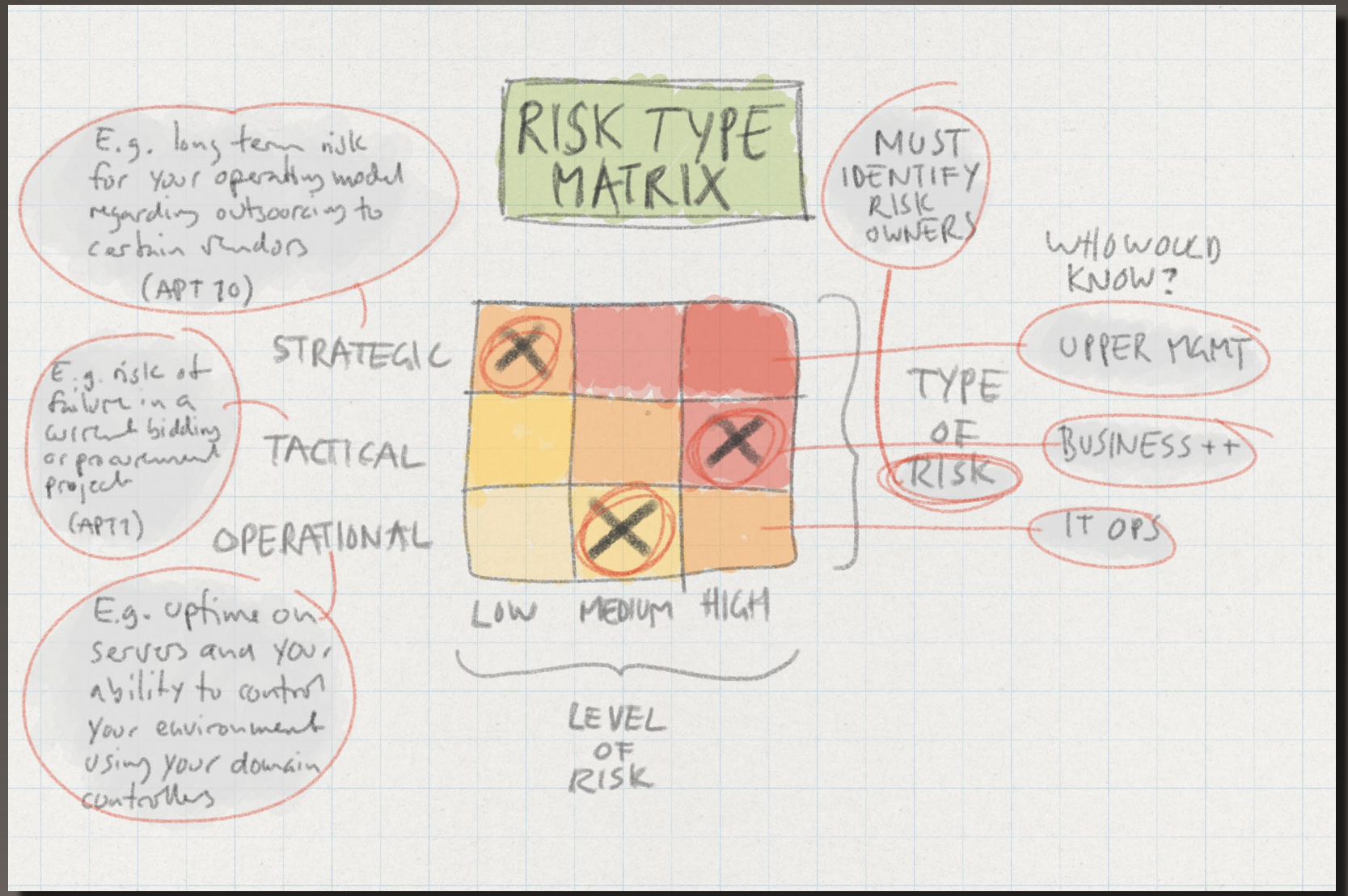
Risk Type:
Strategic | Tactical | Operational

Impact:
Low | Medium | High

Strategic:
Affects your org's long term strategic goals

Tactical:
Affects your org's current and near future execution

Operational:
Affects your org's (IT) operation



The Risk Type Matrix

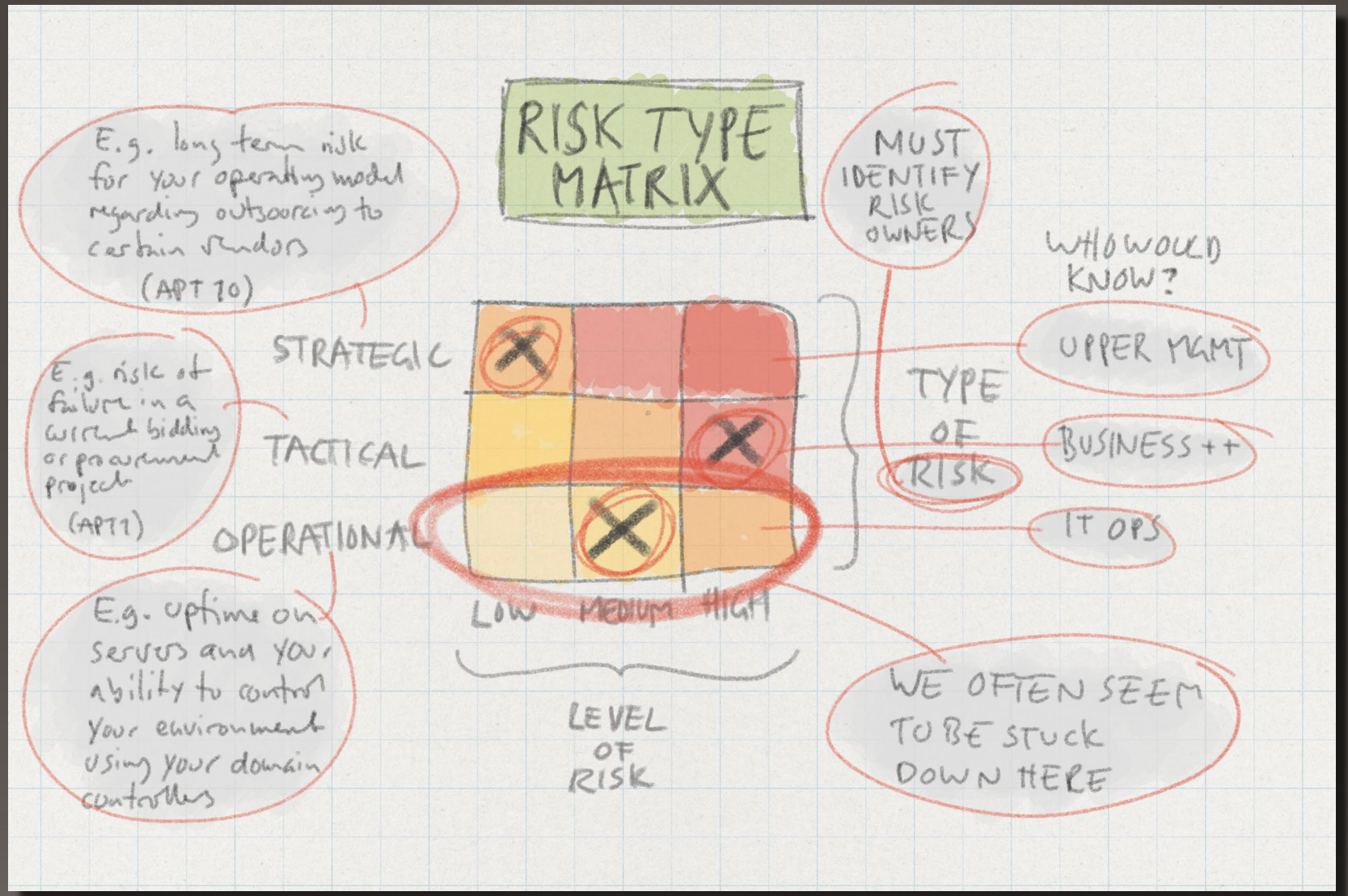
Risk Type:
Strategic | Tactical | Operational

Impact:
Low | Medium | High

Strategic:
Affects your org's long term strategic goals

Tactical:
Affects your org's current and near future execution

Operational:
Affects your org's (IT) operation



The Cyber Threat Intelligence Matrix

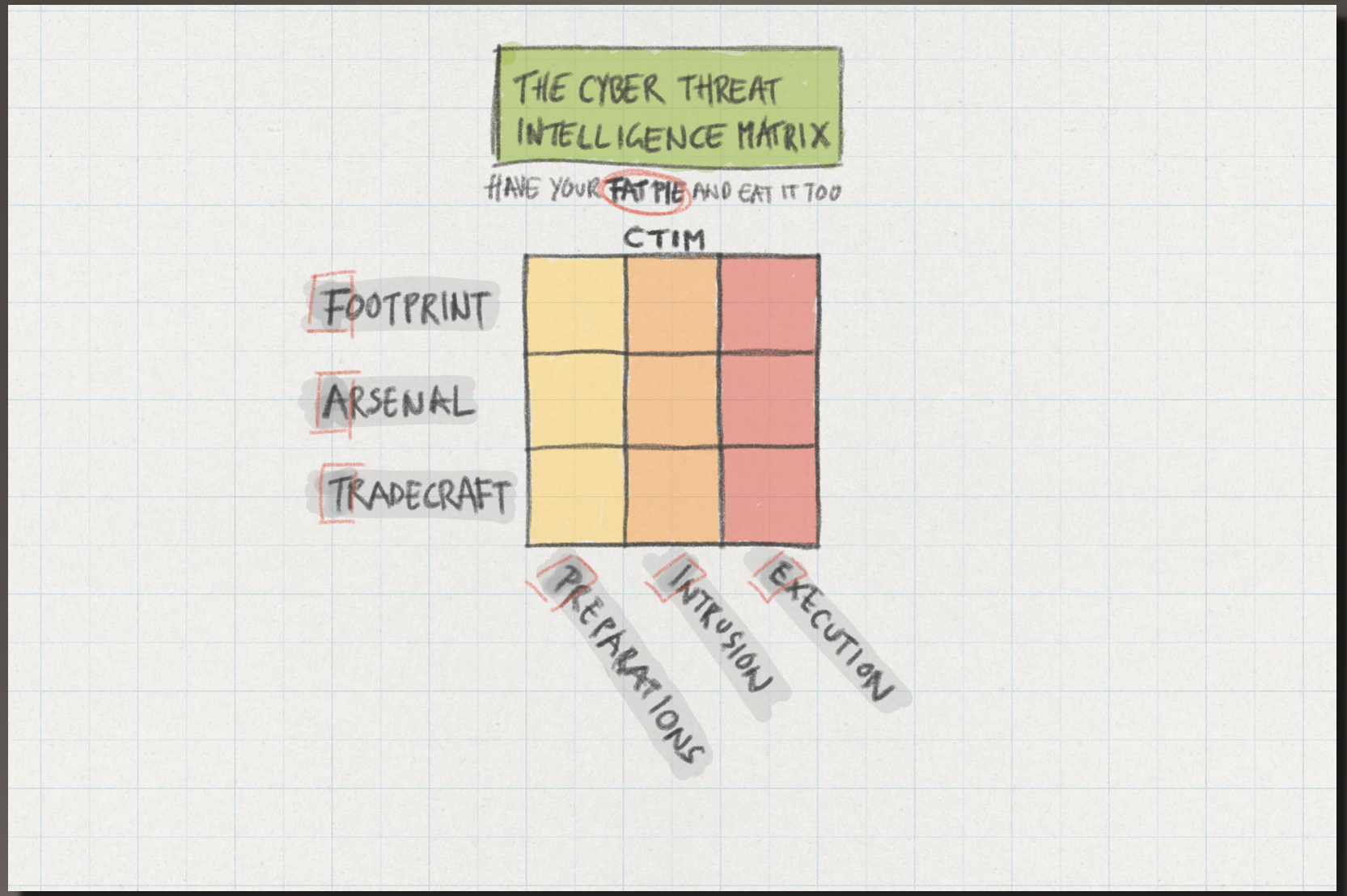
Mapping your knowledge gaps.

Depth of knowledge:
Footprint | Arsenal | Tradecraft

Stages of attack:
Prep. | Intrusion | Execution

Presentation:
https://www.slideshare.net/FrodeHommedal/the-cyber-threat-intelligence-matrix

Essay:
https://www.mnemonic.no/security-report/making-your-move



The Cyber Threat Intelligence Matrix

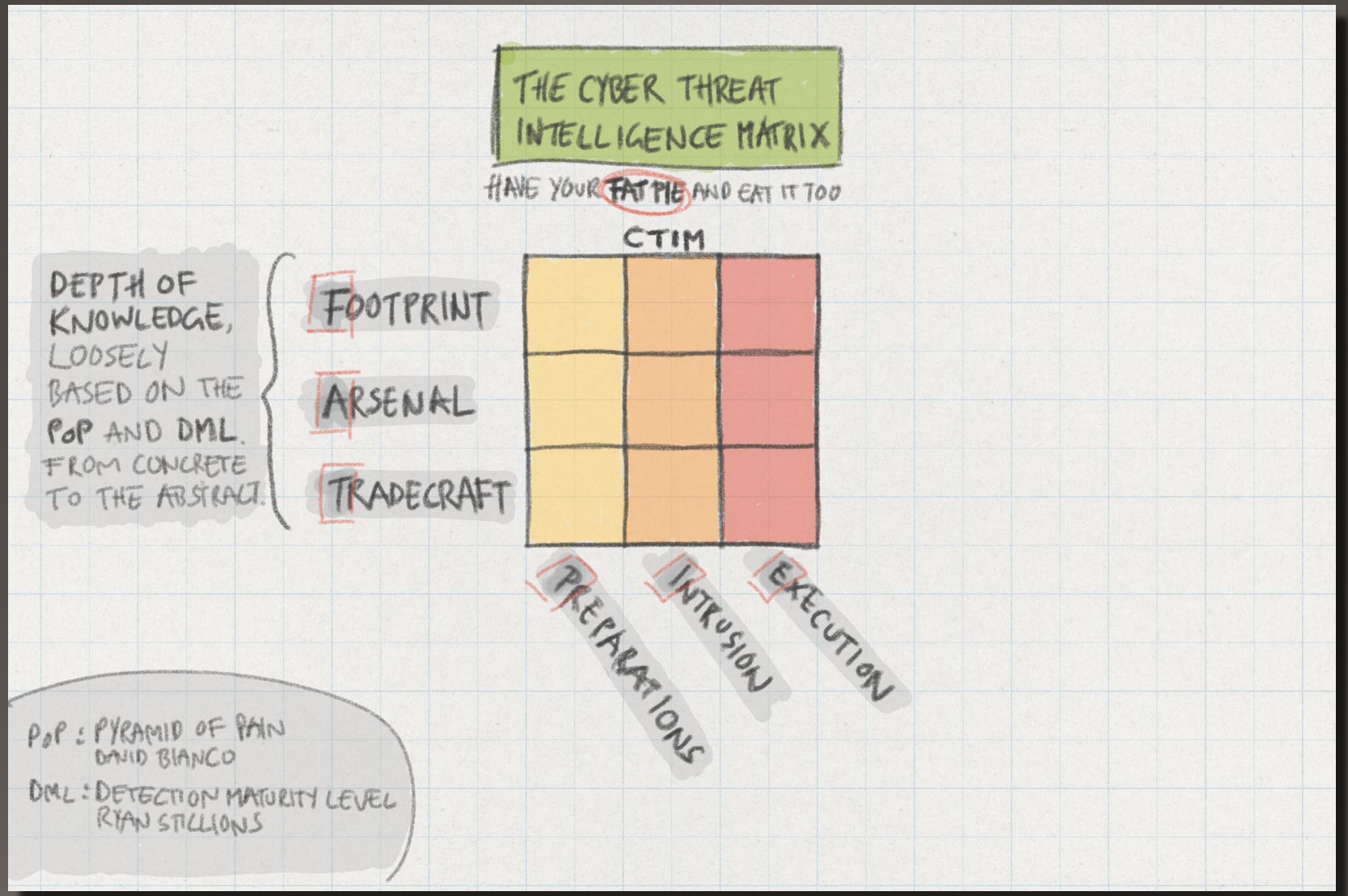
Mapping your knowledge gaps.

Depth of knowledge:
Footprint | Arsenal | Tradecraft

Stages of attack:
Prep. | Intrusion | Execution

Presentation:
https://www.slideshare.net/FrodeHommedal/the-cyber-threat-intelligence-matrix

Essay:
https://www.mnemonic.no/security-report/making-your-move



The Cyber Threat Intelligence Matrix

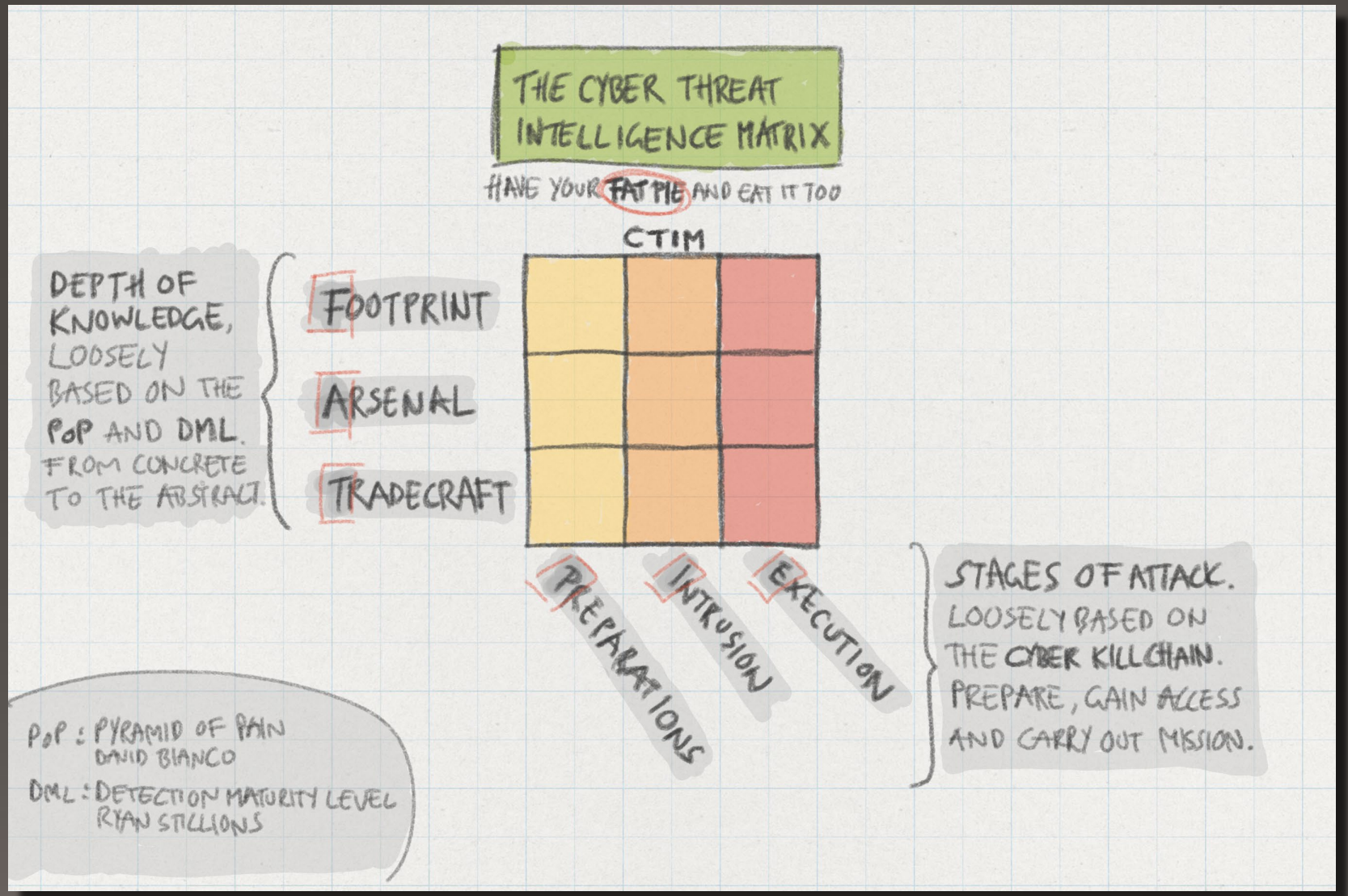
Mapping your knowledge gaps.

Depth of knowledge:
Footprint | Arsenal | Tradecraft

Stages of attack:
Prep. | Intrusion | Execution

Presentation:
https://www.slideshare.net/FrodeHommedal/the-cyber-threat-intelligence-matrix

Essay:
https://www.mnemonic.no/security-report/making-your-move



The Cyber Threat Intelligence Matrix

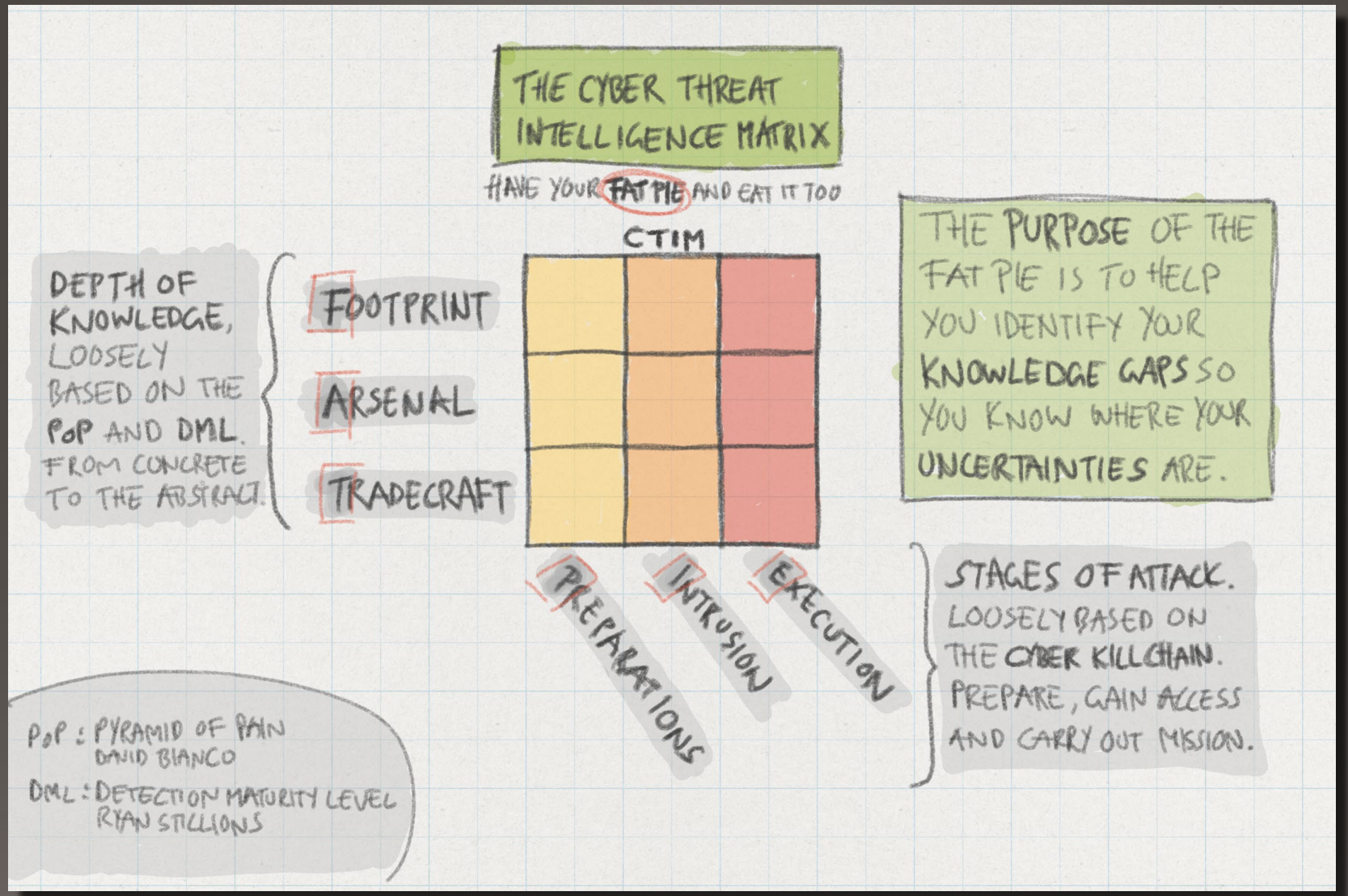
Mapping your knowledge gaps.

Depth of knowledge:
Footprint | Arsenal | Tradecraft

Stages of attack:
Prep. | Intrusion | Execution

Presentation:
https://www.slideshare.net/FrodeHommedal/the-cyber-threat-intelligence-matrix

Essay:
https://www.mnemonic.no/security-report/making-your-move



The Cyber Threat Intelligence Matrix

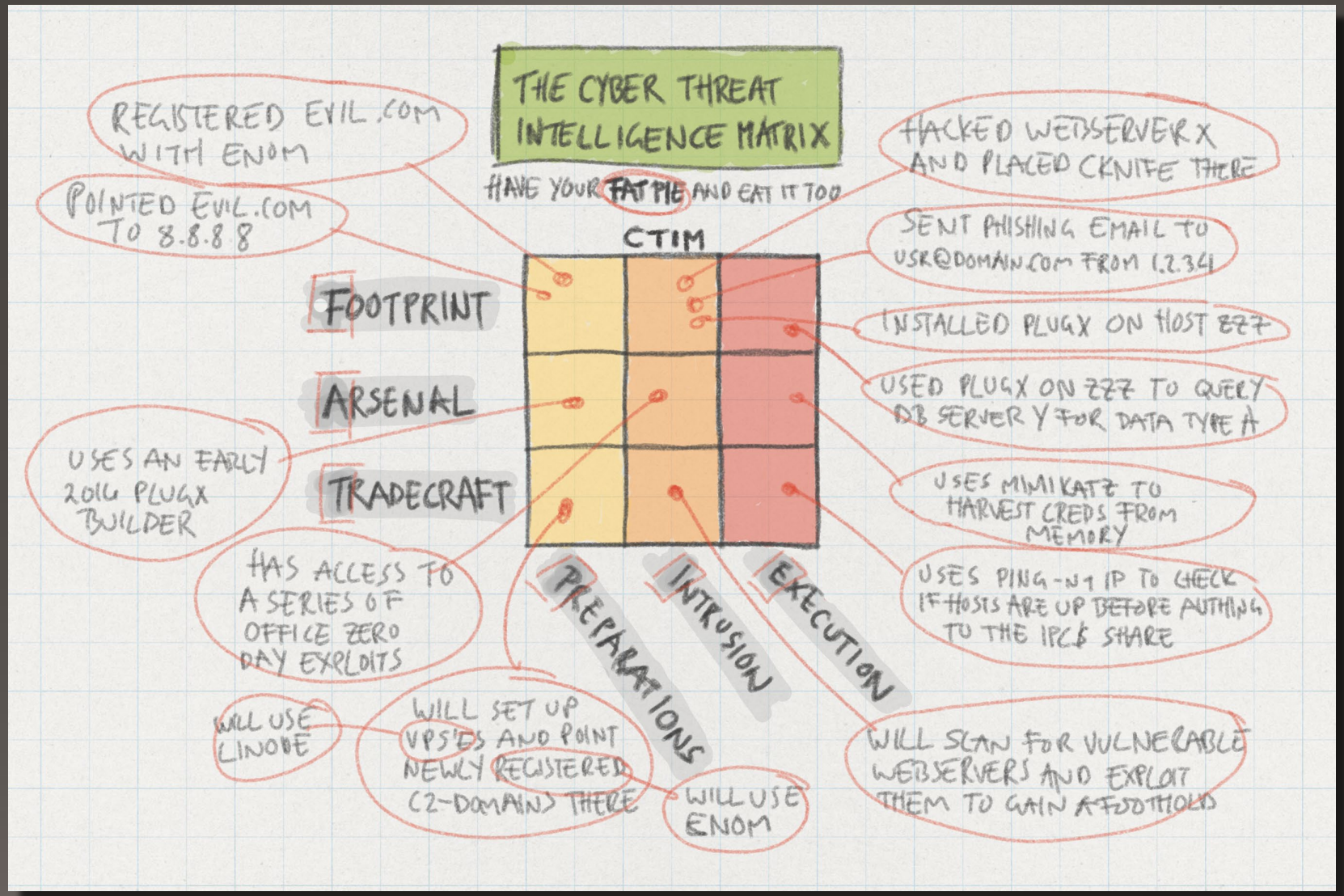
Mapping your knowledge gaps.

Depth of knowledge:
Footprint | Arsenal | Tradecraft

Stages of attack:
Prep. | Intrusion | Execution

Presentation:
https://www.slideshare.net/FrodeHommedal/the-cyber-threat-intelligence-matrix

Essay:
https://www.mnemonic.no/security-report/making-your-move



The Cyber Threat Intelligence Matrix

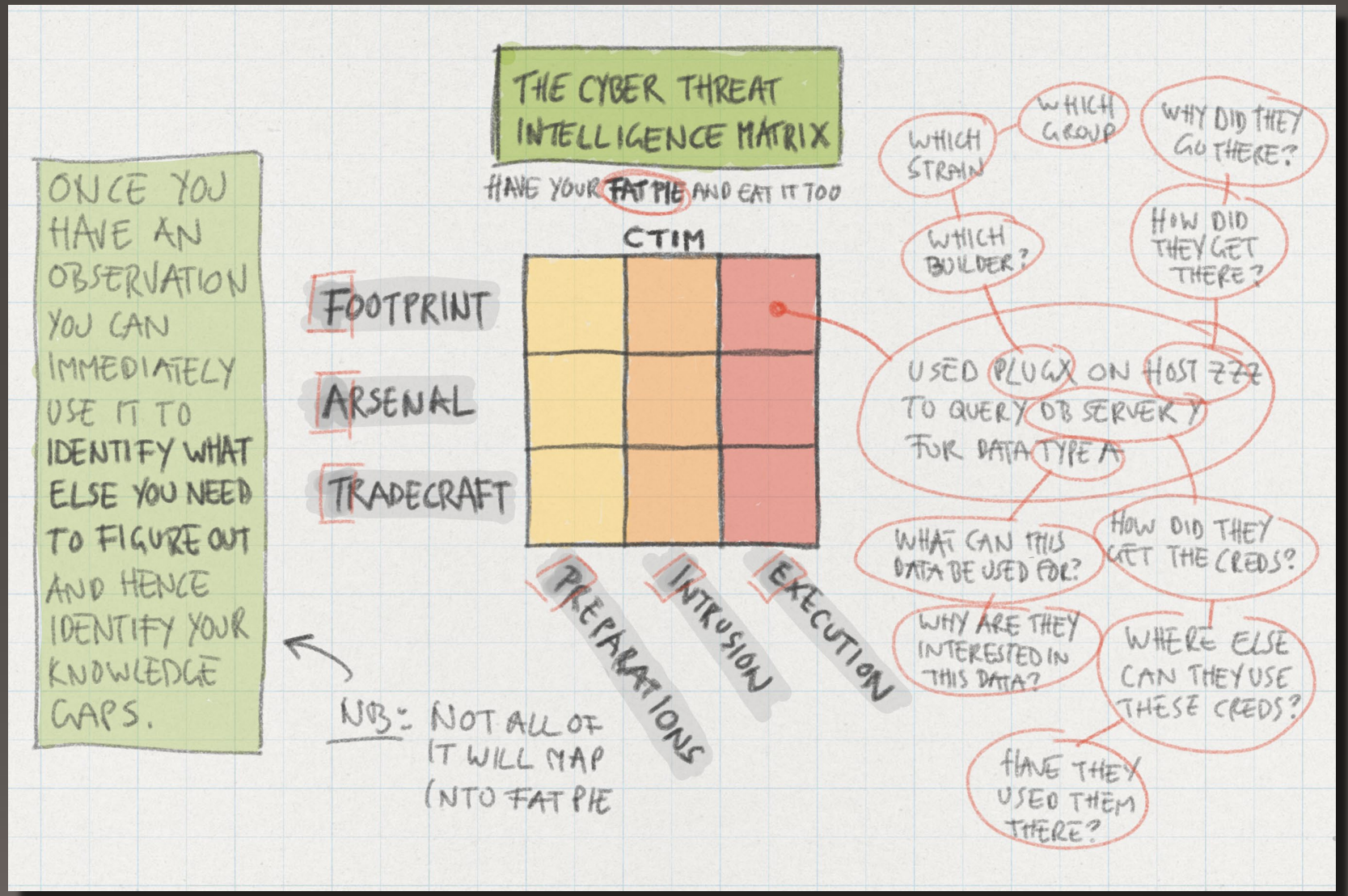
Mapping your knowledge gaps.

Depth of knowledge:
Footprint | Arsenal | Tradecraft

Stages of attack:
Prep. | Intrusion | Execution

Presentation:
https://www.slideshare.net/FrodeHommedal/the-cyber-threat-intelligence-matrix

Essay:
https://www.mnemonic.no/security-report/making-your-move



The Cyber Threat Intelligence Matrix

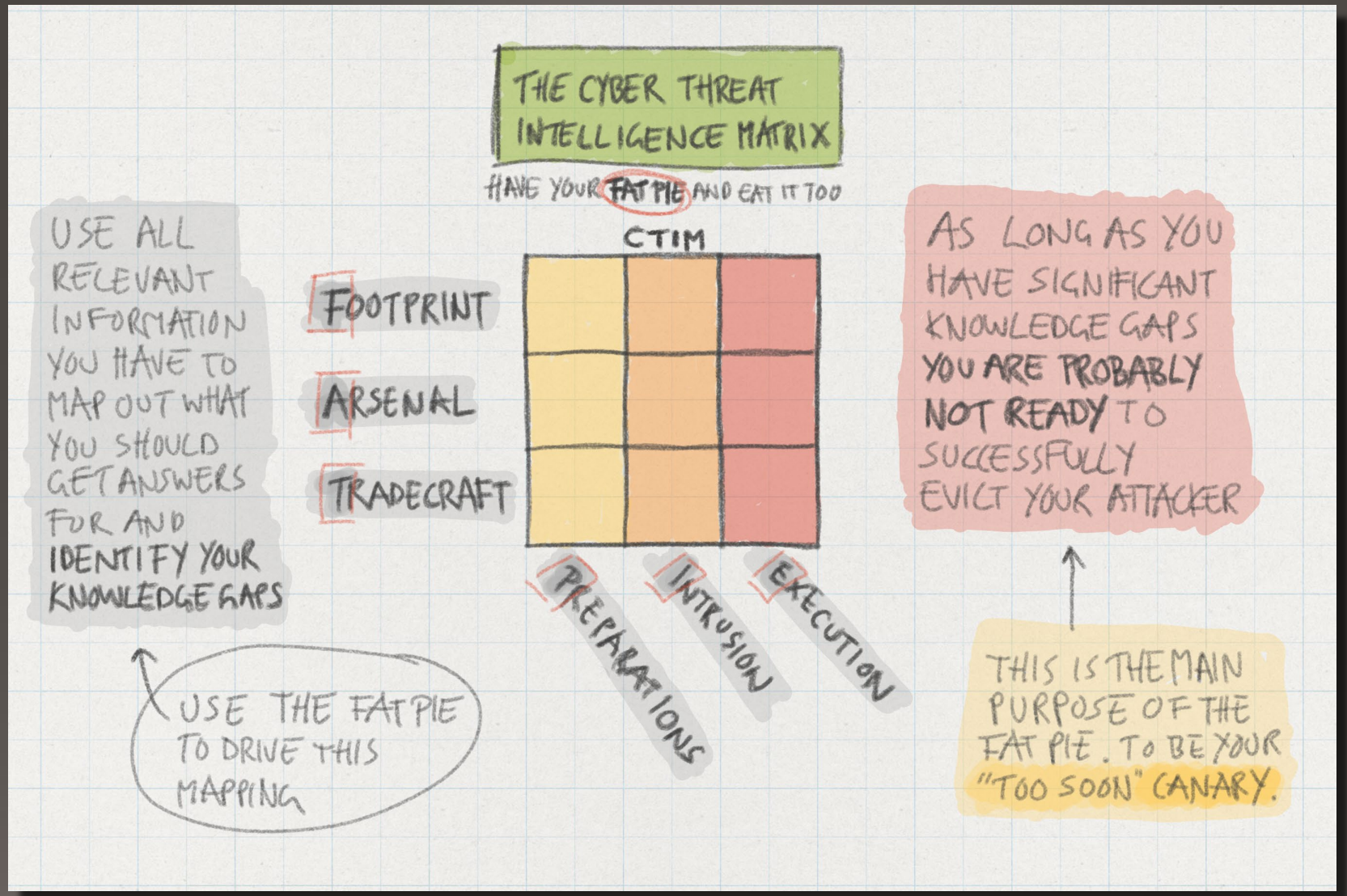
Mapping your knowledge gaps.

Depth of knowledge:
Footprint | Arsenal | Tradecraft

Stages of attack:
Prep. | Intrusion | Execution

Presentation:
https://www.slideshare.net/FrodeHommedal/the-cyber-threat-intelligence-matrix

Essay:
https://www.mnemonic.no/security-report/making-your-move



Threat Metrics

to help you navigate

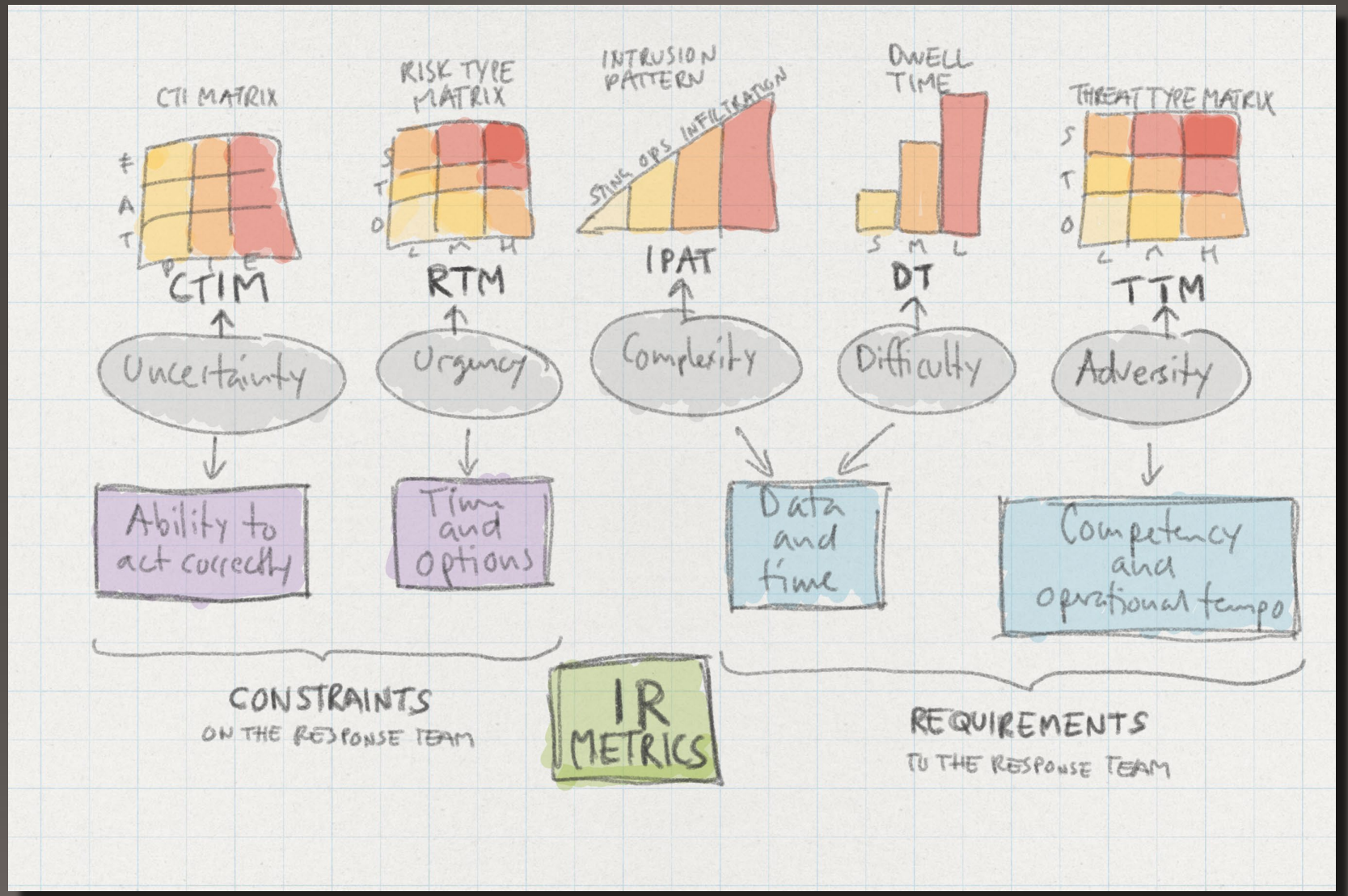
CTI Matric:
Identifying knowledge gaps.

Threat Type Matric:
Identifying type of threat.

Risk Type Matric:
Identifying type of risk.

Intrusion Pattern:
Identifying type of infiltration.

Dwell Time:
Identifying length of infiltration.



With these models in mind we will look at some

response patterns

Response Patterns

for your consideration

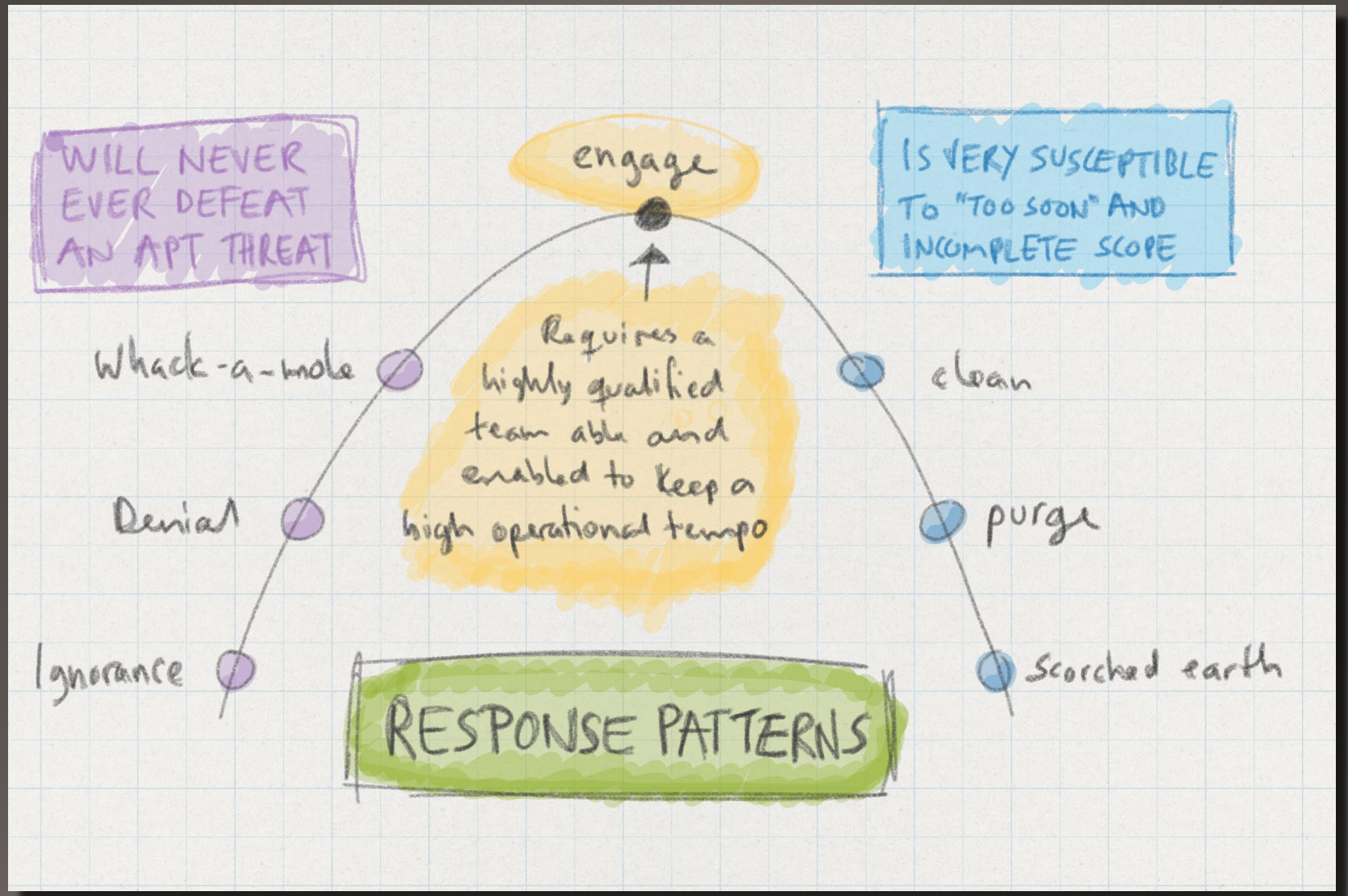
Ignore:
Ignorance or actively ignoring.

Disrupt:
Continuous remediation.

Engage:
A game of chess heavily reliant on intelligence and a high operational tempo.

Clean:
Scope, shut down and clean.

Migrate:
Build new and migrate.



Response Patterns

for your consideration

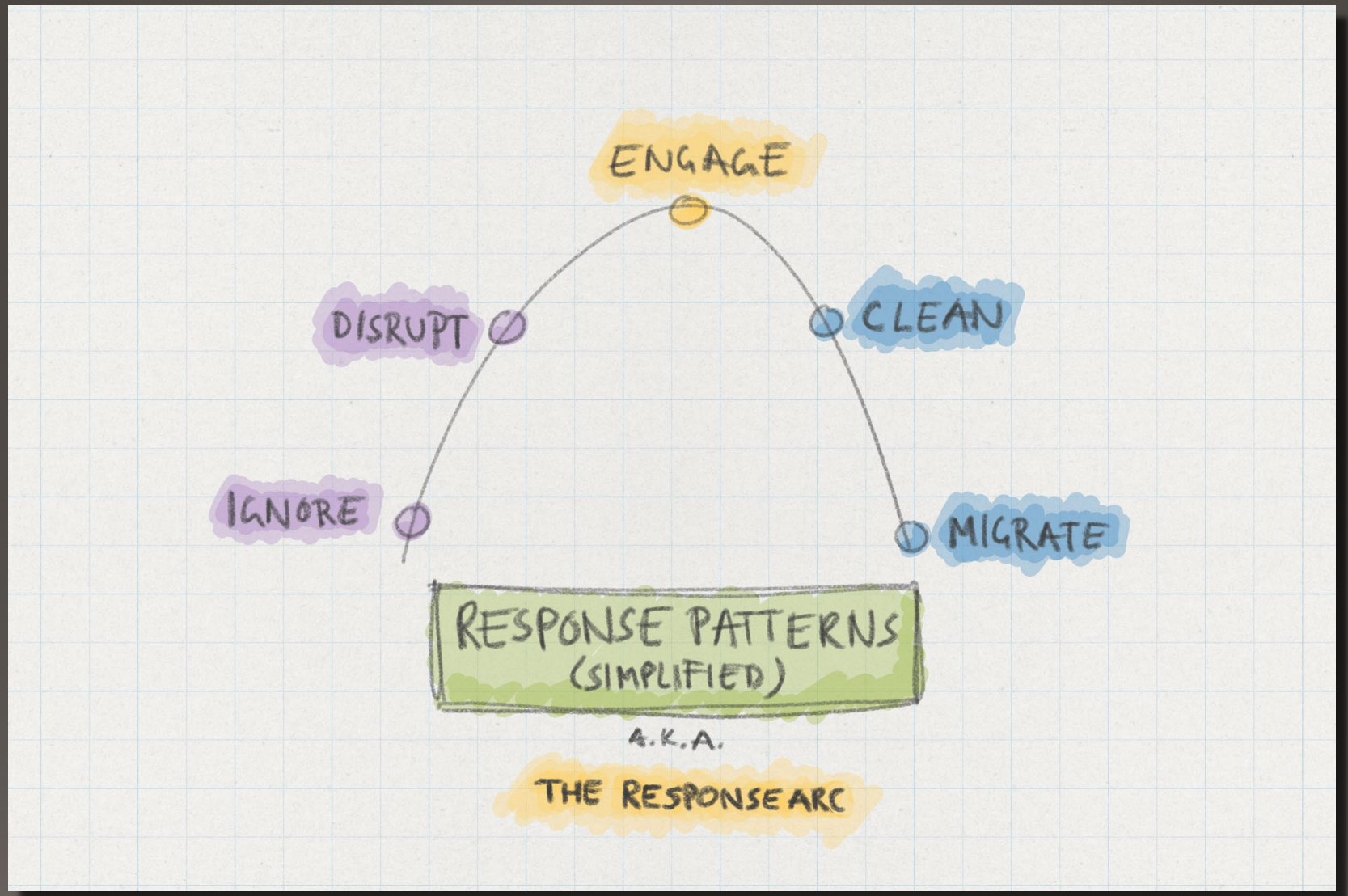
Ignore:
Ignorance or actively ignoring.

Disrupt:
Continuous remediation.

Engage:
A game of chess heavily reliant on intelligence and a high operational tempo.

Clean:
Scope, shut down and clean.

Migrate:
Build new and migrate.



Response Patterns

for your consideration

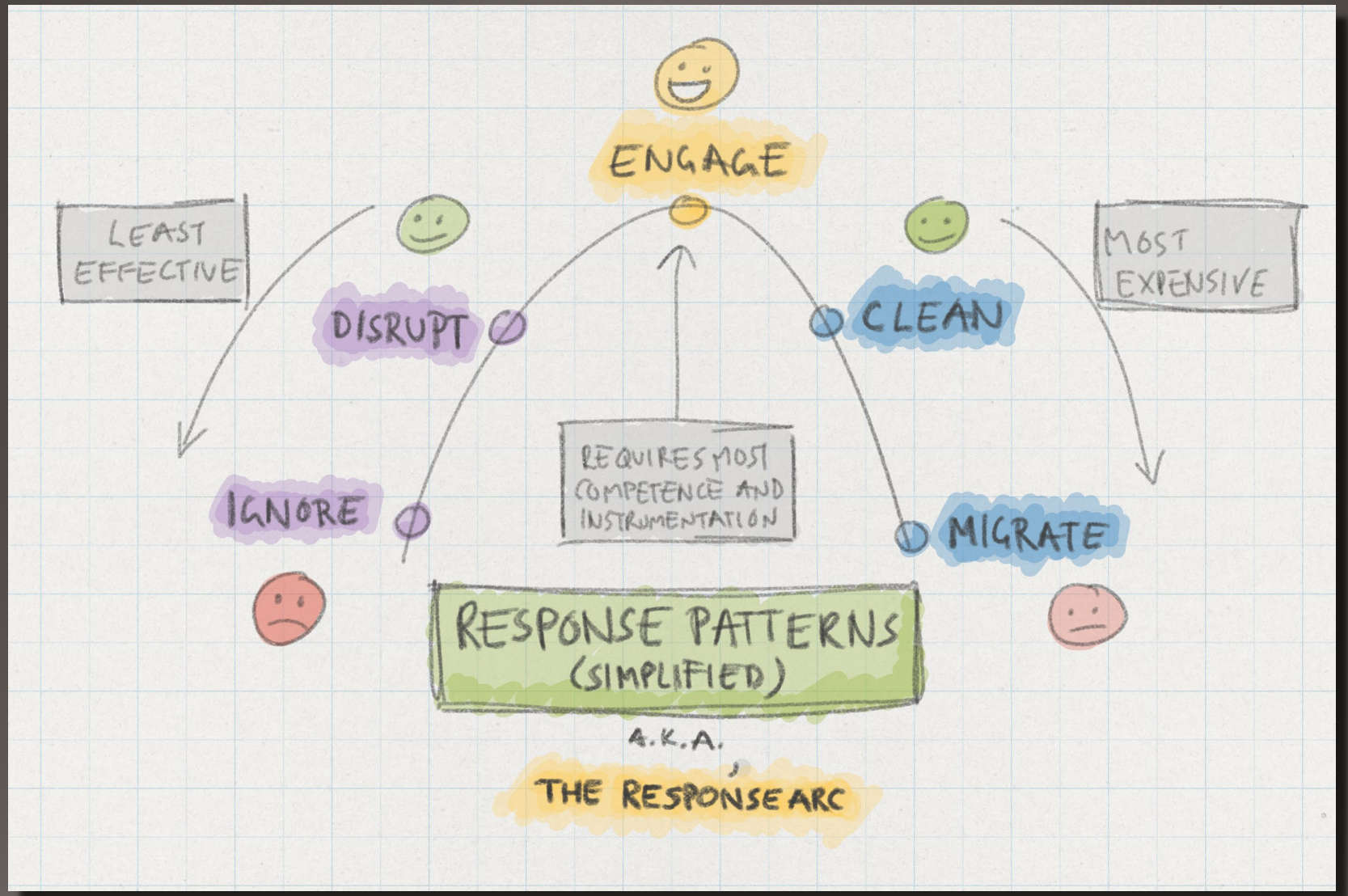
Ignore:
Ignorance or actively ignoring.

Disrupt:
Continuous remediation.

Engage:
A game of chess heavily reliant on intelligence and a high operational tempo.

Clean:
Scope, shut down and clean.

Migrate:
Build new and migrate.



Response Patterns

for your consideration

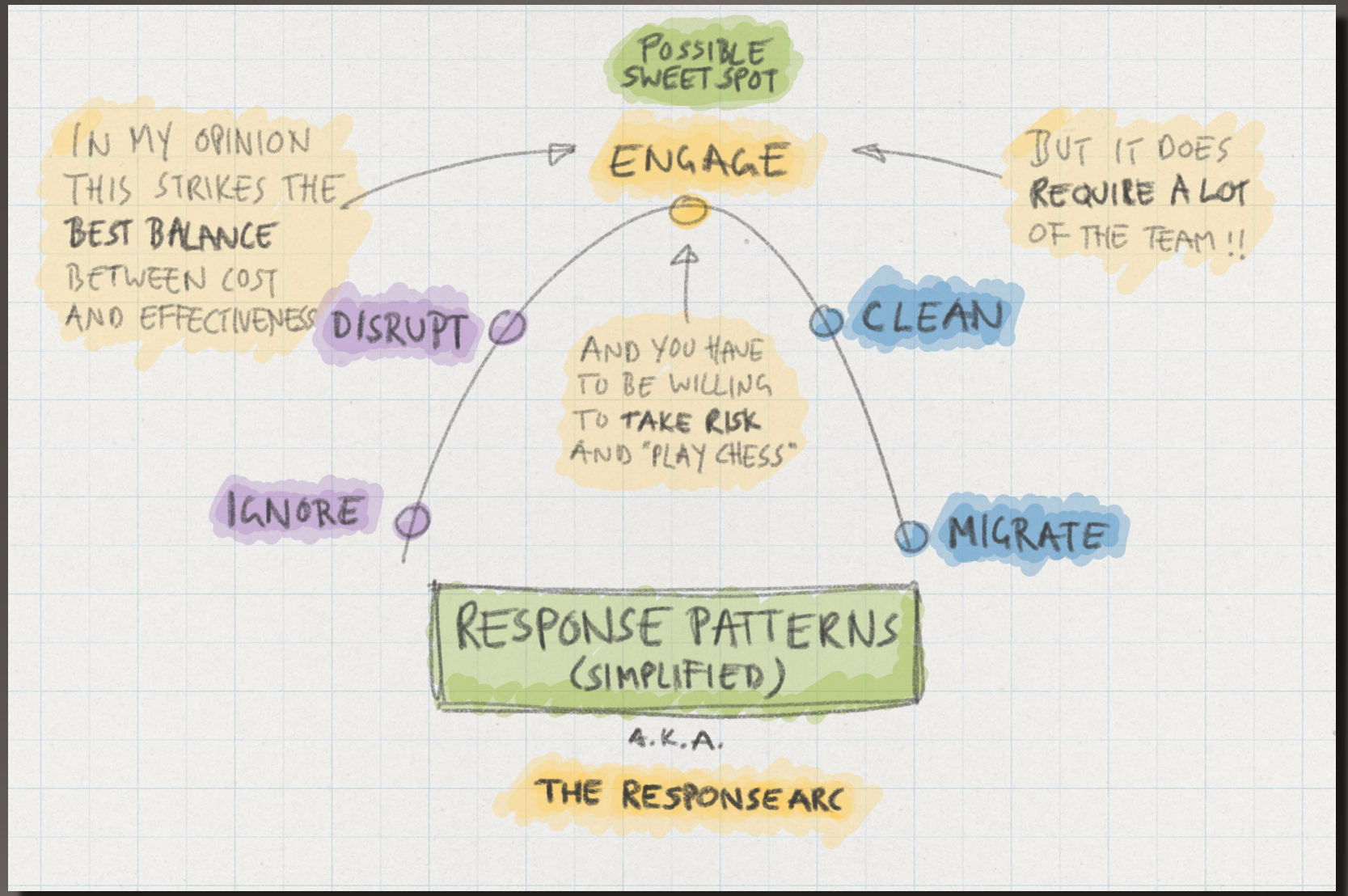
Ignore:
Ignorance or actively ignoring.

Disrupt:
Continuous remediation.

Engage:
A game of chess heavily reliant on intelligence and a high operational tempo.

Clean:
Scope, shut down and clean.

Migrate:
Build new and migrate.



Wrap up

So what truth is

THE RED PILL

of attacker eviction exposing?

A way more

complex and malevolent

incident response reality than most responders are ready to acknowledge

The key takeaway is that if you

understand

your attacker you will be able to

improve

your response significantly

Then you can apply the right

response pattern

to the identified

intrusion pattern

and the identified

threat and risk types

Always outnumbered.

Never outgunned!

@FrodeHommedal
no.linkedin.com/in/hommedal
frodehommedal.no