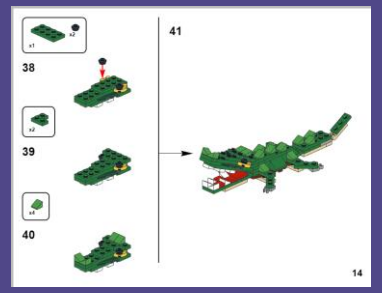
Prioritise risk through structured threat content

Gert-Jan Bruggink
University of Oslo
19 May 2022

Why am I here?

- Puzzle solving & scenario-based thinking
- Practitioner lessons learned on using structured taxonomies
- Detailing how structured content can be produced and used



Who am I?

Gert-Jan Bruggink

cyber threat cartographer

&

founder Venation

Practitioner & continously curious
Cyber threat intelligence (CTI) based risk management.
Intelligence-led Red Teaming.
Capability building & leadership.
Strategic change through (CTI, SOC & Cyber) transformation programs.
High tech, manufacturing, financial services, governmental.
Father x 2, Entrepreneurship, Gaming, Painting, Lego, Meme's.

@gertjanbruggink
github.com/gertjanbruggink
/gertjanbruggink

What am I going to talk about?

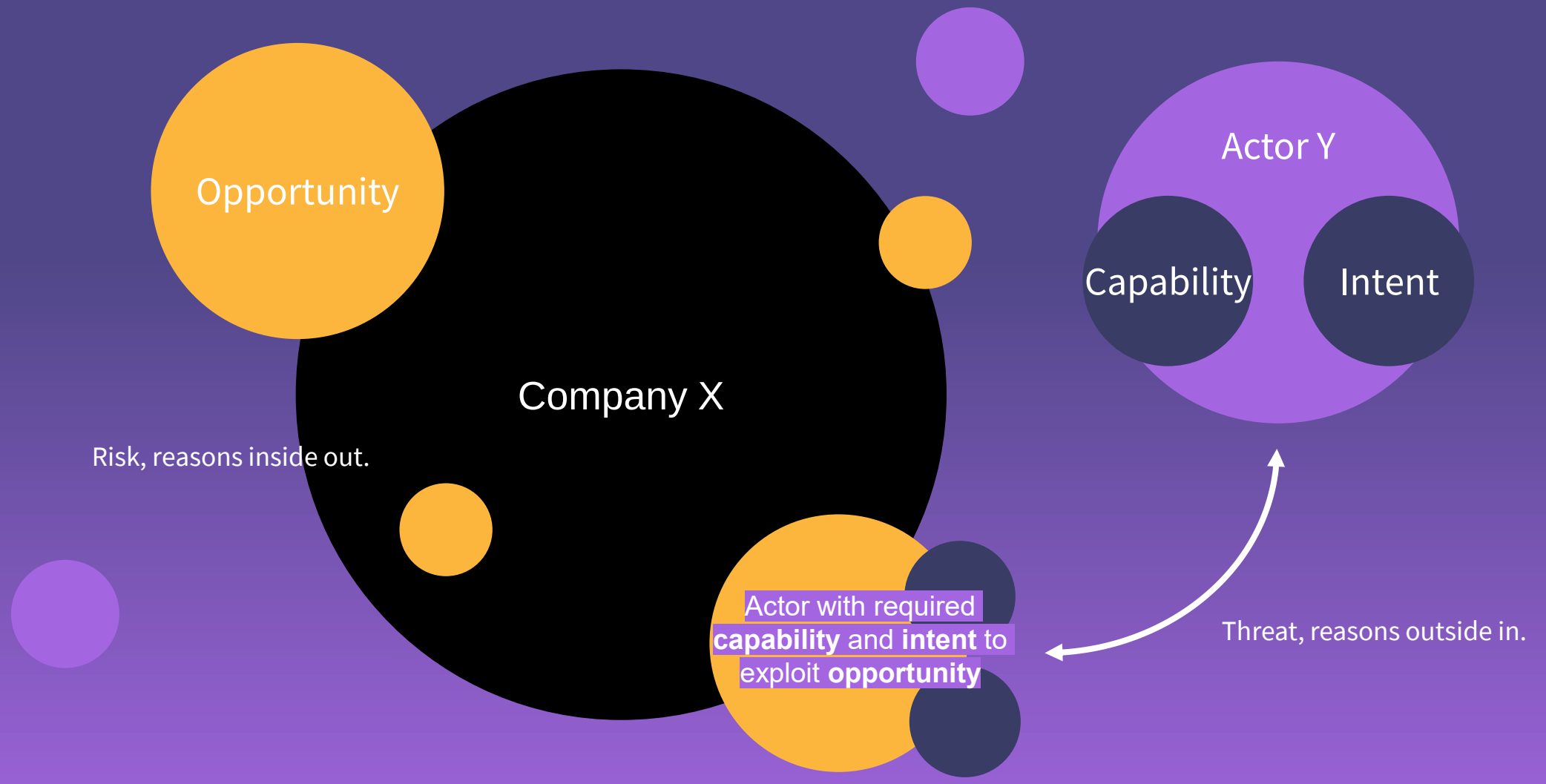
- ✓ Understanding ‘threat’
- ✓ Structuring threat into content
- ✓ Prioritising digital risk through content

Understanding ‘threat’

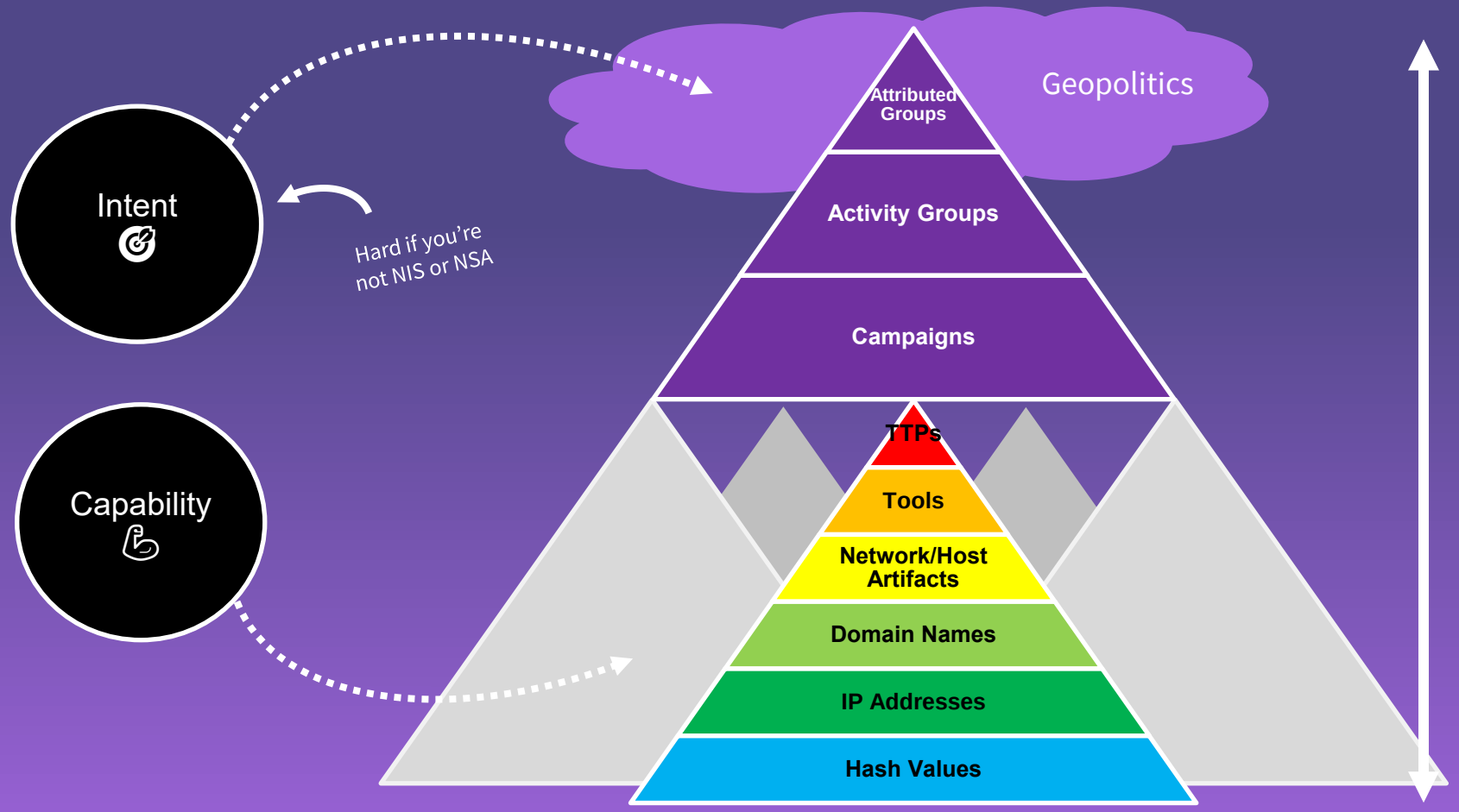
Explicit consideration of capability and intent helps reduce grey areas in risk

- Risk = Impact x likelihood
- Risk = Impact x likelihood (threat x asset x vulnerability)
- **Risk = Impact x likelihood x threat (capability x intent x opportunity)**
- Risk = Threat x vulnerability/capacity
- Risk = Impact x likelihood

Understanding (cyber) threat



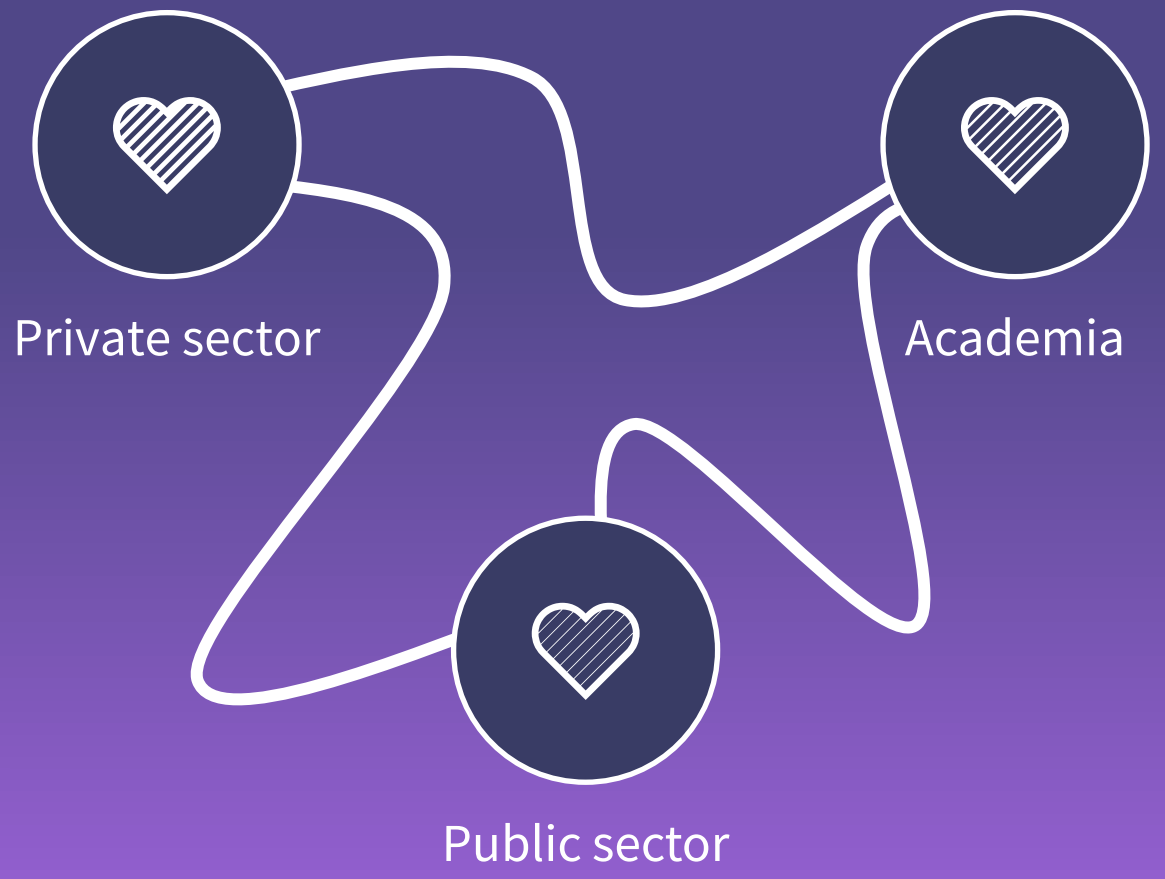
Current approach



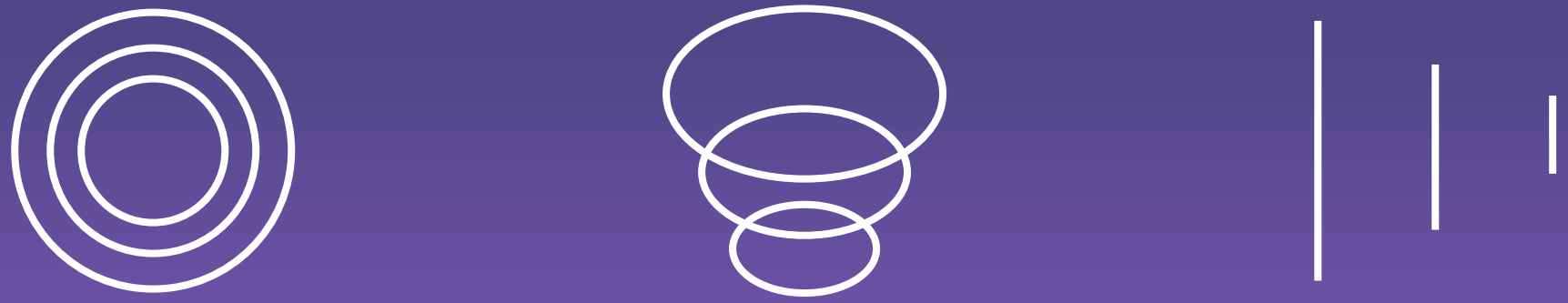
Exploring a better story to talk about capability & intent

Extending the 'Pyramid of pain'

The industry problem

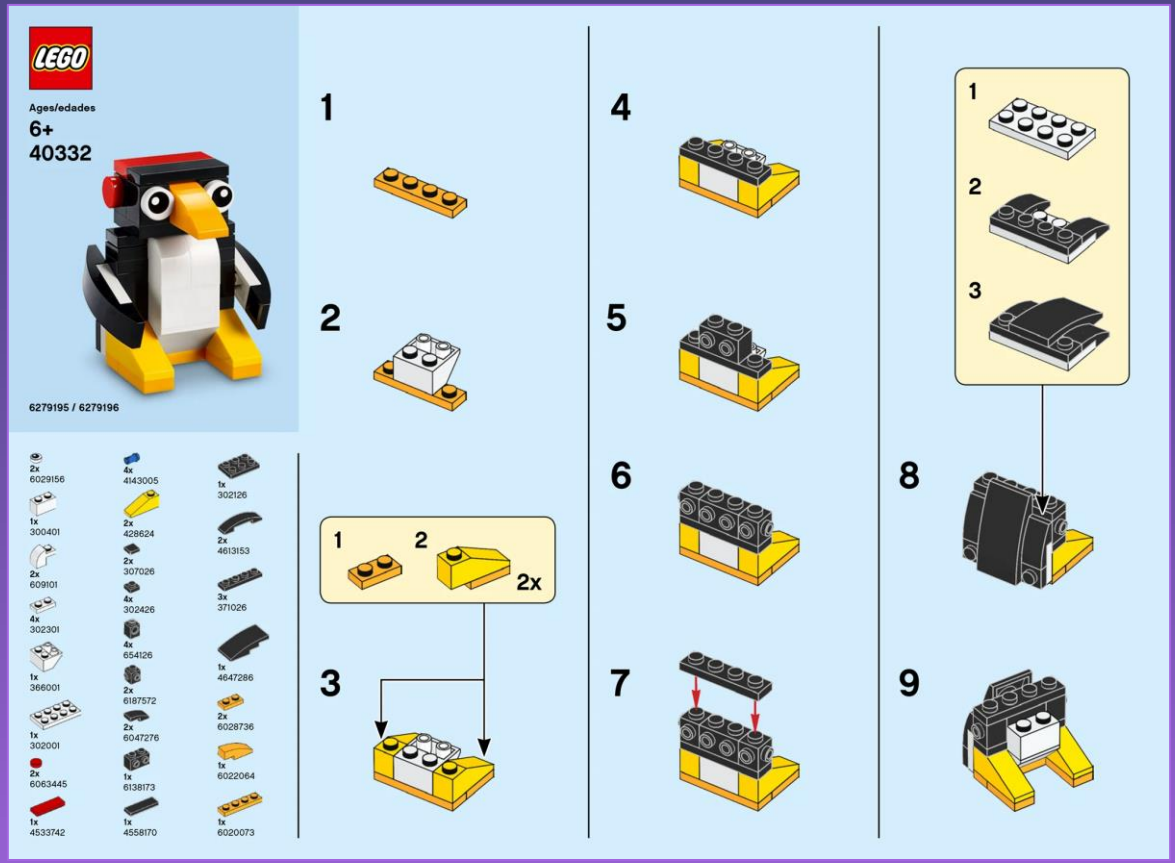


Current trend: more details



Different perspectives. Same situation.

Future trend:
Simplified, end-to-end, storytelling



Structuring threat into content

‘Storytelling’ content

Means:
Deliverable is
Structured threat scenarios

End:
Guide security Investment

Exploring a scenario-based structure

```
# Title, detailing what happens in this scenario, by whom, and directed by
what objective

## Overview
---

**Identifier:** YEARMONTH-NAME (e.g. 202110-SCENARIO_HAPPENS_ABC)

**Timestamp:** YEAR-MONTH-DAY - time (e.g. 2021-11-11, 10:00)

**Author(s):** [Venation](https://venation.digital/)

**Industry Tagging:**
'Financial Services'
'Customer banking'
'Maritime'
'High Tech'
'Semiconductors'

**Scenario Tagging:**
'APT28'
'Mobile malware'
'Watering hole'
'Application access token'

<!---
Tags for each scenario are listed here, used by the back-end to correlate
analyse scenario's. For example to determine trending scenarios per run.
Tagging should consist of key activities in each scenario, e.g. 'exploit
vulnerability' or 'ransomware'
-->

## Scenario breakdown
---

**Objective(s):**

Any_relevant_input_is_detailed_here

<!---
Detailing the most-likely objective(s) of the scenario. Should there be mo
than one objective, items shall be listed through numbering and ordered fr
most-likely to least likely.
-->

**Summary:**

Any_relevant_input_is_detailed_here

<!---
The summary describes the why, how, what for each scenario. The text shall
3 paragraphs, aligned with the why-how-what, and should consist of 2 rows
text per paragraph. Rows of text written shall follow BLUF writing and act
voice.
-->

**Functions and/or systems targeted:**

Any_relevant_input_is_detailed_here

<!---
```

Title, detailing what happens in this scenario, by whom, and directed by what objective

Overview

Identifier: YEARMONTH-NAME (e.g. 202110-SCENARIO_HAPPENS_ABC)

Timestamp: YEAR-MONTH-DAY - time (e.g. 2021-11-11, 10:00)

Author(s): Venation

Industry Tagging: 'Financial Services' 'Customer banking' 'Maritime' 'High Tech' 'Semiconductors'

Scenario Tagging: 'APT28' 'Mobile malware' 'Watering hole' 'Application access token'

Scenario breakdown

Objective(s):

Any_relevant_input_is_detailed_here

Summary:

Any_relevant_input_is_detailed_here

Functions and/or systems targeted:

Any_relevant_input_is_detailed_here

Scenario sequence:

1. Step - Reconnaissance
2. Step - Initial access
3. Step - Lateral movement

Adversary playbook

Considerations:

Any_relevant_input_is_detailed_here

Associated threat actor profile:

Name	Category	Capability	Intent	Comments
APT28	State-sponsored entity	High	High	TBD

TTP breakdown:

Tactic_ID	Tactic_ID	Technique_ID	Technique	Procedure(s)	Detection Opportunity
TA0043	Reconnaissance	T1589	Gather Victim Identity Information	Acquired mobile phone numbers of potential targets, possibly for mobile malware or additional phishing operations.	Detection_tagging

Example scenario format, available via: https://github.com/venation-digital/

Markdown format

Quick demo 1/4: Overview

```
# Title, detailing what happens in this scenario, by whom, and directed by what objective

## Overview
---
**Identifier:** YEARMONTH-NAME (e.g. 202110-SCENARIO_HAPPENS_ABC)

**Created:** {{date}} {{time}}

**Modified:** YEAR-MONTH-DAY (e.g. 2021-11-11, 10:00)

**Status:** #Status/Open

**Author(s):** [Venation](https://venation.digital/)

**Category:**
#Category/Example

<!---
Tag all items that would be relevant for the scenario on a high level. Usecase is sorting and structuring content.
-->

**Tags:**
#Tags/Example

<!---
Tag all items that would be relevant for the scenario on a low level. Usecase is performing deeper research between different scenarios.
-->

**Priority Intelligence Requirement(s):**
<!---
Describe any relevant (priority) intelligence requirements that link to this scenario.

Preferably standardise on Intel471's 'General Intelligence Requirements Handbook'.
-->
```

- ✓ Operational tracking
- ✓ Tags for future research
- ✓ Priority intelligence requirement relation

Source
https://github.com/venation-digital/

Quick demo 2/4: Scenario breakdown

```
## Scenario breakdown
---

**Objective(s):**

Any_relevant_input_is_detailed_here

<!---
Detailing the most-likely objective(s) of the scenario. Should there be more than one objective, items shall be listed through numbering
and ordered from most-likely to least likely.
-->

**Summary:**

Any_relevant_input_is_detailed_here

<!---
The summary describes the why, how, what for each scenario. The text shall be 3 paragraphs, aligned with the why, how, what, and should
consist of 2 rows of text per paragraph. Rows of text written shall follow BLUF writing and active voice.
-->

**Industry Tagging:**
#Industry/Example


**Functions and/or systems targeted:**

Any_relevant_input_is_detailed_here

<!---
If specific functions or systems are targeted, they are broken down here.
-->

**Scenario walkthrough:**

* Step - Reconnaissance
* Step - Initial access
* Step - Lateral movement

<!---
Providing a listed walkthrough of events, describing how it happens, what we know and what we don't know. Important to note, this is not
a sequence. A sequence would imply that all events happen lineair, while in reality we know that this is never the case.
-->

**Considerations:**

Any_relevant_input_is_detailed_here

<!---
Annotate all relevant considerations for this particular scenario.
-->
```

- ✓ Walking through the ‘scenario’ with a narrative
- ✓ Tagging industry and functions for customization
- ✓ Extensive research to ‘fill in the gaps’

Source
https://github.com/venation-digital/

Quick demo 3/4: Adversary playbook

```
## Adversary playbook
---
**Associated threat actor profile:**

| Name    | Tag | Category | Capability  | Intent | Comments |
| --------| --- |-------------| -----| -----| --- |
| APT28 | #Actor/Example | State-sponsored entity | High | High | TBD |

**TTP breakdown:**

| Tactic_ID | Tactic | Technique_ID | Technique | Procedure(s) | Detection Opportunity | Comments
| --------|-------------| -----|-----| -----|-----|-----|
| TA0043 | Reconnaissance | T1589 | Gather Victim Identity Information  | Acquired mobile phone numbers of
for mobile malware or additional phishing operations. | Detection_tagging | TBD |
| TA0001 | Initial Access  | T1189 | Drive-by Compromise | Use watering hole attack to gain initial access
IP range. | Detection_tagging | TBD |
| TA0008 | Lateral Movement | T1550.001 | Use Alternate Authentication Material: Application Access Token
applications that abused OAuth access tokens to gain access to target email accounts. | Detection_tagging | TBD |
<!---
Based on the listed scenario sequence, describing what actually happened or is forecasted to happen in the event.

More details on tactic & technique referencing, please visit: [https://attack.mitre.org/](https://attack.mitre.org/)
-->
```

- ✓ Tagging groups with known association
- ✓ Including techniques & procedures, mapped to ATT&CK – emphasis on procedures

TAC integration

Source
https://github.com/venation-digital/

Quick demo 4/4: Other

```
## Other
---
**Wrap-up:**

Any_relevant_input_is_detailed_here

**Sources:**

* LINKED_URL

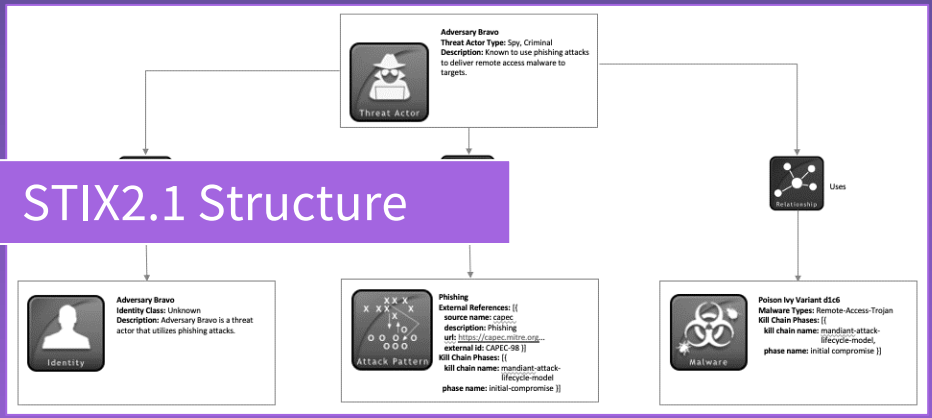
<!---
List all relevant and available OPEN-SOURCE source references.
-->


**JSON:**

```{toggle}
{
  "firstName": "John",
  "lastName": "Smith",
  "age": 25
}
```
```

- ✓ Relevant final items for the scenario
- ✓ Listing sources where possible
- ✓ JSON tagging placeholder

STIX2.1 Structure



Source
https://github.com/venation-digital/

Mark down is unreadable, what's next?

Markdown format

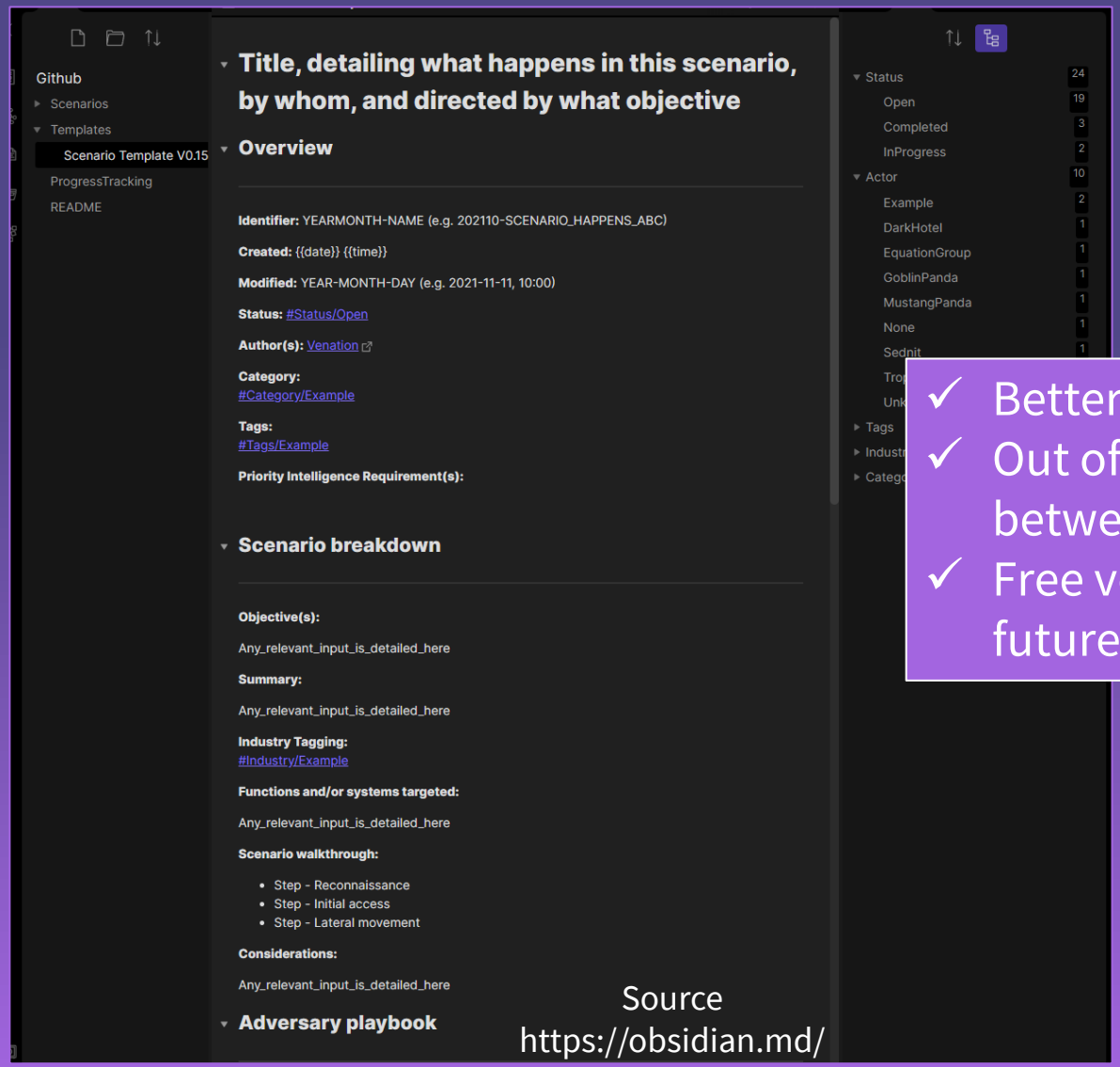
Ingest in open source notekeeping tool

Production!

OBSIDIAN

https://obsidian.md/

Load existing template into tool



Source
https://obsidian.md/

- ✓ Better fit for production
- ✓ Out of the box tagging links between scenarios
- ✓ Free version already useful for future audience

Production of a single scenario

Identifier: 202112-SKIPTHEGAP

Created: 2021-12-03

Modified: 2022-05-06

Status: #Status/Completed

Author(s): Venation

Category:
#Category/Malware/Air-gap/Air-gapTargeting

Tags:
#Tags/Malware/Air-gap
#Tags/Malware/USB

Priority Intelligence Requirement(s):
Identify characteristics of existing, new and emerging malware campaigns
gapped infrastructure.

Making sure overview details are consistent

Objective(s):

The objective of this scenario is to gain access to an air-gapped network.

Summary:

This scenario details how malware, or malware frameworks, implements an offline, covert communication mechanism between an air-gapped system and an attacker that is bi-directional. Specifically, it emphasises automated execution: getting malicious code executed just by connecting a malicious USB drive into a computer to compromise an air-gapped system.

All frameworks devised unique ways to reach the target air-gapped network and execute malware on a first system. They all have one thing in common, though: they all used weaponized USB drives. The main difference between connected and offline frameworks is how the drive is weaponized in the first place. Connected frameworks usually deploy a component on the connected system that will monitor the insertion of new USB drives and automatically place the malicious component needed to compromise the air-gapped system.

Industry Tagging:
#Industry/Manufacturing
#Industry/Energy

Functions and/or systems targeted:

All known malware frameworks included in this scenario focus on Microsoft Windows systems.

Scenario walkthrough:

- **Initial compromise**: An attacker targets users through one of the following: phishing with malicious attachment, human asset installation or watering hole attacks. Gaining access to an internet-connected system that is connected alongside the air-gapped network. Using the Establishing a persistent shell on a system that connects to the C&C server. Spearphishing using malicious attachments.
- **Weaponize USB drives**: Once compromised, that system is used to weaponize USB drives with a malicious payload and some mechanism to compromise the next target: the air-gapped system. Should the scenario be executed from a **assume breach** perspective, then the scenario initiates here.
- **Compromise air-gapped system**: Air-gapped system is compromised through usb drive injection. There are no Once the malware is l e malware that enable that most of the frame l at system startup or lo tall and persist in ne ameworks present the tall or execute new in already

Breaking down the how, adding research where required

Adversary playbook

Associated threat actor profile:

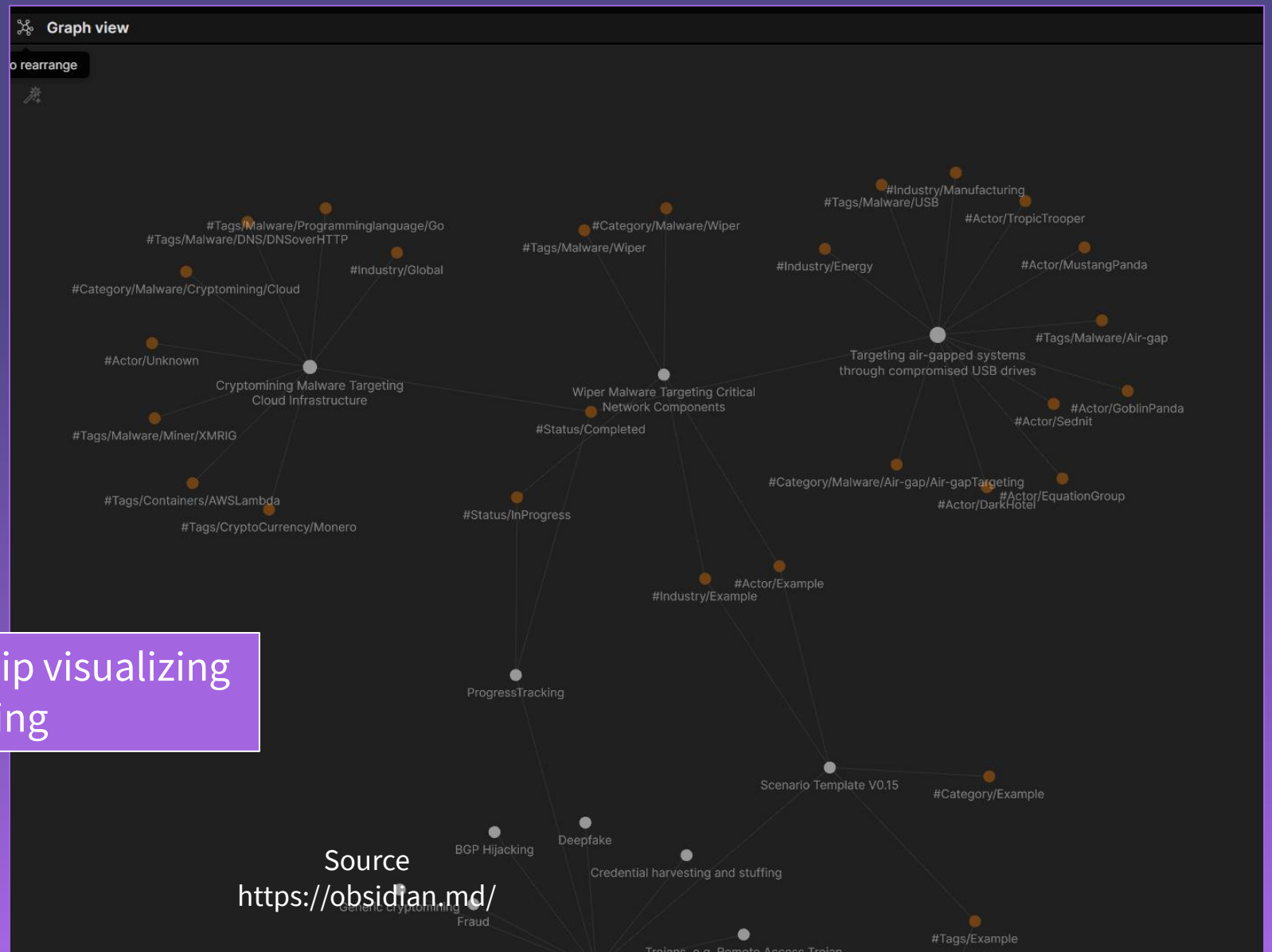
Name	Tag	Category	Capability	Intent	Comments
DarkHotel	#Actor/DarkHotel	State-sponsored entity	High	High	'Retro' campaign in 2017-2019, 'Ramsay' campaign in 2019-2020.
Sednit	#Actor/Sednit	State-sponsored entity	High	High	'USBStealer' campaign in 2005-2015.
Tropic Trooper	#Actor/TropicTrooper	State-sponsored entity	High	High	'USBFerry' campaign in 2014-2020.
Equation Group	#Actor/EquationGroup	State-sponsored entity	High	High	'Fanny' campaign in 2008-2012.
Goblin Panda	#Actor/GoblinPanda	State-sponsored entity	High	High	'USBCulprit' campaign in 2014-2019.
Mustang Panda	#Actor/MustangPanda	State-sponsored entity	High	High	'PlugX' campaign in 2018-2020.

TTP breakdown:

Tactic_ID	Tactic	Technique_ID	Technique	Procedure(s)	Detection Opportunity	Comments
TA0043	Reconnaissance	T1589	Gather Victim Identity Information	Acquired names and email addresses of potential targets for malware or additional	Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial	NA
TA0001	Ini					

Breaking down the how, research intelligence gaps

Mandatory cool spider chart

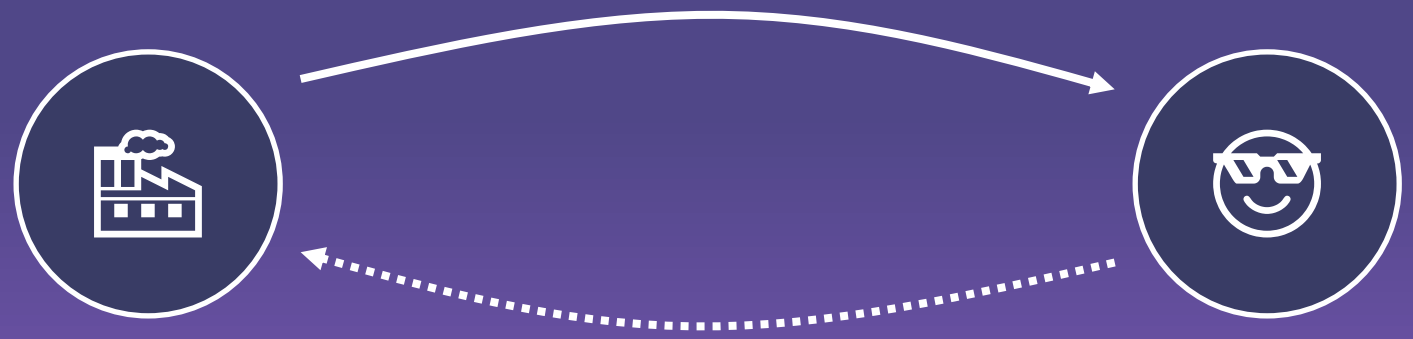


Out of the box relationship visualizing based on tagging

Source
https://obsidian.md/

Prioritising digital risk through content

So, how does this work in real life?



Production workflow

CTI team using a scenario-based approach

Vendor

Client

Our workflow

Vendor

Monthly threat assessment on industry verticals & new developments

Develop and/or adjust into scenario deliverables

Quality flow

Deploy to production

Their workflow

Client

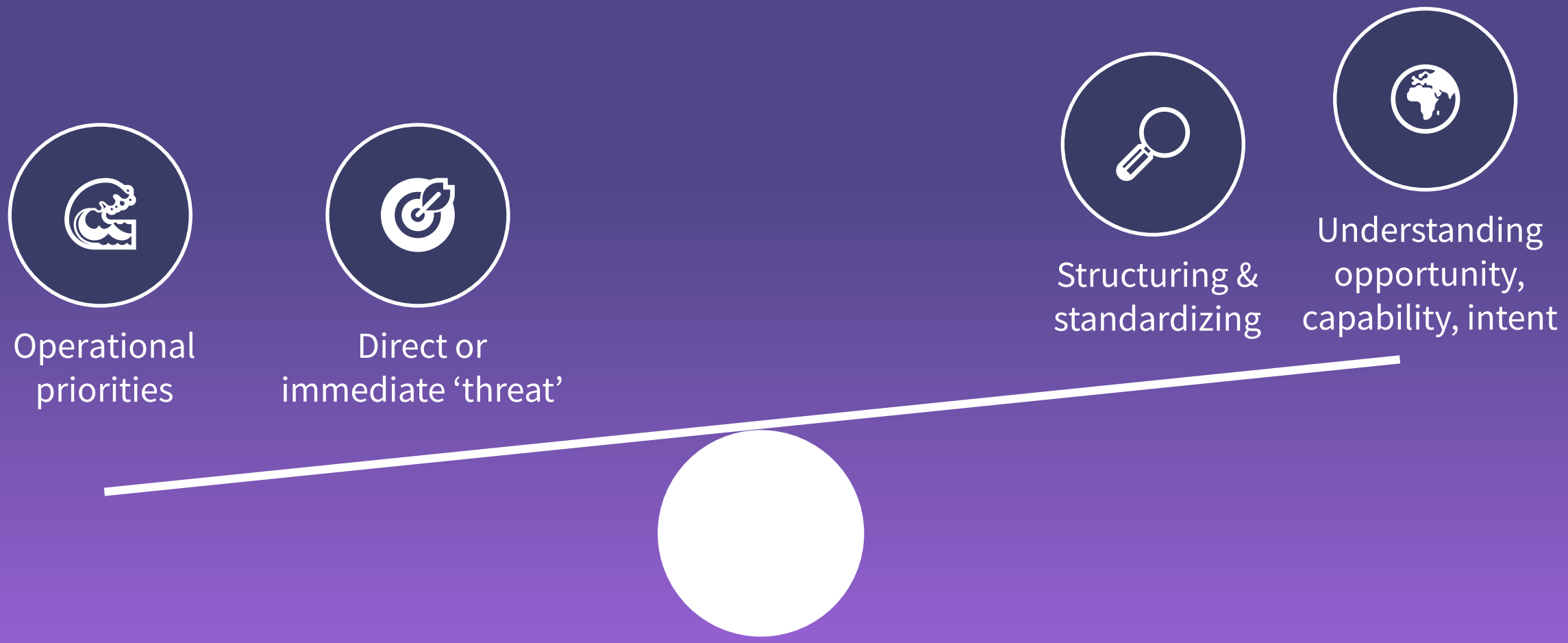
Part of an existing process, not just CTI

Priorities & stakeholder management

Yearly threat assessment (if even!)

Fast paced environment

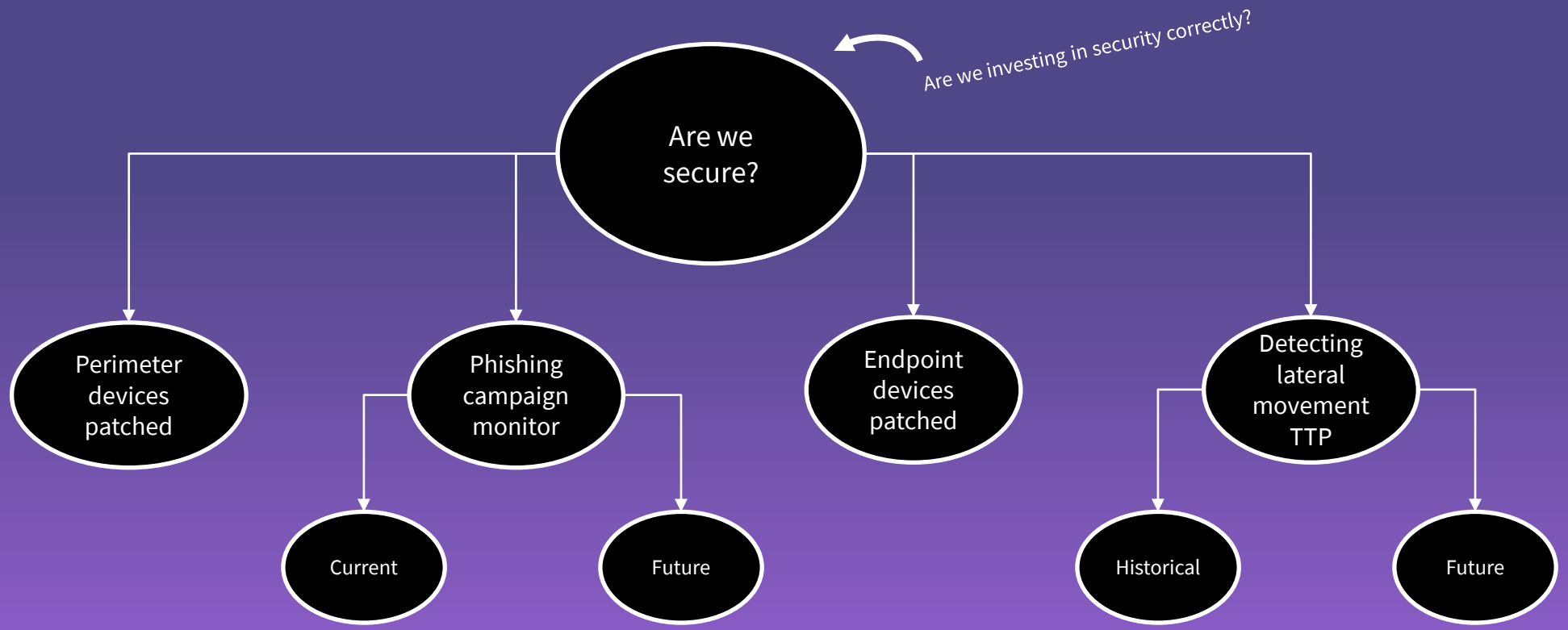
Managing risk is complicated



Stop asking big questions, start asking small questions

From this:

To this:



Bayesian question clustering

Scenarios provide a common ‘story’ to prioritise investment

From

Subjective

To

Qualitative

Scenario breakdown *(e.g. objectives, targets, walkthrough)*

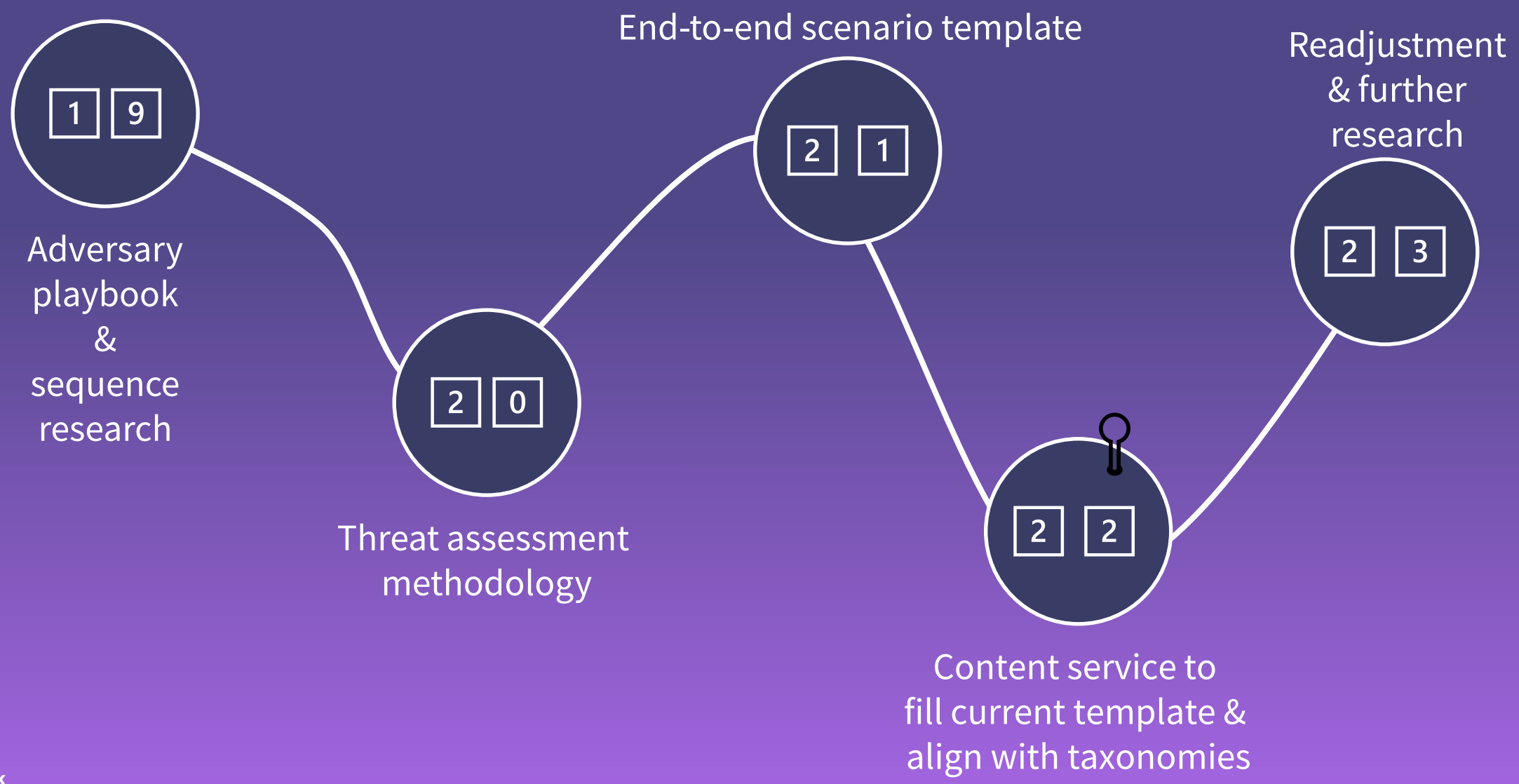
Adversary playbook *(e.g. associated threat actor profiles, ttps)*

Using ‘cyber threat’ scenario planning to break down what scenarios you forecast to happen

Using scenario testing and validation to reduce threat and/or risk scoring

Wrapping it up

Research trajectory



Recap & course of action

- Remember where in the CLIENT process your research resides
- Giving analysis actual priority is not always that easy.
- Small steps are big steps in the private sector .

Let’s continue to explore further!

Gert-Jan Bruggink
gertjanbruggink@venation.digital

@gertjanbruggink
/gertjanbruggink