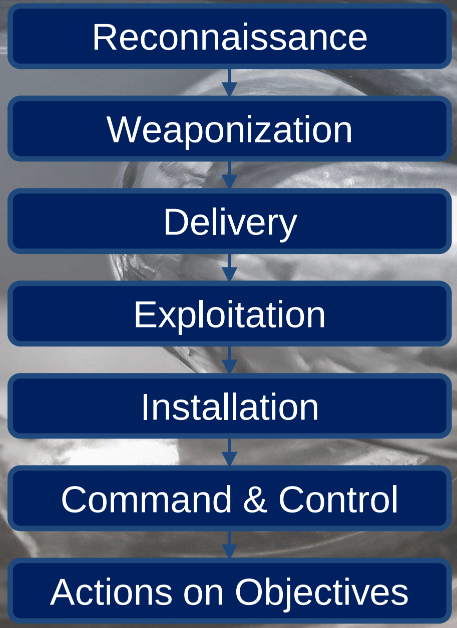
Kill Chains & Attack Anatomy

Rob van Os – Product Owner Cyber Defense Center
rob.vanos@devolksbank.nl

Cyber Kill Chain

Cyber Kill Chain

- Defined by Lockheed Martin
- Describes the anatomy of an APT attack in 7 stages
- Describes possible courses of action for each stage (D6)



Reconnaissance

Weaponization

Delivery

Exploitation

Installation

Command & Control

Actions on Objectives

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Cyber Kill Chain - CoA

D6

- Detect
- Deny
- Disrupt
- Degrade
- Deceive
- Destroy

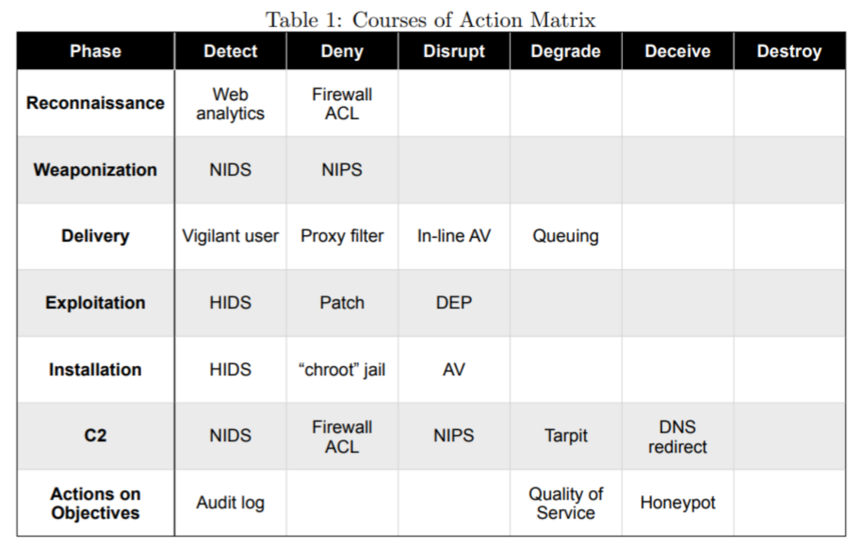


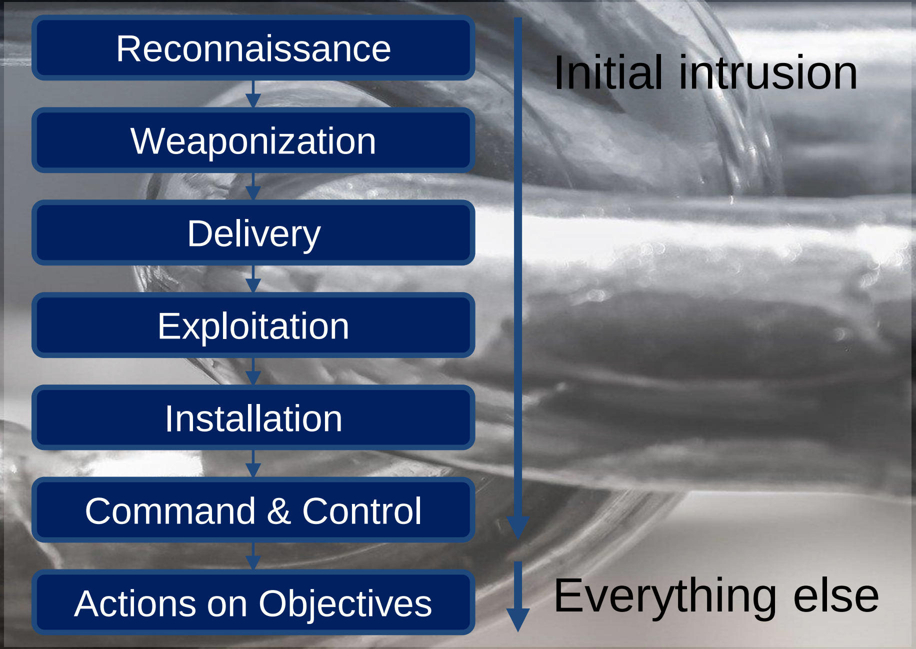
Table 1: Courses of Action Matrix

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

Cyber Kill Chain - shortcomings

Shortcomings

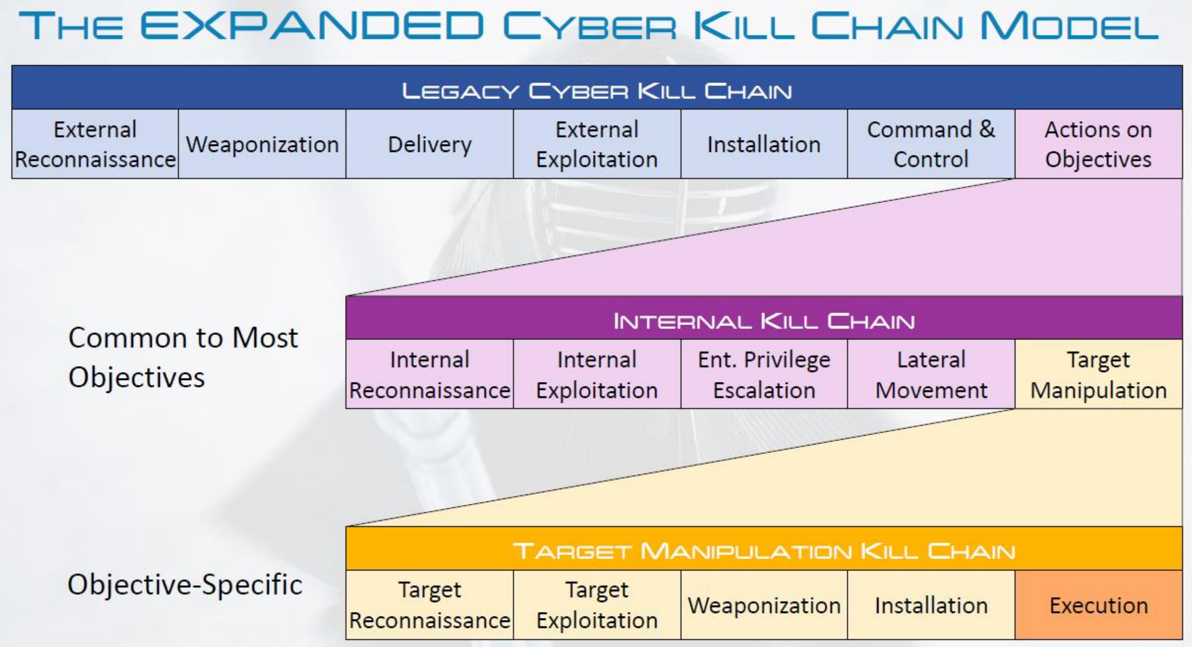
- Everything after initial intrusion is ‘actions on objectives’
- Limited to APT attacks (e.g. does not apply to insider threat)



Expanded Cyber Kill Chain

Expanded CKC

- Takes Actions on Objectives and adds 2 chains
- Internal KC: what happens within the target infrastructure?
- Target manipulation KC: what happens to the target of attack?



THE EXPANDED CYBER KILL CHAIN MODEL

LEGACY CYBER KILL CHAIN

External Reconnaissance	Weaponization	Delivery	External Exploitation	Installation	Command & Control	Actions on Objectives

Common to Most Objectives

INTERNAL KILL CHAIN

Internal Reconnaissance	Internal Exploitation	Ent. Privilege Escalation	Lateral Movement	Target Manipulation

Objective-Specific

TARGET MANIPULATION KILL CHAIN

Target Reconnaissance	Target Exploitation	Weaponization	Installation	Execution

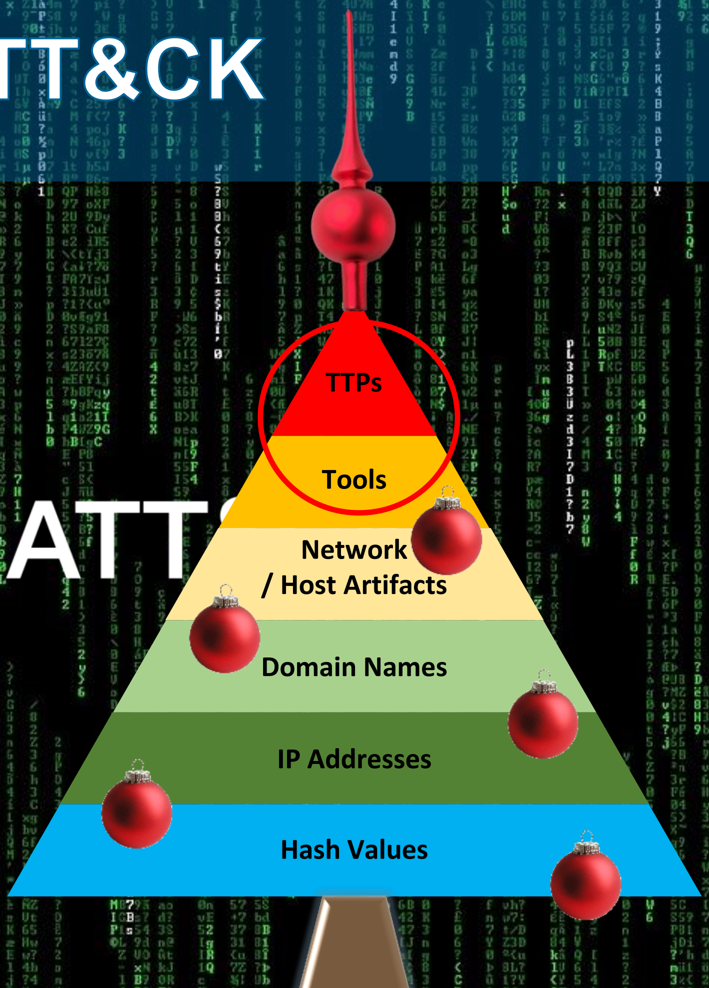
https://www.seantmalone.com/research/

MITRE ATT&CK

ATT&CK

- Description of tactics and techniques used by attackers during attacks
- 12 tactics in total
- Lists data sources for detection
- Lists attacker groups and tools / software used in attacks
- TTP – P = ATT&CK

https://attack.mitre.org/

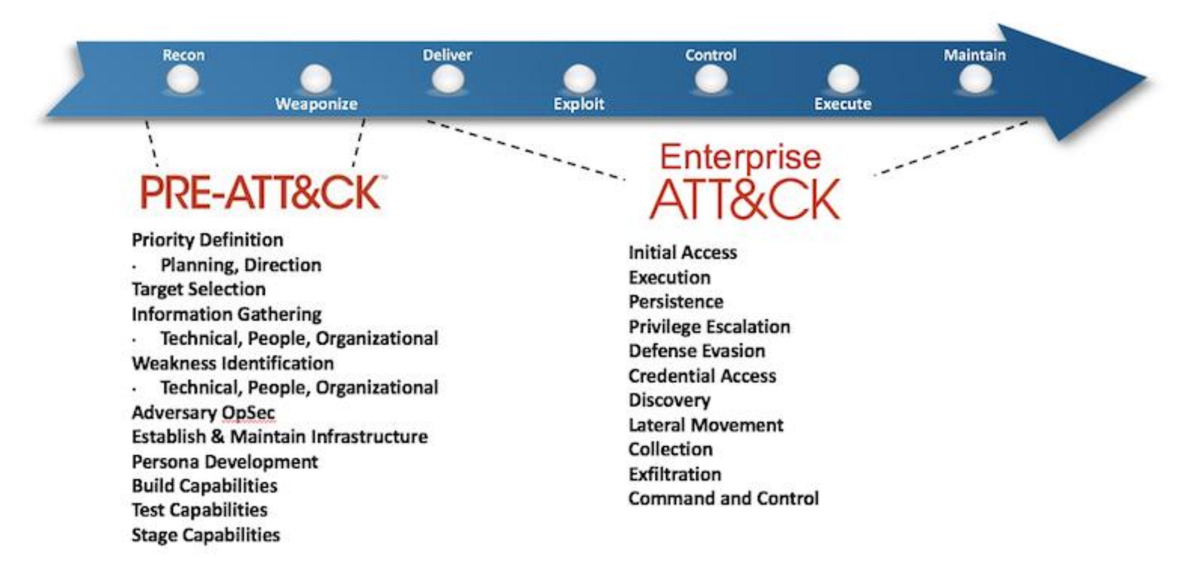


http://detect-respond.blogspot 13/03/the-pyramid-of-pain.html

MITRE PRE-ATT&CK

PRE-ATT&CK

- Description of tactics and techniques used by attackers in preparation for attacks
- 15 tactics in total
- Most techniques can not be monitored



PRE-ATT&CK™

Priority Definition
- Planning, Direction

Target Selection
Information Gathering
- Technical, People, Organizational

Weakness Identification
- Technical, People, Organizational

Adversary OpSec
Establish & Maintain Infrastructure
Persona Development
Build Capabilities
Test Capabilities
Stage Capabilities

Enterprise ATT&CK

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

https://attack.mitre.org/matrices/pre/

Unified Cyber Kill Chain

ATT&CK vs. CKC

- Attempts to align MITRE (PRE)ATT&CK and the traditional Cyber Kill Chain
- 18 stages in total

Unified Kill Chain	Cyber Kill Chain	Expanded KC	PRE-ATT&CK	ATT&CK
Reconnaissance	V	V	V	
Weaponization	V	V	V	
Delivery	V	V		Initial Access
Social Engineering			V	
Exploitation	V	V		Execution
Persistence	Installation	Installation		V
Defense Evasion				V
Command & Control	V	V		V
Pivoting	Actions on objectives			
Discovery		int. recon.		V
Privilege Escalation		V		V
Execution				Execution
Credential Access				V
Lateral Movement		V		V
Collection				V
Exfiltration				V
Target Manipulation		V		Impact
Objectives		Execution		Impact

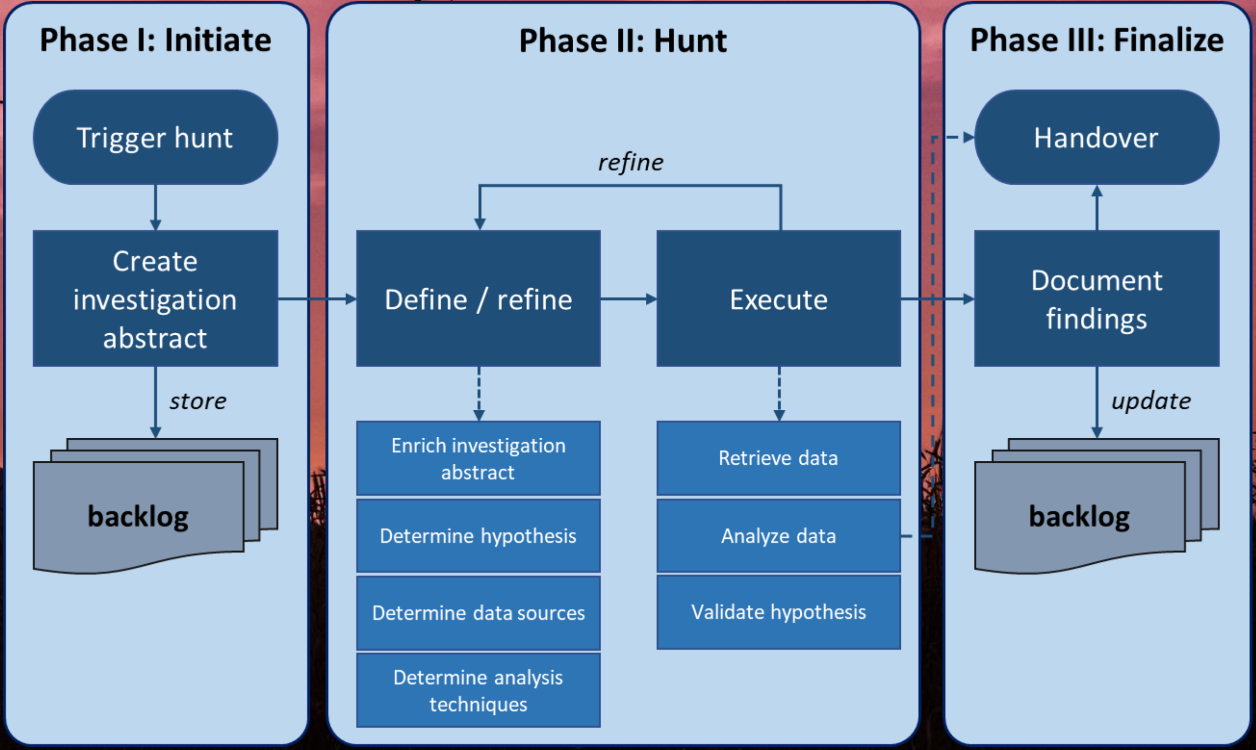
https://www.csacademy.nl/images/scripties/2018/Paul_Pols_-_The_Unified_Kill_Chain_1.pdf

Applications of MITRE ATT&CK

Threat Hunting

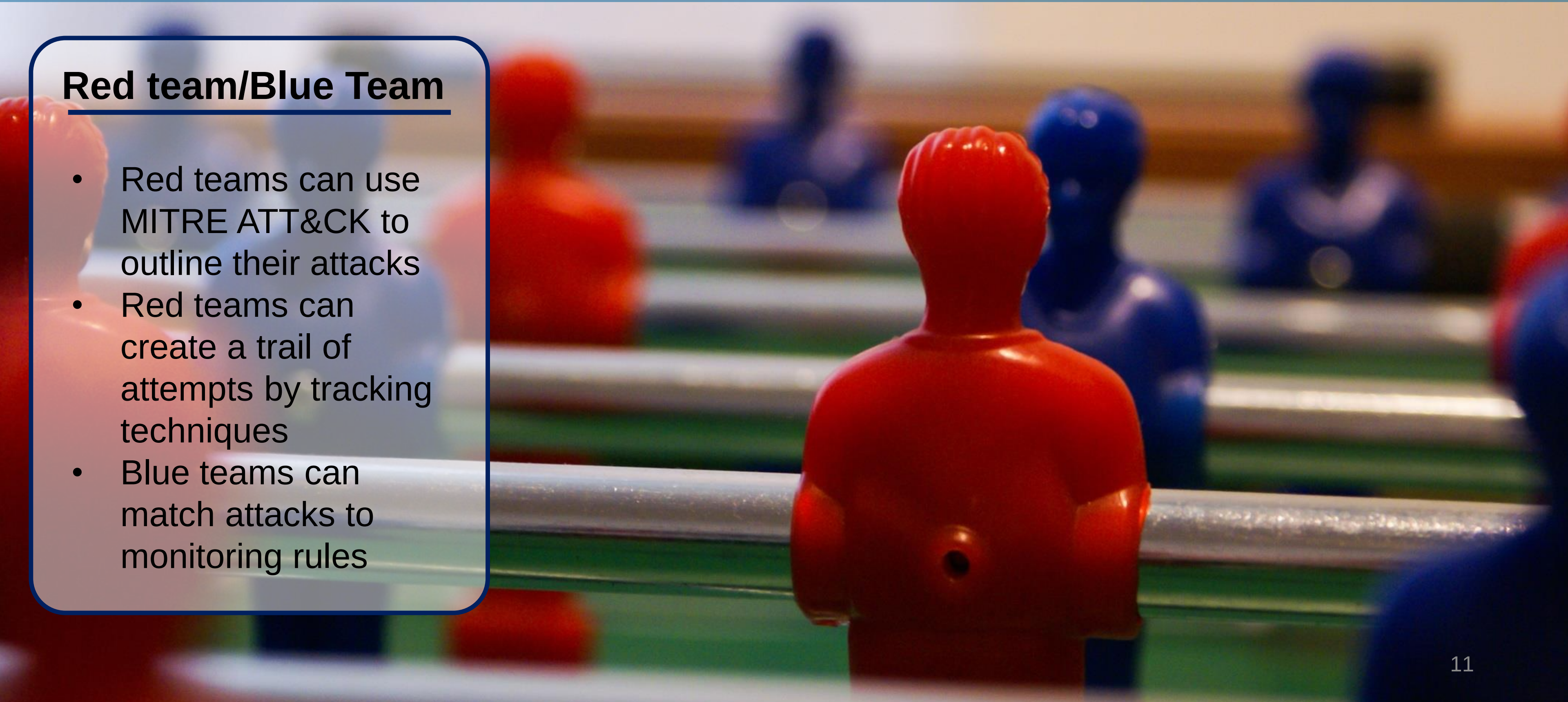
TaHiTI

- Hunting teams can use MITRE ATT&CK as a source of input for defining hunting investigations



https://www.betaalvereniging.nl/en/safety/tahiti

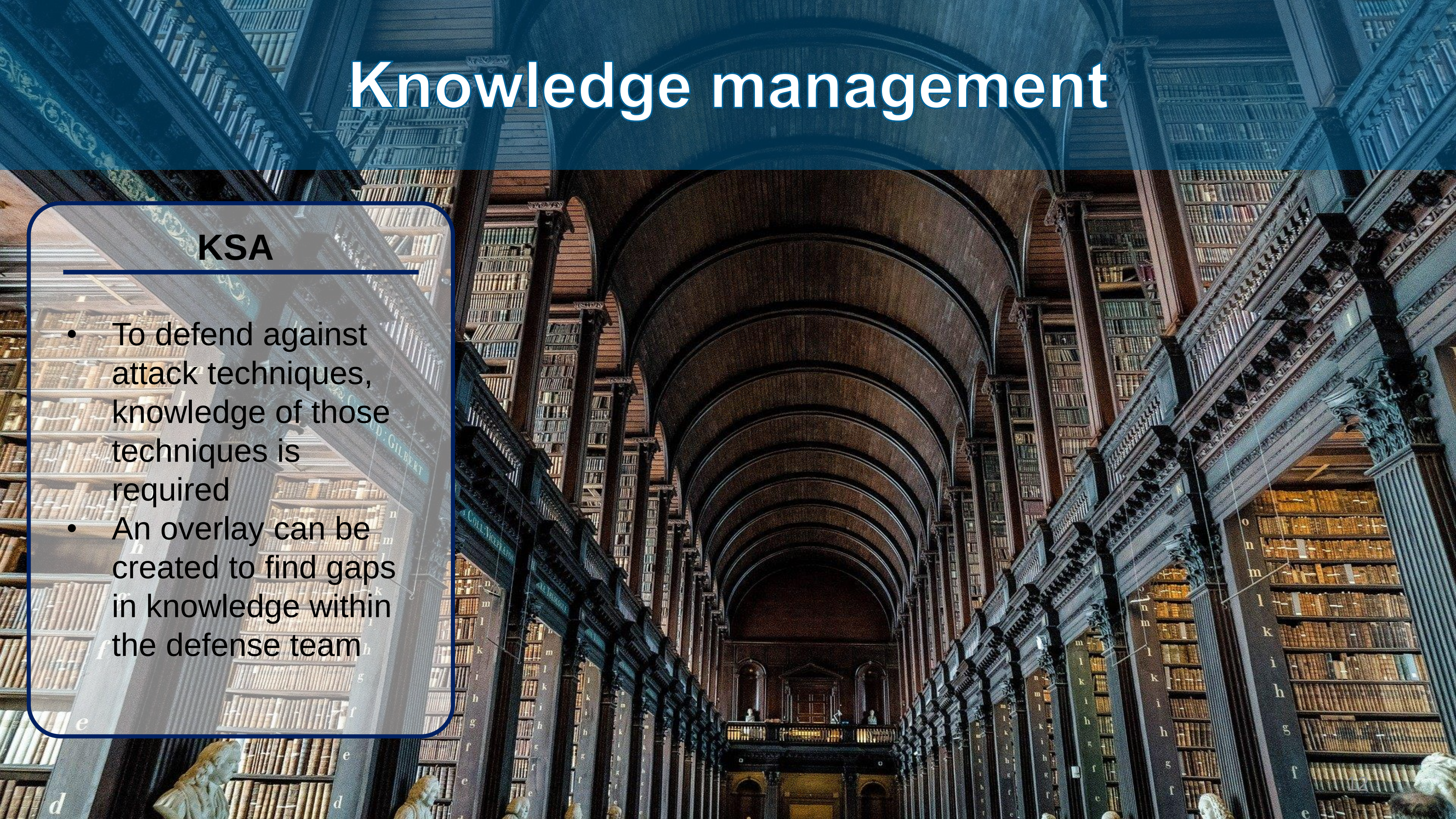
Red Teaming



Red team/Blue Team

- Red teams can use MITRE ATT&CK to outline their attacks
- Red teams can create a trail of attempts by tracking techniques
- Blue teams can match attacks to monitoring rules

Knowledge management



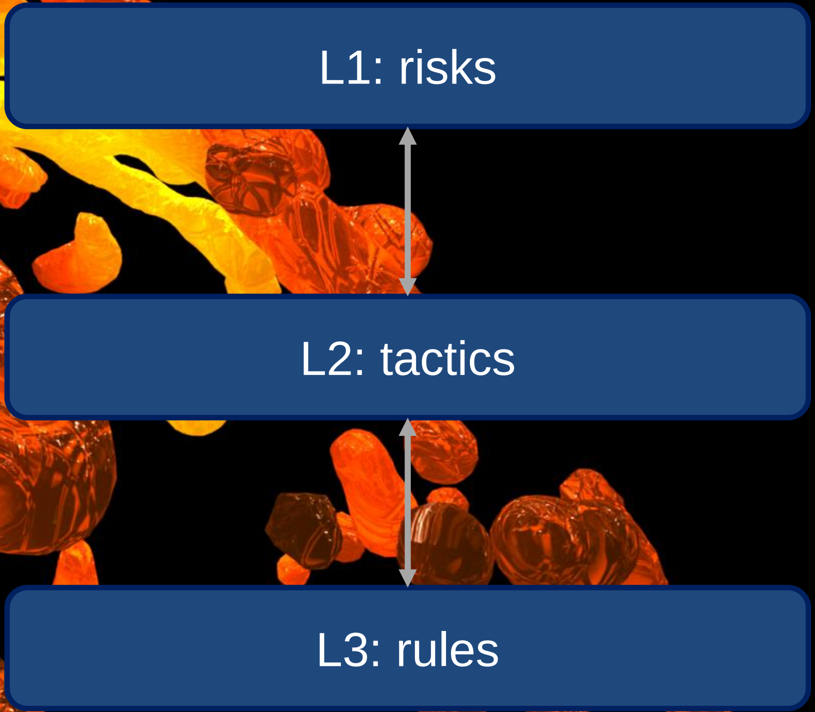
KSA

- To defend against attack techniques, knowledge of those techniques is required
- An overlay can be created to find gaps in knowledge within the defense team

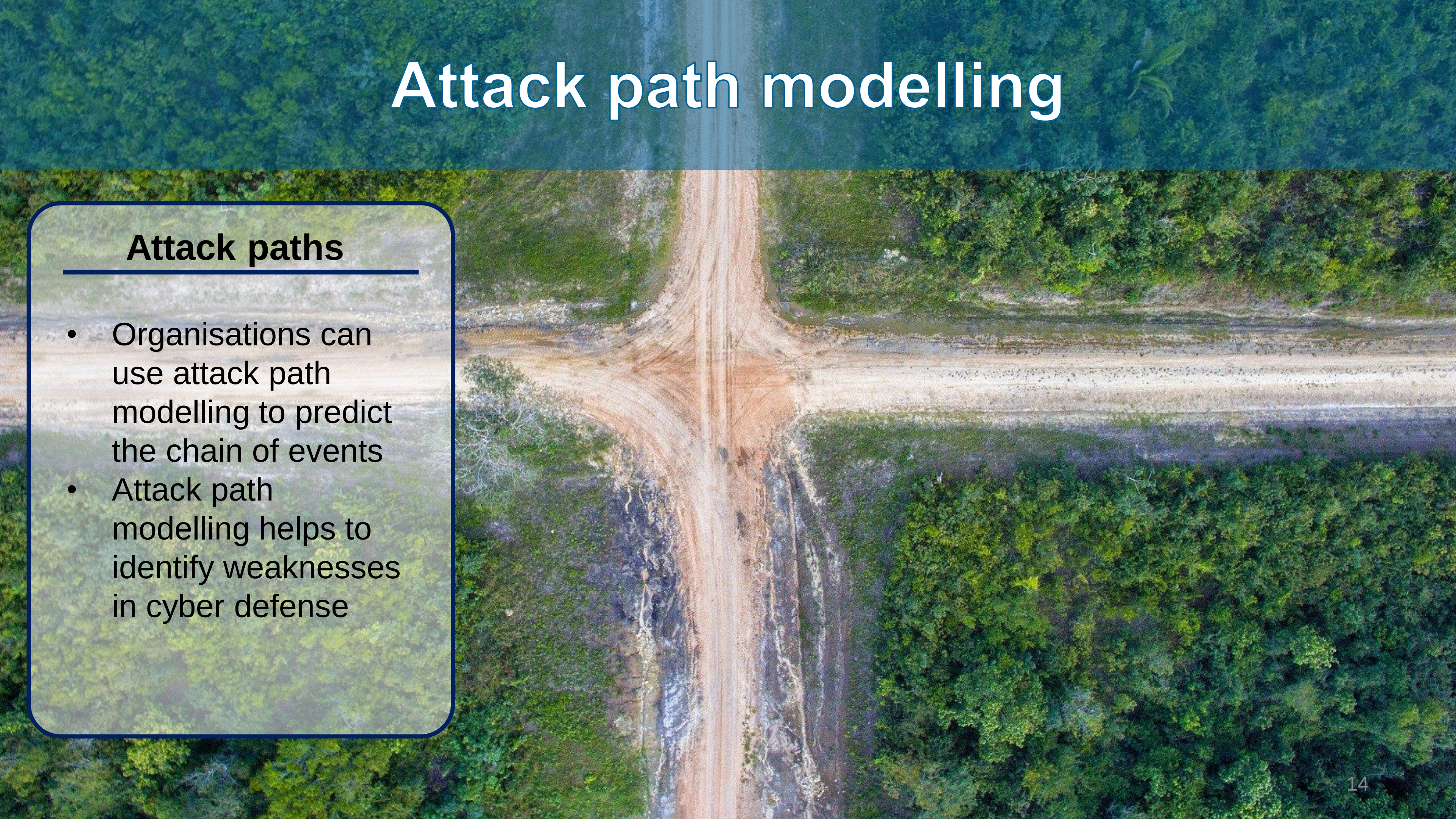
Security monitoring use cases

MaGMa

- L3 is aligned with MITRE ATT&CK
- L1 is aligned with the traditional Cyber Kill Chain
- MITRE ATT&CK can be used to find gaps in security monitoring deployments



https://www.betaalvereniging.nl/en/safety/magma



Attack path modelling

Attack paths

- Organisations can use attack path modelling to predict the chain of events
- Attack path modelling helps to identify weaknesses in cyber defense

Threat intelligence

TI context

- TI can be contextualised using MITRE ATT&CK technique references
- Allows for a single ‘language’ for detailed attack analysis

Determine visibility and detection

DeTT&CT

- More on this later….

ATT&CK Use Cases

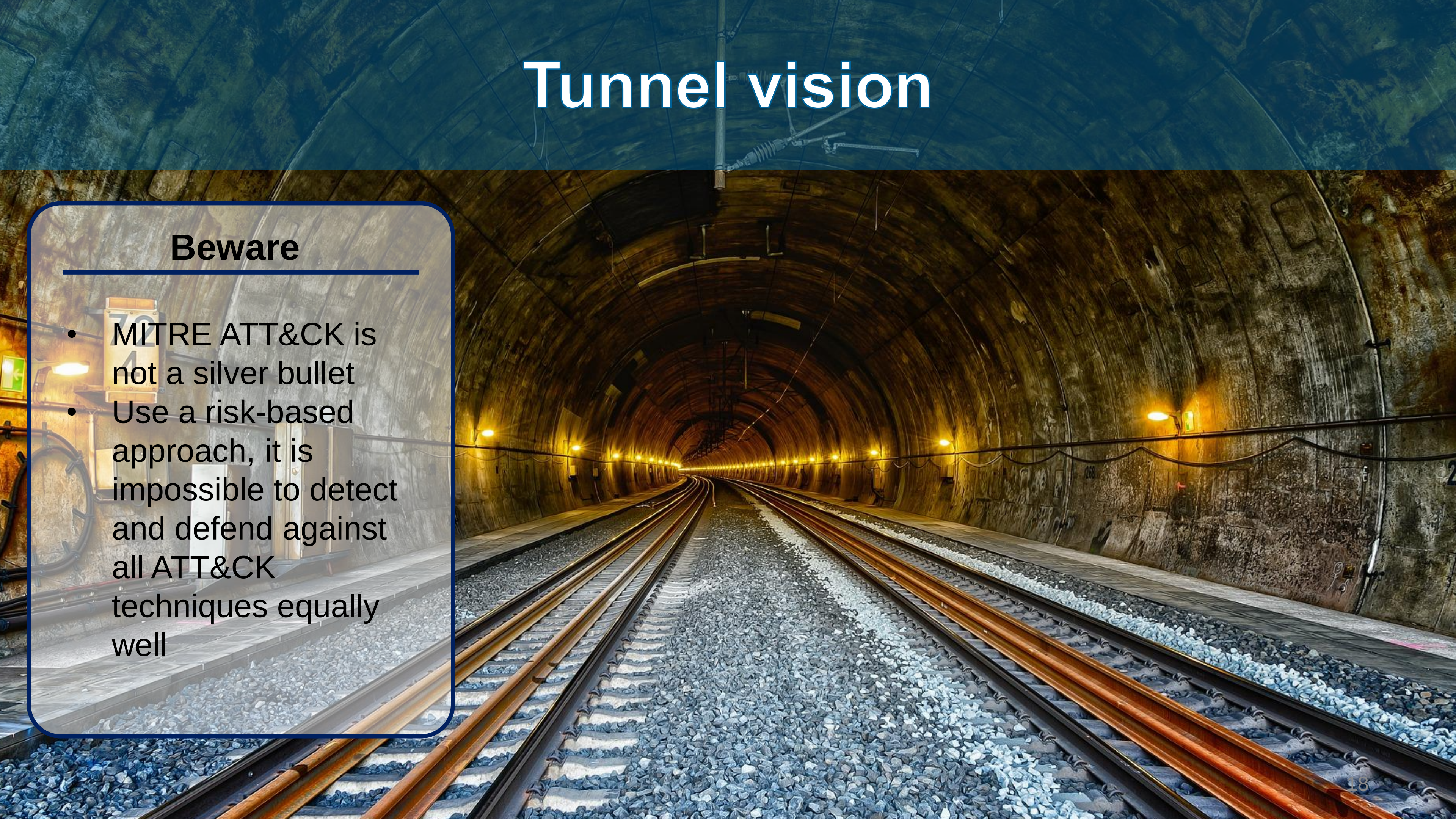
MITRE

- Analyze CND capabilities
- Determine capability coverage
- Describe an intrusion chain of events
- Identify common tradecrafts
- Connect mitigations, weaknesses, and adversaries

MITRE | ATT&CK™

https://attack.mitre.org/resources/enterprise-introduction/

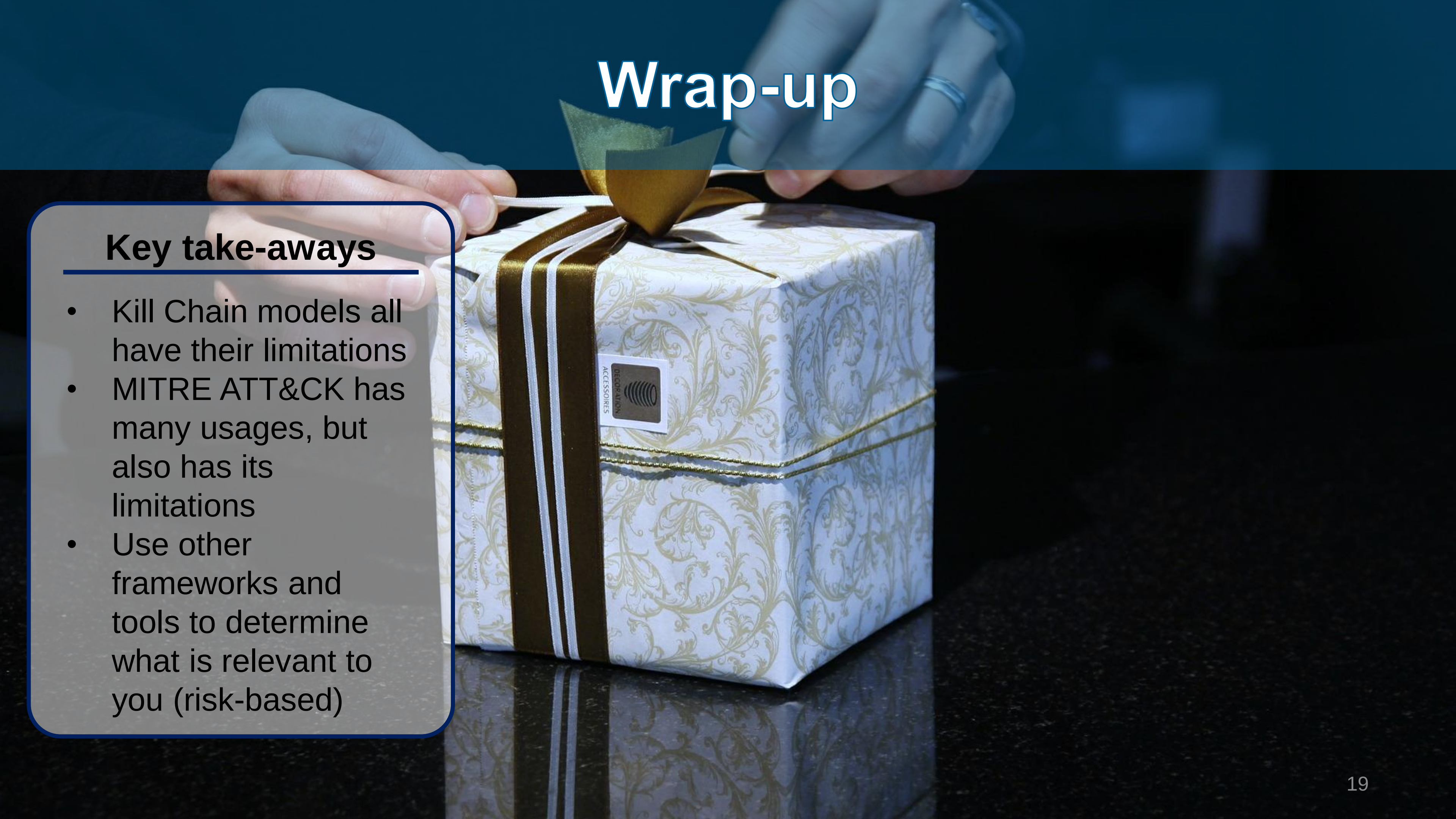
Tunnel vision



Beware

- MITRE ATT&CK is not a silver bullet
- Use a risk-based approach, it is impossible to detect and defend against all ATT&CK techniques equally well

Wrap-up



Key take-aways

- Kill Chain models all have their limitations
- MITRE ATT&CK has many usages, but also has its limitations
- Use other frameworks and tools to determine what is relevant to you (risk-based)

Questions?

Rob van Os – Product Owner Cyber Defense Center
rob.vanos@devolksbank.nl