TaHiTI

Threat Hunting Methodology

Rob van Os
Marcus Bakker

PvIB Security Congres 2019

About us

Rob van Os

- Product Owner Cyber Defense Center @Volksbank
- Extensive experience in cyber defense
- Lead author of the TaHiTI methodology and the MaGMa use case framework

Marcus Bakker

- Freelance Cyber Defense Expert @MB Secure / Rabobank
- Extensive experience in cyber defense and offensive IT security
- Co-developer of the DeTT&CT framework
- Co-author of the TaHiTI methodology

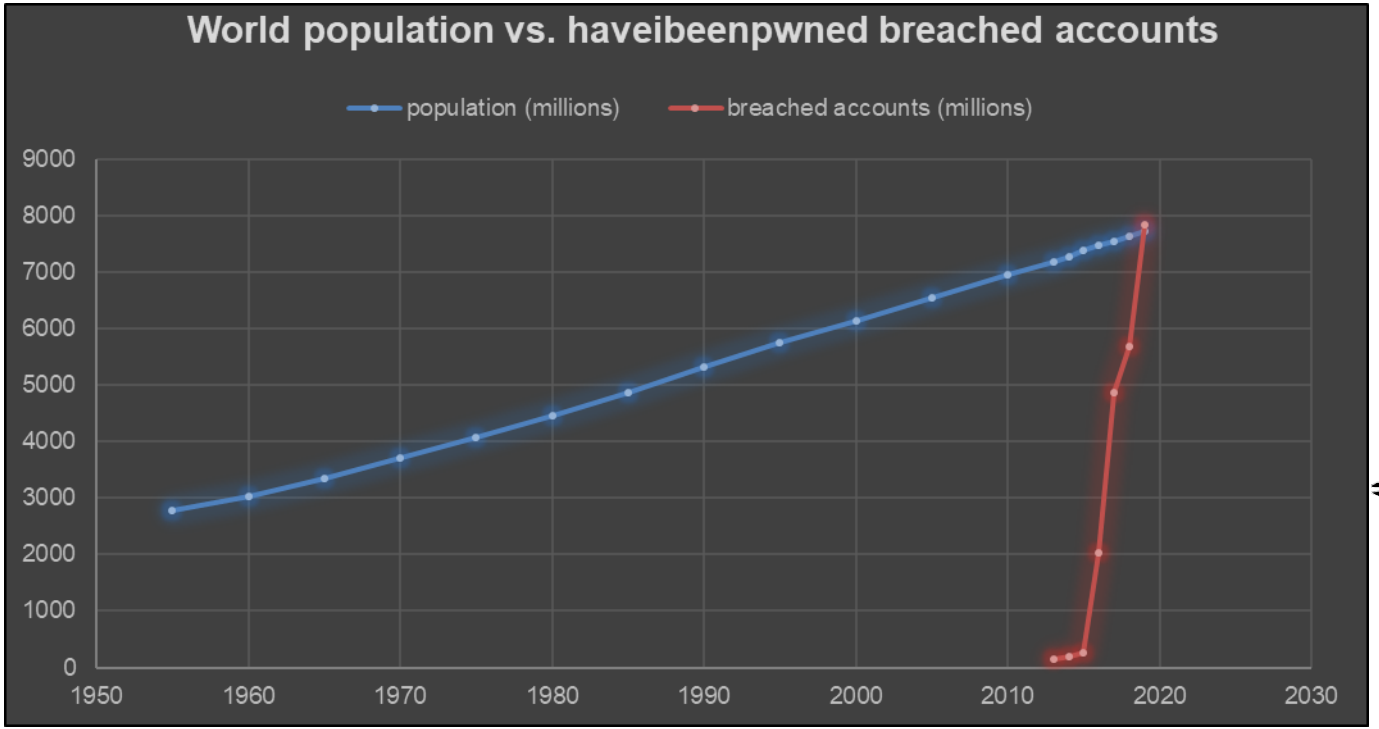
@Bakk3rM

Agenda

Why?

TaHiTI

Sad statistics ‘;--



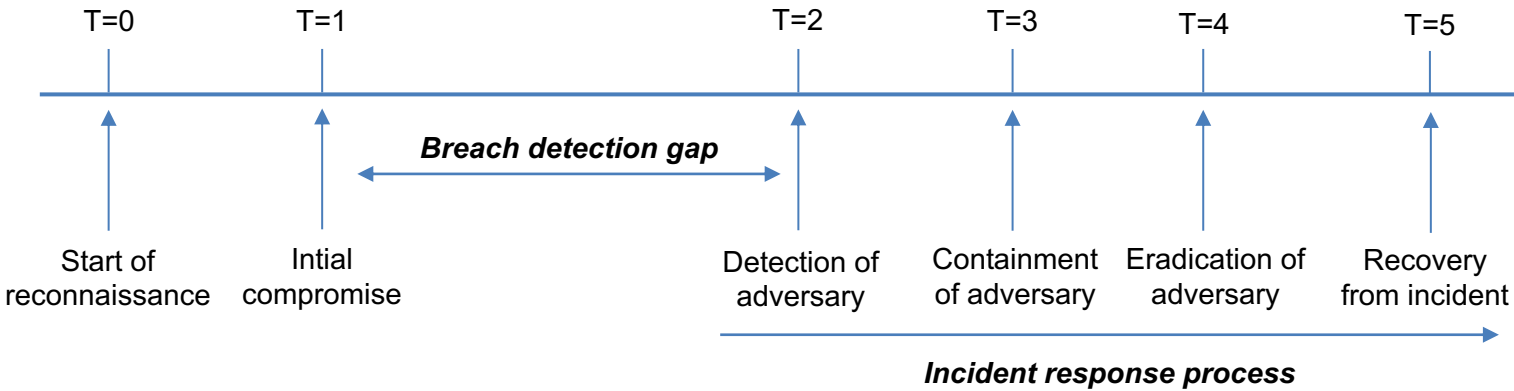
Assume breach

TaHiTI

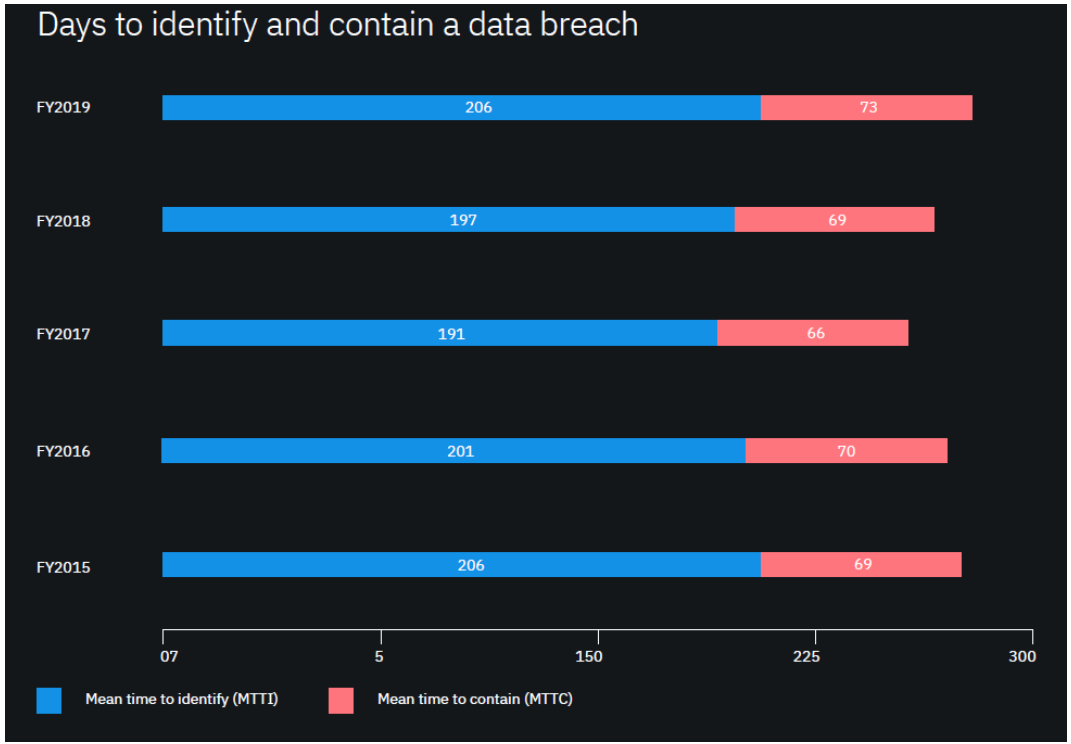
Prevent – Detect - Hunt

Prevent *what you can,* ***Detect*** *what you can't prevent and* ***Hunt*** *what you can't detect*

Dwell Time


T=0
T=1
T=2
T=3
T=4
T=5
Breach detection gap
Start of reconnaissance
Intial compromise
Detection of adversary
Containment of adversary
Eradication of adversary
Recovery from incident
Incident response process

Dwell Time



Source: Ponemon Cost of a Data Breach Report 2019

Dwell Time

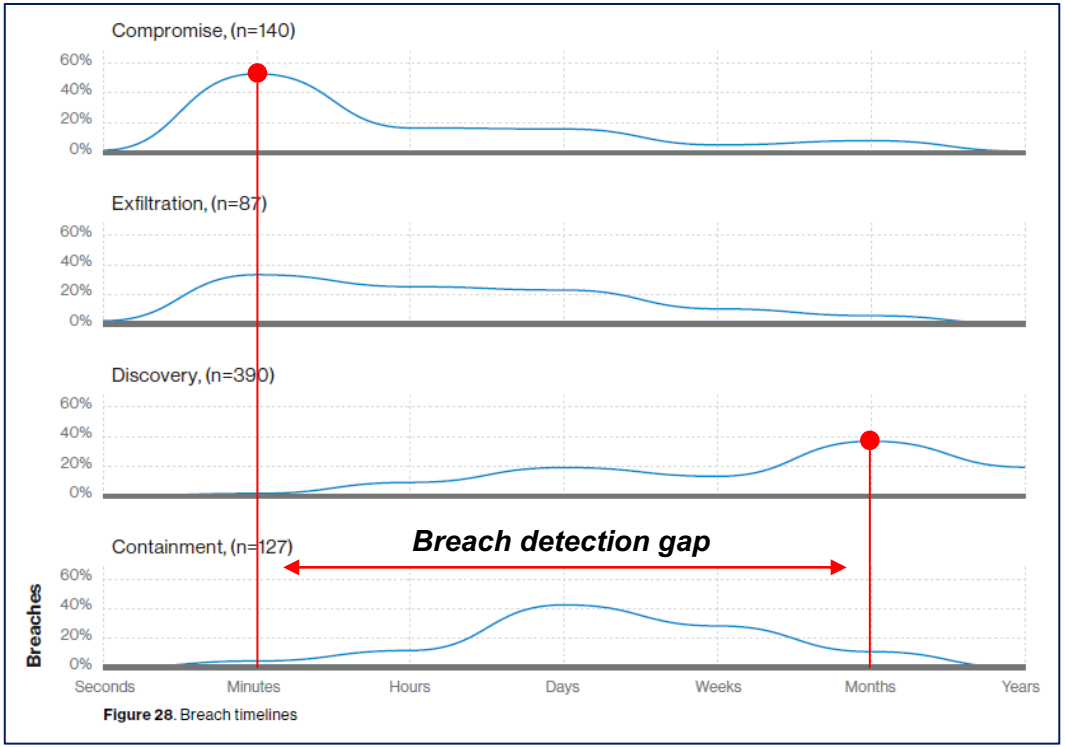
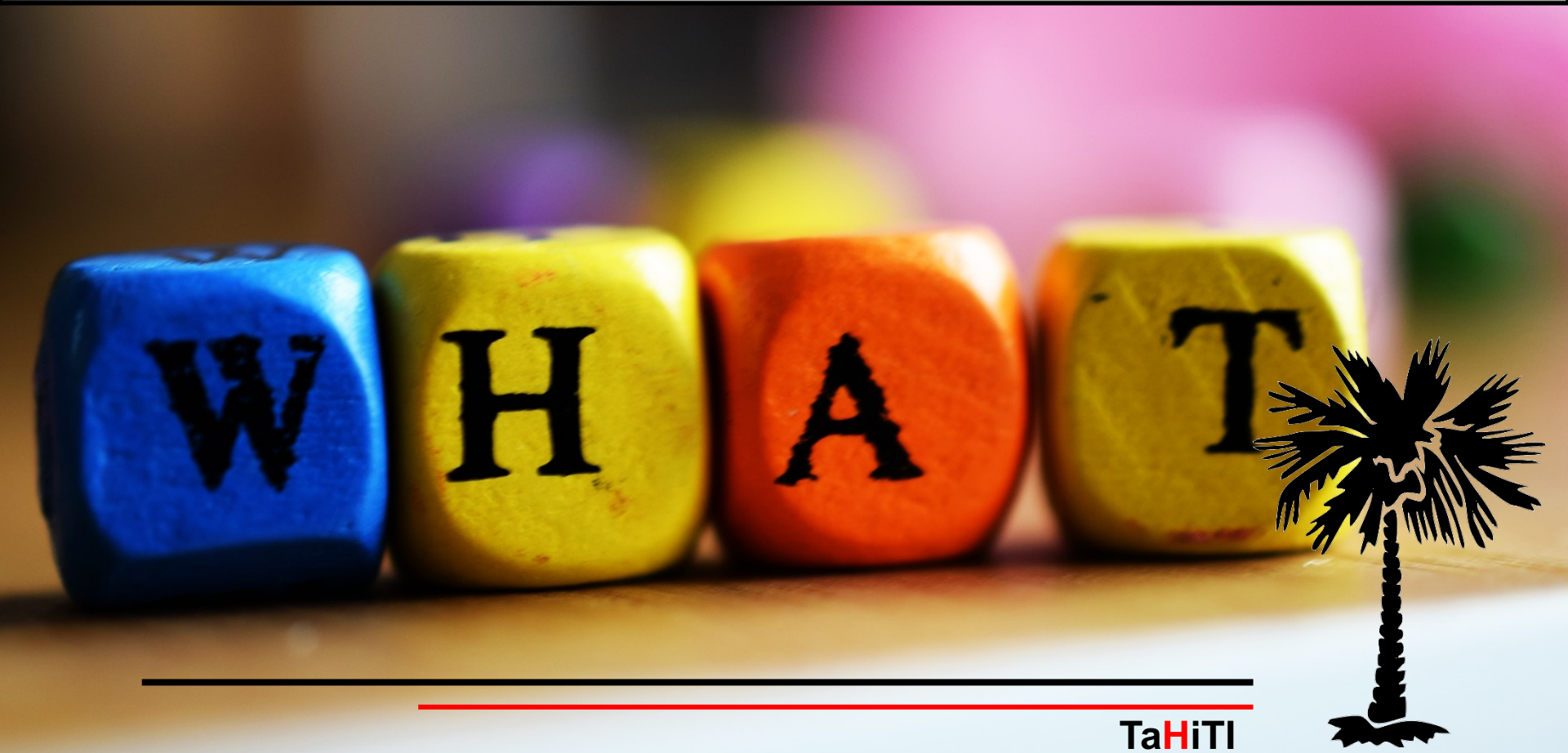


Figure 28. Breach timelines

Source: Verizon Data Breach Investigations Report 2019

TaHiTI

What?



What is (not) threat hunting?

Hunting is:

- a proactive team effort
- searching for signs of malicious behaviour in the IT infrastructure
- applied to current and historical data

Hunting is not:

- a form of pen testing, red teaming or purple teaming
- searching for IoCs
- security monitoring or incident response
- running a query in a tool
- a process with guaranteed results
- easy to conduct

What is TaHiTI?

Targeted Hunting integrating Threat Intelligence

Collaborative effort

ING

ABN·AMRO

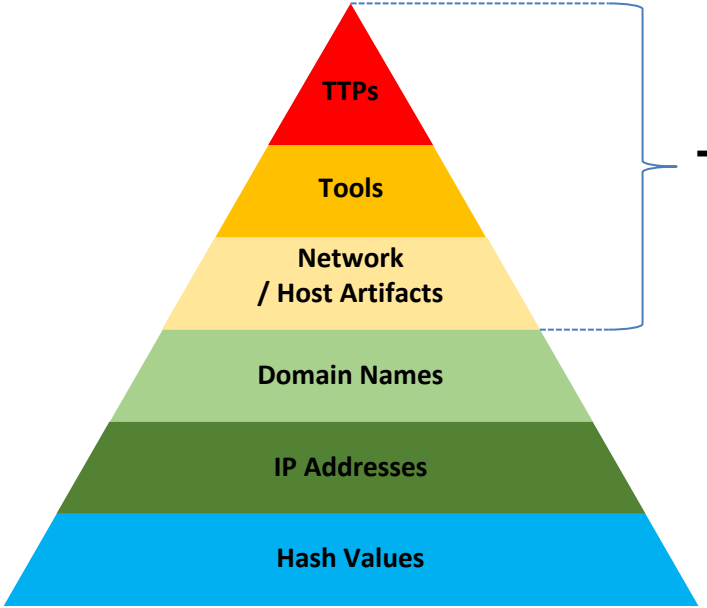
Rabobank

de volksbank

Intelligence driven

Focused on **TTPs**

Pyramid of Pain

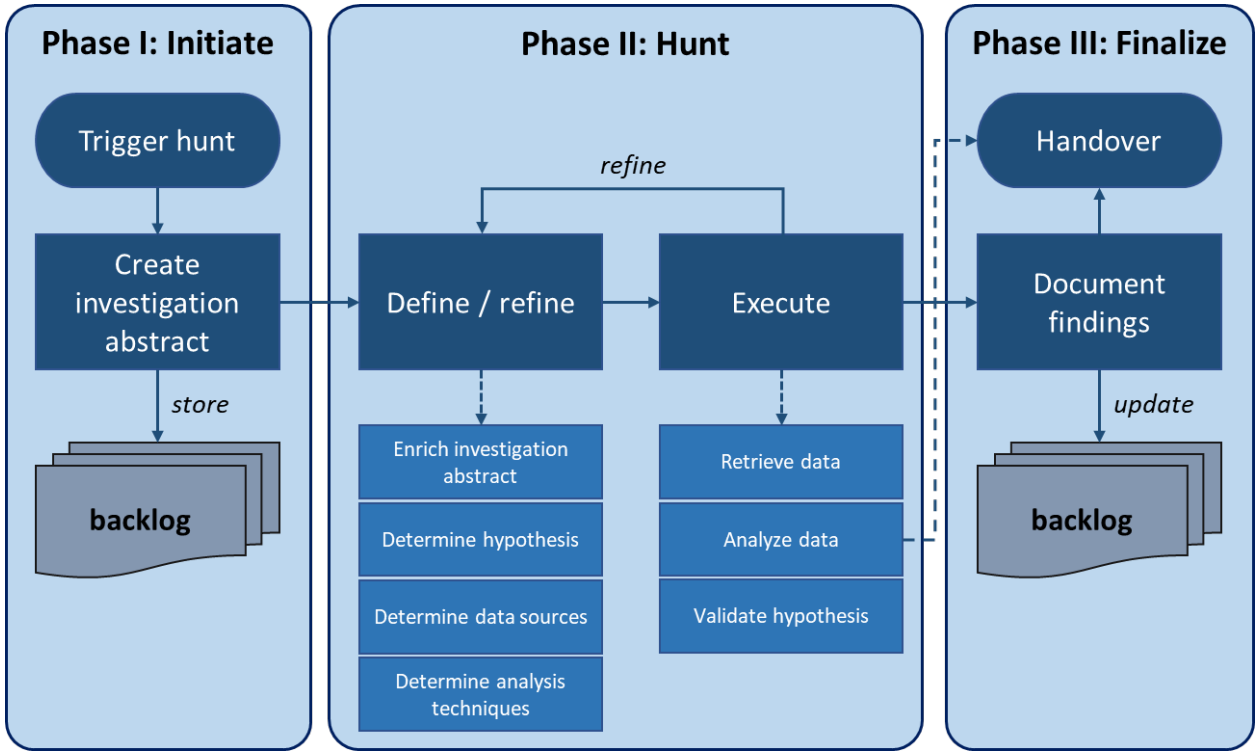


Source: David Bianco, detect-respond blog

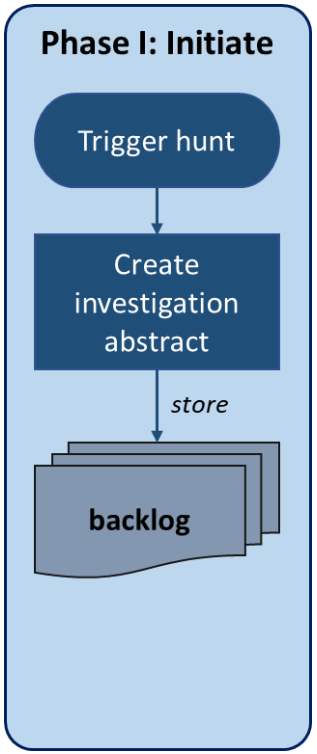
How?

TaHiTI

TaHiTI process



Phase I - Initiate



Triggers

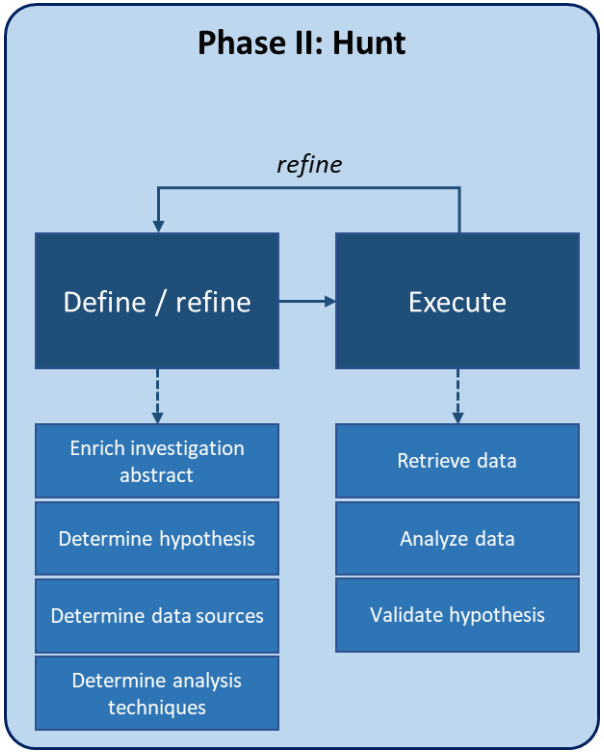
Threat intelligence	Threat hunting	Security monitoring	Security incident response	Other
Threat actor intelligence	Other hunting investigations	Incomplete use cases	Historical incidents	Crown Jewel Analysis
			Red teaming	Domain expertise
				MITRE ATT&CK

Threat Intelligence

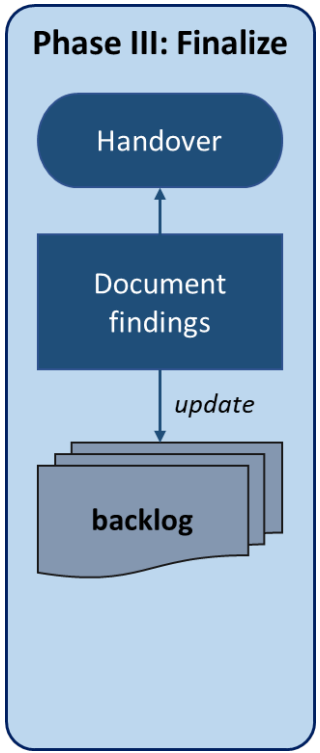
“When you have high quality CTI and effective cyber defence, you need not fear the outcome of a hundred APT attacks.”

- Sun Tzu, The Art of Cyber War

Phase II - Hunt



Phase III - Finalize

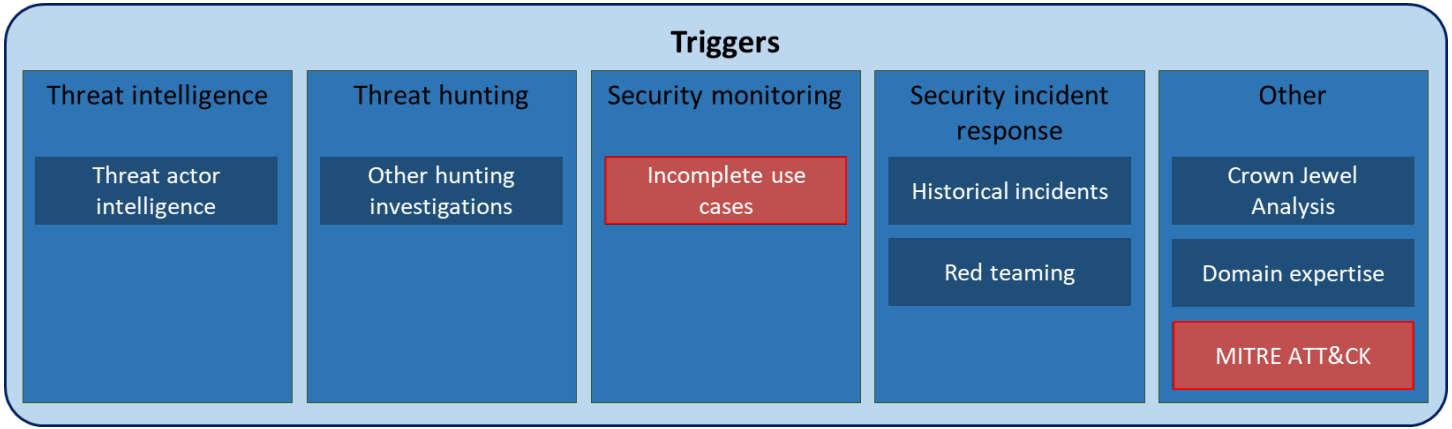


Handover

Security incident response	Security monitoring	Threat intelligence	Vulnerability management	Other
Initiate security incident response	Create or update use cases	Generate TTPs	Resolve vulnerabilities	Other recommendations
		Disseminate		

What to hunt for?

Hunting triggers



Gaps in monitoring (MaGMa)

MaGMa

Use case framework

MaGMa

- **Ma**nagement, **G**rowth, **M**etrics & **a**ssessment
- Use case management framework
- Structure and **score** use cases
- Uncover **gaps** in implemented use cases

TaHiTI

Prioritize defence/hunting efforts (DeTT&CT)

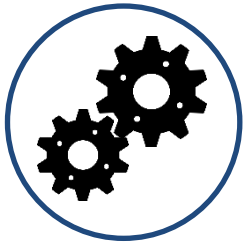
DeTT&CT

DeTT&CT

- **D**etect **T**actics, **T**echniques **&** **C**ombat **T**hreats
- Score and compare **data log source quality**, **visibility** coverage, **detection** coverage and **threat actor behaviors**
- Prioritize defense efforts

Best practices

Best practices for threat hunting



Automate and **standardize** where possible

Use a **dedicated** team if possible

Track and learn from **mistakes**

Use **metrics** to show added value

Wrap up

- Threat hunting is used to **reduce the dwell time** of security incidents
- **TaHiTI** provides a methodology for conducting threat hunting
- Use **threat intelligence** to **trigger** hunting investigations and **contextualize** hunts
- Investigations must be scoped and based on **hypotheses**
- Use frameworks and tools like **MaGMa** and **DeTT&CT** to find **gaps** in visibility and monitoring

Thank you

TaHiTI

www.betaalvereniging.nl/en/safety/tahiti

MaGMa

Use case framework

www.betaalvereniging.nl/en/safety/magma

DeTT&CT

github.com/rabobank-cdc/DeTTECT