BANK OF ENGLAND | CYBER DEFENCE CENTRE

Threat Operations using ATT&CK at the Bank of England

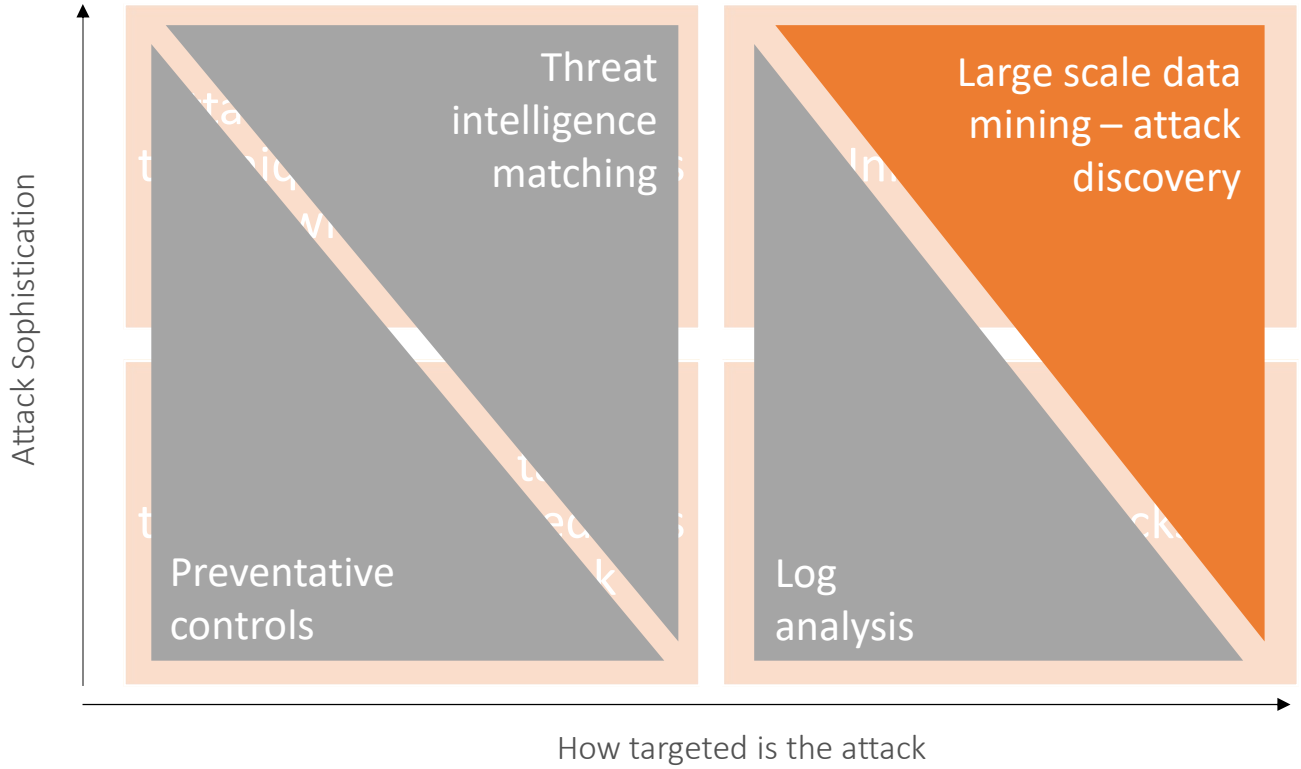
James Morrin

Cyber Defence Intelligence Lead

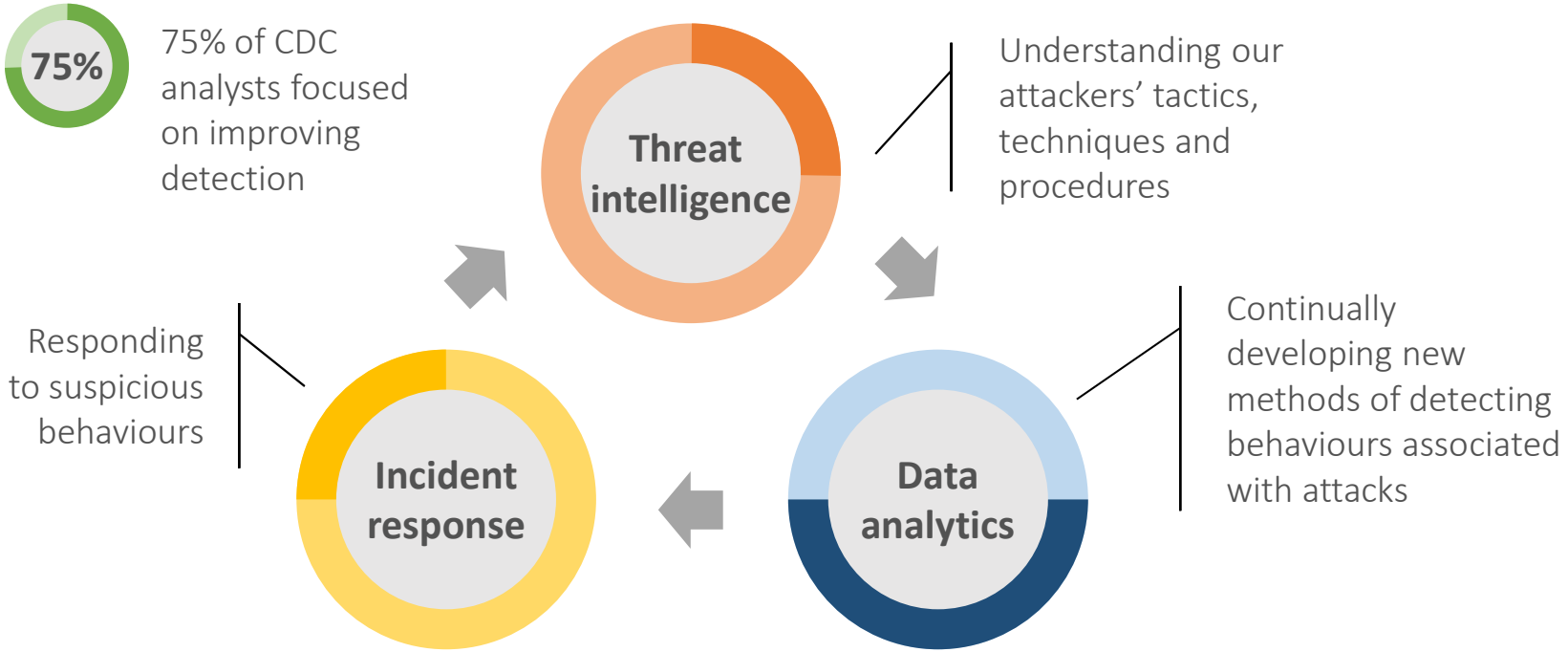
Detect and respond to cyber-attacks against the Bank of England

BANK OF ENGLAND | CYBER DEFENCE CENTRE

CDC – Our approach



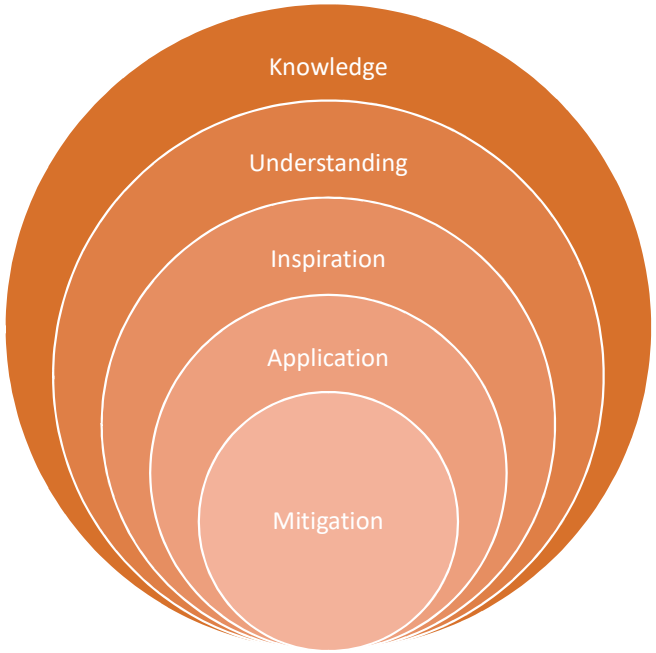
CDC – Our operating model



Point 1: Introducing Threat Operations & ATT&CK

Threat Operations goals:

1. Clear and unified purpose
   - Understand our adversaries and their TTPs
   - Threat-led use case generation
2. Use of a common language
   - Collaborate across TI, red & blue teams – and partners
   - Irrespective of the source format or focus
3. Consistent output and knowledge retention
   - Drive efficiency through consistency
   - Enforced through a compatible threat intelligence platform



DISTILLERY – Distilling raw threat intelligence into use case ideas

- Assessing the value, relevance and confidence of the intelligence
- Assign a rating

- Structuring the intelligence in the TIP

- Extract viable TTP snippets against ATT&CK
- Creating UC ideas
- Assessing against current understanding

- Gap Analysis
- Determine effectiveness of existing UCs
- Prioritisation for UC generation
- Update threat matrices

- UC development process
- UC fed back into TIP
- IM/IR utilise knowledge in support of triage
- Campaign patterns

DISTILLERY – View from the TIP

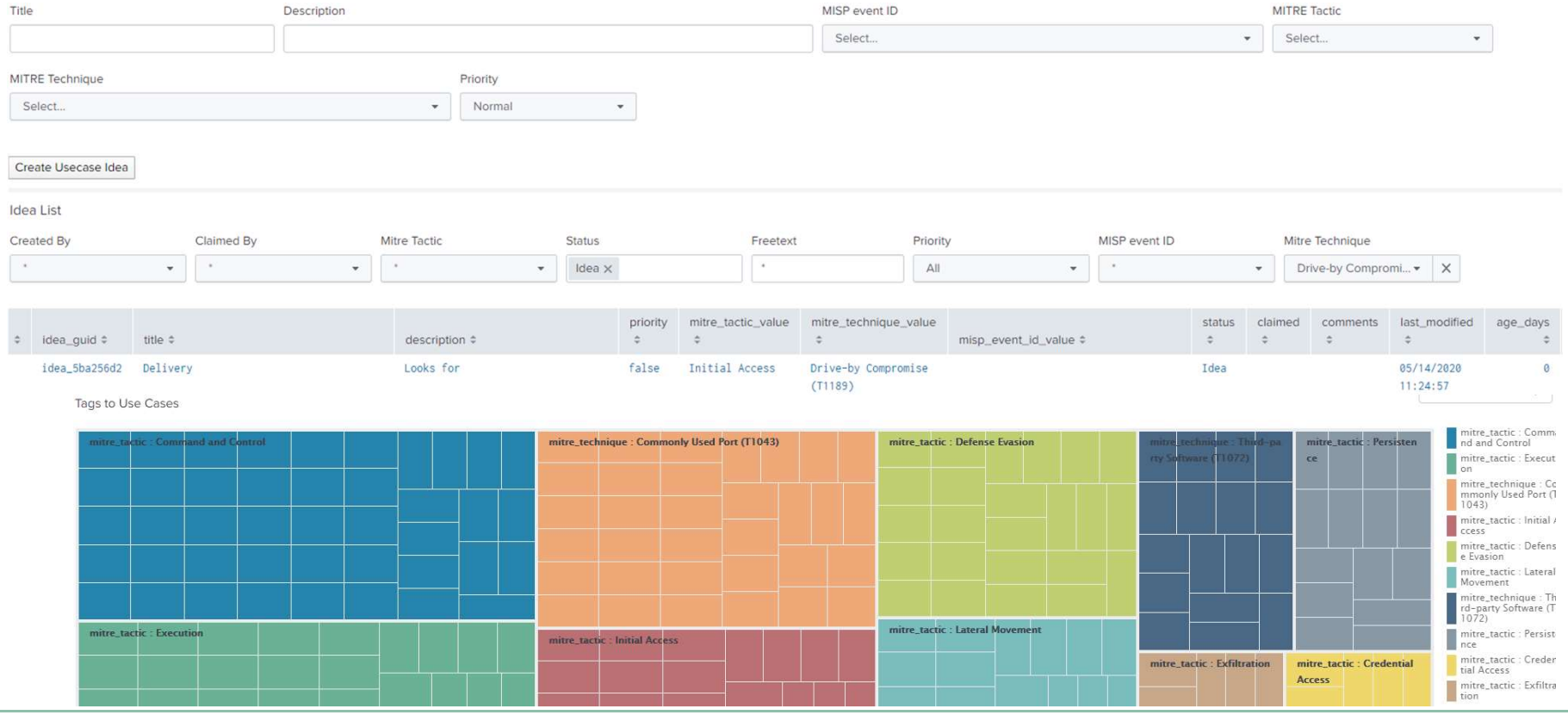
Event ID	10564
UUID	5ebbeecb-2b58-44d1-a03f-44fd0a000004
Creator org	Cyber Defence Centre
Owner org	Cyber Defence Centre
Email	
Tags	CDC Sources: x CDC TIRS:3-Use Case x CDC Workflow:TI-triage-complete x tlp:amber x CDC DA: x CDC Feedback:Rating="#Useful" x CDC Workflow:DA-review-complete x

Galaxies

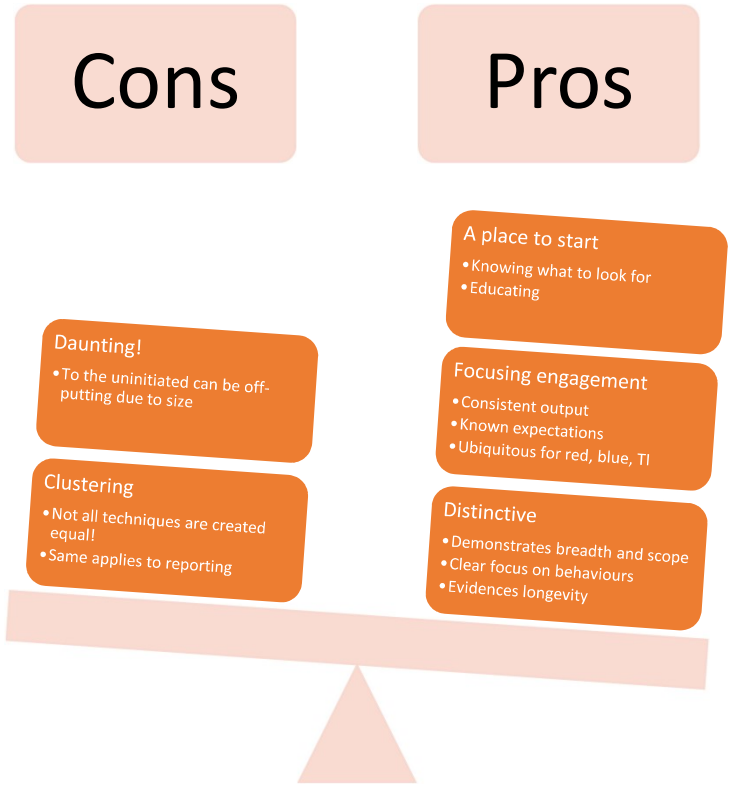
Intrusion Set
+ APT32 - G0050
Attack Pattern
+ Drive-by Compromise - T1189
+ Spearphishing Attachment - T1193
+ Service Execution - T1035

2020-05-18	Name: cdc-kojak References: 0				
2020-05-18	Internal reference	technique-description: text	C2	CDC Feedback:Technique="Technique Created" x	Attack Pattern Domain Generation Algorithms - T1483
2020-05-14	Internal reference	idea: text	C2	CDC Feedback:Kojak="UC Exists" x	CDC Use Cases SOC-LIVE SOC-LIVE SOC-LIVE SOC-LIVE SOC-LIVE Attack Pattern Domain Generation Algorithms - T1483
2020-05-18	Name: cdc-kojak References: 0				
2020-05-18	Internal reference	technique-description: text	Delivery	CDC Feedback:Technique="Technique Created" x	Attack Pattern Drive-by Compromise - T1189
2020-05-14	Internal reference	idea: text	Title:Delivery Description:	CDC Feedback:Kojak="Idea Created" x	Attack Pattern Drive-by Compromise - T1189

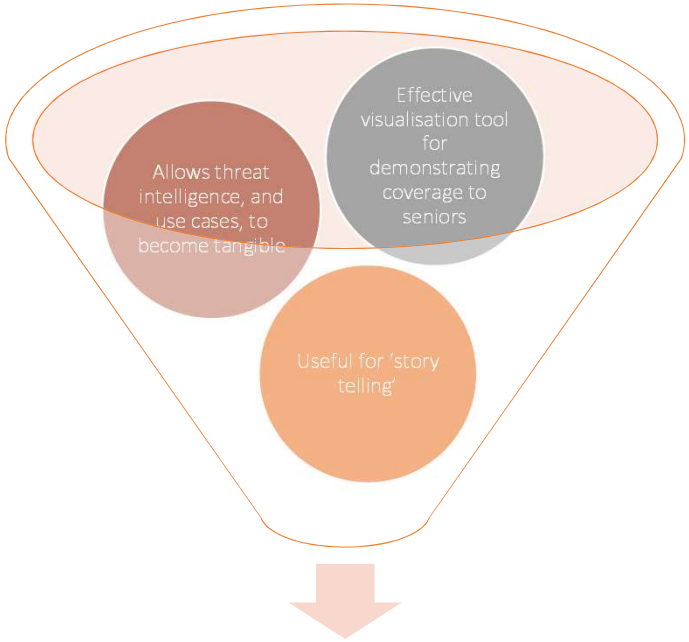
DISTILLERY – View from the SIEM



Point 2: Training and clarity



Point 3: Communicating with seniors



Assurance and understanding

BANK OF ENGLAND | CYBER DEFENCE CENTRE