Thomas V Fischer

Threats versus Capabilities

Building Better Detect and Respond Capabilities

- **Current focus is SecOps**
- **25+ years experience in InfoSec**
  - Security Advocate, Architect & Threat Researcher focused on Data Protection
  - Spent number years in corporate IR team positions

GCFA

GNFA

GCIH

CISSP®

I am @Fvt…

BSidesLondon Director

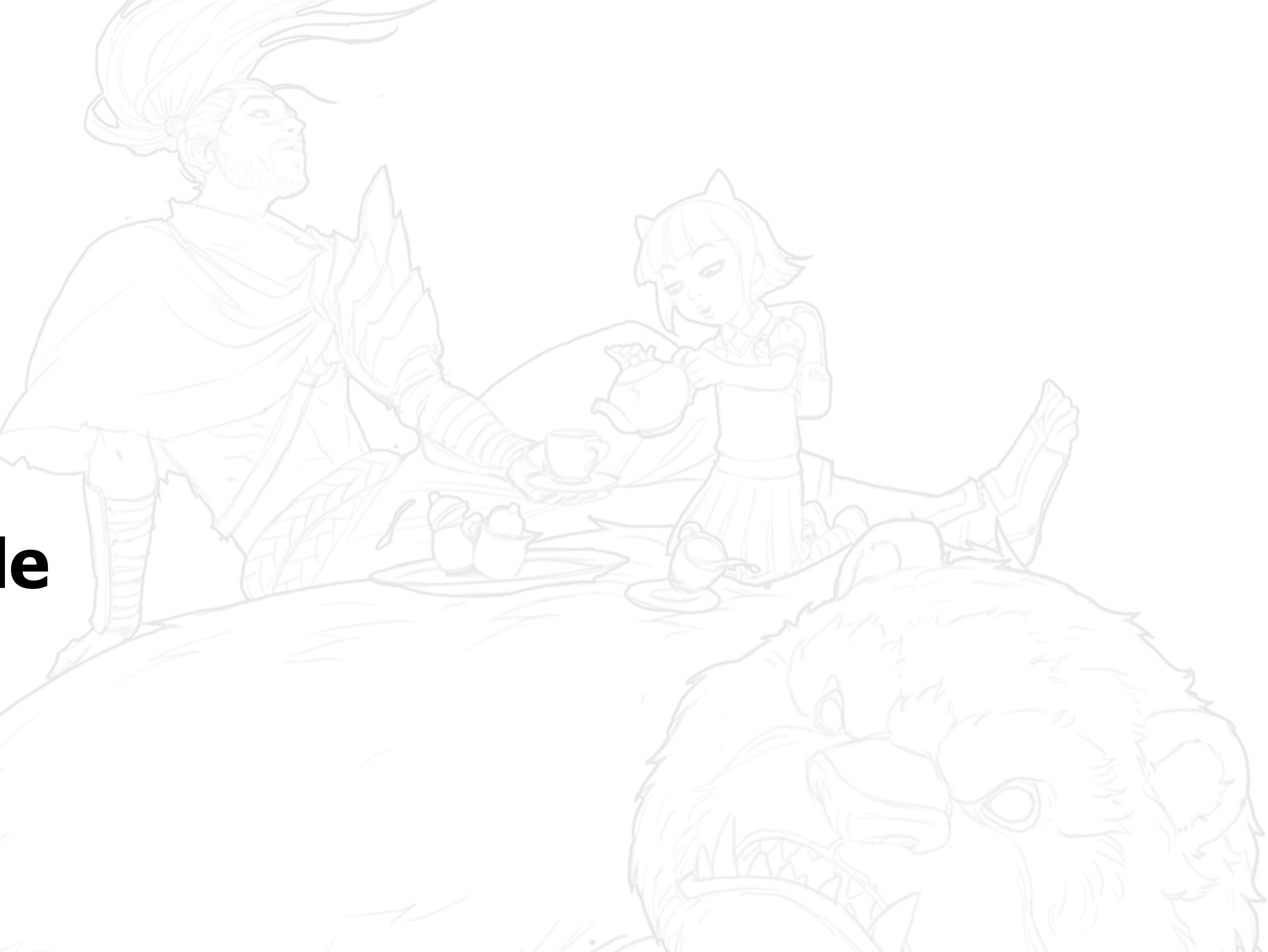
- **Contact**
  - tvfischer+sec at gmail[.]com | tvfischer at pm[.]me
  - keybase.io/fvt

RIOT GAMES

Threats versus Capabilities

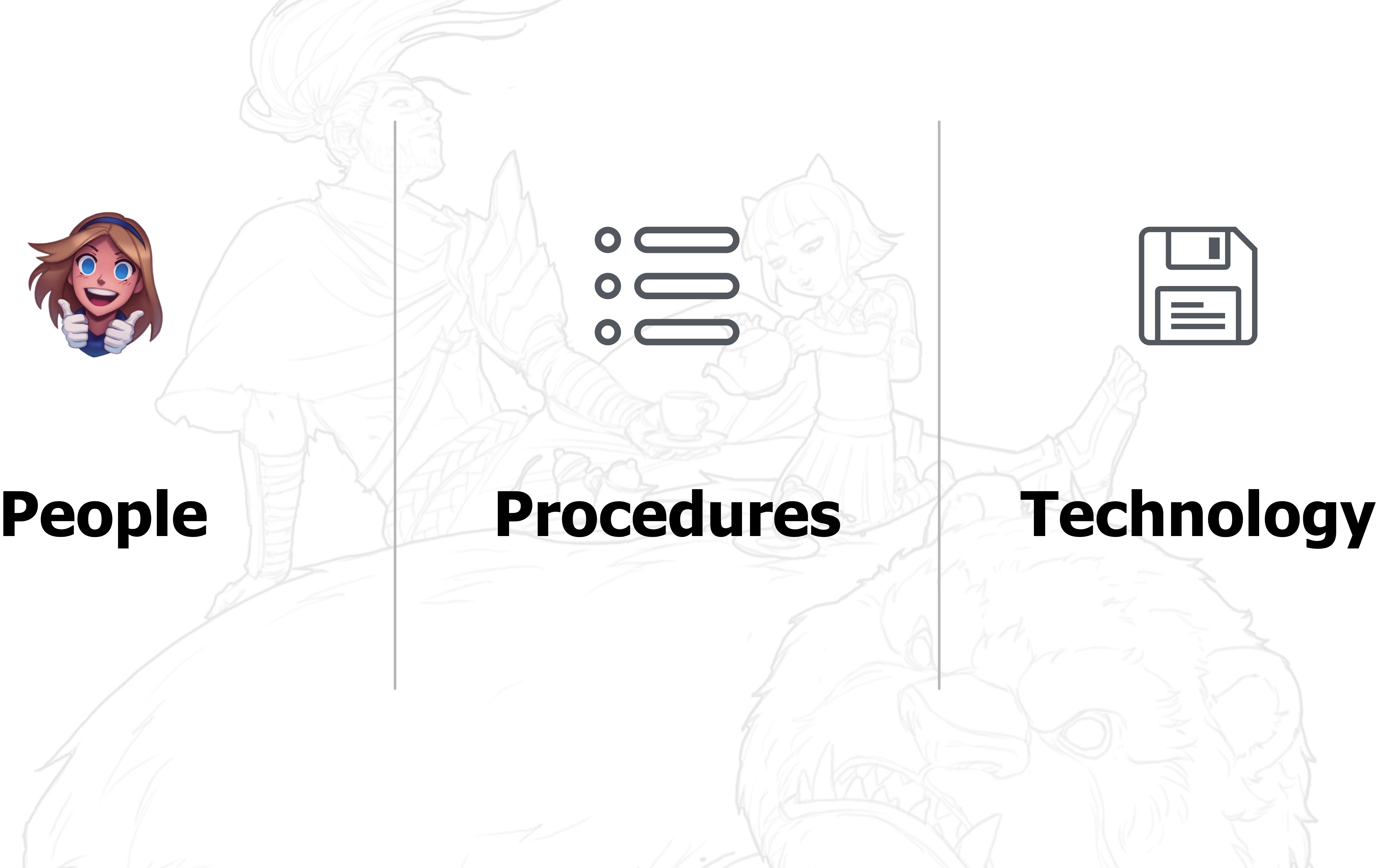
Threat Actors Get In

People



People

Procedures



People

Procedures

Technology

Threats versus Capabilities

> Our failures are a consequence of many factors, but possibly one of the most important is the fact that society operates on the theory that specialization is the key to success, not realizing that specialization precludes comprehensive thinking
>
> *Buckminster Fuller*

Threats versus Capabilities

> "Our failures are a consequence of many factors, but possibly one of the most important is the fact that ~~society~~ operates on the theory that specialization is the key to success, not realizing that specialization precludes comprehensive thinking

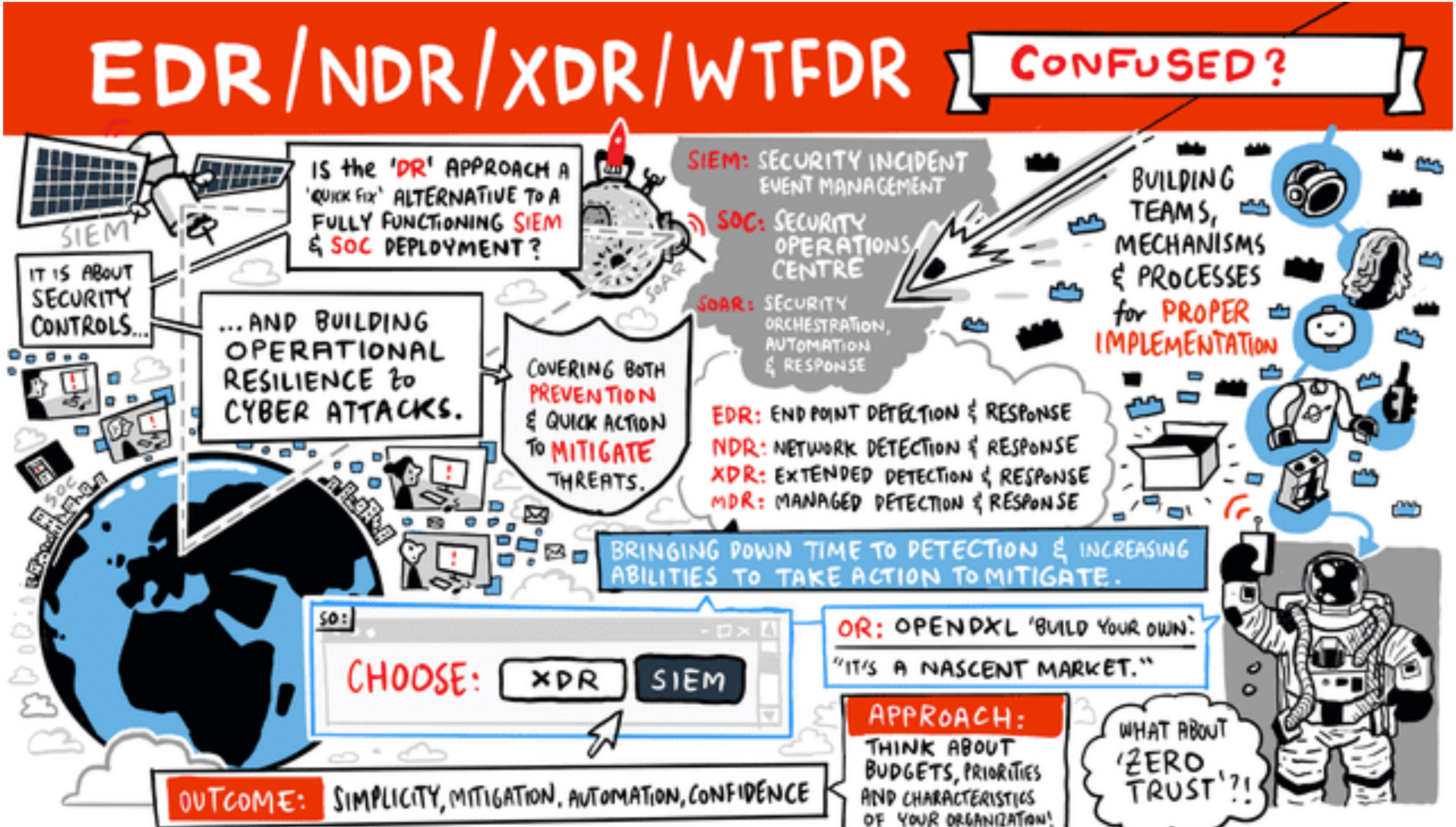
Security

> "Our failures are a consequence of many factors, but possibly one of the most important is the fact that ~~society~~ operates on the theory that ~~specialization~~ is the key to success, not realizing that ~~specialization~~ precludes comprehensive thinking

Security

Tools

Threats versus Capabilities



EDR/NDR/XDR/WTFDR

CONFUSED?

IS the 'DR' APPROACH A 'QUICK FIX' ALTERNATIVE TO A FULLY FUNCTIONING SIEM & SOC DEPLOYMENT?

IT IS ABOUT SECURITY CONTROLS...

...AND BUILDING OPERATIONAL RESILIENCE to CYBER ATTACKS.

COVERING BOTH PREVENTION & QUICK ACTION TO MITIGATE THREATS.

SIEM: SECURITY INCIDENT EVENT MANAGEMENT

SOC: SECURITY OPERATIONS CENTRE

SOAR: SECURITY ORCHESTRATION, AUTOMATION & RESPONSE

BUILDING TEAMS, MECHANISMS & PROCESSES for PROPER IMPLEMENTATION

EDR: END POINT DETECTION & RESPONSE

NDR: NETWORK DETECTION & RESPONSE

XDR: EXTENDED DETECTION & RESPONSE

MDR: MANAGED DETECTION & RESPONSE

BRINGING DOWN TIME TO DETECTION & INCREASING ABILITIES TO TAKE ACTION TO MITIGATE.

SO:

CHOOSE: XDR SIEM

OR: OPENDXL 'BUILD YOUR OWN.'

"IT'S A NASCENT MARKET."

OUTCOME: SIMPLICITY, MITIGATION, AUTOMATION, CONFIDENCE

APPROACH: THINK ABOUT BUDGETS, PRIORITIES AND CHARACTERISTICS OF YOUR ORGANIZATION!

WHAT ABOUT 'ZERO TRUST'?!

Thanks to Secrutiny – EDR/NDR/XDR/WTFDR?

Vendors Want You to Believe

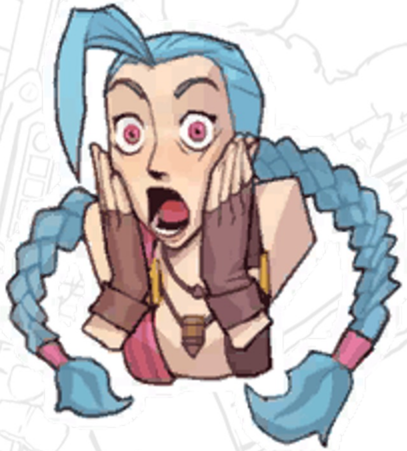
Detec
t

Prote
ct

Threats versus Capabilities

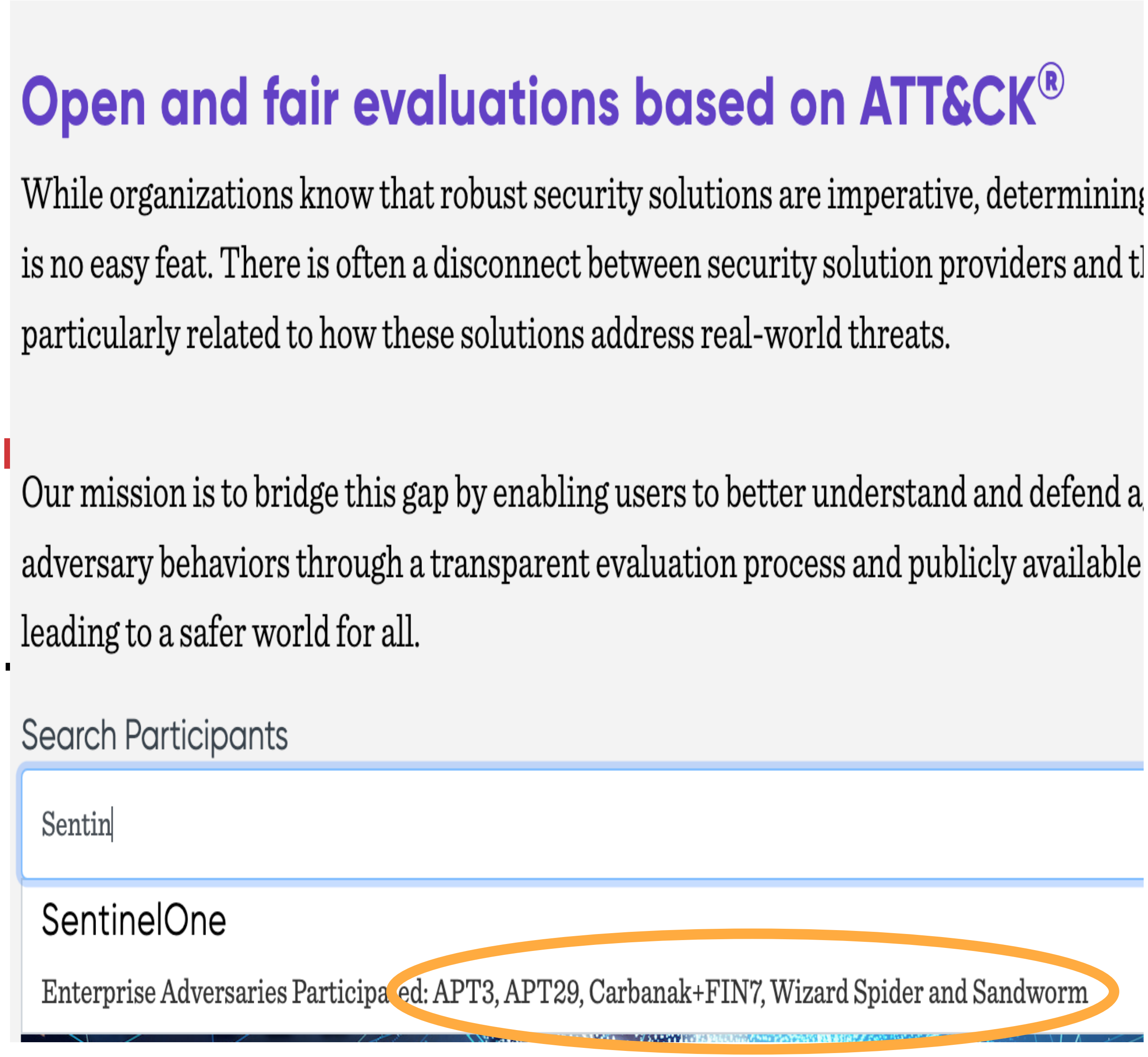
MITRE

ATT&CK™



The Issue?

- Too focused on specific **threat actor**
- Yeah so you cover a bunch of TTPs...



Open and fair evaluations based on ATT&CK®

While organizations know that robust security solutions are imperative, determining is no easy feat. There is often a disconnect between security solution providers and t particularly related to how these solutions address real-world threats.

Our mission is to bridge this gap by enabling users to better understand and defend a adversary behaviors through a transparent evaluation process and publicly available leading to a safer world for all.

Search Participants

Sentin

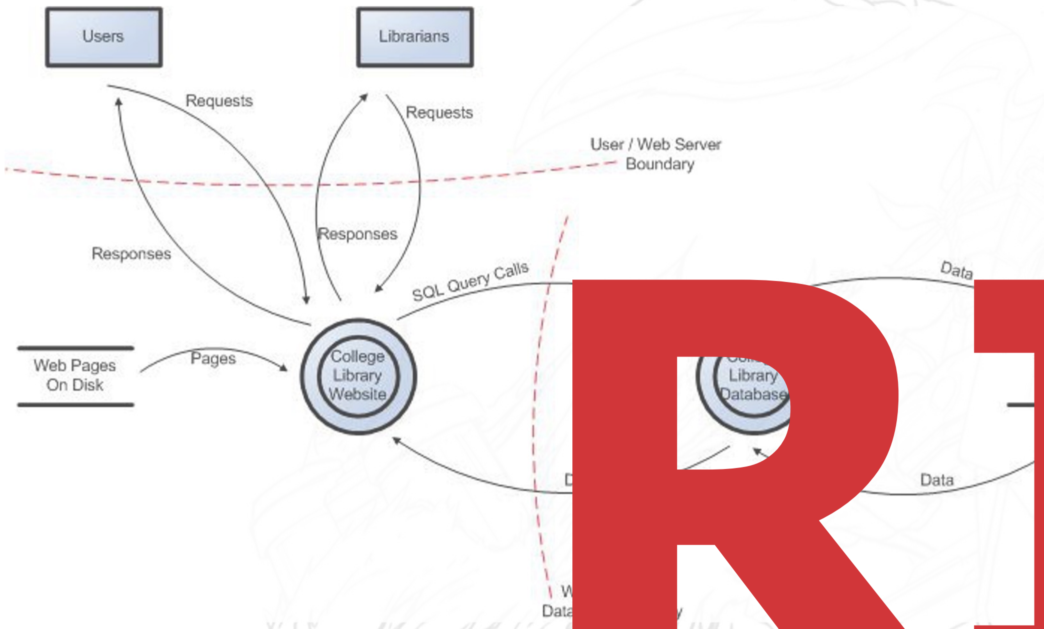
SentinelOne

Enterprise Adversaries Participated: APT3, APT29, Carbanak+FIN7, Wizard Spider and Sandworm

SOLVABLE?

What Can be Done Differently?

Threat modelling works to identify, communicate, and understand threats and mitigations within the context of protecting something of value



RISK

approach

But Does It Work?

Incident Responder

Detection Engineer

Want Practical Approach

Wants & Needs

1. Threat Driven Approach

2. Understand Capabilities

3. Helps Define What/How Detection is Achieved

4. Identifies How Effective Response Is

Premise

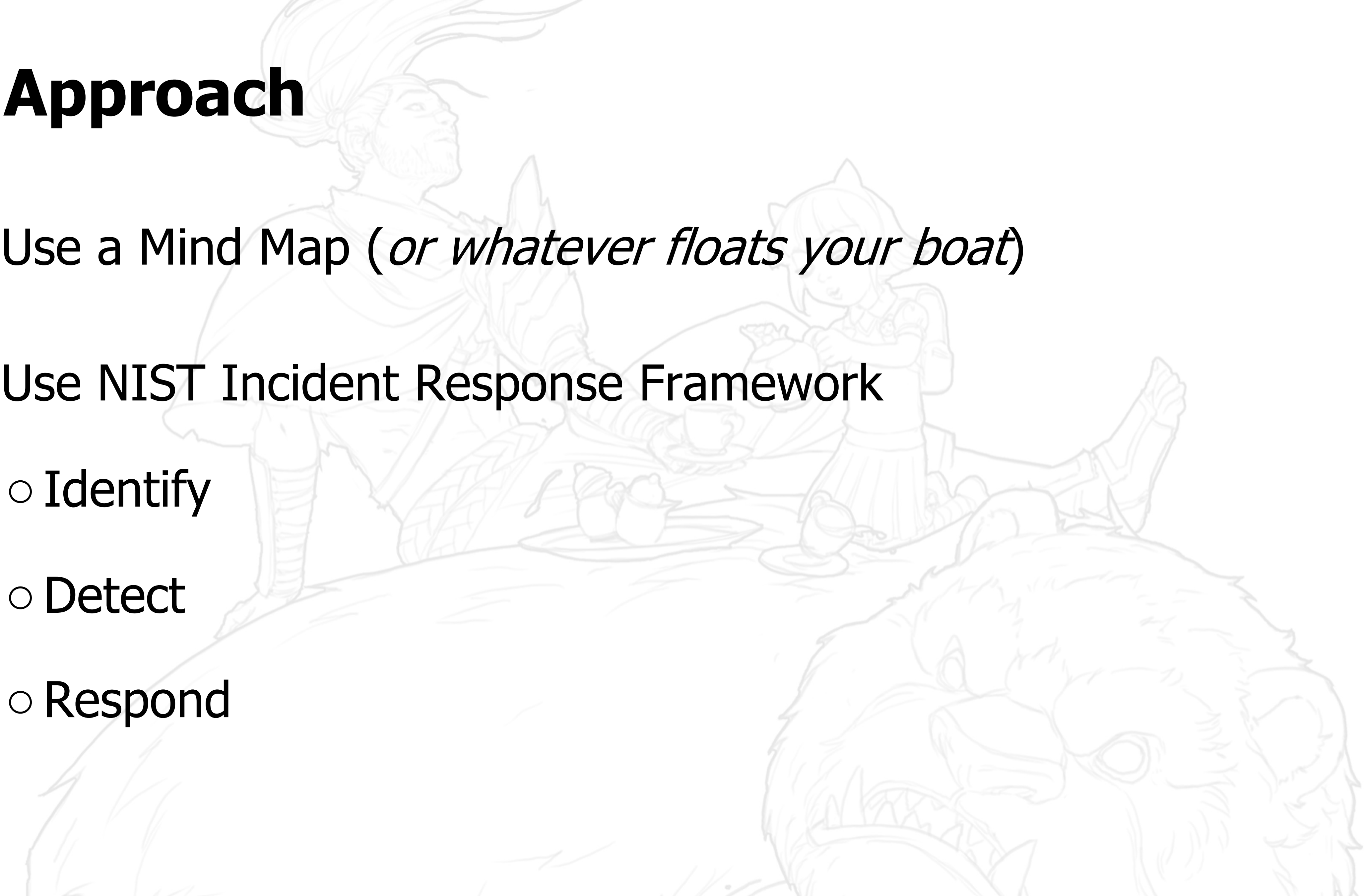
1 What Threat is the Organization Concerned with

2 Identify the Assets

3 Determine Detection Data Points

4 Determine Response Actions and Data Points

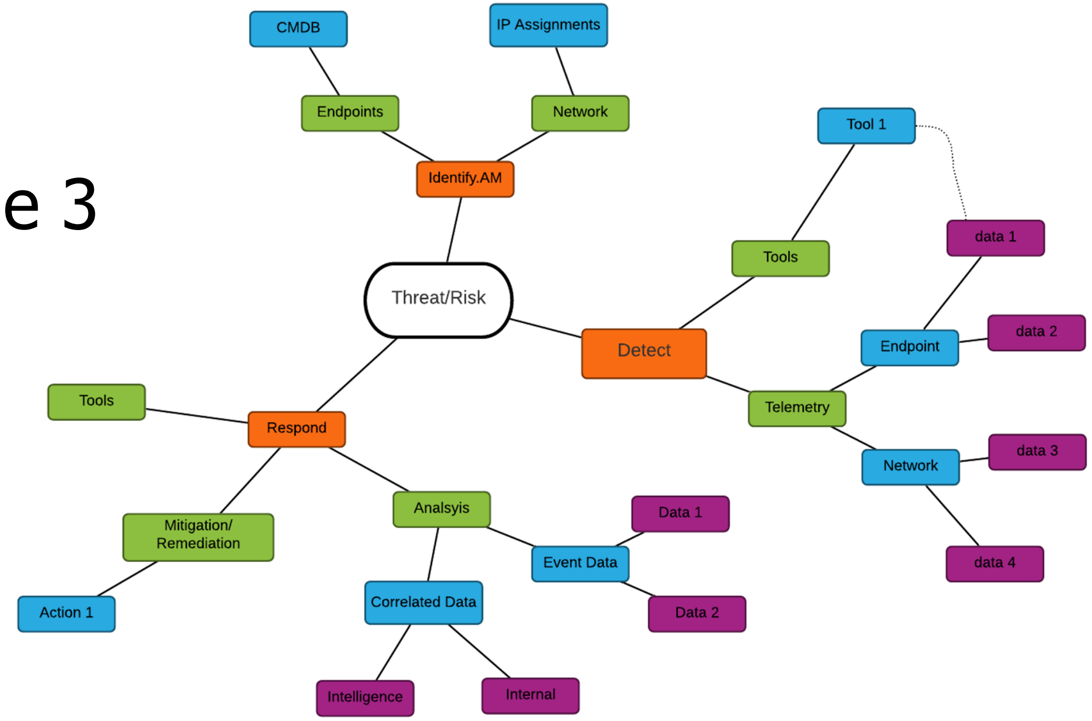
The Approach



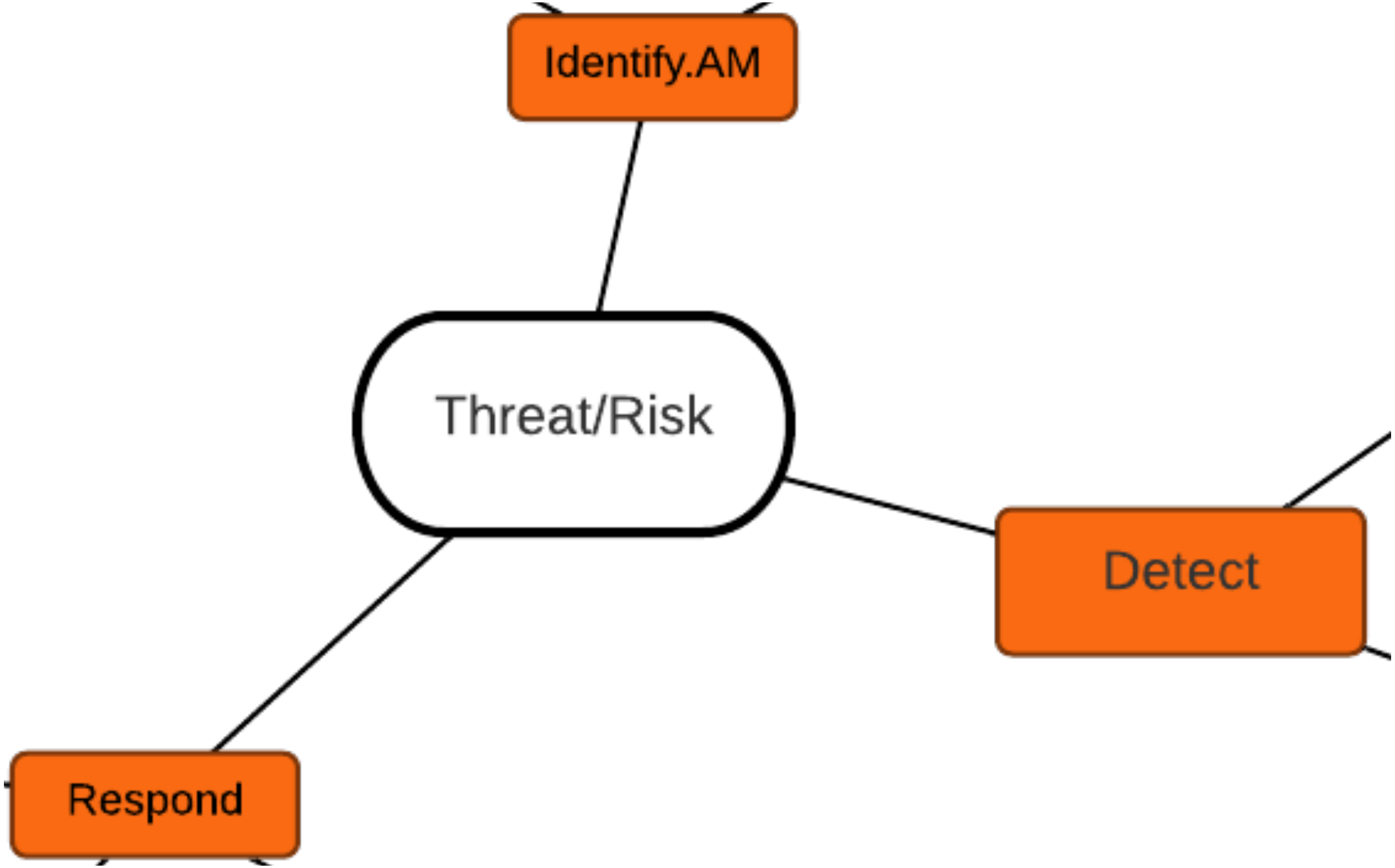
- Use a Mind Map (*or whatever floats your boat*)
- Use NIST Incident Response Framework
  - Identify
  - Detect
  - Respond

Using the Mind Map

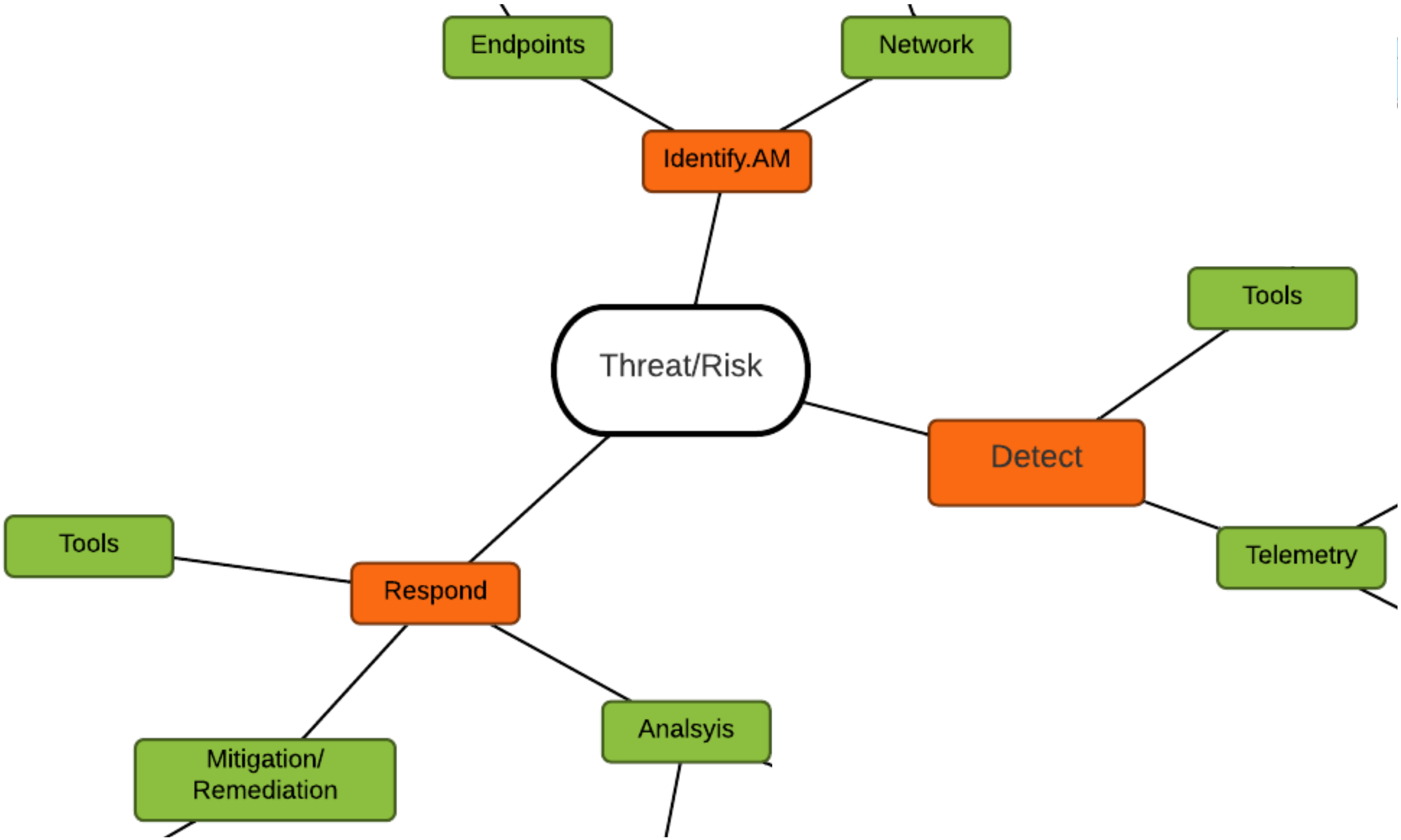
- Mind map is primarily a reference graph
- Graph view of requirements based on the 3 domains:
  - Identify.Asset Management
  - Detect
  - Respond
- You can use the graph to quickly identify where telemetry, information or activities belong



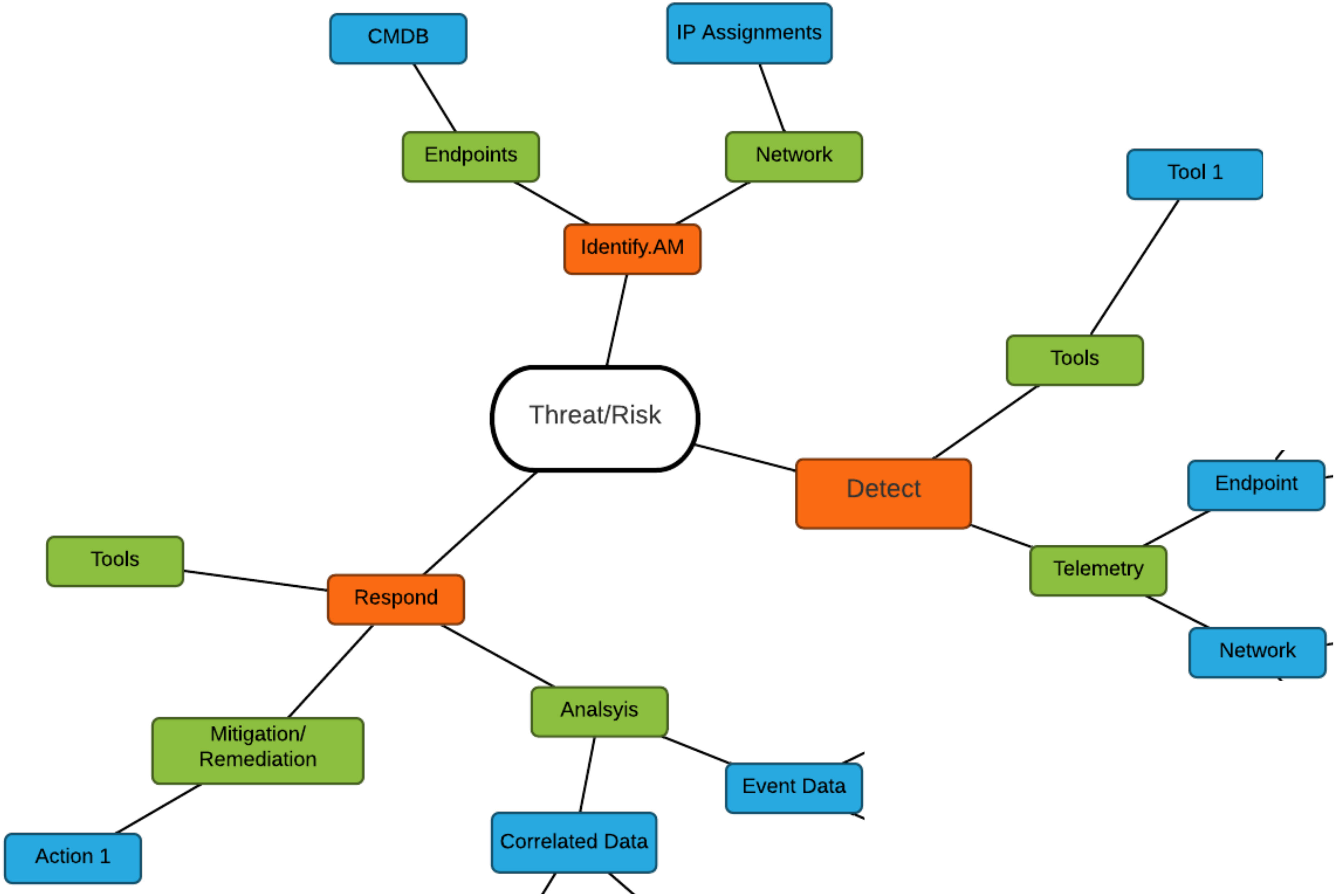
Threats versus Capabilities



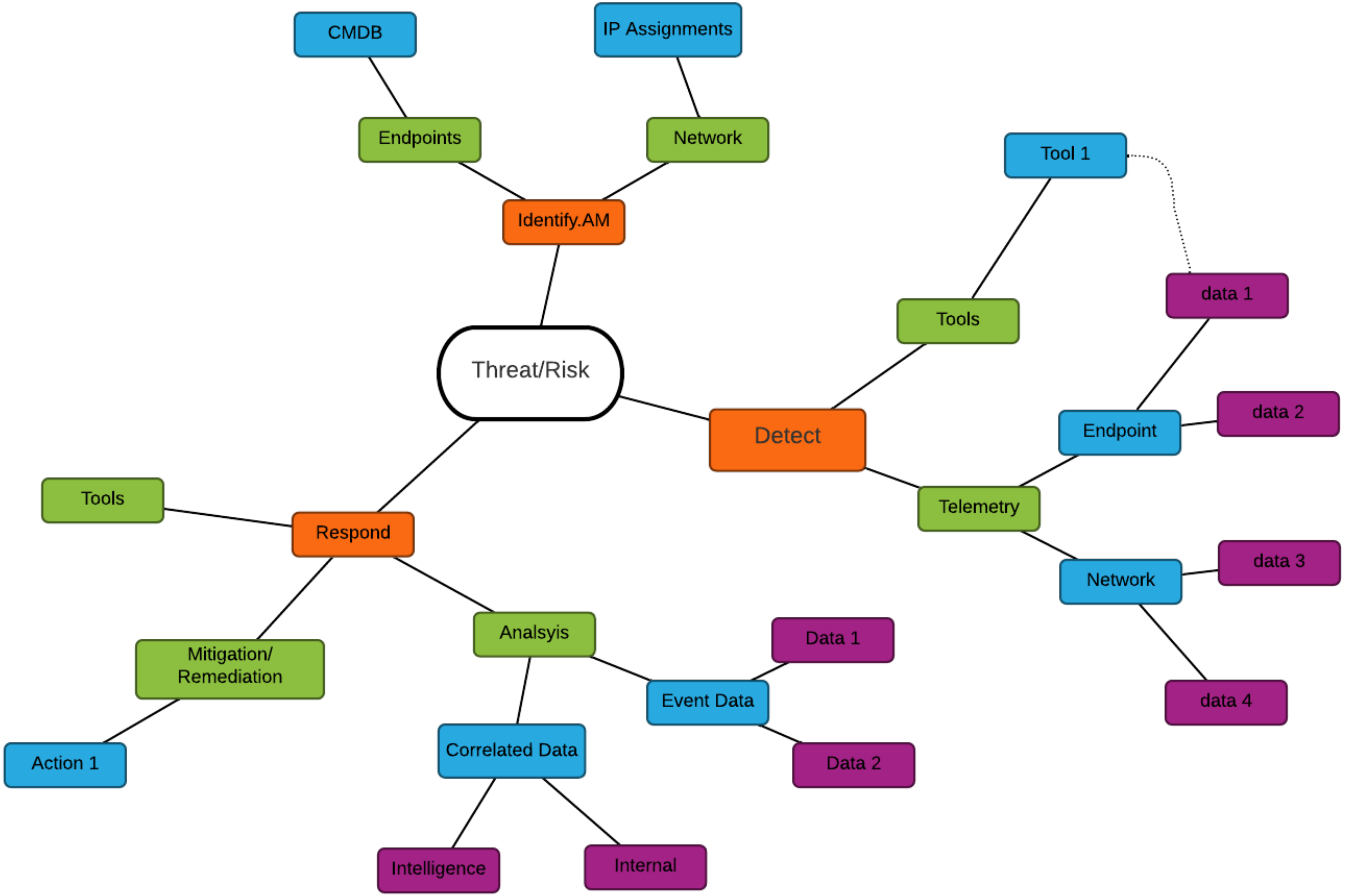
Threats versus Capabilities



Threats versus Capabilities

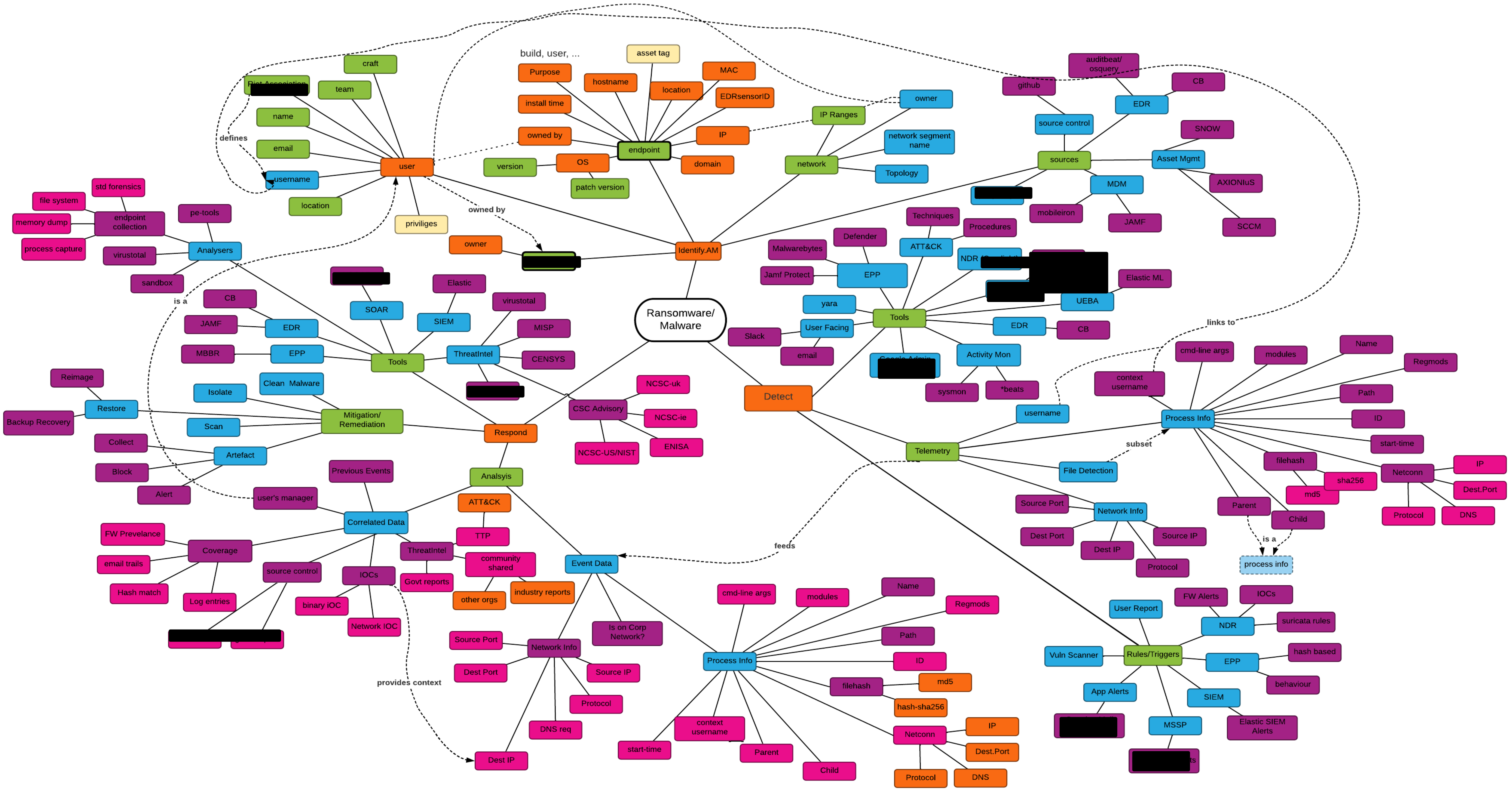


Threats versus Capabilities

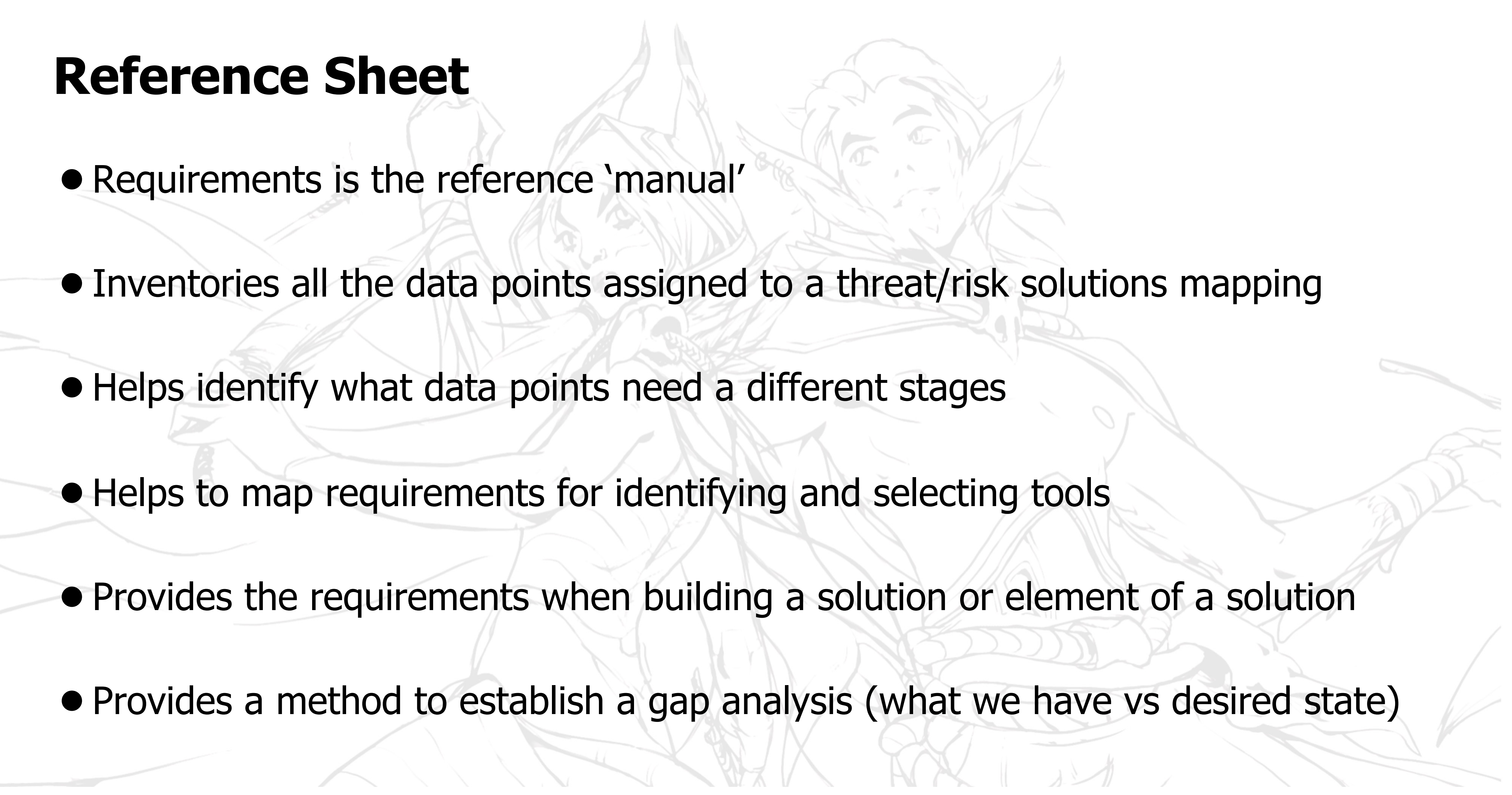


Threats versus Capabilities

BSides Dublin 2022



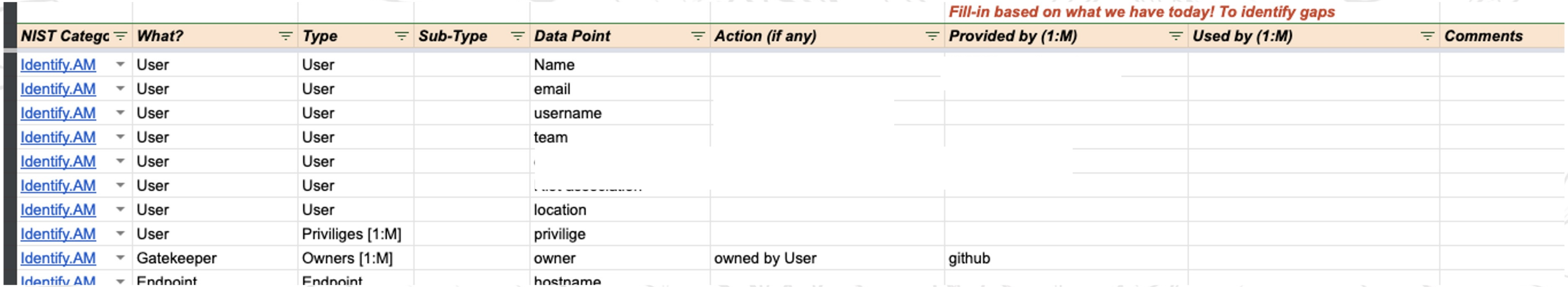
Reference Sheet



- Requirements is the reference ‘manual’
- Inventories all the data points assigned to a threat/risk solutions mapping
- Helps identify what data points need a different stages
- Helps to map requirements for identifying and selecting tools
- Provides the requirements when building a solution or element of a solution
- Provides a method to establish a gap analysis (what we have vs desired state)

Gap Analysis How-To

- Determined by completing “Provided by” & “Used by” columns
- Fill-in columns based on the availability and use of the data point
- Blanks are gaps we need to address



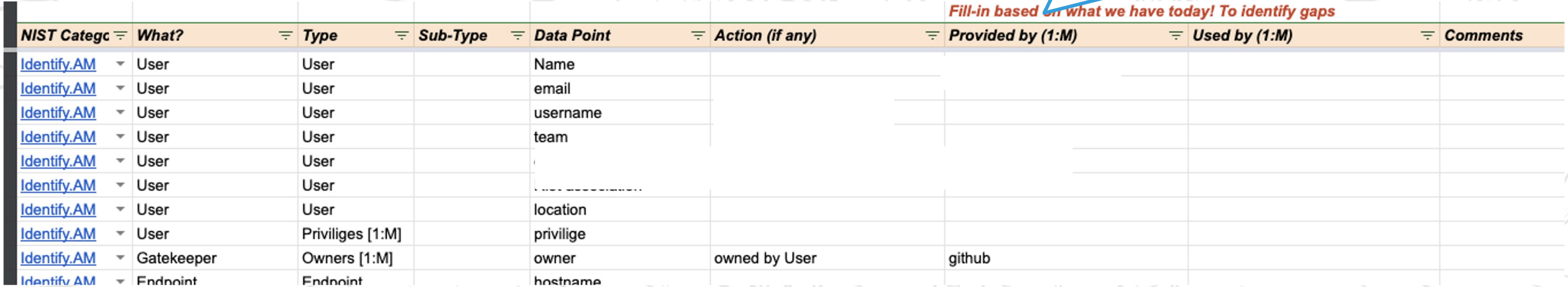
Fill-in based on what we have today! To identify gaps

NIST Catego	What?	Type	Sub-Type	Data Point	Action (if any)	Provided by (1:M)	Used by (1:M)	Comments
Identify.AM	User	User		Name				
Identify.AM	User	User		email				
Identify.AM	User	User		username				
Identify.AM	User	User		team				
Identify.AM	User	User		[redacted]				
Identify.AM	User	User		[redacted]				
Identify.AM	User	User		location				
Identify.AM	User	Priviliges [1:M]		privilige				
Identify.AM	Gatekeeper	Owners [1:M]		owner	owned by User	github		
Identify.AM	Endpoint	Endpoint		hostname				

Gap Analysis How-To: Provided by

Provided by

1. tell us where the information comes from (can be multiple sources): a tool (Carbon black); an app
2. Populate with source tools/apps that provide the data
3. Data can come from multiple sources



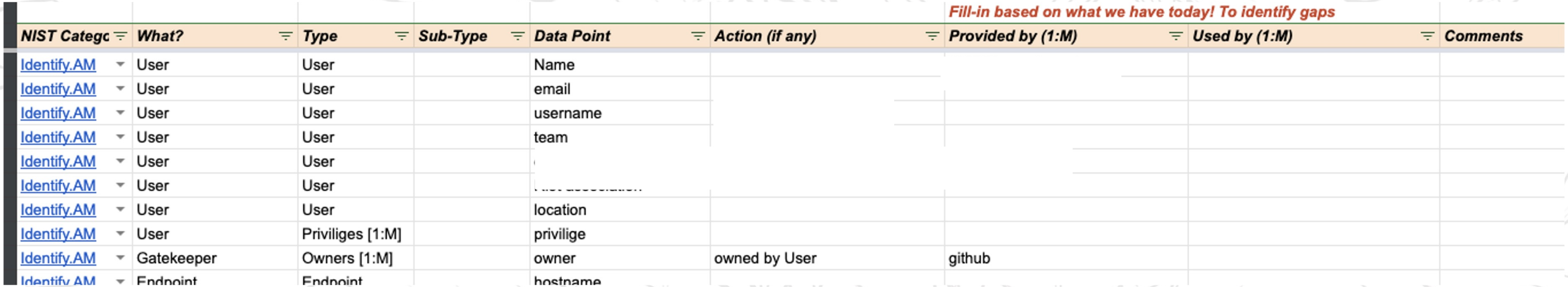
Fill-in based on what we have today! To identify gaps

NIST Catego	What?	Type	Sub-Type	Data Point	Action (if any)	Provided by (1:M)	Used by (1:M)	Comments
Identify.AM	User	User		Name				
Identify.AM	User	User		email				
Identify.AM	User	User		username				
Identify.AM	User	User		team				
Identify.AM	User	User		[redacted]				
Identify.AM	User	User		[redacted]				
Identify.AM	User	User		location				
Identify.AM	User	Priviliges [1:M]		privilige				
Identify.AM	Gatekeeper	Owners [1:M]		owner	owned by User	github		
Identify.AM	Endpoint	Endpoint		hostname				

Gap Analysis How-To: Used by

Used by

1. tell us where the information is used (can be multiple sources):Tool (carbon black), Incident Ticket (XSOAR)
2. Populate where the data is being used
3. Data can be used in multiple places

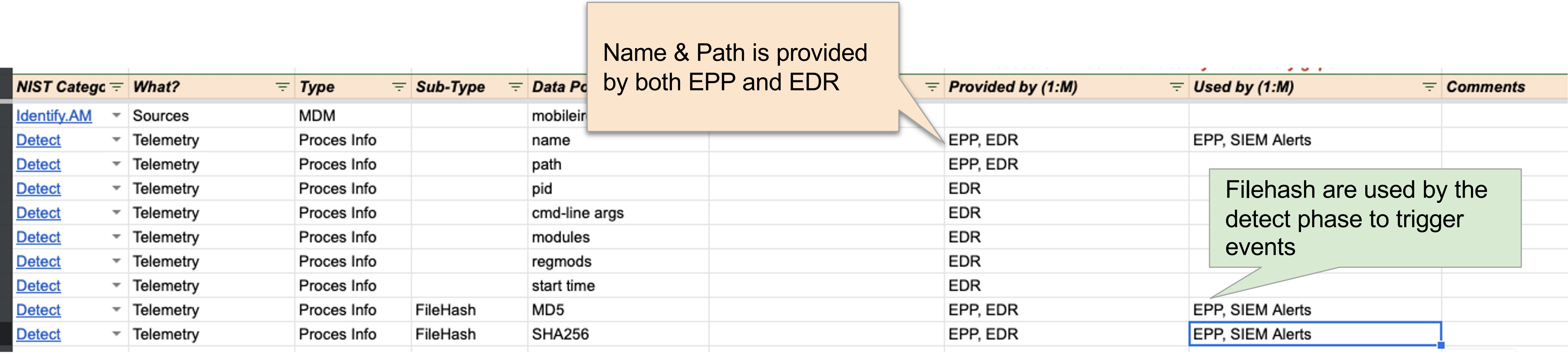


Fill-in based on what we have today! To identify gaps

NIST Catego	What?	Type	Sub-Type	Data Point	Action (if any)	Provided by (1:M)	Used by (1:M)	Comments
Identify.AM	User	User		Name				
Identify.AM	User	User		email				
Identify.AM	User	User		username				
Identify.AM	User	User		team				
Identify.AM	User	User						
Identify.AM	User	User		[illegible]				
Identify.AM	User	User		location				
Identify.AM	User	Priviliges [1:M]		privilige				
Identify.AM	Gatekeeper	Owners [1:M]		owner	owned by User	github		
Identify.AM	Endpoint	Endpoint		hostname				

Gap Analysis How-To: Example

- Example below shown
- We note that the detect telemetry for process info is primarily provided by EPP & EDR
- Detection uses name, md5 & sha256 from process info to trigger events

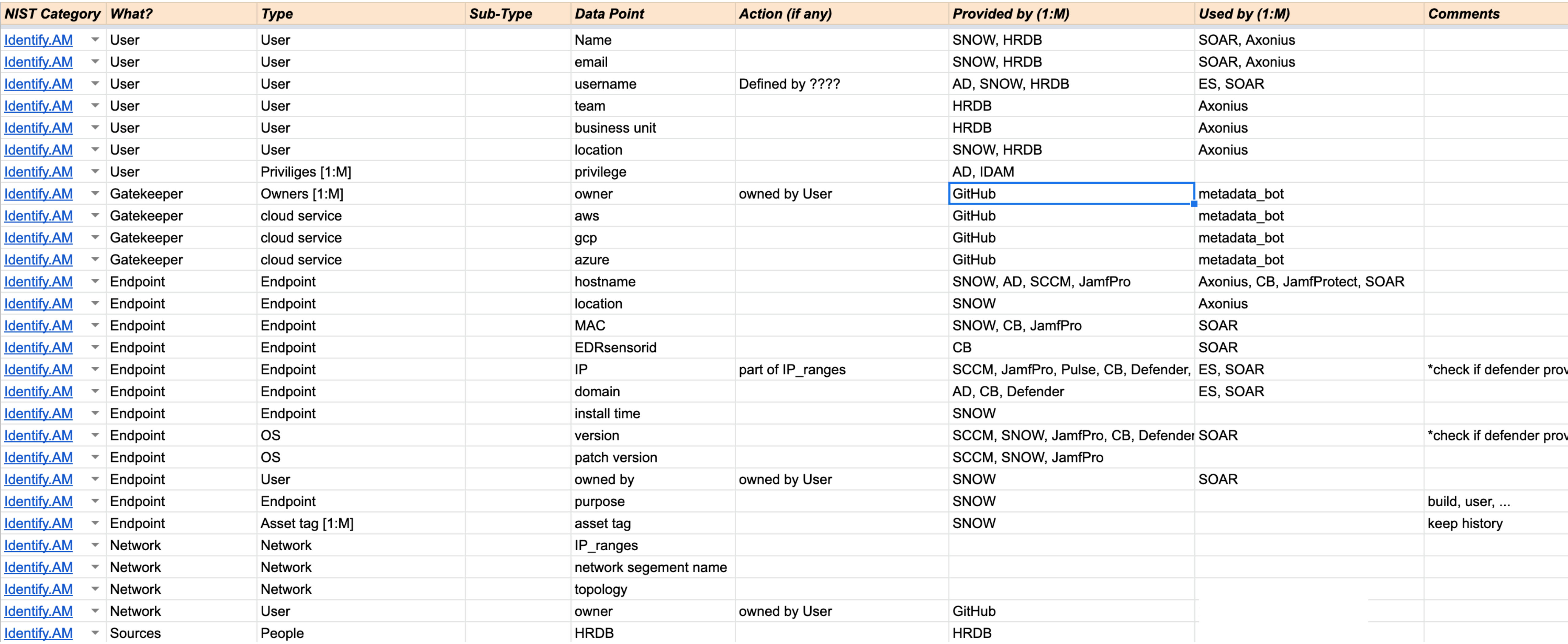


Name & Path is provided by both EPP and EDR

Filehash are used by the detect phase to trigger events

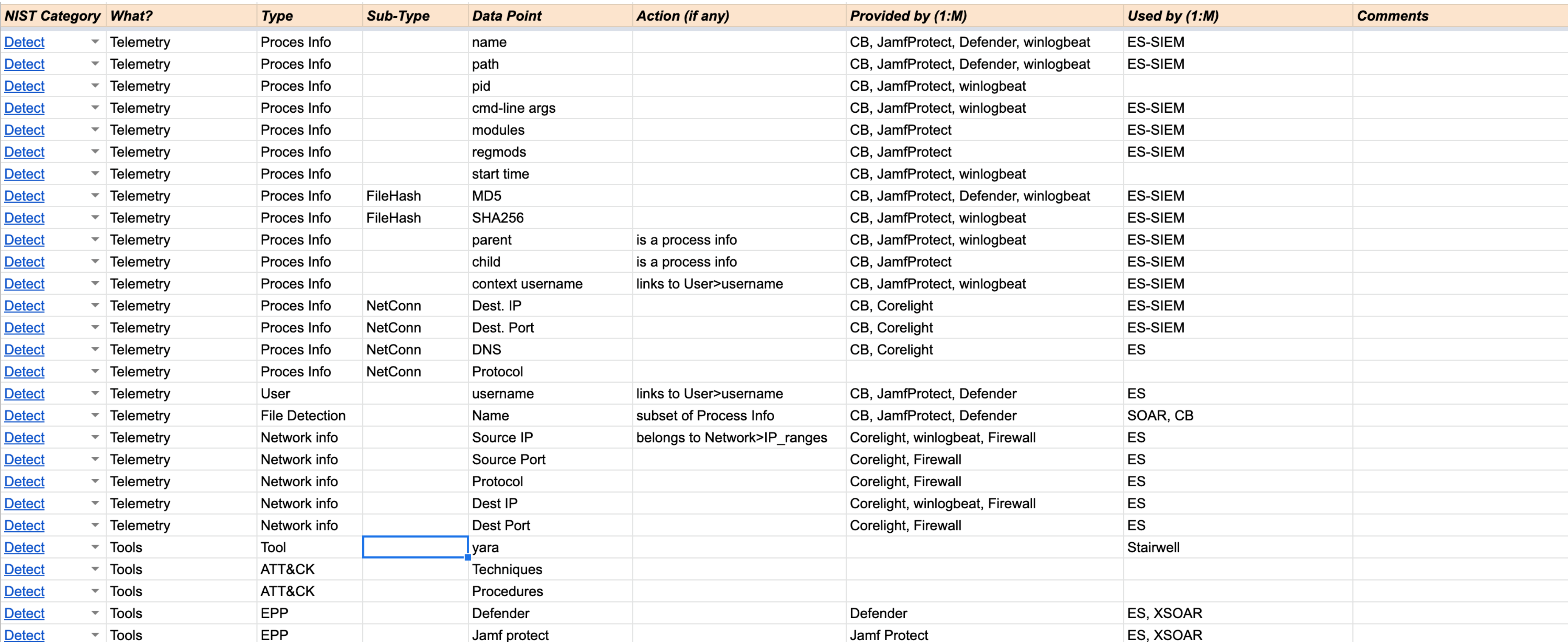
NIST Categc	What?	Type	Sub-Type	Data Po		Provided by (1:M)	Used by (1:M)	Comments
Identify.AM	Sources	MDM		mobileir				
Detect	Telemetry	Proces Info		name		EPP, EDR	EPP, SIEM Alerts	
Detect	Telemetry	Proces Info		path		EPP, EDR		
Detect	Telemetry	Proces Info		pid		EDR		
Detect	Telemetry	Proces Info		cmd-line args		EDR		
Detect	Telemetry	Proces Info		modules		EDR		
Detect	Telemetry	Proces Info		regmods		EDR		
Detect	Telemetry	Proces Info		start time		EDR		
Detect	Telemetry	Proces Info	FileHash	MD5		EPP, EDR	EPP, SIEM Alerts	
Detect	Telemetry	Proces Info	FileHash	SHA256		EPP, EDR	EPP, SIEM Alerts	

Threats versus Capabilities



NIST Category	What?	Type	Sub-Type	Data Point	Action (if any)	Provided by (1:M)	Used by (1:M)	Comments
Identify.AM	User	User		Name		SNOW, HRDB	SOAR, Axonius	
Identify.AM	User	User		email		SNOW, HRDB	SOAR, Axonius	
Identify.AM	User	User		username	Defined by ????	AD, SNOW, HRDB	ES, SOAR	
Identify.AM	User	User		team		HRDB	Axonius	
Identify.AM	User	User		business unit		HRDB	Axonius	
Identify.AM	User	User		location		SNOW, HRDB	Axonius	
Identify.AM	User	Priviliges [1:M]		privilege		AD, IDAM		
Identify.AM	Gatekeeper	Owners [1:M]		owner	owned by User	GitHub	metadata_bot	
Identify.AM	Gatekeeper	cloud service		aws		GitHub	metadata_bot	
Identify.AM	Gatekeeper	cloud service		gcp		GitHub	metadata_bot	
Identify.AM	Gatekeeper	cloud service		azure		GitHub	metadata_bot	
Identify.AM	Endpoint	Endpoint		hostname		SNOW, AD, SCCM, JamfPro	Axonius, CB, JamfProtect, SOAR	
Identify.AM	Endpoint	Endpoint		location		SNOW	Axonius	
Identify.AM	Endpoint	Endpoint		MAC		SNOW, CB, JamfPro	SOAR	
Identify.AM	Endpoint	Endpoint		EDRsensorid		CB	SOAR	
Identify.AM	Endpoint	Endpoint		IP	part of IP_ranges	SCCM, JamfPro, Pulse, CB, Defender,	ES, SOAR	*check if defender prov
Identify.AM	Endpoint	Endpoint		domain		AD, CB, Defender	ES, SOAR	
Identify.AM	Endpoint	Endpoint		install time		SNOW		
Identify.AM	Endpoint	OS		version		SCCM, SNOW, JamfPro, CB, Defender	SOAR	*check if defender prov
Identify.AM	Endpoint	OS		patch version		SCCM, SNOW, JamfPro		
Identify.AM	Endpoint	User		owned by	owned by User	SNOW	SOAR	
Identify.AM	Endpoint	Endpoint		purpose		SNOW		build, user, ...
Identify.AM	Endpoint	Asset tag [1:M]		asset tag		SNOW		keep history
Identify.AM	Network	Network		IP_ranges				
Identify.AM	Network	Network		network segement name				
Identify.AM	Network	Network		topology				
Identify.AM	Network	User		owner	owned by User	GitHub		
Identify.AM	Sources	People		HRDB		HRDB		

Threats versus Capabilities



NIST Category	What?	Type	Sub-Type	Data Point	Action (if any)	Provided by (1:M)	Used by (1:M)	Comments
Detect	Telemetry	Proces Info		name		CB, JamfProtect, Defender, winlogbeat	ES-SIEM	
Detect	Telemetry	Proces Info		path		CB, JamfProtect, Defender, winlogbeat	ES-SIEM	
Detect	Telemetry	Proces Info		pid		CB, JamfProtect, winlogbeat		
Detect	Telemetry	Proces Info		cmd-line args		CB, JamfProtect, winlogbeat	ES-SIEM	
Detect	Telemetry	Proces Info		modules		CB, JamfProtect	ES-SIEM	
Detect	Telemetry	Proces Info		regmods		CB, JamfProtect	ES-SIEM	
Detect	Telemetry	Proces Info		start time		CB, JamfProtect, winlogbeat		
Detect	Telemetry	Proces Info	FileHash	MD5		CB, JamfProtect, Defender, winlogbeat	ES-SIEM	
Detect	Telemetry	Proces Info	FileHash	SHA256		CB, JamfProtect, winlogbeat	ES-SIEM	
Detect	Telemetry	Proces Info		parent	is a process info	CB, JamfProtect, winlogbeat	ES-SIEM	
Detect	Telemetry	Proces Info		child	is a process info	CB, JamfProtect	ES-SIEM	
Detect	Telemetry	Proces Info		context username	links to User>username	CB, JamfProtect, winlogbeat	ES-SIEM	
Detect	Telemetry	Proces Info	NetConn	Dest. IP		CB, Corelight	ES-SIEM	
Detect	Telemetry	Proces Info	NetConn	Dest. Port		CB, Corelight	ES-SIEM	
Detect	Telemetry	Proces Info	NetConn	DNS		CB, Corelight	ES	
Detect	Telemetry	Proces Info	NetConn	Protocol				
Detect	Telemetry	User		username	links to User>username	CB, JamfProtect, Defender	ES	
Detect	Telemetry	File Detection		Name	subset of Process Info	CB, JamfProtect, Defender	SOAR, CB	
Detect	Telemetry	Network info		Source IP	belongs to Network>IP_ranges	Corelight, winlogbeat, Firewall	ES	
Detect	Telemetry	Network info		Source Port		Corelight, Firewall	ES	
Detect	Telemetry	Network info		Protocol		Corelight, Firewall	ES	
Detect	Telemetry	Network info		Dest IP		Corelight, winlogbeat, Firewall	ES	
Detect	Telemetry	Network info		Dest Port		Corelight, Firewall	ES	
Detect	Tools	Tool		yara			Stairwell	
Detect	Tools	ATT&CK		Techniques				
Detect	Tools	ATT&CK		Procedures				
Detect	Tools	EPP		Defender		Defender	ES, XSOAR	
Detect	Tools	EPP		Jamf protect		Jamf Protect	ES, XSOAR	

Understanding of Organization’s Capabilities

Focus Making Good Tooling Decisions

Framework to PoC New Tools

“identify **pertinent information**, prioritize it, draw conclusions from it, and communicate it...”

Amy E. Herman

@Fvt

- tvfischer+sec at gmail[.]com
- tvfischer at pm[.]me
- keybase.io/fvt