



**COMBITECH**

# INTRODUCTION TO CYBER THREAT INTELLIGENCE

# WHAT IS CYBER THREAT INTELLIGENCE?



The background is a vibrant, abstract composition. On the left, a dense array of blue and purple fiber optic lines radiates outwards, creating a sense of depth and movement. On the right, a pink and red checkerboard pattern transitions into a soft, out-of-focus bokeh of light circles. The overall color palette is a mix of cool blues and purples on the left, and warm pinks and reds on the right.

# **COMBITECH**

Thanks for listening!

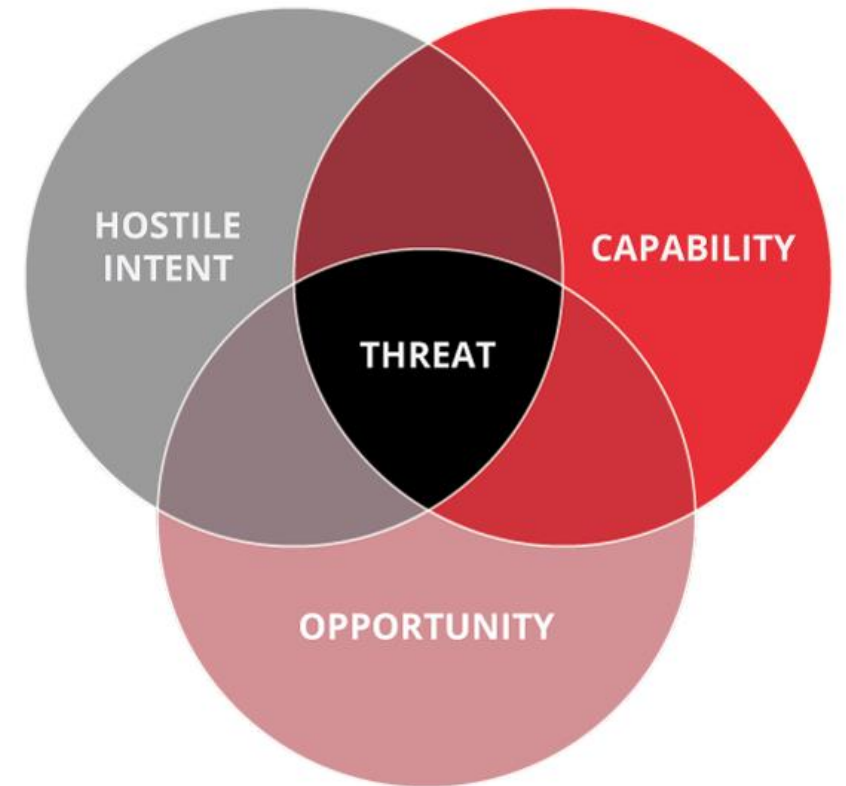
BUT SERIOUSLY NOW...

# WHAT IS CYBER THREAT INTELLIGENCE?

Lets break it down a little bit first...

What is a threat?

Threat = Intent + Capability + Opportunity



# SLIGHT DETOUR - OPPORTUNITY



- Opportunity is within an organizations influence
  - Public facing vulnerabilities
  - Technical or design flaws (architecture)
  - User awareness
- With enough time and resources and attacker will get the opportunity to become a threat.
- This is why we do incident response!

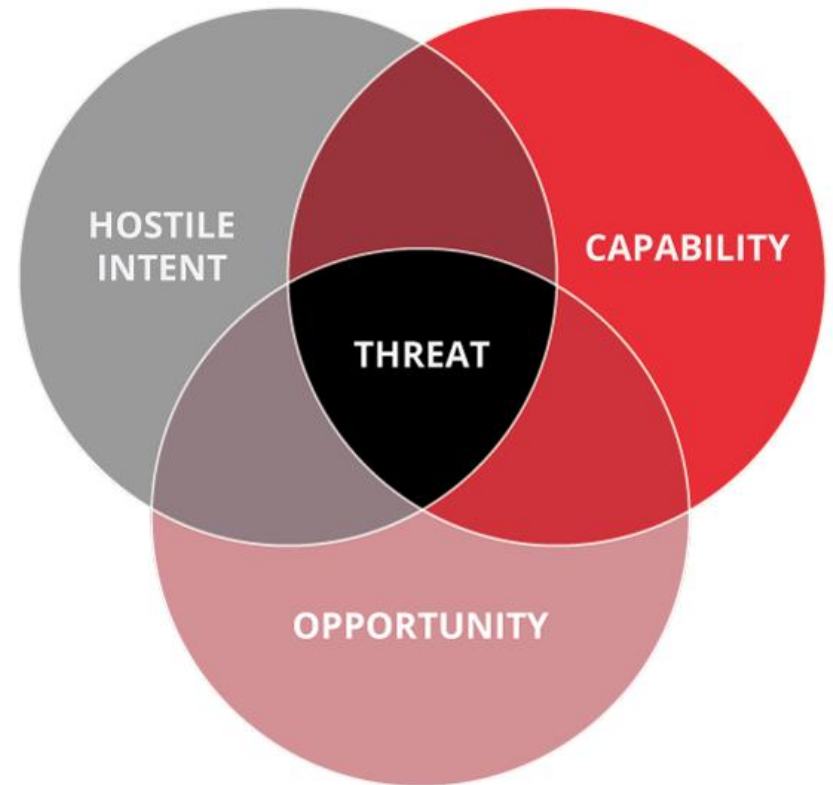
# EXAMPLE - HAFNIUM

"Hafnium" – The actor which utilized a vulnerability in MS Exchange Server and got large attention globally in Q1-2021. But many companies misunderstood the context of the threat and panicked even if they were utilizing Microsoft Exchange Online which was not affected by this vulnerability.

So lets say you are an organization using Exchange Online, was Hafnium a threat in this campaign?

- **Intent** = Cyber espionage
- **Capability** = Covenant or other C2 frameworks
- **Opportunity** = Only worked against on-premise Exchange servers

[Everything you need to know about the Microsoft Exchange Server hack | ZDNet](#)





BEFORE WE ADD INTELLIGENCE WE START WITH DATA



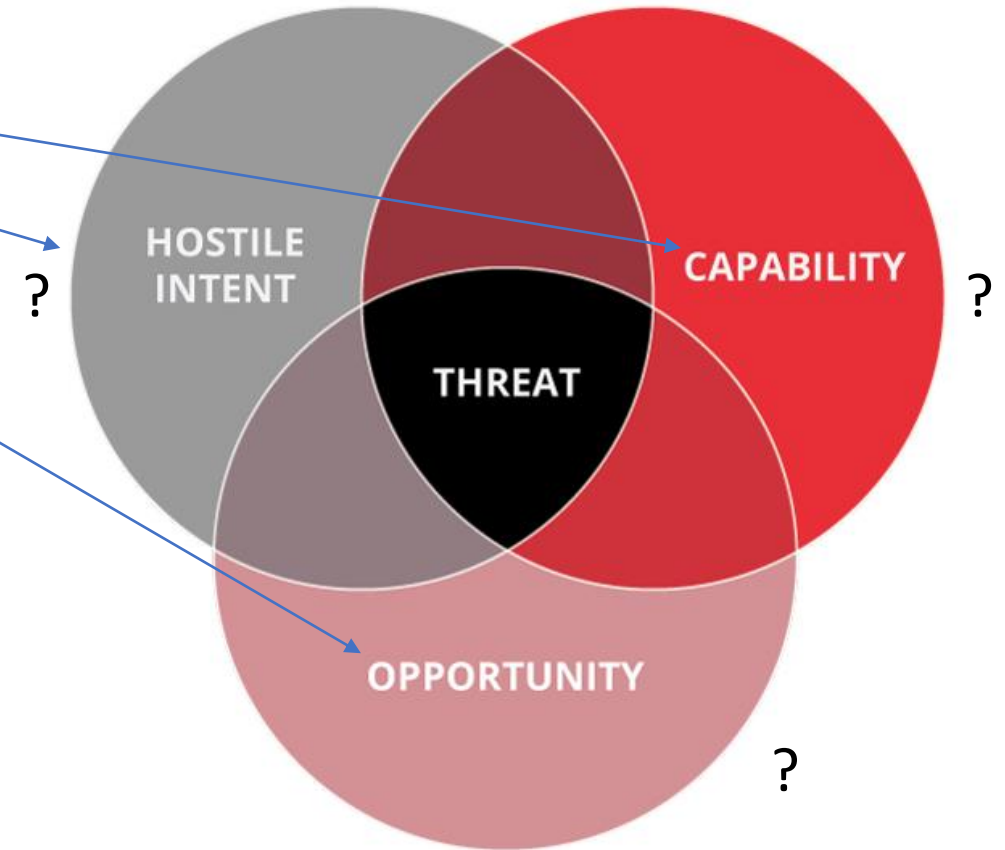


# THREAT DATA

**101.24.100.101**

Is this something we should act on?

There is something missing before we can take a decision on how to treat this data....



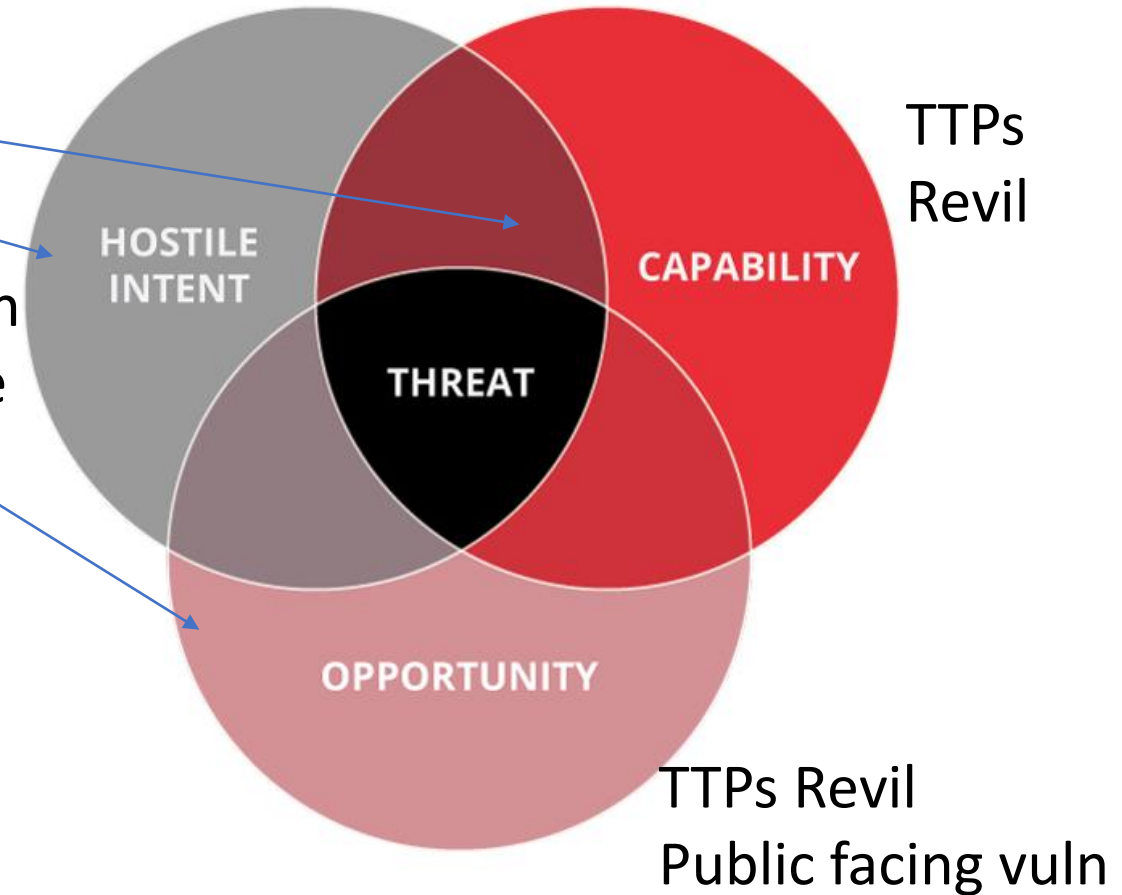
# ADDING THE INTELLIGENCE

**101.24.100.101**

Is this something we should act on?

Financial gain  
Ransomware

Yes, we know that REvil is targetting our sector



## FAVOURITE QUOTE



**Katie Nickels** ✓  
@likethecoins



Intelligence teams have a superpower. We don't just say "you should do this", we get to say "you should do this BECAUSE...." This makes a big difference. "You should look for adfind because ransomware operators have used it for discovery" is more powerful than "Look for adfind".

9:41 PM · Nov 10, 2020 · Twitter Web App

# DIFFERENT TYPES OF INTELLIGENCE

## Technical Intelligence

Indicator specific

**Stakeholders:** Exclusively technical audience

*"Hash values, IP addresses"*

## Strategic Intelligence

None technical, risk-based intelligence used by c-level decision makers.

**Stakeholders:** C Suite/Board level

*"Is expanding into this sector likely to open us up to increased cyber risk?"*

## Tactical Intelligence

Provides information about tactics, techniques and procedures (TTPs) used by a threat actor.

**Stakeholders:** CISO/technical audience

*"Which attackers are targeting our sector and how should we prepare for an attack from them?"*

## Operational Intelligence

Relates to specific attacks or campaigns

**Stakeholders:** Exclusively technical audience


*"That attack last night against the metro service in the UK, utilized a vulnerability in Citrix Netscaler, we have the same version, lets patch the vulnerability and block the indicators"*



HOW DO WE  
GET  
INTELLIGENCE?



# INTELLIGENCE SOURCES

- Create your own
  - Incident metrics
  - Utilize incident classification framework
- Join a sharing community
  - Keep it relevant, no point joining a intelligence community for the Energy sector if you are in Finance.
- Consume external incident metrics
  - Verizon DBIR
- Blogs/Articles
  - Research papers too
- Intelligence feeds!



<https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf>

# KEY POINT!

Always keep it relevant!

Without context and relevancy intelligence is just data...



# CREATE YOUR OWN

- Record your own incidents...

But wait...

If someone asked you describe a specific cyber security incident you have been involved in, what words would you use?

# INCIDENT CLASSIFICATION FRAMEWORKS

- A common language for describing incidents
- Often overlooked – Bringing BI into Cyber Security
- Tell the story
  - Keep it relevant for the right audience
    - Granularity is key!
  - CISO ammo

This is a topic we will cover a lot more in future sessions!

# INTRUSION ANALYSIS – CREATE YOUR OWN

- Diamond Model
  - Useful for a high-level overview of specific threat actors
- Kill Chain
- MITRE ATT&CK

# WAIT WAIT...

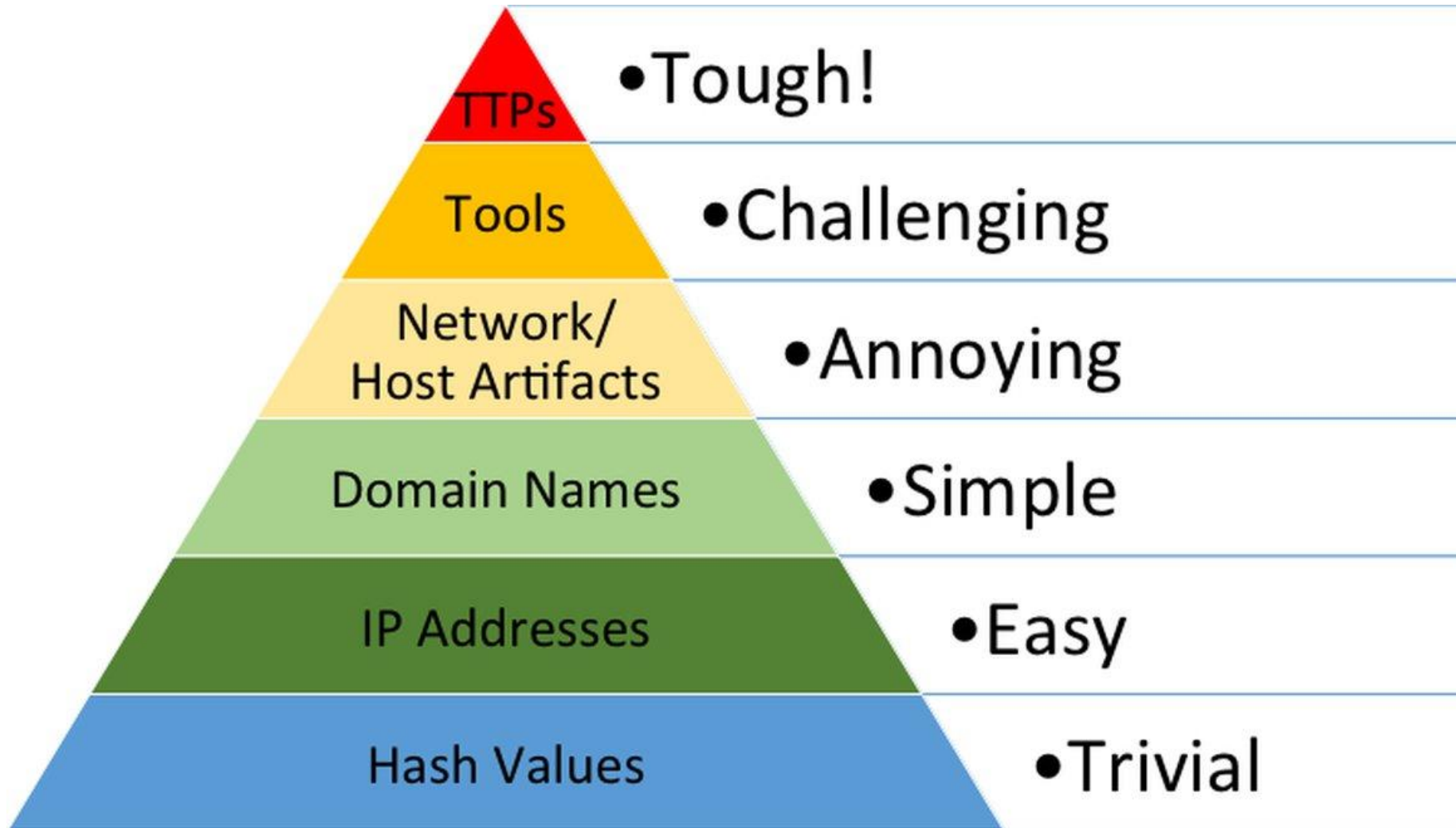
Before we dive into intrusion analysis...

Let's have some pain...

A pyramid of pain!



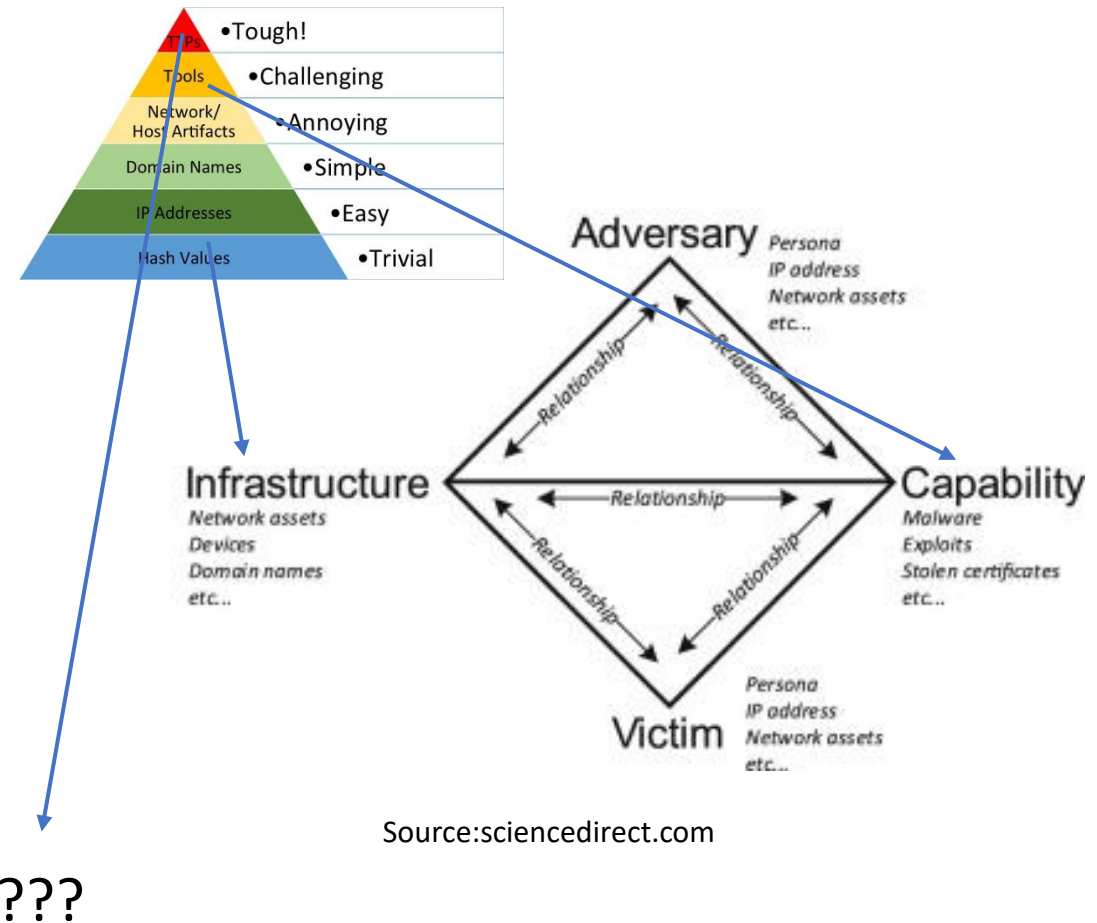
# PYRAMID OF PAIN



# DIAMOND MODEL

This model is used to:-

- Show the relationship between the adversary it's capabilities, infrastructure and it's chosen victim.
- Aid analysts in attribution
  - Overlapping diamond models for intrusions could indicate the same adversary.



# EXAMPLE EXAMPLE

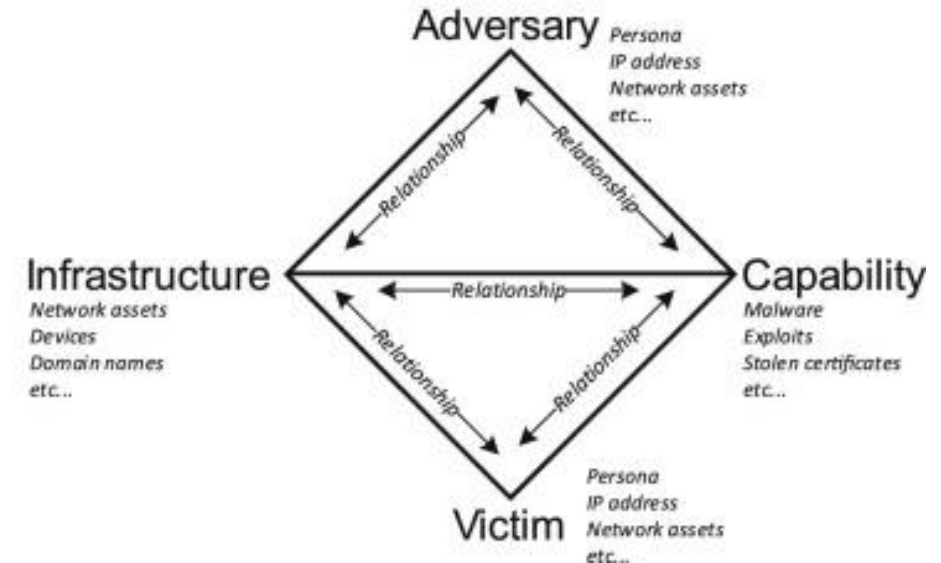
Lets take a look at an example to make it clearer...

# DIAMOND MODEL - EXAMPLE

## On Premise Exchange Server 0 day attacks

- Adversary
  - Persona: Nation State
  - Origin: China
  - Group: Hafnium
- Infrastructure
  - Devices: VPS's in USA
- Capability
  - Exploits 0 day's in Exchange
  - Covenant C2 framework
  - Web shell
- Victim
  - Persona: NGO's, think tanks, higher education, infectious disease researchers, law firms etc
  - Devices: On premise Exchange Servers

Source for analysis: <https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/>  
<https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/>



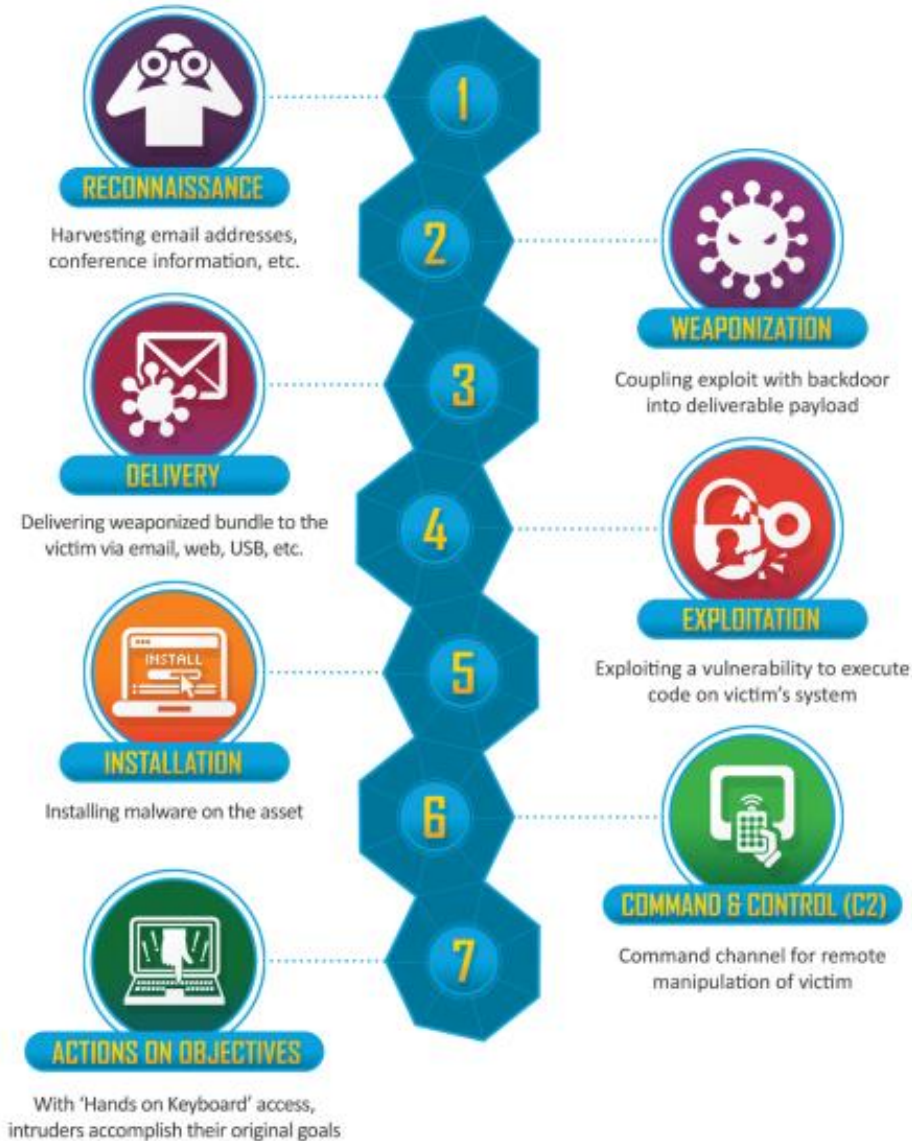
Source: sciencedirect.com



# IS THIS ENOUGH?

That's great but we need to understand more about how the attacker utilizes their capabilities and infrastructure...

# CYBER KILL CHAIN



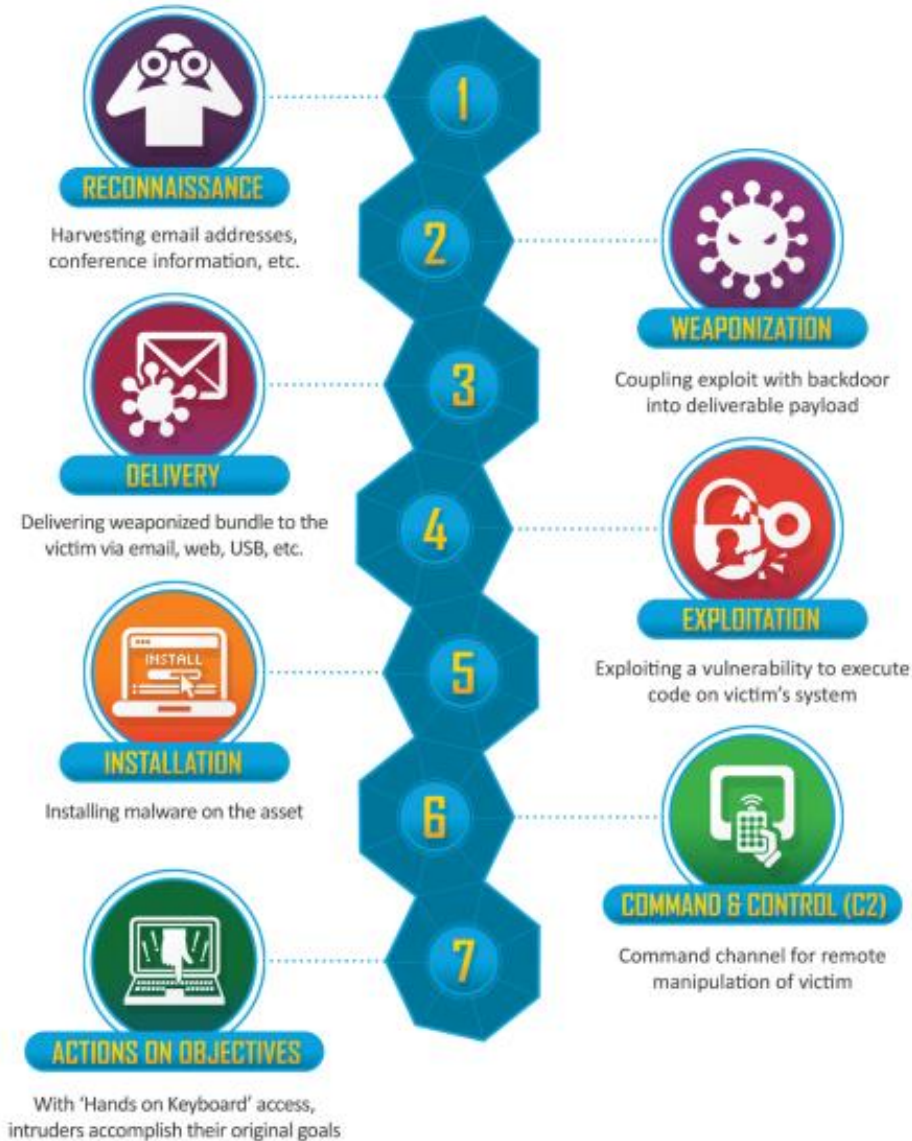
Source: lockheedmartin.com

- Breaks the intrusion down into a chain of events
- Free hand recording of actions within the chain

Issues:-

- Too much freedom when describing phases

# CYBER KILL CHAIN



Source: lockheedmartin.com

## Solar Winds Example

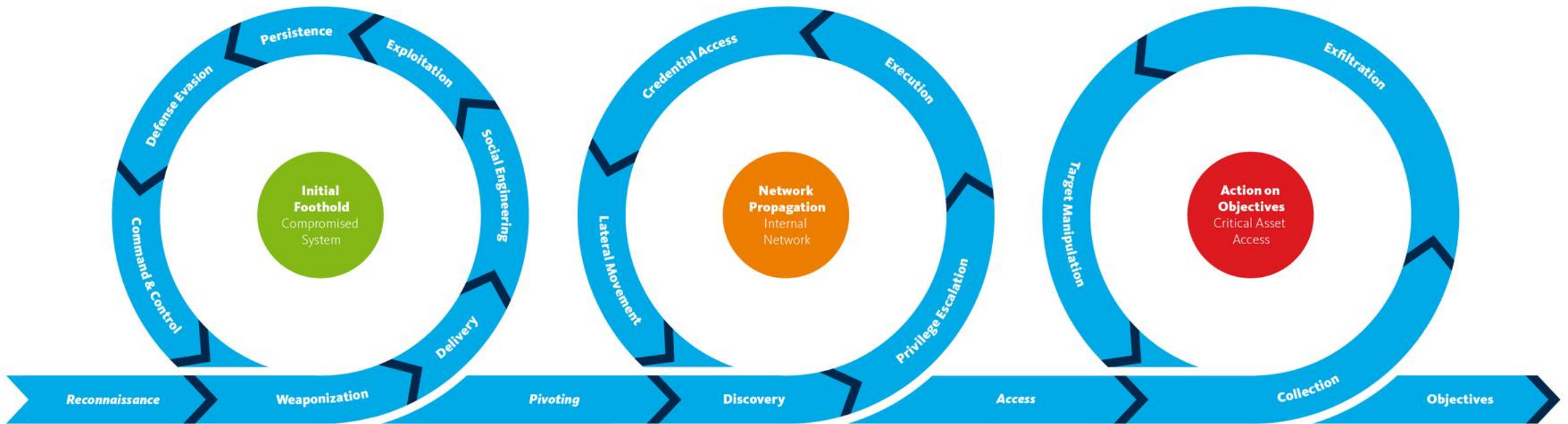
- Recon:- Unknown
- Weaponization:- SolarWinds compromise
- Delivery:- Via the software update system
- Exploitation:- SolarWinds Orion
- Installation:- Backdoor into Solar Winds Orion
- Command and Control:- CNAME response
- Actions on Objectives:- Further recon/espionage

# CYBER KILL CHAIN LINKING

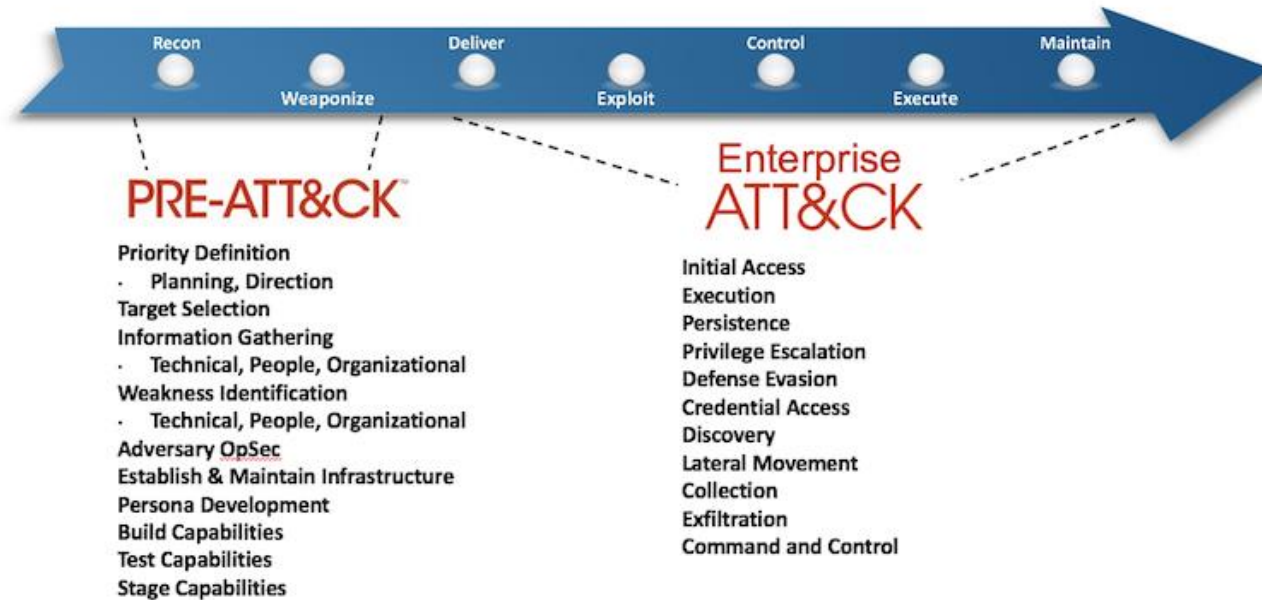
Multiple kill chains are required to describe a single incident

- See next slide for some fun!

# COMPLEX COMPLEX COMPLEX



# MITRE ATT&CK



- Breaks an intrusion down into various phases
- Deep dive into specific TTPs of threat actors in phases
  - TTPs = Techniques, Tactics and Procedures

Reconnaissance   Resource Development   Initial Access   Execution   Persistence   Privilege Escalation   Defense Evasion   Credential Access   Discovery   Lateral Movement   Collection   Command and Control   Exfiltration   Impact

<https://attack.mitre.org/>



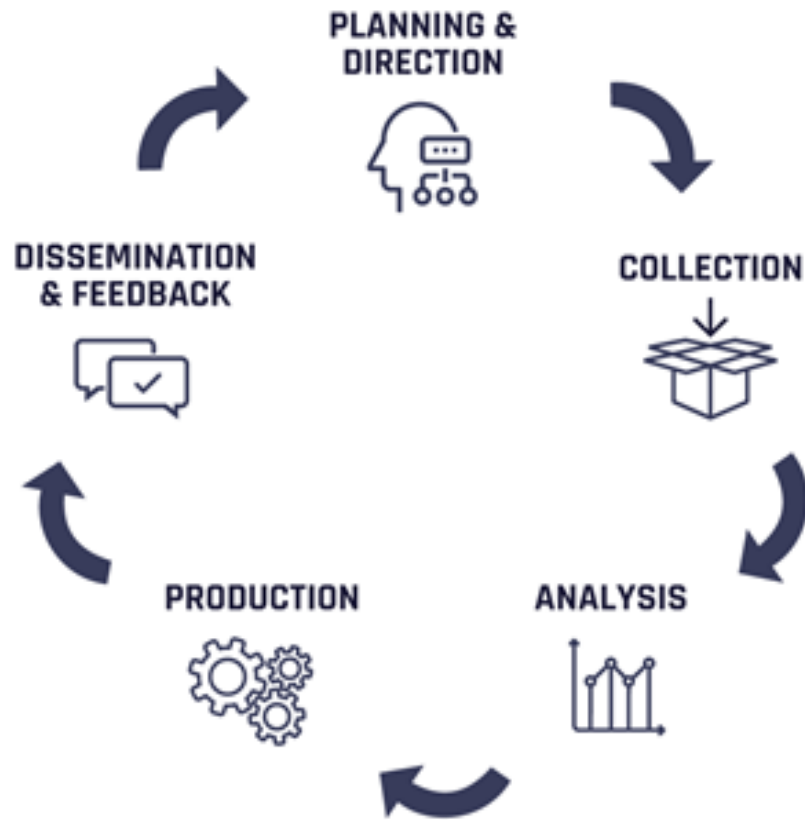
# MITRE ATT&CK – KEY POINTS

- Defacto standard for the industry when describing threat actors and incidents
- Obsession with completing the heatmap
  - Gotta catch em all!
- Great for Red Teams
- Great for Blue Teams
- Great for Purple Teams





# INTELLIGENCE LIFECYCLE



When consuming any sort of CTI, there is a lifecycle/process/guiding principle...

- Gather requirements
  - Start the lifecycle

BE CAREFUL!



# BIAS

When creating intelligence we must be aware of our innate human ability to use bias as a tool to support our analysis of information.

We will use a very interesting recent news article to look at examples of how journalists utilize bias to hit their point home.

<https://www.version2.dk/artikel/eksperter-kritiserer-nationalbankens-solarwinds-haandtering-hele-virker-too-little-too-late>

# BIAS – ARGUMENT FROM AUTHORITY

The journalist in the article uses 4 “experts”.

- A university lecturer in IT – No IR experience
- A university lecturer in Cyber Policy – No IR experience
- A SIEM architect – No IR experience
- A security consultant – Probable IR experience

Only one of the experts has experience in assessing this type of case yet the experts are used to enforce an appearance of authoritative reason.

# BIAS – CONFIRMATION BIAS

- Selectively interpret information to confirm a prior belief
- Rather than searching through all the relevant evidence, they phrase questions to receive an affirmative answer that supports their theory.

*”Slettede de filen? Nej. NEEEEJ! Angriberne ved helt sikkert, de er opdaget, hvis det er deres ZIP-fil, og den slettes. Nationalbanken er gået lige i fælden. I stedet skulle de have puttet logning på filen og kopieret den ind i et sikkert miljø for at se, hvordan den opfører sig, og hvad den indeholder,« siger Lucas Lundgren.”*

In the SolarWinds attack there was absolutely no evidence reported that the attacker utilized a zip file of the vulnerable SolarWinds application. Remember that the attacker already would have had an open connection via the already compromised SolarWinds application. They would not need to redownload the vulnerable application, there are far more stealthy ways to move around compromised infrastructure. Ask the experts...

# BIAS – HINDSIGHT BIAS

- People often believe that after an event has happened they would have been able to predict the outcome.
- Hindsight bias is a big source of overconfidence regarding predictions of future events.

*"Hvis jeg så en ZIP-fil, jeg ikke selv havde hentet, ville jeg tænke 'hvad fanden?!' Som det fremgår af den mail, er det en kæmpe Indication of Compromise,« lyder det fra hackeren, der bakkes op af sin kollegiale konkurrent, sikkerhedsrådgiver."*

*"Når der er tale om kritisk infrastruktur, bør man have styr på, hvilke enheder, der er i ens netværk,« siger sikkerhedsrådgiveren."*

The other "experts" do this too throughout the articles published on the NationalBank case.





## anchoring

The first thing you judge influences your judgment of all that follows.

Human minds are associative in nature, so the order in which we receive information helps determine the course of our judgments and perceptions.

Be especially mindful of this bias during financial negotiations such as houses, cars, and salaries. The initial price offered is proven to have a significant effect.



## confirmation bias

You look for ways to justify your existing beliefs.

We are primed to see and agree with ideas that fit our preconceptions, and to ignore and dismiss information that conflicts with them.

Think of your ideas and beliefs as software you're actively trying to find problems with rather than things to be defended.

"The first principle is that you must not fool yourself -- and you are the easiest person to fool."

- Richard Feynman



## backfire effect

When core beliefs are challenged, it can cause you to believe even more strongly.

We can experience being wrong about some ideas as an attack upon our very selves, or our tribal identity. This can lead to motivated reasoning which causes us to double-down, despite disconfirming evidence.

"It ain't what you don't know that gets you into trouble. It's what you know for sure that just ain't so."

- Mark Twain



## declinism

You see the past as better than it was, and expect the future to be worse than is likely.

Despite living in the most peaceful and prosperous time in history, many people believe things are getting worse. The 24 hour news cycle, with its reporting of overly negative and violent events, may account for some of this effect.

Instead of relying on nostalgic impressions of how great things used to be, use measurable metrics such as life expectancy, levels of crime and violence, and prosperity statistics.



## just world hypothesis

Your preference for a just world makes you presume that it exists.

A world in which people don't always get what they deserve, hard work doesn't always pay off, and injustice happens is an uncomfortable one that threatens our preferred narrative. However, it is also the reality.

A more just world requires understanding rather than blame. Remember that everyone has their own life story, we're all fallible, and bad things happen to good people.



## sunk cost fallacy

You irrationally cling to things that have already cost you something.

When we've invested our time, money, or emotion into something, it hurts us to let it go. This aversion to pain can distort our better judgment and cause us to make unwise investments.

To regain objectivity, ask yourself: had I not already invested something, would I still do so now? What would I counsel a friend to do if they were in the same situation?



## dunning-kruger effect

The less you know about something, the more confident you'll be.

Because experts know just how much they don't know, they tend to underestimate their ability, but it's easy to be over-confident when you have only a simple idea of how things are.

"The whole problem with the world is that fools and fanatics are so certain of themselves, yet wiser people so full of doubts."

- Bertrand Russell



## barnum effect

You see personal specifics in vague statements by filling in the gaps.

Because our minds are given to making connections, it's easy for us to take nebulous statements and find ways to interpret them so that they seem specific and personal.

Psychics, astrologers and others use this bias to make it seem like they're telling you something relevant. Consider how things might be interpreted to apply to anyone, not just you.



## framing effect

You allow yourself to be unduly influenced by context and delivery.

We all like to think that we think independently, but the truth is that all of us are, in fact, influenced by delivery, framing and subtle cues. This is why the ad industry is a thing, despite almost everyone believing they're not affected by advertising messages.

Only when we have the intellectual humility to accept the fact that we can be manipulated, can we hope to limit how much we are. Try to be mindful of how things are being put to you.

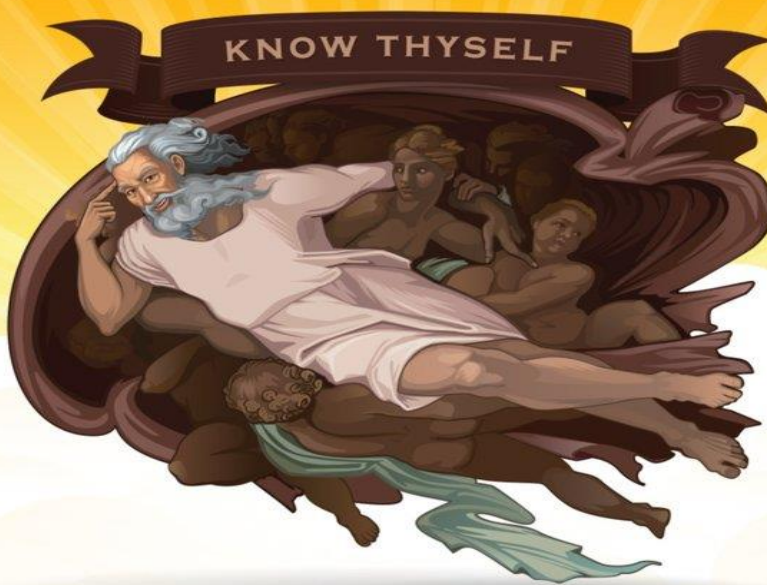


## in-group bias

You unfairly favor those who belong to your group.

We presume that we're fair and impartial, but the truth is that we automatically favor those who are most like us, or belong to our groups.

Try to imagine yourself in the position of those in out-groups; whilst also attempting to be dispassionate when judging those who belong to your in-groups.



## availability heuristic

Your judgments are influenced by what springs most easily to mind.

How recent, emotionally powerful, or unusual your memories are can make them seem more relevant. This, in turn, can cause you to apply them too readily.

Try to gain different perspectives and relevant statistical information rather than relying purely on first judgments and emotive influences.



## belief bias

If a conclusion supports your beliefs, you'll rationalize anything that supports it.

It's difficult for us to set aside our existing beliefs to consider the true merits of an argument. In practice this means that our ideas become impervious to criticism, and are perpetually reinforced.

A useful thing to ask is 'when and how did I get this belief?'

We tend to automatically defend our ideas without ever really questioning them.



## groupthink

You let the social dynamics of a group situation override the best outcomes.

Dissent can be uncomfortable and dangerous to one's social standing, and so often the most confident or first voice will determine group decisions.

Rather than openly contradicting others, seek to facilitate objective means of evaluation and critical thinking practices as a group activity.



## optimism bias

You overestimate the likelihood of positive outcomes.

There can be benefits to a positive attitude, but it's unwise to allow such an attitude to adversely affect our ability to make rational judgments (they're not mutually exclusive).

If you make rational, realistic judgments you'll have a lot more to feel positive about.



## reactance

You'd rather do the opposite of what someone is trying to make you do.

When we feel our liberty is being constrained, our inclination is to resist, however in doing so we can over-compensate.

Be careful not to lose objectivity when someone is being coercive/manipulative, or trying to force you to do something. Wisdom springs from reflection, folly from reaction.



## curse of knowledge

Once you understand something you presume it to be obvious to everyone.

Things makes sense once they make sense, so it can be hard to remember why they didn't. We build complex networks of understanding and forget how intricate the path to our available knowledge really is.

When teaching someone something new, go slow and explain like they're ten years old (without being patronizing). Repeat key points and facilitate active practice to help embed knowledge.



## self-serving bias

You believe your failures are due to external factors, yet your successes are your own.

Many of us enjoy unearned privileges, luck and advantages that others do not. It's easy to tell ourselves that we deserve these things, whilst blaming circumstance when things don't go our way.

When judging others, be mindful of how this bias interacts with the just-world hypothesis, fundamental attribution error, and the in-group bias.



## negativity bias

You allow negative things to disproportionately influence your thinking.

The pain of loss and hurt are felt more keenly and persistently than the feeling gratification of pleasant things. We are primed for survival and our aversion to pain can distort our judgment for a modern world.

Pro-and-con lists, as well as thinking in terms of probabilities, can help you evaluate things more objectively than relying on a cognitive impression.



## pessimism bias

You overestimate the likelihood of negative outcomes.

Pessimism is often a defense mechanism against disappointment, or it can be the result of depression and anxiety disorders. Perhaps the worst aspect of pessimism is that even if something good happens, you'll probably feel pessimistic about it anyway.



## spotlight effect

You overestimate how much people notice how you look and act.

Most people are much more concerned about themselves than they are about you. Absent overt prejudices, people generally want to like and get along with you as it gives them validation too.

Instead of worrying about how you're being judged, consider how you make others feel. They'll remember this much more, and you'll make the world a better place.

# thou shalt not suffer cognitive biases

Cognitive biases make our judgments irrational. We have evolved to use shortcuts in our thinking, which are often useful, but a cognitive bias means there's a kind of misfiring going on causing us to lose objectivity. This poster has been designed to help you identify some of the most common biases and how to avoid falling victim to them. Help people become aware of their biases generally by sharing the website [yourbias.is](http://yourbias.is) or more specifically e.g. [yourbias.is/confirmation-bias](http://yourbias.is/confirmation-bias)



This poster is published under a Creative Commons BY-NC-ND license 2020 by Jesse Richardson. You are free to print and redistribute this artwork non-commercially with the binding proviso that you reproduce it in full so that others may share alike. To learn more about biases you should read the books Thinking, Fast and Slow and You Are Not So Smart.

The illustration above is a reference to Michelangelo's 'Creation of Adam', which many believe depicted the human brain in God's surrounding decoration.

Download this poster at [www.yourbias.is](http://www.yourbias.is)





## strawman

Misrepresenting someone's argument to make it easier to attack.

By exaggerating, misrepresenting, or just completely fabricating someone's argument, it's much easier to present your own position as being reasonable, but this kind of dishonesty serves to undermine rational debate.

After Will said that we should be nice to litterers because they're fluffy and cute, Bill says that Will is a mean jerk who wants to be mean to poor defenseless puppies.



## slippery slope

Asserting that if we allow A to happen, then Z will consequently happen too, therefore A should not happen.

The problem with this reasoning is that it avoids engaging with the issue at hand, and instead shifts attention to baseless extreme hypotheticals. The merits of the original argument are then tainted by unsubstantiated conjecture.

Colin asserts that if we allow children to play video games, then the next thing you know we'll be living in a post-apocalyptic zombie wasteland with no money for guard rails to protect people from slippery slopes.



## special pleading

Moving the goalposts or making up exceptions when a claim is shown to be false.

Humans are funny creatures and have a foolish aversion to being wrong. Rather than appreciate the benefits of being able to change one's mind through better understanding, many will invent ways to cling to old beliefs.

Edward Johns claimed to be psychic, but when his 'abilities' were tested under proper scientific conditions, they magically disappeared. Edward explained this saying that one had to have faith in his abilities for them to work.



## the gambler's fallacy

Believing that 'runs' occur to statistically independent phenomena such as roulette wheel spins.

This commonly believed fallacy can be said to have helped create a city in the desert of Nevada USA. Though the overall odds of a big run happening may be low, each spin of the wheel is itself entirely independent from the last.

Red had come up six times in a row on the roulette wheel, so Greg knew that it was close to certain that black would be next up. Suffering an economic form of natural selection with this thinking, he soon lost all of his savings.



## black-or-white

Where two alternative states are presented as the only possibilities, when in fact more possibilities exist.

Also known as the false dilemma, this insidious tactic has the appearance of forming a logical argument, but under closer scrutiny it becomes evident that there are more possibilities than the either/or choice that is presented.

Whilst rallying support for his plan to fundamentally undermine citizens' rights, the Supreme Leader told the people they were either on his side, or on the side of the enemy.



## false cause

Presuming that a real or perceived relationship between things means that one is the cause of the other.

Many people confuse correlation (things happening together or in sequence) for causation (that one thing actually causes the other to happen). Sometimes correlation is coincidental, or it may be attributable to a common cause.

Pointing to a fancy chart, Roger shows how temperatures have been rising over the past few centuries, whilst at the same time the numbers of pirates have been decreasing. Thus pirates cool the world and global warming is a hoax.



## ad hominem

Attacking your opponent's character or personal traits in an attempt to undermine their argument.

Ad hominem attacks can take the form of overtly attacking somebody, or casting doubt on their character. The result of an ad hominem attack can be to undermine someone without actually engaging with the substance of their argument.

After Sally presents an eloquent and compelling case for a more equitable taxation system, Sam asks the audience whether we should believe anything from a woman who isn't married and probably eats her own boogers.



## loaded question

Asking a question that has an assumption built into it so that it can't be answered without appearing guilty.

Loaded question fallacies are particularly effective at derailing rational debates because of their inflammatory nature - recipients of a loaded question are compelled to defend themselves and may appear flustered or on the back foot.

Grace and Helen were both romantically interested in Brad. One day, with Brad sitting within earshot, Grace asked in an inquisitive tone whether Helen was having any problems with a fungal infection.



## bandwagon

Appealing to popularity or the fact that many people do something as an attempted form of validation.

The flaw in this argument is that the popularity of an idea has absolutely no bearing on its validity. If it did, then the Earth would have made itself flat for most of history to accommodate this popular belief.

Shamus pointed a finger at Sean and asked him to explain how so many people could believe in leprechauns if they're only a silly old superstition. Sean wondered how so many people could believe in things based on popularity.



## begging the question

A circular argument in which the conclusion is included in the premise.

This logically incoherent argument often arises in situations where people have an assumption that is very ingrained, and therefore taken in their minds as a given. Circular reasoning is bad mostly because it's not very good.

The word of Zorbo the Great is flawless and perfect. We know this because it says so in The Great and Infallible Book of Zorbo's Best and Most True Things that are Definitely True and Should Not Ever Be Questioned.



## appeal to emotion

Manipulating an emotional response in place of a valid or compelling argument.

Appeals to emotion include appeals to fear, envy, hatred, pity, guilt, and more. Though a valid, and reasoned, argument may sometimes have an emotional aspect, one must be careful that emotion doesn't obscure or replace reason.

Luke didn't want to eat his sheep brains with chopped liver and Brussels sprouts, but his father told him to think about the poor, starving children in a third world country who weren't fortunate enough to have any food at all.



## tu quoque

Avoiding having to engage with criticism by turning it back on the accuser - answering criticism with criticism.

Literally translating as 'you too!' this fallacy is commonly employed as an effective red herring because it takes the heat off the accused having to defend themselves and shifts the focus back onto the accuser themselves.

Nicola identified that Hannah had committed a logical fallacy, but instead of addressing the substance of her claim, Hannah accused Nicola of committing a fallacy earlier on in the conversation.



## burden of proof

Saying that the burden of proof lies not with the person making the claim, but with someone else to disprove.

The burden of proof lies with someone who is making a claim, and is not upon anyone else to disprove. The inability, or disinclination, to disprove a claim does not make it valid (however we must always go by the best available evidence).

Bertrand declares that a teapot is, at this very moment, in orbit around the Sun between the Earth and Mars, and that because no one can prove him wrong his claim is therefore a valid one.



## no true scotsman

Making what could be called an appeal to purity as a way to dismiss relevant criticisms or flaws of an argument.

This fallacy is often employed as a measure of last resort when a point has been lost. Seeing that a criticism is valid, yet not wanting to admit it, new criteria are invoked to disassociate oneself or one's argument.

Angus declares that Scotsmen do not put sugar on their porridge, to which Lachlan points out that he is a Scotsman and puts sugar on his porridge. Furious, like a true Scot, Angus yells that no true Scotsman sugars his porridge.



## the texas sharpshooter

Cherry-picking data clusters to suit an argument, or finding a pattern to fit a presumption.

This false causal fallacy is coined after a marksman shooting at barns and then painting a bullseye target around the spot where the most bullet holes appear. Clusters naturally appear by chance, and don't necessarily indicate causation.

The makers of Sugarette Candy Drinks point to research showing that of the five countries where Sugarette drinks sell the most units, three of them are in the top ten healthiest countries on Earth, therefore Sugarette drinks are healthy.



## the fallacy fallacy

Presuming a claim to be necessarily wrong because a fallacy has been committed.

It is entirely possible to make a claim that is false yet argue with logical coherence for that claim, just as it is possible to make a claim that is true and justify it with various fallacies and poor arguments.

Recognising that Amanda had committed a fallacy in arguing that we should eat healthy food because a nutritionist said it was popular, Alyse said we should therefore eat bacon double cheeseburgers every day.



## personal incredulity

Saying that because one finds something difficult to understand, it's therefore not true.

Subjects such as biological evolution via the process of natural selection require a good amount of understanding before one is able to properly grasp them. This fallacy is usually used in place of that understanding.

Mike drew a picture of a fish and a human and with effusive disdain asked Richard if he really thought we were stupid enough to believe that a fish somehow turned into a human through just, like, random things happening over time.



## ambiguity

Using double meanings or ambiguities of language to mislead or misrepresent the truth.

Politicians are often guilty of using ambiguity to mislead and will later point to how they were technically not outright lying if they come under scrutiny. It's a particularly tricky and premeditated fallacy to commit.

When the judge asked the defendant why he hadn't paid his parking fines, he said that he shouldn't have to pay them because the sign said 'fine for parking here' and so he naturally presumed that it would be fine to park there.



## genetic

Judging something good or bad on the basis of where it comes from, or from whom it comes.

To appeal to prejudices surrounding something's origin is another red herring fallacy. This fallacy has the same function as an ad hominem, but applies instead to perceptions surrounding something's source or context.

Accused on the 6 o'clock news of corruption and taking bribes, the senator said that we should all be very wary of the things we hear in the media, because we all know how very unreliable the media can be.



## middle ground

Saying that a compromise, or middle point, between two extremes must be the truth.

Much of the time the truth does indeed lie between two extreme points, but this can bias our thinking: sometimes a thing is simply untrue and a compromise of it is also untrue. Half way between truth and a lie, is still a lie.

Holly said that vaccinations caused autism in children, but her scientifically well-read friend Caleb said that this claim had been debunked and proven false. Their friend Alice offered a compromise that vaccinations cause some autism.

# thou shalt not commit logical fallacies

A logical fallacy is a flaw in reasoning. Strong arguments are void of logical fallacies, whilst arguments that are weak tend to use fallacies in place of cogent logic. They're like tricks or illusions of thought, and they're often very sneakily used by politicians, the media, and others to fool people. Don't be fooled!

This poster has been designed to help you identify and call out dodgy logic wherever it may raise its ugly, incoherent head. If you see someone committing a logical fallacy online, link them to the relevant fallacy to school them in thinkness e.g. [yourfallacyis/strawman](http://yourfallacyis/strawman)

© 2018 This poster is published under a Creative Commons Attribution and Non-commercial license 2018 by The School of Thought, a 501(c)3 non-profit organization. You are free to print, copy, and redistribute this artwork, with the binding proviso that you reproduce it in full so that others may share alike.

Download this poster at [yourfallacy.is](http://yourfallacy.is)



OK SO NOW WE HAVE GATHERED SOME GOOD CTI

Lets share share share!

## ISAC Communities



## Consuming Threat Data/Intelligence

- Data which is relevant to us
  - Threat feeds
  - Automated actions
    - Prevention
    - Detection
    - Hunting



# TLP PROTOCOL

	<b>TLP: RED</b>	<b>TLP: AMBER</b>	<b>TLP: GREEN</b>	<b>TLP: WHITE</b>
Information sharing boundaries	<b>Not for disclosure</b> <b>Restricted to participants only</b>	<b>Limited disclosure</b> <b>Participant organisations only</b>	<b>Limited disclosure</b> <b>Restricted to community only</b>	<b>Disclosure is not limited</b>
When to use	Impacts privacy, reputation or operations	Risk to privacy, reputation or operations if shared outside participating organisations	Useful for participating organisations and broader community	Minimal or no foreseeable risk of misuse, suitable for public release
How to share	Participating organisations only	Organisation members only. Additional restrictions can be set.	Peer and partner organisations only. Not suitable for public release	No restrictions

Source: <https://support.aaf.edu.au/>

# WHAT DID WE LEARN??

Can we answer the following questions?

# WHAT DID WE LEARN??

I read that REvil ransomware just hit our competitor, can we detect it using our current capabilities?

If we takeover this company and move into a new sector, are we exposing ourselves to new threats?

How many times did we see Emotet malware last year?

The background is a vibrant, abstract composition. On the left, a dense field of blue and purple fiber optic lines radiates outwards, creating a sense of depth and movement. On the right, a pink and red checkerboard pattern transitions into a soft, out-of-focus bokeh of light circles. The overall color palette is a mix of cool blues and purples with warm pinks and reds.

# **COMBITECH**

Thanks for listening!