Reimagining the intelligence deliverable

Gert-Jan Bruggink
BSides Cheltenham 2023
03 June 2023

Key takeaways

✓ One key industry problem is storytelling

✓ Structured content improves stakeholder engagement, making ‘threat informed’ storytelling way more effective

✓ Applying structured content in practice is easy to start with, very hard to master

Hi there! 👋

Practitioner & hands-on client support in

- Cyber Threat Intelligence
- Risk Management
- Capability Building
- Intelligence-led Red Teaming
- Transformation Programs
- Strategic Change

Most notably in these industries

- Financial Services
- High Tech
- Manufacturing

Rest of my time goes into

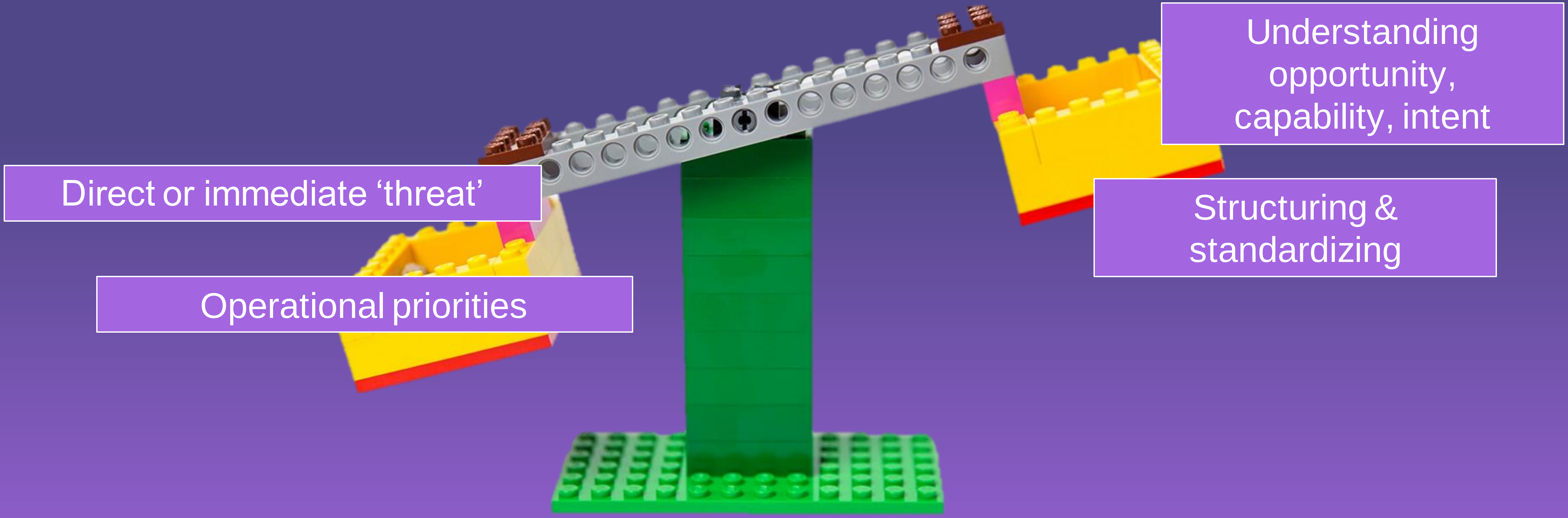
- Entrepreneurship
- Coaching
- Volunteering
- Research
- Father x 2
- Gaming
- Lego
- Meme’s
- Sports

Gert-Jan Bruggink

Cyber threat cartographer
Builder of high-performance teams
Lego afficionado

@gertjanbruggink
github.com/gertjanbruggink
/gertjanbruggink

Threat Informed Risk Management is hard



Direct or immediate ‘threat’

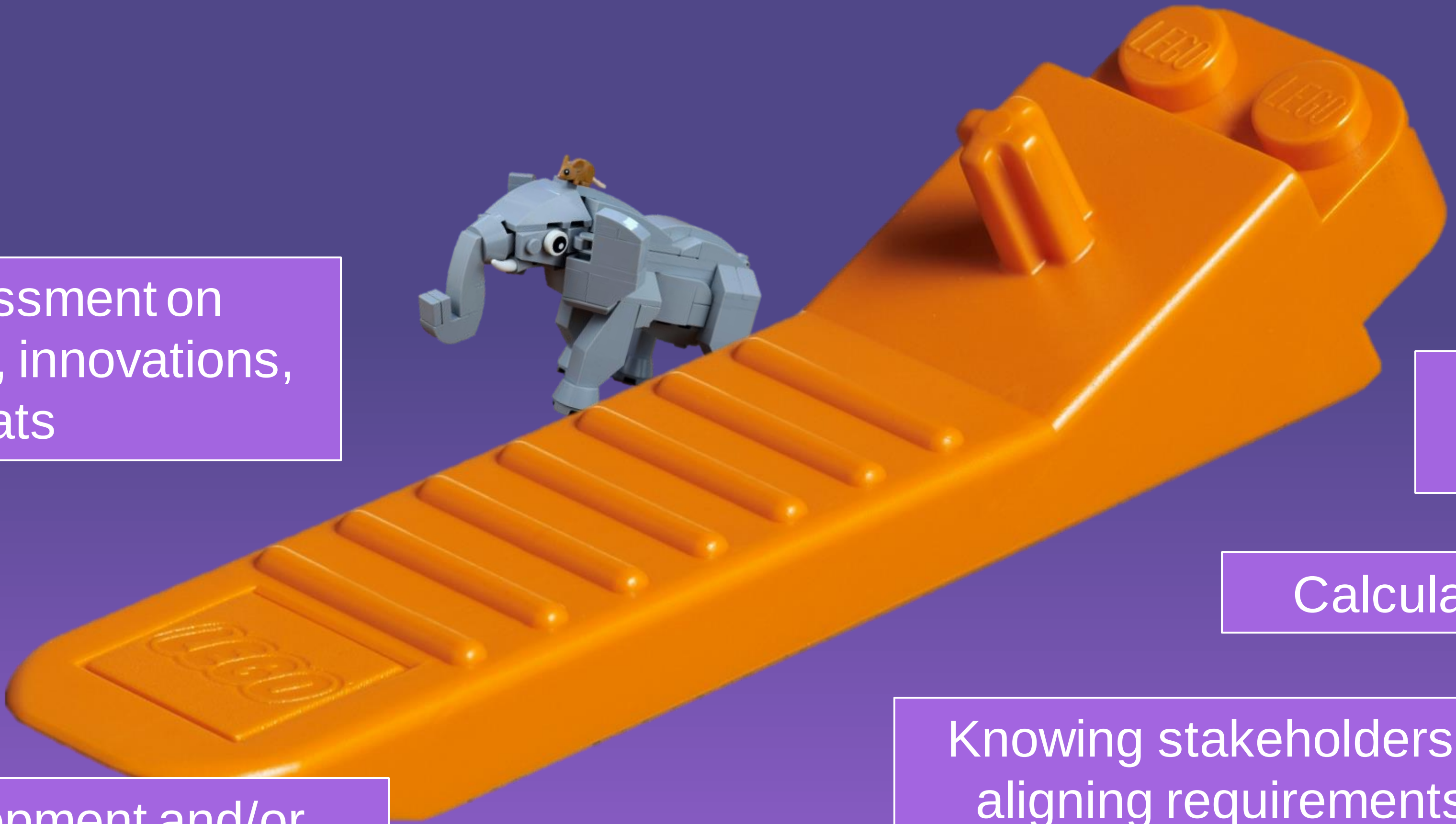
Operational priorities

Understanding opportunity, capability, intent

Structuring & standardizing

Source: https://kidsactivitiesblog--o--com.follycdn.com/wp-content/uploads/2018/11/LEGO-Inventions-3-copy.jpg

CTI capabilities struggle with their own success



Periodic assessment on industry verticals, innovations, & threats

Quality baseline & expertise required

Calculating value

Knowing stakeholders & aligning requirements

Development and/or adjustment of deliverables

Structured content takes time

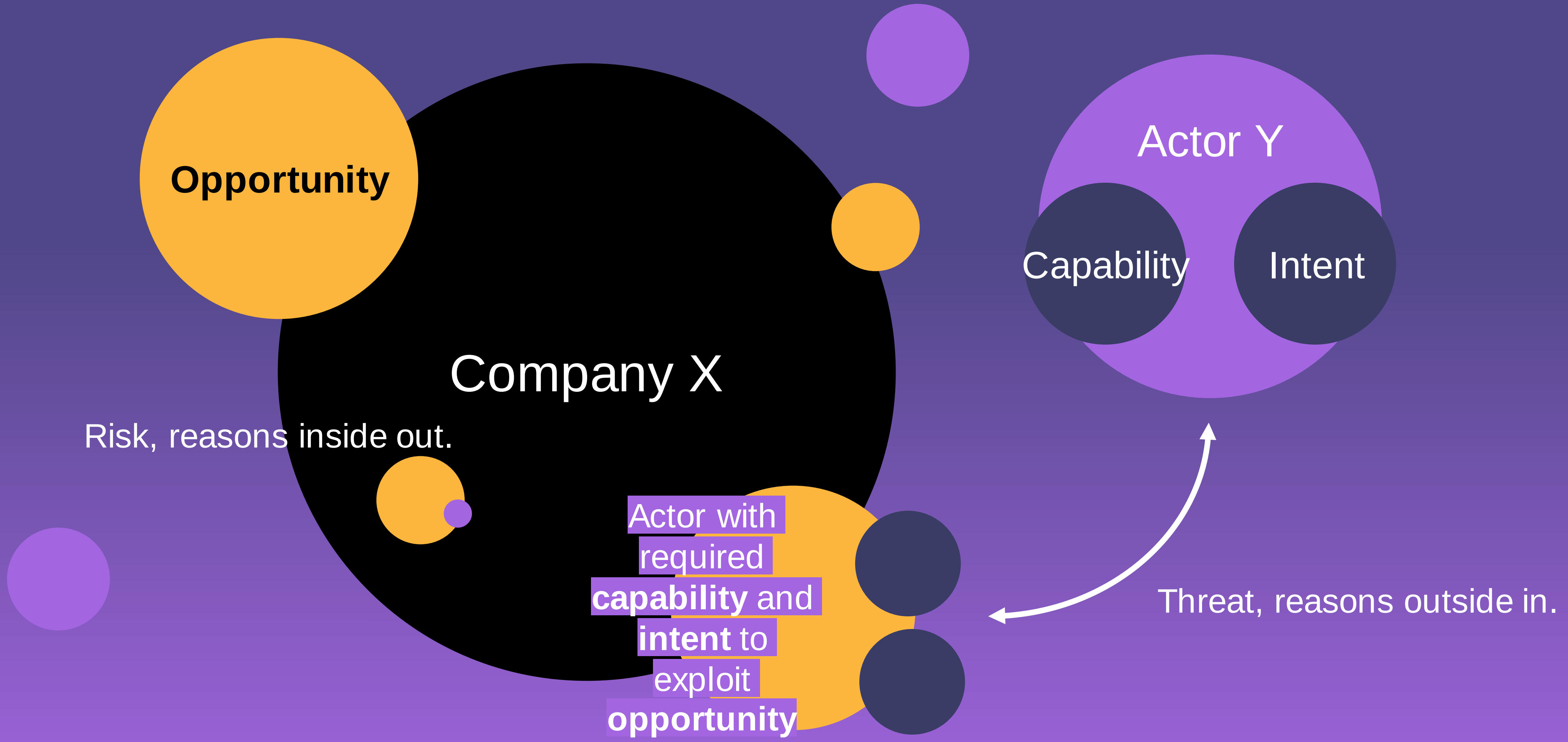
Source: amazon & https://www.brothers-brick.com/2021/04/14/the-elephant-and-the-mouse/

Talking the same language

Common Risk Management language

- 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

(Cyber) threat in context of risk



Opportunity

Company X

Risk, reasons inside out.

Actor Y

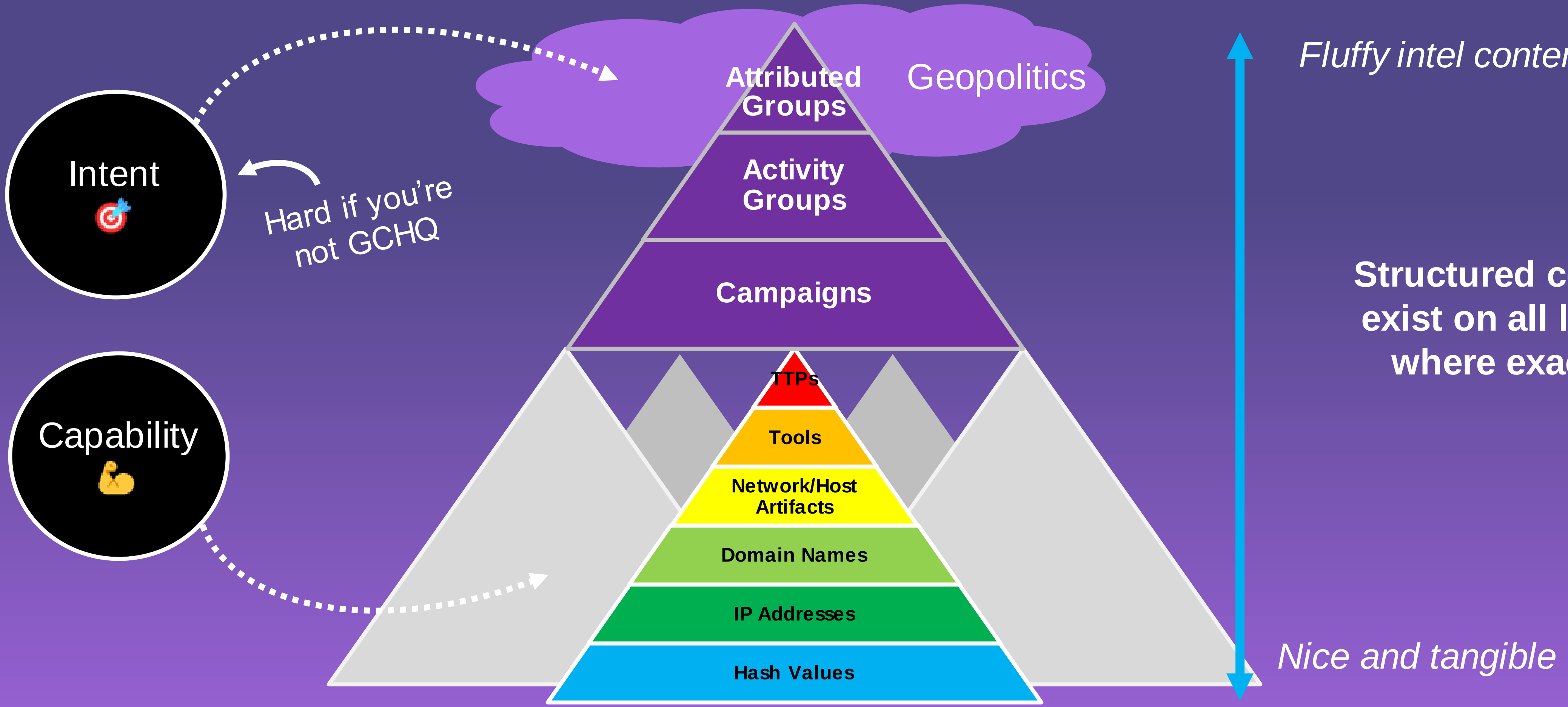
Capability

Intent

Actor with required **capability** and **intent** to exploit **opportunity**

Threat, reasons outside in.

Talking the right stakeholder language



Structured content exist on all levels, where exactly?

Extending the 'Pyramid of pain'

Non-exhaustive structured content overview

Framework / Knowledge bases

Abbrev.	Description
ATT&CK	Taxonomy of adversary tactics and techniques.
CAPEC	Structured characterization of tactics, techniques, and procedures (TTP) attack patterns.

Models / Schemas

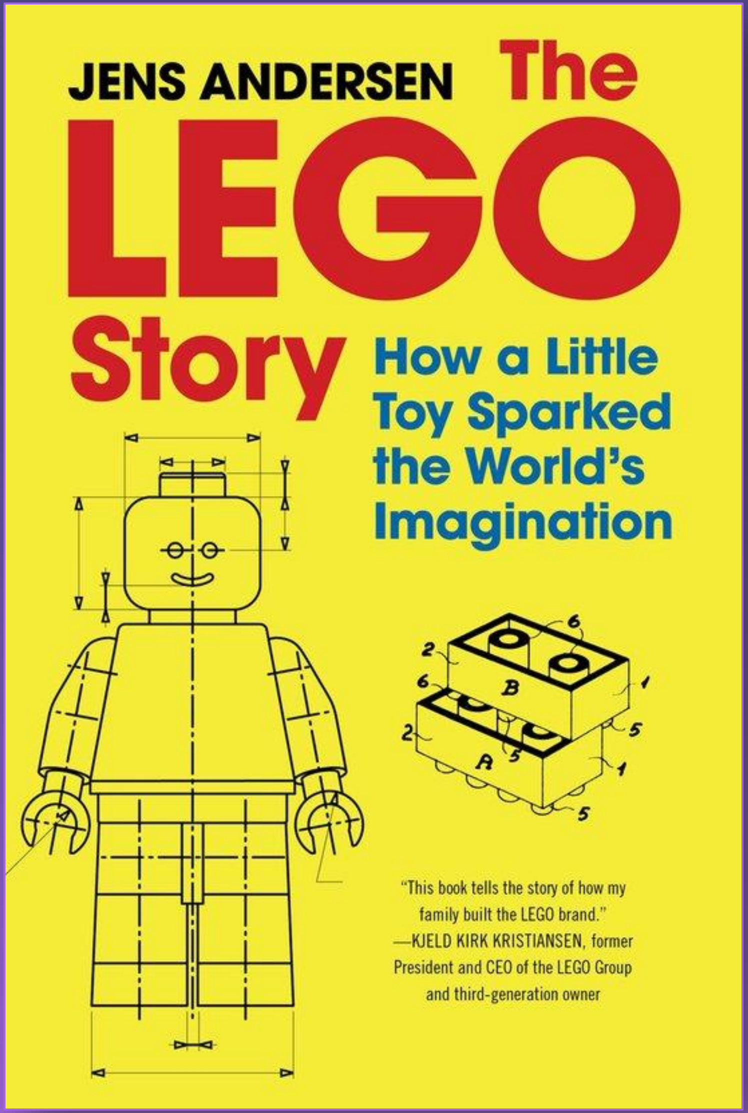
Abbrev.	Description
STIX	Structured language and serialization format used for describing cyber threat information.
MISP Object template	Various object attributes, supporting specific MISP attribute types.
OCSF	Open-source project for developing schemas, along with a vendor-agnostic core security schema.
VERIS	Metrics framework providing common language for describing security incidents and their effects.

Machine Readable Formats

Abbrev.	Description
XML	OG format from 24 years ago.
YAML	Compact markup language.
Mark down	Lightweight markup language.
JSON	JavaScript Object Notation.

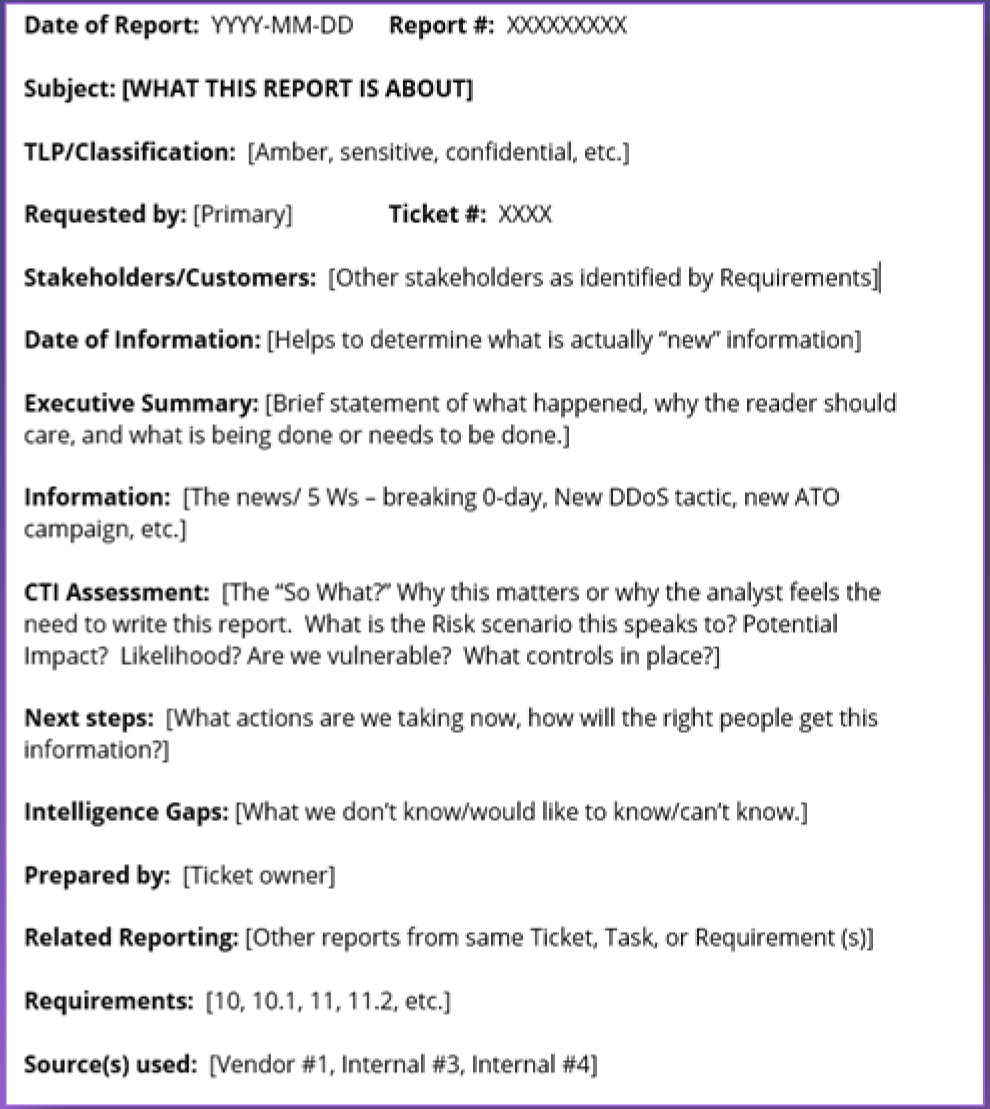
References added to last page.

Telling our (current) cyber threat stories



JENS ANDERSEN
The LEGO Story
How a Little Toy Sparked the World's Imagination
"This book tells the story of how my family built the LEGO brand."
—KJELD KIRK KRISTIANSEN, former President and CEO of the LEGO Group and third-generation owner

Source: Amazon



Date of Report: YYYY-MM-DD **Report #:** XXXXXXXXX

Subject: [WHAT THIS REPORT IS ABOUT]

TLP/Classification: [Amber, sensitive, confidential, etc.]

Requested by: [Primary] **Ticket #:** XXXX

Stakeholders/Customers: [Other stakeholders as identified by Requirements]

Date of Information: [Helps to determine what is actually "new" information]

Executive Summary: [Brief statement of what happened, why the reader should care, and what is being done or needs to be done.]

Information: [The news/ 5 Ws – breaking 0-day, New DDoS tactic, new ATO campaign, etc.]

CTI Assessment: [The "So What?" Why this matters or why the analyst feels the need to write this report. What is the Risk scenario this speaks to? Potential Impact? Likelihood? Are we vulnerable? What controls in place?]

Next steps: [What actions are we taking now, how will the right people get this information?]

Intelligence Gaps: [What we don't know/would like to know/can't know.]

Prepared by: [Ticket owner]

Related Reporting: [Other reports from same Ticket, Task, or Requirement (s)]

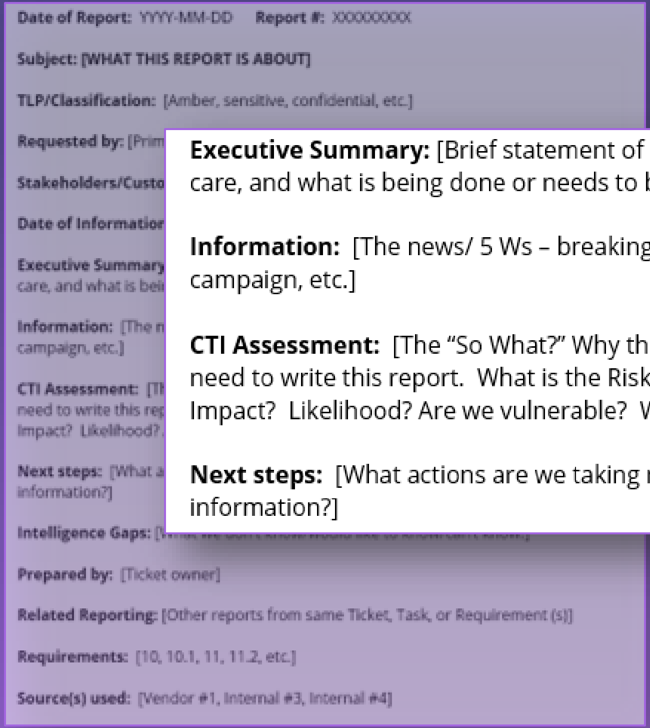
Requirements: [10, 10.1, 11, 11.2, etc.]

Source(s) used: [Vendor #1, Internal #3, Internal #4]

Source: ReqFast & Venation

Challenges of translation

Intelligence product



Date of Report: YYYY-MM-DD **Report #:** XXXXXXXXX

Subject: [WHAT THIS REPORT IS ABOUT]

TLP/Classification: [Amber, sensitive, confidential, etc.]

Requested by: [Prim

Stakeholders/Custo

Date of Informatior

Executive Summary
care, and what is bei

Information: [The n
campaign, etc.]

CTI Assessment: [Th
need to write this rep
Impact? Likelihood?

Next steps: [What a
information?]

Intelligence Gaps: [

Prepared by: [Ticket owner]

Related Reporting: [Other reports from same Ticket, Task, or Requirement (s)]

Requirements: [10, 10.1, 11, 11.2, etc.]

Source(s) used: [Vendor #1, Internal #3, Internal #4]

Executive Summary: [Brief statement of what happened, why the reader should care, and what is being done or needs to be done.]

Information: [The news/ 5 Ws – breaking 0-day, New DDoS tactic, new ATO campaign, etc.]

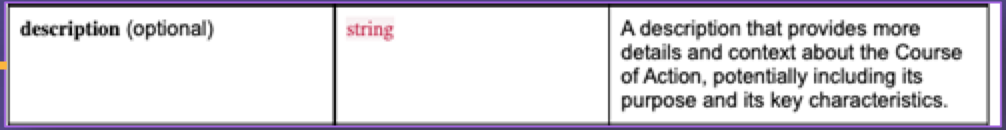
CTI Assessment: [The "So What?" Why this matters or why the analyst feels the need to write this report. What is the Risk scenario this speaks to? Potential Impact? Likelihood? Are we vulnerable? What controls in place?]

Next steps: [What actions are we taking now, how will the right people get this information?]

Source: Venation & ReqFast

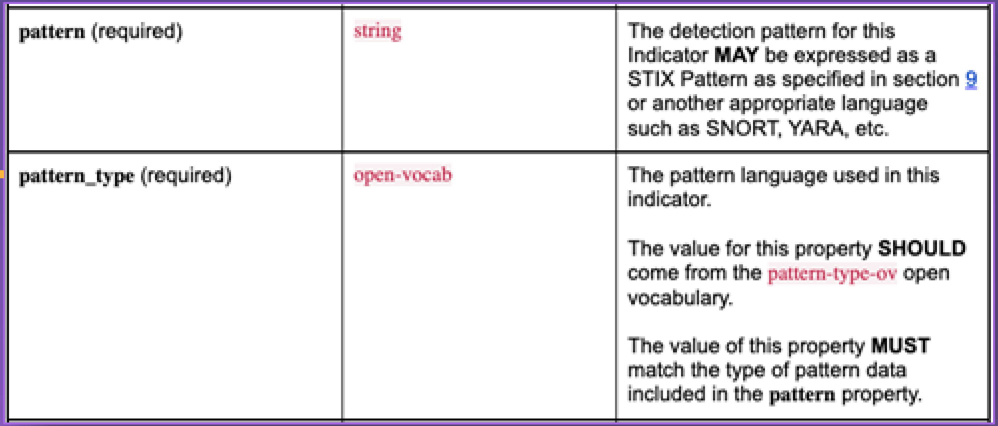
Structured technical content

Unstructured (currently)



description (optional)	string	A description that provides more details and context about the Course of Action, potentially including its purpose and its key characteristics.

Structured

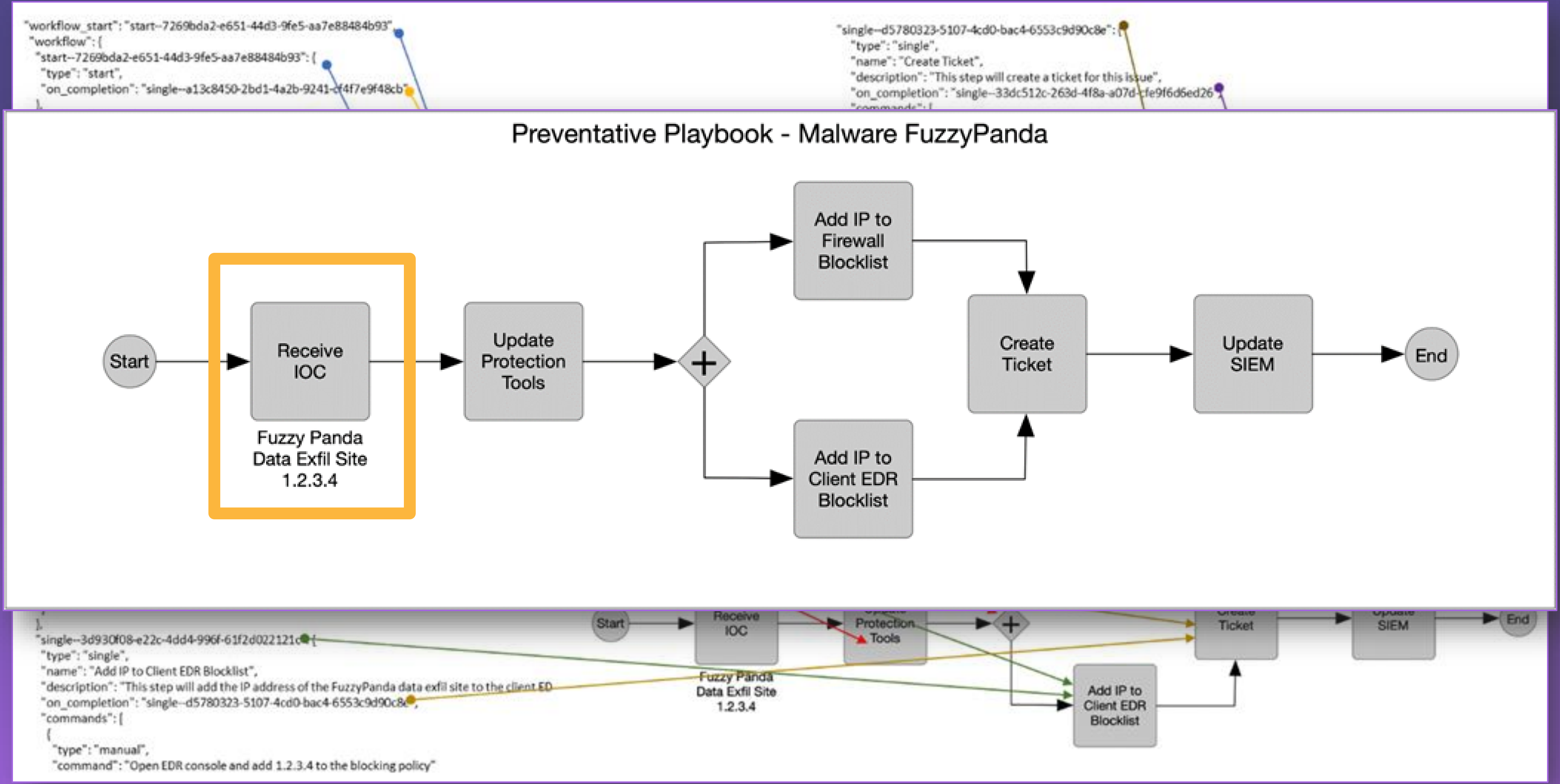


pattern (required)	string	The detection pattern for this Indicator **MAY** be expressed as a STIX Pattern as specified in section 9 or another appropriate language such as SNORT, YARA, etc.
pattern_type (required)	open-vocab	The pattern language used in this indicator. The value for this property **SHOULD** come from the pattern-type-ov open vocabulary. The value of this property **MUST** match the type of pattern data included in the **pattern** property.

Source: STIX 2.1 documentation

https://adventurebricks.com/images/detailed/19/3626cpb2272-head-dual-large-simple-eyes-open-mouth-tongue-happy-sad.jpg

Tying it to stakeholder demands



```
"workflow_start": "start--7269bda2-e651-44d3-9fe5-aa7e88484b93",
 "workflow": {
  "start--7269bda2-e651-44d3-9fe5-aa7e88484b93": {
   "type": "start",
   "on_completion": "single--a13c8450-2bd1-4a2b-9241-cf4f7e9f48cb"
```

```
"single--d5780323-5107-4cd0-bac4-6553c9d90c8e": {
  "type": "single",
  "name": "Create Ticket",
  "description": "This step will create a ticket for this issue",
  "on_completion": "single--33dc512c-263d-4f8a-a07d-cfe9f6d6ed26",
```

```
 },
"single--3d930f08-e22c-4dd4-996f-61f2d022121c": {
 "type": "single",
 "name": "Add IP to Client EDR Blocklist",
 "description": "This step will add the IP address of the FuzzyPanda data exfil site to the client ED
 "on_completion": "single--d5780323-5107-4cd0-bac4-6553c9d90c8e",
 "commands": [
  {
   "type": "manual",
   "command": "Open EDR console and add 1.2.3.4 to the blocking policy"
```

Preventative Playbook - Malware FuzzyPanda
Start
Receive IOC
Fuzzy Panda Data Exfil Site 1.2.3.4
Update Protection Tools
+
Add IP to Firewall Blocklist
Add IP to Client EDR Blocklist
Create Ticket
Update SIEM
End

Vasileios Mavroeidis, Towards shareable defenders' tradecraft, CTI-EU 2022

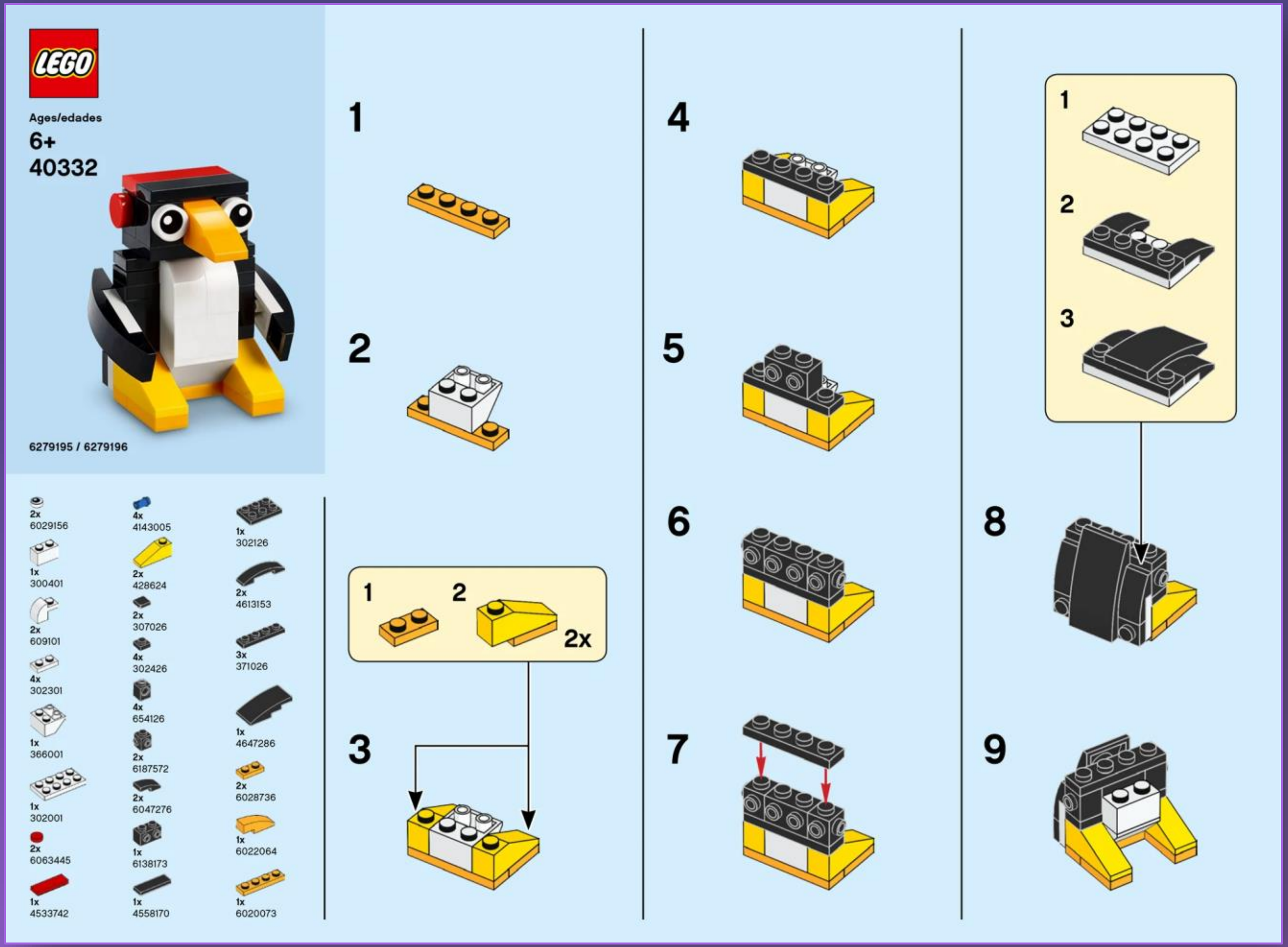
Image source: CACAO Security Playbooks Version 1.0. Edited by Bret Jordan and Allan Thomson. 23 June 2021.

Our age-old frontier: storytelling

Source:
http://bugeyedmonkeys.com/lic/about/img/screen1.png

Applying this in practice

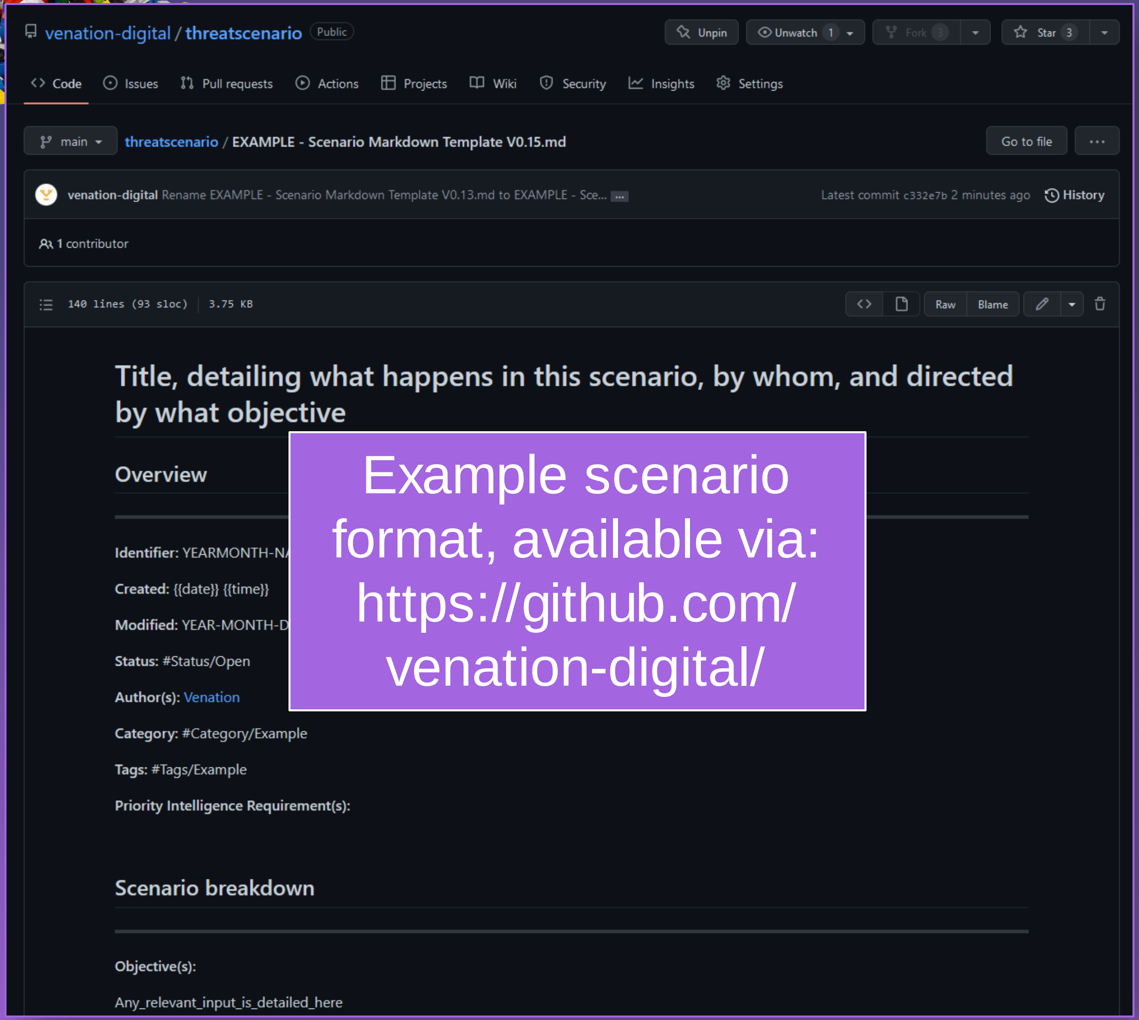
Reimagining CTI ‘storytelling’



Source:
https://cdn.shopify.com/s/files/1/1553/8473/files/201912-MMB-Instructions_Penguin-_40332_-1_2048x2048.png?v=1583304951

TLDR: it is not this simple

Creating individual scenarios using structured content



venation-digital / threatscenario Public

Unpin | Unwatch 1 | Fork 0 | Star 3

Code | Issues | Pull requests | Actions | Projects | Wiki | Security | Insights | Settings

main | threatscenario / EXAMPLE - Scenario Markdown Template V0.15.md | Go to file

venation-digital Rename EXAMPLE - Scenario Markdown Template V0.13.md to EXAMPLE - Sce... Latest commit c332e7b 2 minutes ago History

1 contributor

140 lines (93 sloc) | 3.75 KB | Raw | Blame

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

Overview

Identifier: YEARMONTH-NA

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

Modified: YEAR-MONTH-D

Status: #Status/Open

Author(s): Venation

Category: #Category/Example

Tags: #Tags/Example

Priority Intelligence Requirement(s):

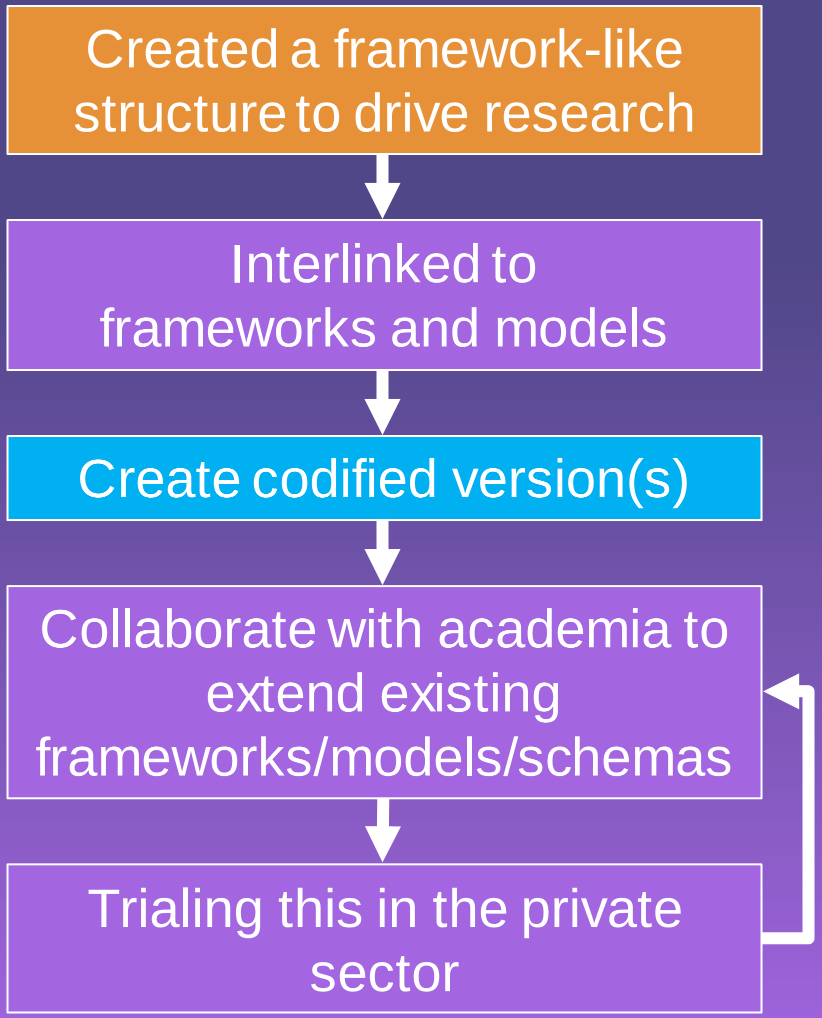
Scenario breakdown

Objective(s):

Any_relevant_input_is_detailed_here

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

Approach



Created a framework-like structure to drive research

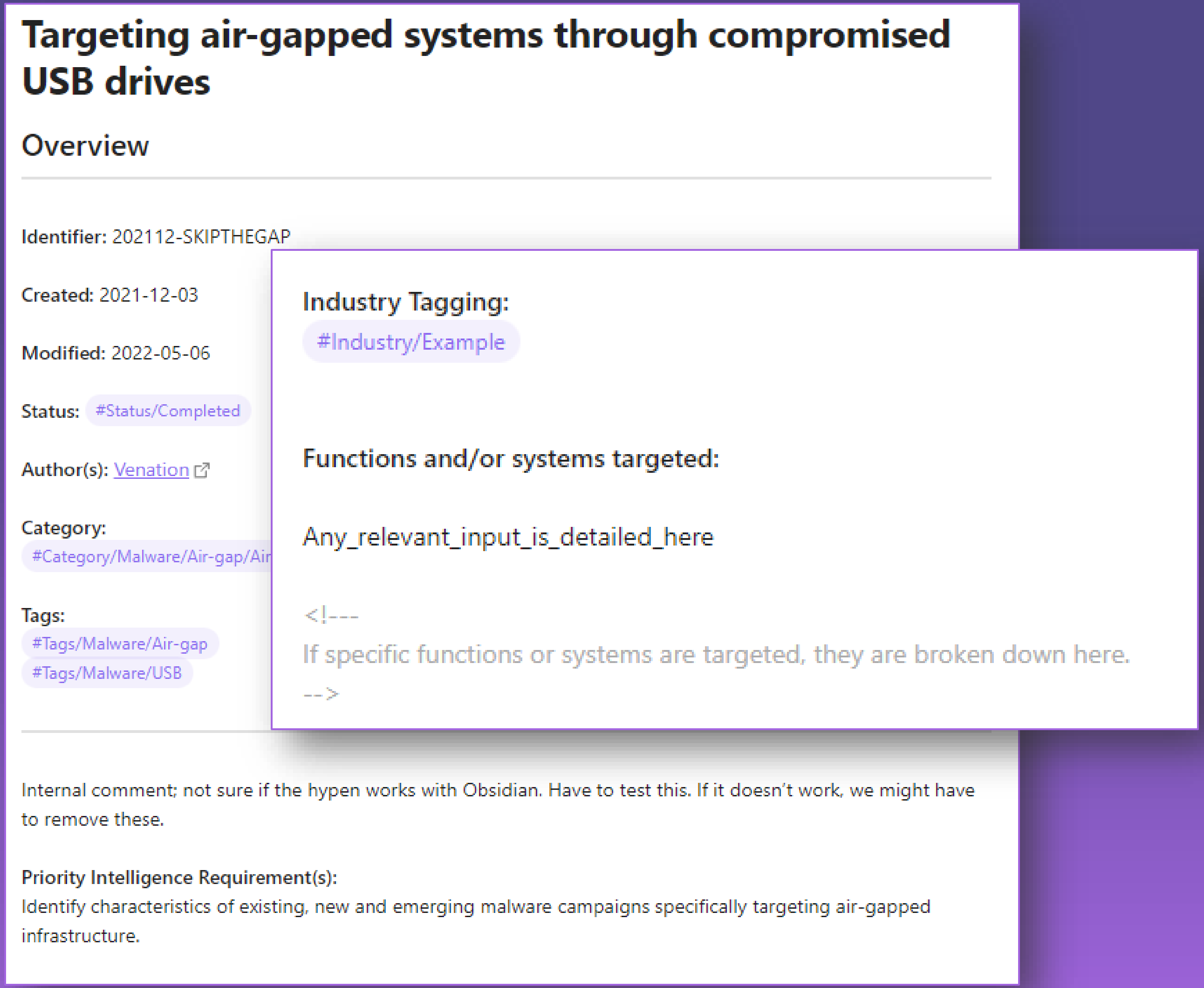
Interlinked to frameworks and models

Create codified version(s)

Collaborate with academia to extend existing frameworks/models/schemas

Trialing this in the private sector

Knowing your threat environment



Targeting air-gapped systems through compromised USB drives

Overview

Identifier: 202112-SKIPTHEGAP

Created: 2021-12-03

Modified: 2022-05-06

Status: #Status/Completed

Author(s): Venation

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

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

Industry Tagging:
#Industry/Example

Functions and/or systems targeted:

Any_relevant_input_is_detailed_here

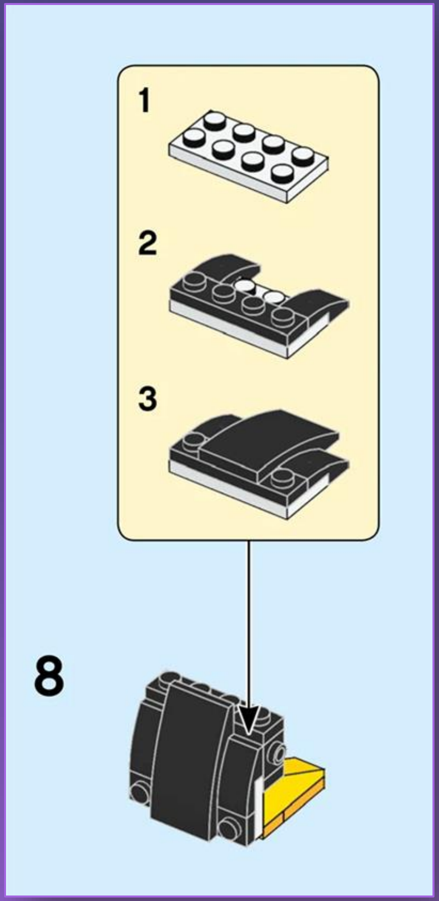
<!---
If specific functions or systems are targeted, they are broken down here.
-->

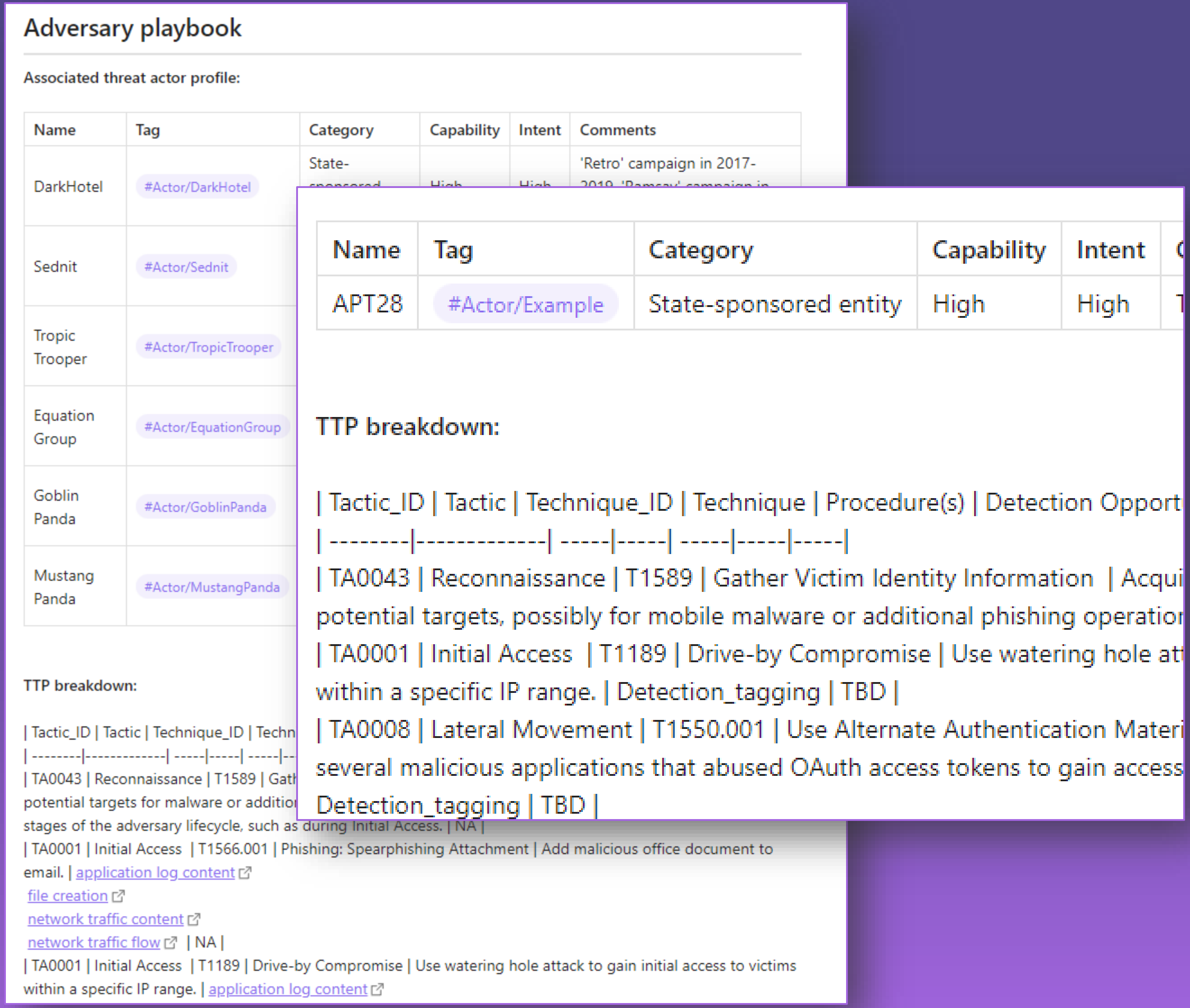
Internal comment; not sure if the hypen works with Obsidian. Have to test this. If it doesn't work, we might have to remove these.

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

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

Translating adversary playbook to practice





Adversary playbook

Associated threat actor profile:

Name	Tag	Category	Capability	Intent	Comments
DarkHotel	#Actor/DarkHotel	State-sponsored	High	High	'Retro' campaign in 2017-2019, 'Ramsay' campaign in
Sednit	#Actor/Sednit				
Tropic Trooper	#Actor/TropicTrooper				
Equation Group	#Actor/EquationGroup				
Goblin Panda	#Actor/GoblinPanda				
Mustang Panda	#Actor/MustangPanda				

TTP breakdown:

```
| Tactic_ID | Tactic | Technique_ID | Techn
| --------|------------| -----|-----| -----|--
| TA0043 | Reconnaissance | T1589 | Gath
potential targets for malware or additio
stages of the adversary lifecycle, such as during Initial Access. | NA |
| TA0001 | Initial Access  | T1566.001 | Phishing: Spearphishing Attachment | Add malicious office document to
email. | application log content
 file creation
 network traffic content
 network traffic flow  | NA |
| TA0001 | Initial Access  | T1189 | Drive-by Compromise | Use watering hole attack to gain initial access to victims
within a specific IP range. | application log content
```

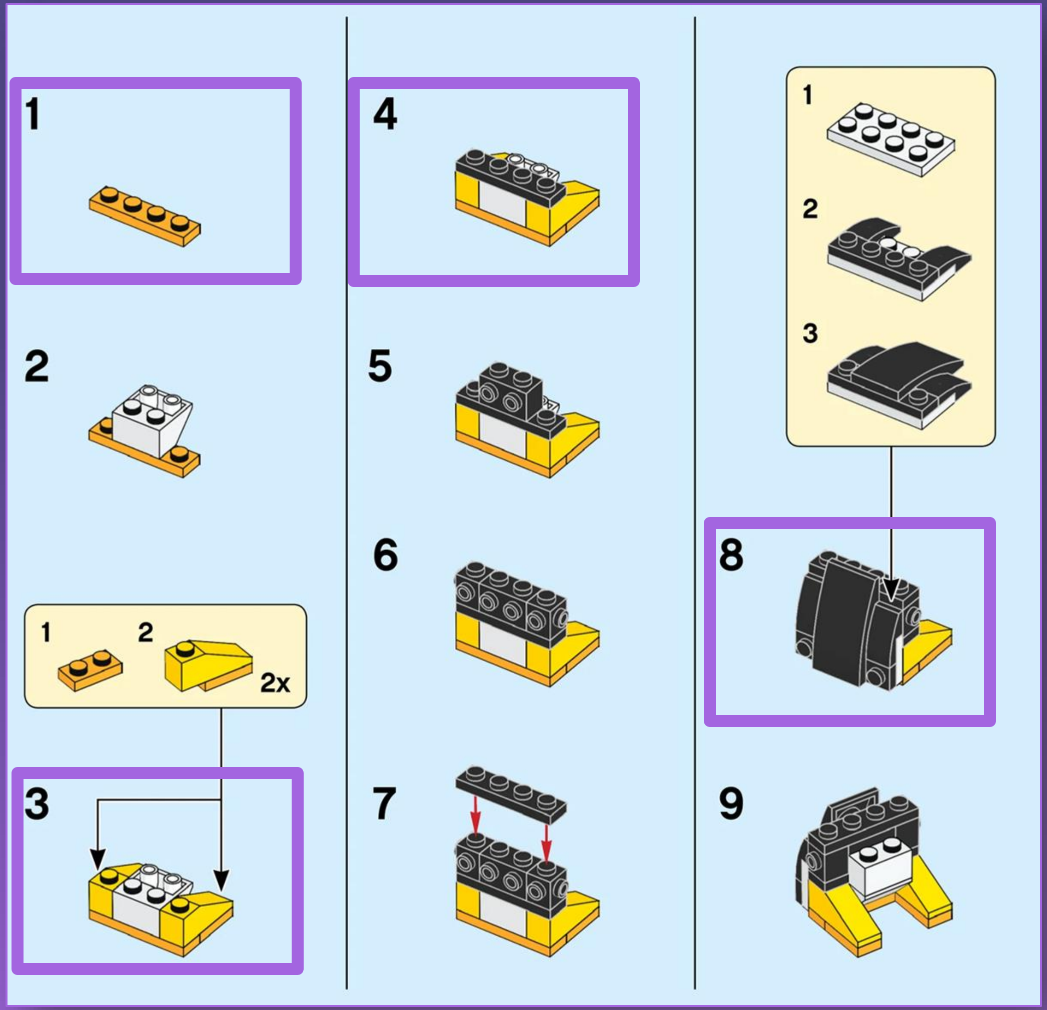
Name	Tag	Category	Capability	Intent	C
APT28	#Actor/Example	State-sponsored entity	High	High	T

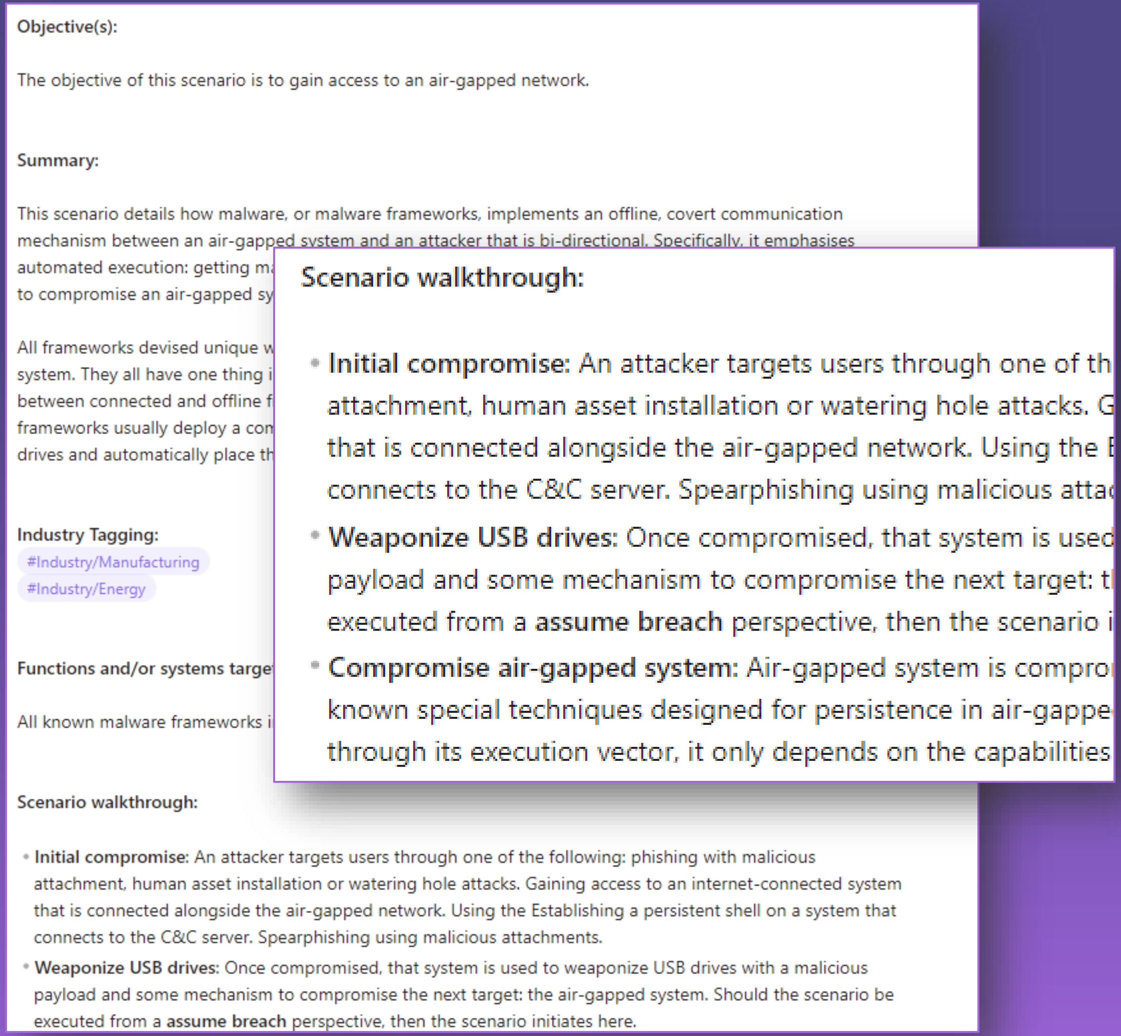
TTP breakdown:

```
| Tactic_ID | Tactic | Technique_ID | Technique | Procedure(s) | Detection Opport
| --------|------------| -----|-----| -----|-----|-----|
| TA0043 | Reconnaissance | T1589 | Gather Victim Identity Information  | Acqui
potential targets, possibly for mobile malware or additional phishing operatio
| TA0001 | Initial Access  | T1189 | Drive-by Compromise | Use watering hole at
within a specific IP range. | Detection_tagging | TBD |
| TA0008 | Lateral Movement | T1550.001 | Use Alternate Authentication Materi
several malicious applications that abused OAuth access tokens to gain access
Detection_tagging | TBD |
```

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

Providing better context through narratives




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 ma
to compromise an air-gapped sy

All frameworks devised unique w
system. They all have one thing i
between connected and offline f
frameworks usually deploy a con
drives and automatically place th

Industry Tagging:
#Industry/Manufacturing
#Industry/Energy

Functions and/or systems targe

All known malware frameworks i

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.

Scenario walkthrough:

- **Initial compromise:** An attacker targets users through one of th
attachment, human asset installation or watering hole attacks. G
that is connected alongside the air-gapped network. Using the E
connects to the C&C server. Spearphishing using malicious attac
- **Weaponize USB drives:** Once compromised, that system is used
payload and some mechanism to compromise the next target: t
executed from a **assume breach** perspective, then the scenario i
- **Compromise air-gapped system:** Air-gapped system is compro
known special techniques designed for persistence in air-gappe
through its execution vector, it only depends on the capabilities

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

@gertjanbruggink

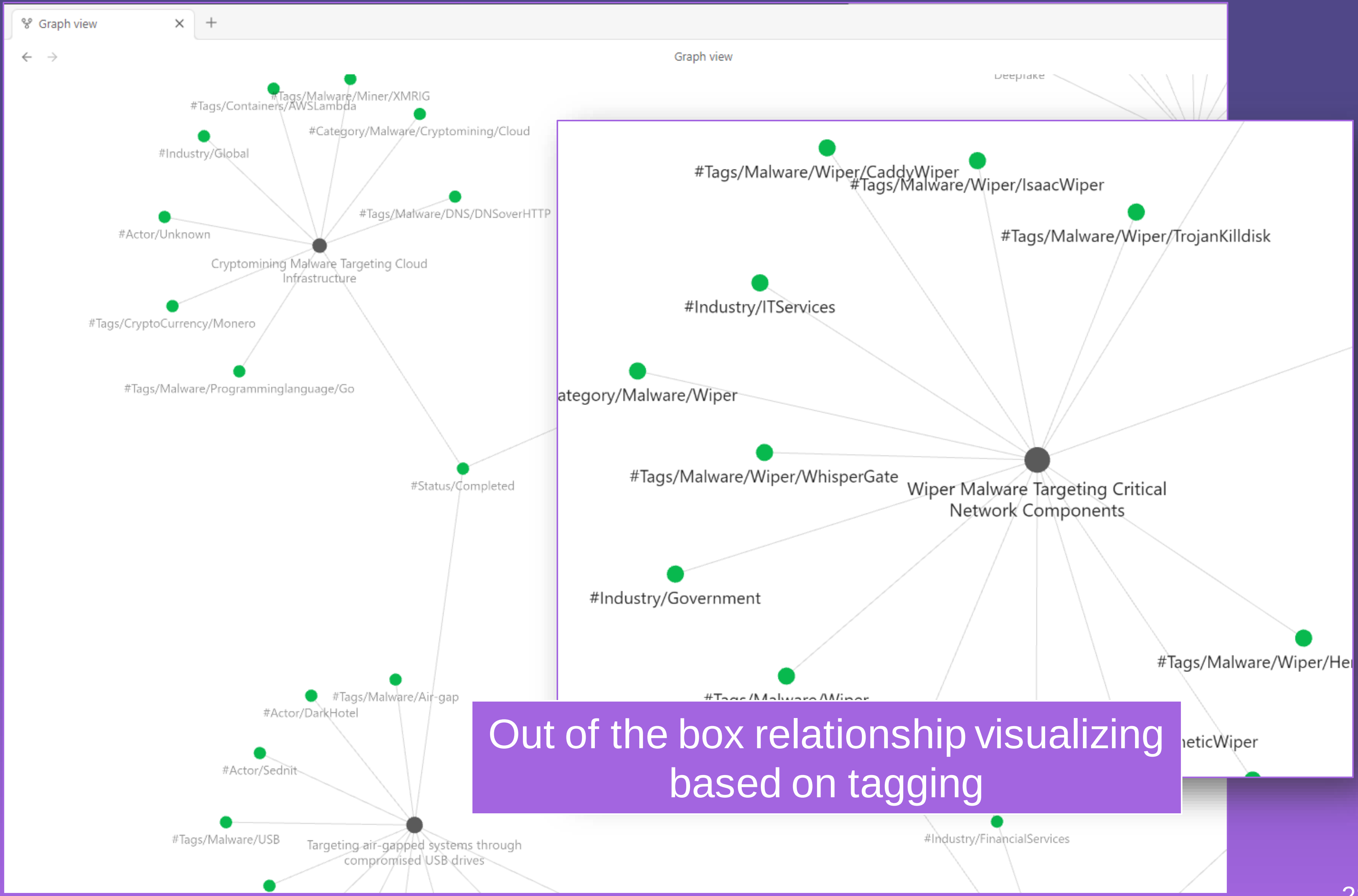
Using encoding to analyze scenario’s more effective

Practically start with Markdown

Ingest in open-source note keeping tool

OBSIDIAN

https://obsidian.md/

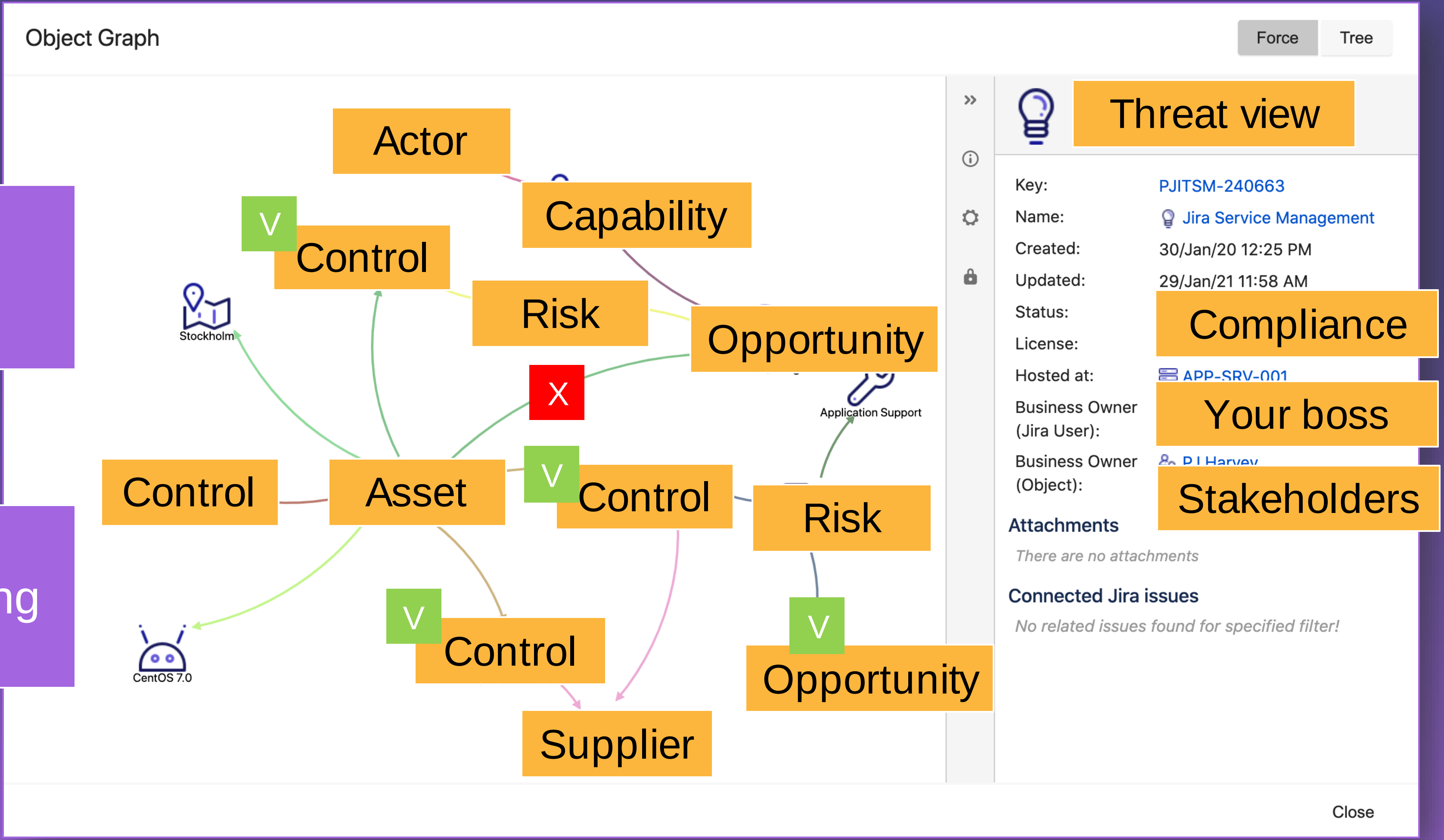

Graph view
Graph view
Deepfake
#Tags/Malware/Miner/XMRIG
#Tags/Containers/AWSLambda
#Category/Malware/Cryptomining/Cloud
#Industry/Global
#Tags/Malware/DNS/DNSoverHTTP
#Actor/Unknown
Cryptomining Malware Targeting Cloud Infrastructure
#Tags/CryptoCurrency/Monero
#Tags/Malware/Programminglanguage/Go
#Status/Completed
#Tags/Malware/Air-gap
#Actor/DarkHotel
#Actor/Sednit
#Tags/Malware/USB
Targeting air-gapped systems through compromised USB drives
#Industry/FinancialServices
#Tags/Malware/Wiper/CaddyWiper
#Tags/Malware/Wiper/IsaacWiper
#Tags/Malware/Wiper/TrojanKilldisk
#Industry/ITServices
ategory/Malware/Wiper
#Tags/Malware/Wiper/WhisperGate
Wiper Malware Targeting Critical Network Components
#Industry/Government
#Tags/Malware/Wiper/He
#Tags/Malware/Wiper
neticWiper

Out of the box relationship visualizing based on tagging

‘Living Off The Land’ CTI

Explore your internal technology stack for creative uses

Identify how your stakeholders are reporting and ‘hook’ in on that



Object Graph

Force Tree

Key: PJITSM-240663

Name: Jira Service Management

Created: 30/Jan/20 12:25 PM

Updated: 29/Jan/21 11:58 AM

Status:

License:

Hosted at: APP-SRV-001

Business Owner (Jira User):

Business Owner (Object): P J Harvey

Attachments

There are no attachments

Connected Jira issues

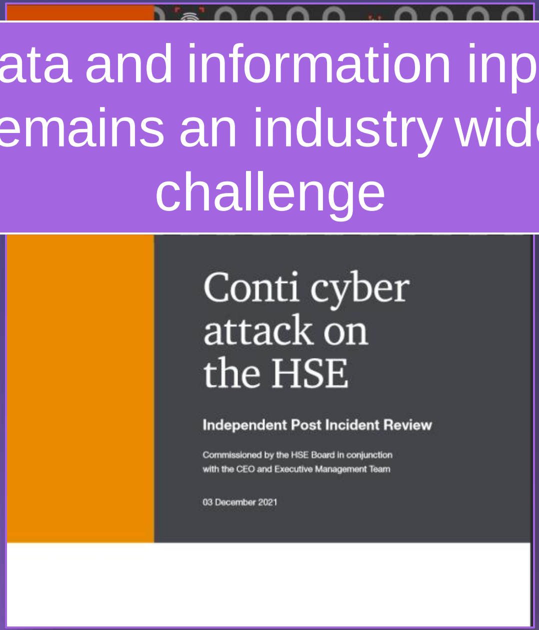
No related issues found for specified filter!

Close

Source
https://www.atlassian.com/software/jira/service-management/resources/insight-data-center-get-started-guide

Emerging model / schema: CACAO

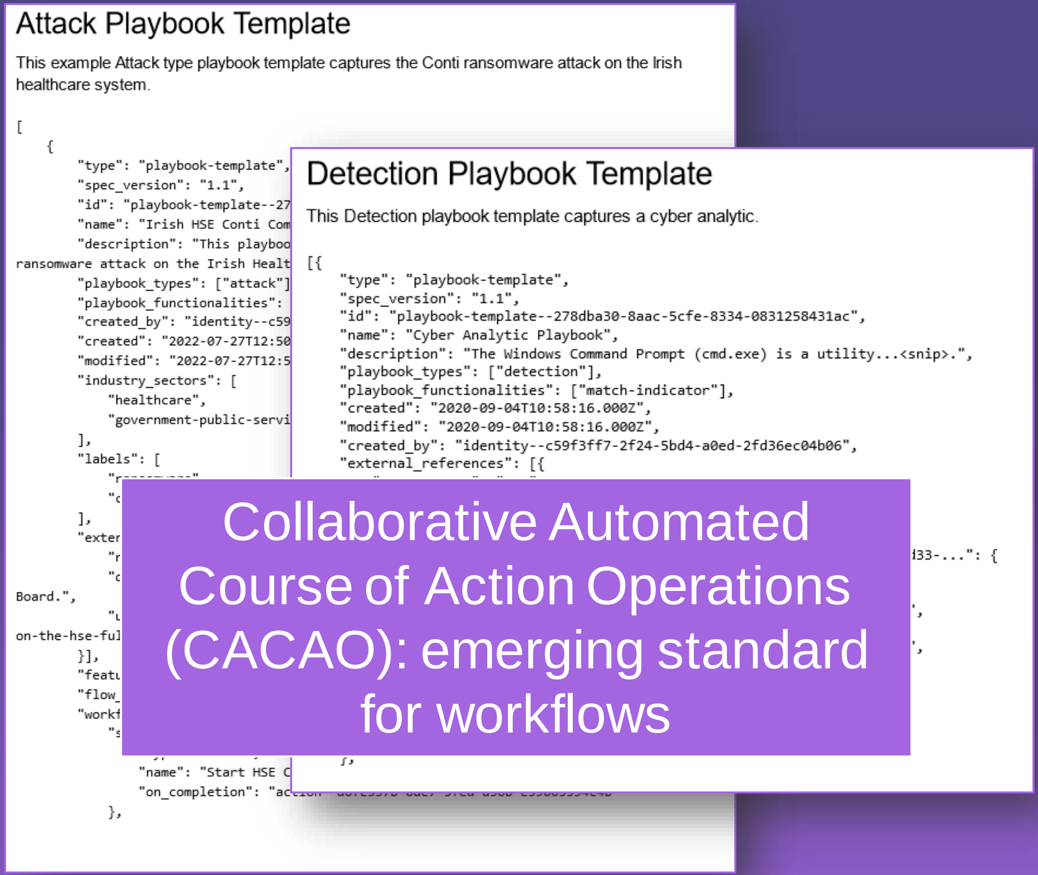
We know how to get from this to that



Data and information input remains an industry wide challenge

Conti cyber attack on the HSE
Independent Post Incident Review
Commissioned by the HSE Board in conjunction with the CEO and Executive Management Team
03 December 2021

Source
https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf



Attack Playbook Template

This example Attack type playbook template captures the Conti ransomware attack on the Irish healthcare system.

```
[
    {
        "type": "playbook-template",
        "spec_version": "1.1",
        "id": "playbook-template--27
        "name": "Irish HSE Conti Com
        "description": "This playboo
ransomware attack on the Irish Healt
        "playbook_types": ["attack"]
        "playbook_functionalities":
        "created_by": "identity--c59
        "created": "2022-07-27T12:50
        "modified": "2022-07-27T12:5
        "industry_sectors": [
            "healthcare",
            "government-public-servi
        ],
        "labels": [
            "r
            "c
        ],
        "exter
            "r
            "c
Board.",
            "u
on-the-hse-ful
        }],
        "featu
        "flow_
        "workf
            "s
                "name": "Start HSE C
                "on_completion": "ac
            },
```

Detection Playbook Template

This Detection playbook template captures a cyber analytic.

```
[{
    "type": "playbook-template",
    "spec_version": "1.1",
    "id": "playbook-template--278dba30-8aac-5cfe-8334-0831258431ac",
    "name": "Cyber Analytic Playbook",
    "description": "The Windows Command Prompt (cmd.exe) is a utility...<snip>.",
    "playbook_types": ["detection"],
    "playbook_functionalities": ["match-indicator"],
    "created": "2020-09-04T10:58:16.000Z",
    "modified": "2020-09-04T10:58:16.000Z",
    "created_by": "identity--c59f3ff7-2f24-5bd4-a0ed-2fd36ec04b06",
    "external_references": [{
                                                           d33-...": {
                                                           ",
                                                           ",
    },
```

Collaborative Automated Course of Action Operations (CACAO): emerging standard for workflows

Desiree A Beck, Principal Cyber Security Engineer, MITRE
Image source: Example CACAO Attack & Detection Playbook(s)

We struggle with these

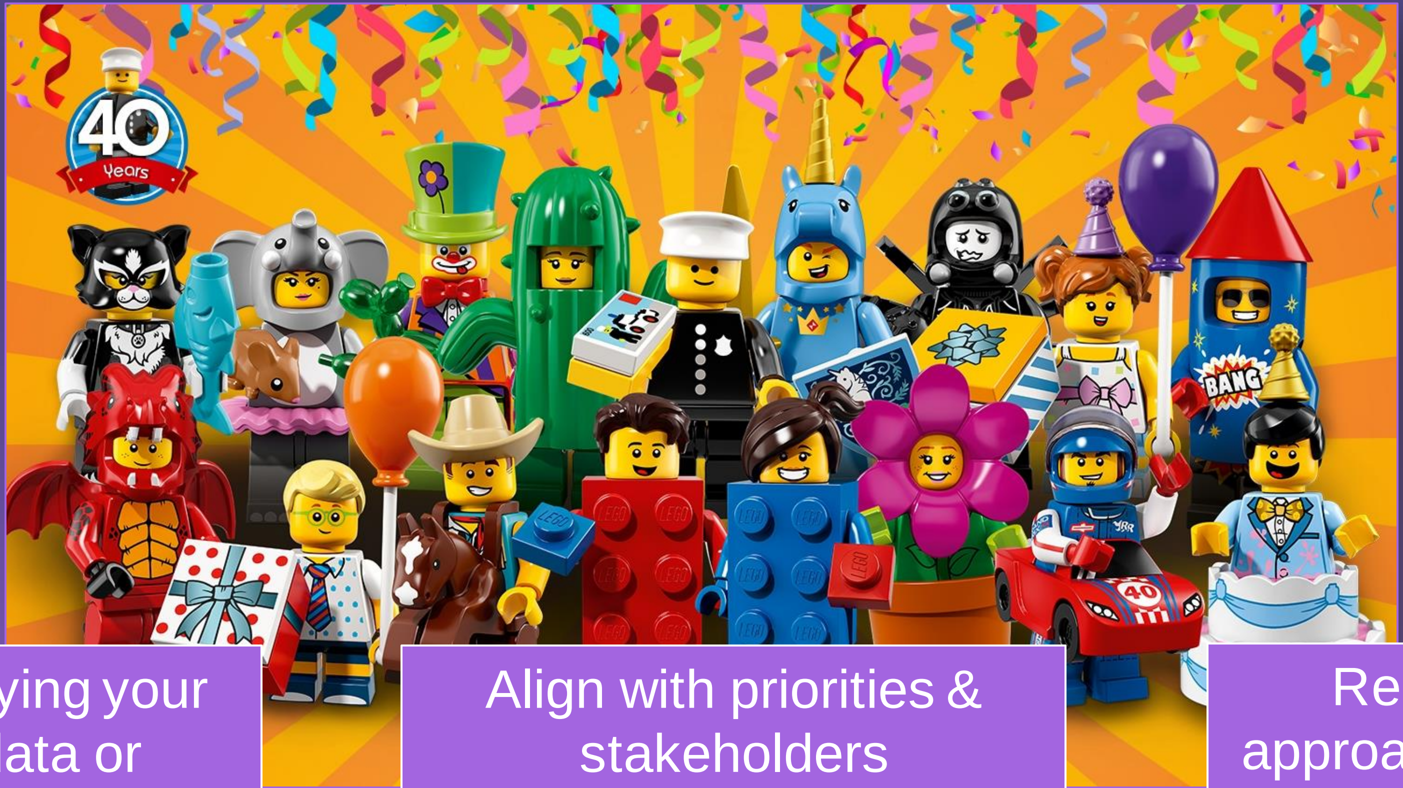
Source
https://martijnvanotterlo.nl/minority.jpg

Correlation
Visualisation
Corresponding action(s)

Source
https://docs.oasis-open.org/cacao/security-playbooks/v1.0/security-playbooks-v1.0.html

Wrapping it up

Success factors to effective ‘threat informed’ storytelling



Explore codifying your (internal) data or information. Regardless of your maturity.

Align with priorities & stakeholders and identify easy machine-readable sharing

Reimagine your approach to storytelling and explore a narrative format

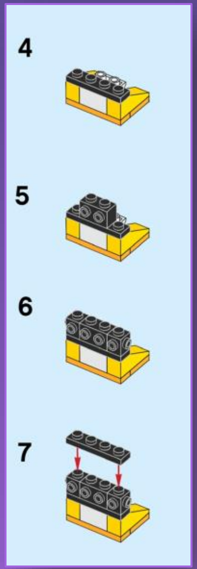
@gertjanbruggink

Source: https://www.lego.com/en-us/kids/sets/minifigures/series-18-party-a96669144123 43c489d153022eeb7c25

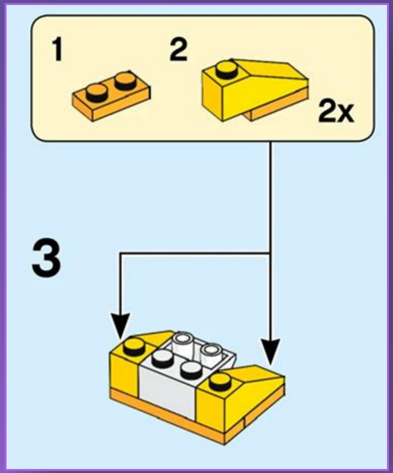
Your reimagined deliverable

Executive

Manager



Specialist



Sources: https://media.npr.org/assets/img/2017/03/01/27769399454_dda030fef6_o_custom-deb6a855d95c6b48879bb7d1aea18069932aa7ee-s800-c85.webp, https://youtu.be/g8-4wXkT60c, https://youtu.be/K4oaSkNTdIY, https://cdn.shopify.com/s/files/1/1553/8473/files/201912-MMB-Instructions_Penguin-_40332_-1_2048x2048.png?v=1583304951, https://rebrickable.com/mocs/MOC-47349/2in1/penguin/#details

Let’s continue exploring further!

Gert-Jan Bruggink
gertjanbruggink@venation.digital

@gertjanbruggink
/gertjanbruggink

References

STIX	https://github.com/mitre-attack/attack-stix-data.
MISP Object templates	https://www.misp-project.org/objects.html
OCSF	https://github.com/ocsf
VERIS	https://github.com/vz-risk/veris
OpenIOC	https://github.com/fireeye/OpenIOC_1.1
CACAO	https://docs.oasis-open.org/cacao/security-playbooks/v1.0/security-playbooks-v1.0.html