5 years in adversary emulation

Does Threat Intelligence have a valid role in testing security resilience?

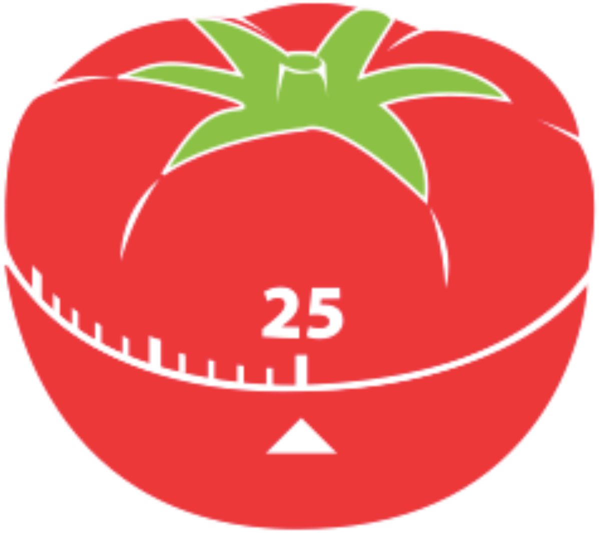
James Chappell – Co-Founder and Chief Innovation Officer
@jimmychappell

digital shadows_

WHO AM I?

In 25 minutes

- Adversary Emulation: brief history
- Experience with CBEST
- Update on TIBER
- Key Takeaways
- The Future?
- Was it worth it?



Disclaimers and Caveats

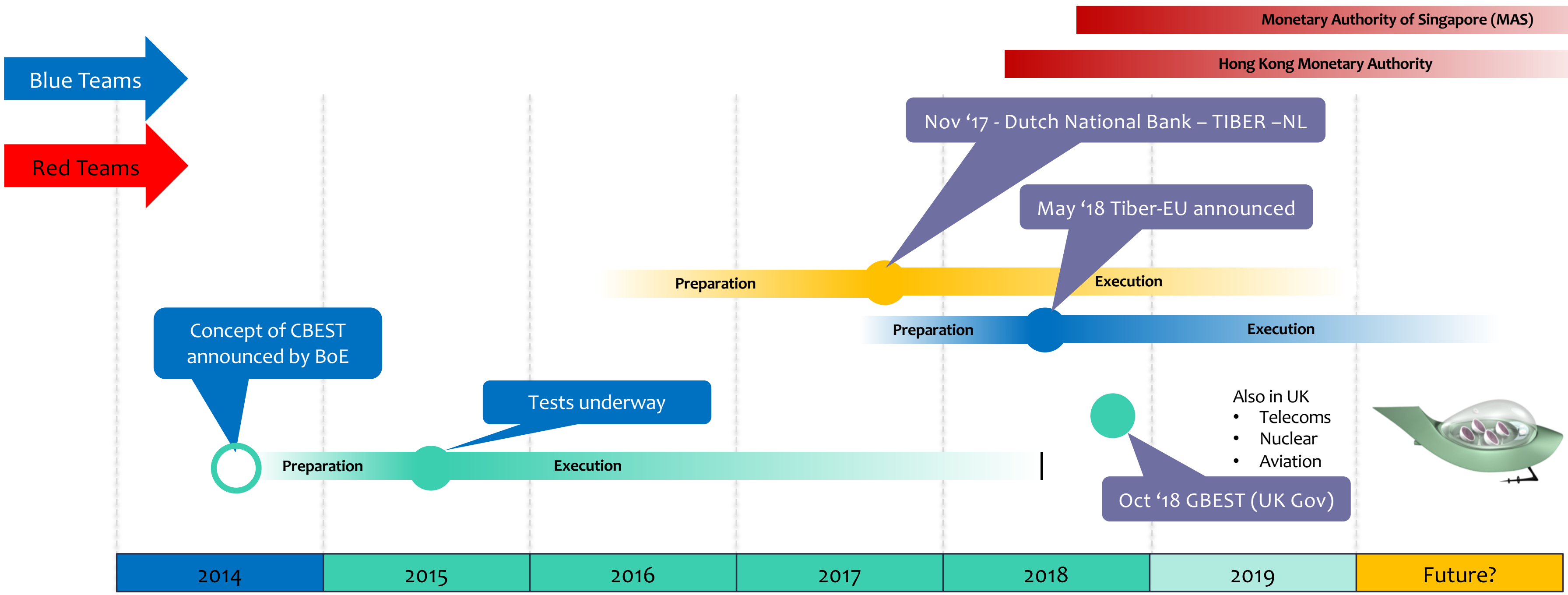
For this presentation:

- I do not represent or speak on behalf of CREST, The Bank of England, Financial Conduct Authority , DNB, ECB or any other regulatory institution – I am simply sharing publicly stated learnings from experience
- I am not able or willing to share details of specific tests but will talk in general about experiences from them
- Digital Shadows do not currently offer CBEST, or TIBER (EU/NL) tests but may do in the future – a good thing: means I can be super honest and direct about our experiences without fear of harming future businesses
- Journalists – please make yourselves known, hopefully this is more about where we take the profession overall, but if you want to write about this I can help!

A journey

digital shadows_

5 (and a bit) years



Monetary Authority of Singapore (MAS)

Hong Kong Monetary Authority

Blue Teams

Red Teams

Nov '17 - Dutch National Bank – TIBER –NL

May '18 Tiber-EU announced

Preparation

Execution

Preparation

Execution

Concept of CBEST announced by BoE

Tests underway

Preparation

Execution

Also in UK
- Telecoms
- Nuclear
- Aviation

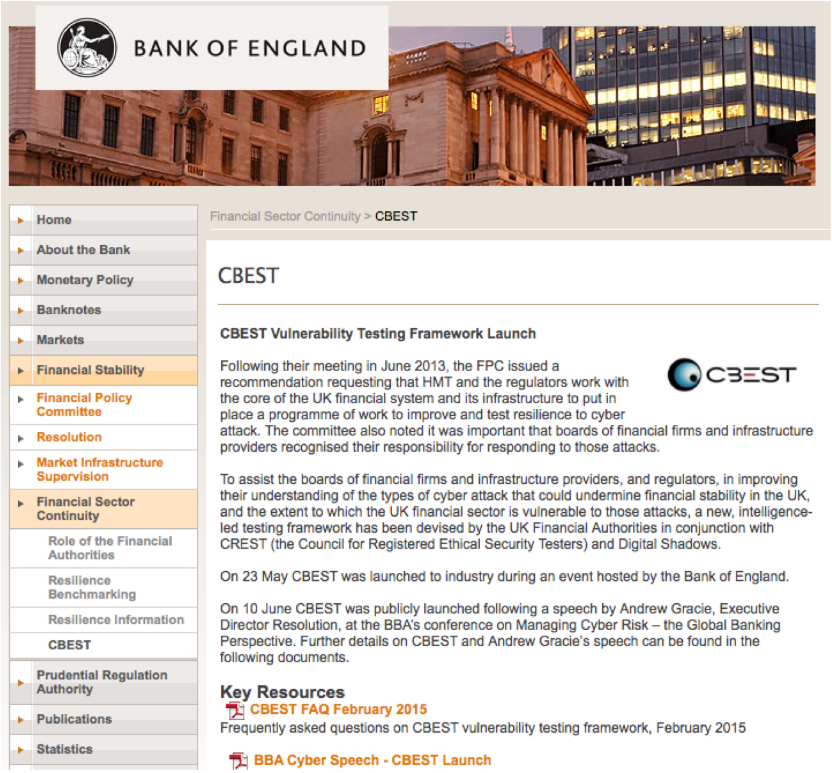
Oct '18 GBEST (UK Gov)

2014	2015	2016	2017	2018	2019	Future?

Phase I - CBEST

digital shadows_

2014 – Threat led security testing


BANK OF ENGLAND
Home
About the Bank
Monetary Policy
Banknotes
Markets
Financial Stability
Financial Policy Committee
Resolution
Market Infrastructure Supervision
Financial Sector Continuity
Role of the Financial Authorities
Resilience Benchmarking
Resilience Information
CBEST
Prudential Regulation Authority
Publications
Statistics
Financial Sector Continuity > CBEST
CBEST

CBEST

CBEST Vulnerability Testing Framework Launch

Following their meeting in June 2013, the FPC issued a recommendation requesting that HMT and the regulators work with the core of the UK financial system and its infrastructure to put in place a programme of work to improve and test resilience to cyber attack. The committee also noted it was important that boards of financial firms and infrastructure providers recognised their responsibility for responding to those attacks.

To assist the boards of financial firms and infrastructure providers, and regulators, in improving their understanding of the types of cyber attack that could undermine financial stability in the UK, and the extent to which the UK financial sector is vulnerable to those attacks, a new, intelligence-led testing framework has been devised by the UK Financial Authorities in conjunction with CREST (the Council for Registered Ethical Security Testers) and Digital Shadows.

On 23 May CBEST was launched to industry during an event hosted by the Bank of England.

On 10 June CBEST was publicly launched following a speech by Andrew Gracie, Executive Director Resolution, at the BBA's conference on Managing Cyber Risk – the Global Banking Perspective. Further details on CBEST and Andrew Gracie's speech can be found in the following documents.

Key Resources

CBEST FAQ February 2015

Frequently asked questions on CBEST vulnerability testing framework, February 2015

BBA Cyber Speech - CBEST Launch

- In May 2014, the Bank of England along with the professional body CREST launched CBEST and STAR testing frameworks
- CBEST introduced a threat led approach to conducting security testing.

Goals:

1. realistic tests based upon a set of evidence of threats observed in the wild. Tailored to the customer
2. Hold institutions accountable to testing being a true test of resilience
3. Broader in scope than a traditional pen test (a red team approach) focused on **critical economic functions (CEF)**

Drivers: Professional and skilled Red Teams are important but…

- Sometimes solely focused on technical outcomes with technical stakeholders - struggle to involve business stakeholders but “managed by IT/InfoSec team”
- Follows well trodden paths (for good reason, but not articulated why)
- Often conducted work separately from organizations risk assessment
- Regulators want to hold institutions to account to justify tests are true measures of resilience rather than tech for tech sake
- Regulators want boards to get involved in their managing their risks
- Testing often change driven with scope set by what is new, rather than what is important

NOTE: Intelligence should be a way of *supporting* a Red Team not dictating actions.

Why do intelligence before a red team at all?

THREAT INTELLIGENCE

Evidence → **SUPPORTING CREDIBILITY**

Real evidence of threats – not just 'theoretical'

Realism → **EMULATION – A NARRITIVE**
realistic targets, tactics, techniques and procedures

Justification → **SUPPORTS testing decisions**
of test methods as being realistic

Tests focus on the PROBABLE threats rather than the theoretically POSSIBLE

Threat Intel in CBEST: Key outputs

Scenarios

- Threat scenario
- Based on detailed research
- Emulating real threat
- Tailored to **Target** assets

Goals

- A set of Goals for the test team
- A set of agreed ‘flags’ the team must capture

Evidence

- A lot of Supporting Evidence to show that the test is real
- Validated by UK Gov

SUPPORTS SELECTION OF TARGET and TEST PLAN

PRIORITISES “FLAGS” AGAINST GOALS AND MOTIVATION

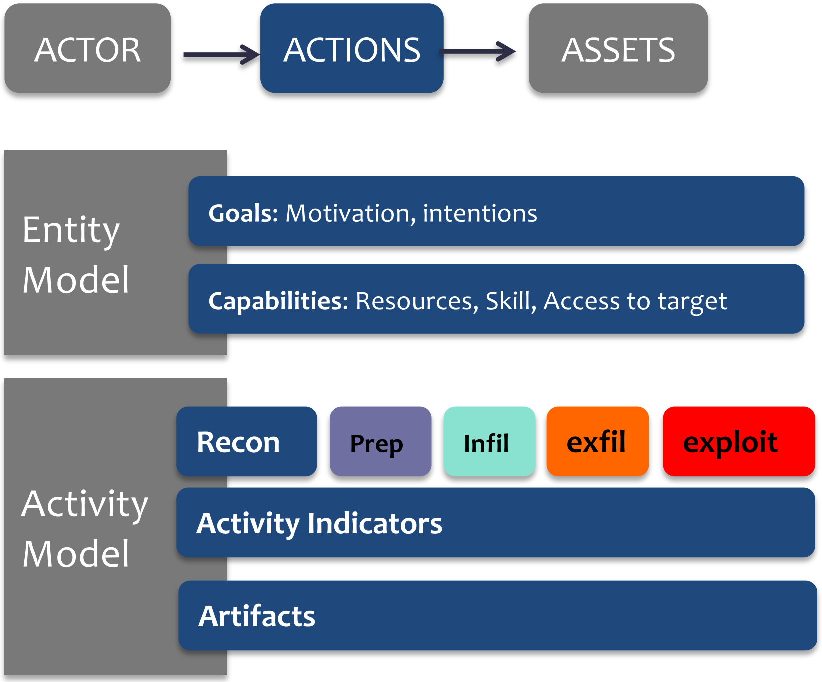
BACKS UP BUSINESS CASE FOR MITIGATING CONTROLS

Model Overview

CBEST

CREST STAR

CBEST Threat Intelligence Framework
Threat Model



ACTOR → ACTIONS → ASSETS

Entity Model

- **Goals:** Motivation, intentions
- **Capabilities:** Resources, Skill, Access to target

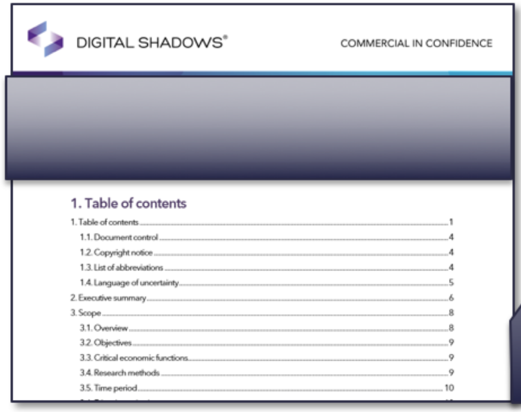
Activity Model

- Recon | Prep | Infil | exfil | exploit
- Activity Indicators
- Artifacts

Output: Threat Scenarios to be used in a test

Threat Intelligence Products

① Threat Intelligence Report



DIGITAL SHADOWS®

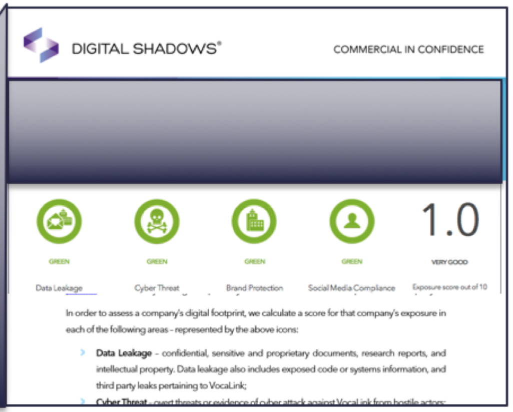
COMMERCIAL IN CONFIDENCE

1. Table of contents

1. Table of contents 1
   1.1. Document control 4
   1.2. Copyright notice 4
   1.3. List of abbreviations 4
   1.4. Language of uncertainty 5
2. Executive summary 6
3. Scope 8
   3.1. Overview 8
   3.2. Objectives 9
   3.3. Critical economic functions 9
   3.4. Research methods 9
   3.5. Time period 10

- Provides analysis of threat groups based on thorough research
- Evidence to justify and support actions of testing team
- **OUTPUT**: Threat Scenarios
- **USE CASE**: Provides supporting evidence for use in security test.

② Targeting (Foot printing) Report



DIGITAL SHADOWS®

COMMERCIAL IN CONFIDENCE

				1.0
GREEN	GREEN	GREEN	GREEN	VERY GOOD
Data Leakage	Cyber Threat	Brand Protection	Social Media Compliance	Exposure score out of 10

In order to assess a company's digital footprint, we calculate a score for that company's exposure in each of the following areas – represented by the above icons:

- **Data Leakage** – confidential, sensitive and proprietary documents, research reports, and intellectual property. Data leakage also includes exposed code or systems information, and third party leaks pertaining to VocaLink;
- **Cyber Threat** – overt threats or evidence of cyber attack against VocaLink from hostile actors;

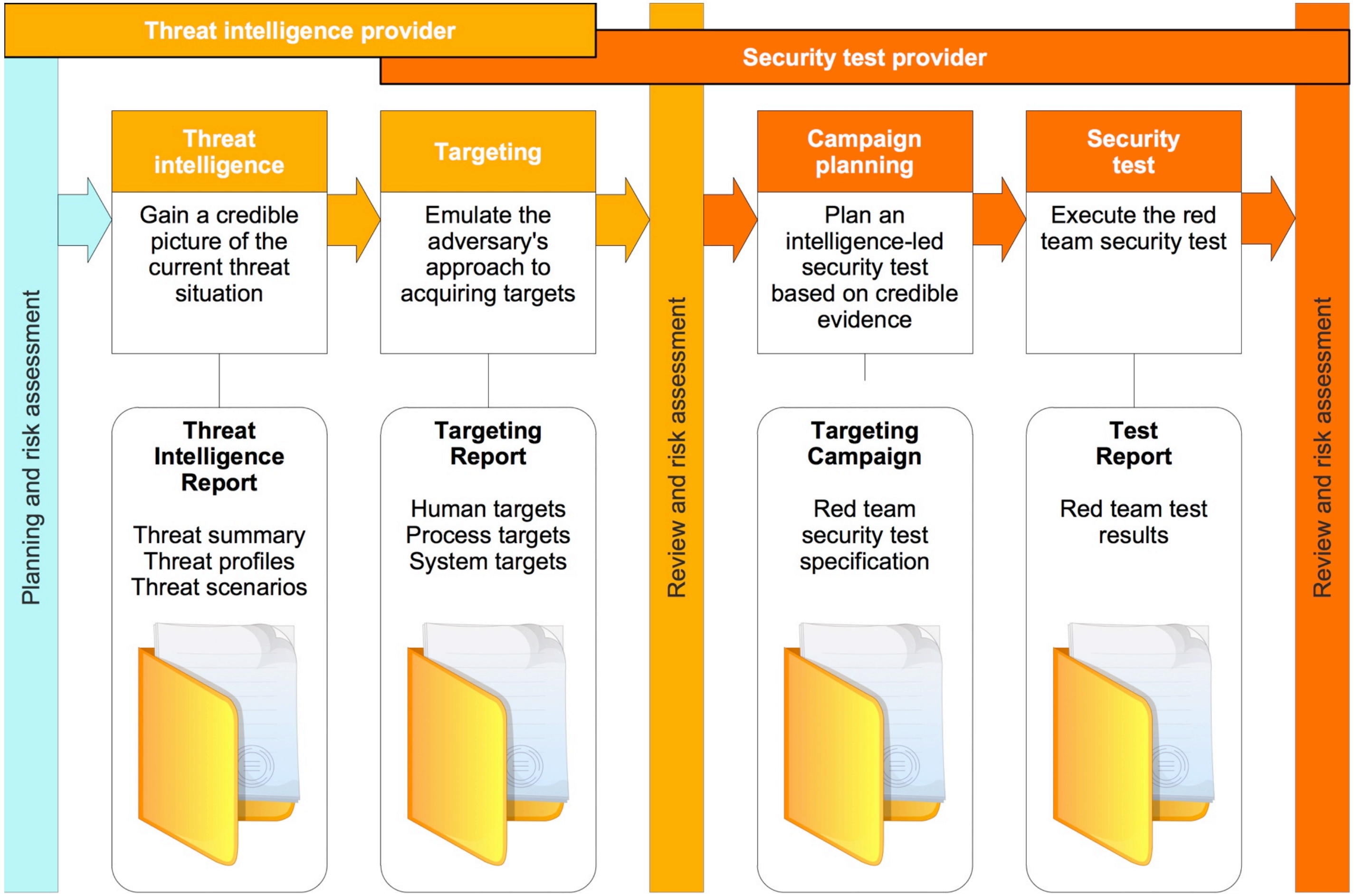
- Broad analysis of digital footprint to identify riskier areas
- NOT a full reconnaissance exercise
- **OUTPUT**: Initial targets for test
- **USE CASE**: Provides input into reconnaissance phase of security test.

Threat landscape

Threat source	Capability	Intent/ activity	Threat score to Client
Insider intentional*	H	H	16
Nation State – Disruption and Attack (CNA)	VH	M	15
Nation State – Espionage (CNE)	VH	M	15
Organised Crime – Economic	H	M	12
Nation State Proxy	M	M	9
Hacktivist	L-M	M	6
Journalist/researcher	L	L	4
Organised Crime – Extortion	M	VL	3
Insider unintentional	VL	VL	1

Scoring based on high watermark assessment

CBEST intelligence and testing processes



Threat intelligence provider

Security test provider

Planning and risk assessment

Threat intelligence

Gain a credible picture of the current threat situation

Targeting

Emulate the adversary's approach to acquiring targets

Review and risk assessment

Campaign planning

Plan an intelligence-led security test based on credible evidence

Security test

Execute the red team security test

Review and risk assessment

Threat Intelligence Report

Threat summary
Threat profiles
Threat scenarios

Targeting Report

Human targets
Process targets
System targets

Targeting Campaign

Red team security test specification

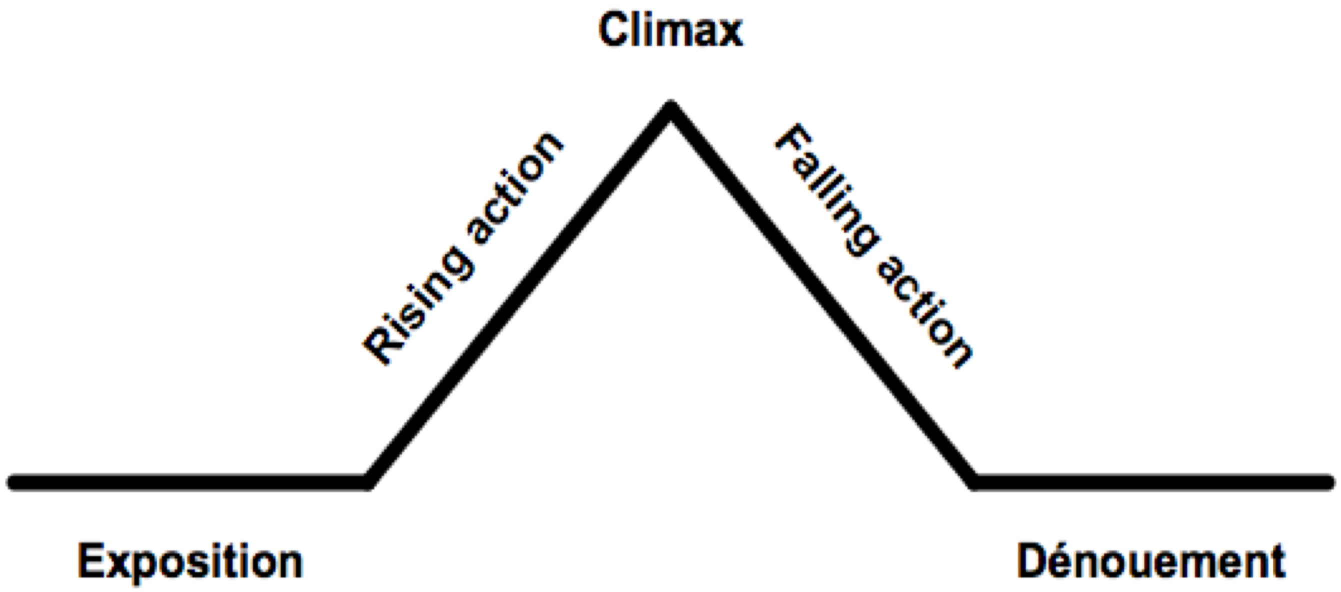
Test Report

Red team test results

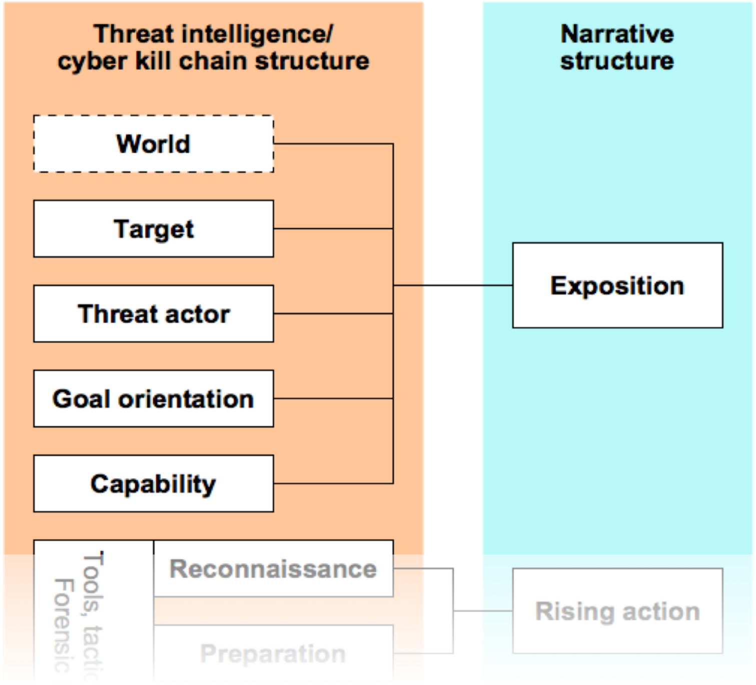
THREAT PROFILES CONSIDERED

- FUZZYSNUGGLYDUCK
- APT7334
- FANCYMOOSE
- Angry Cyber fighters (CNA)
- AnonUnChuffed

Threat Scenarios follow a narrative structure



Mapping to a storyline



Threat intelligence/ cyber kill chain structure

World

Target

Threat actor

Goal orientation

Capability

Tools, tactic

Forensic

Reconnaissance

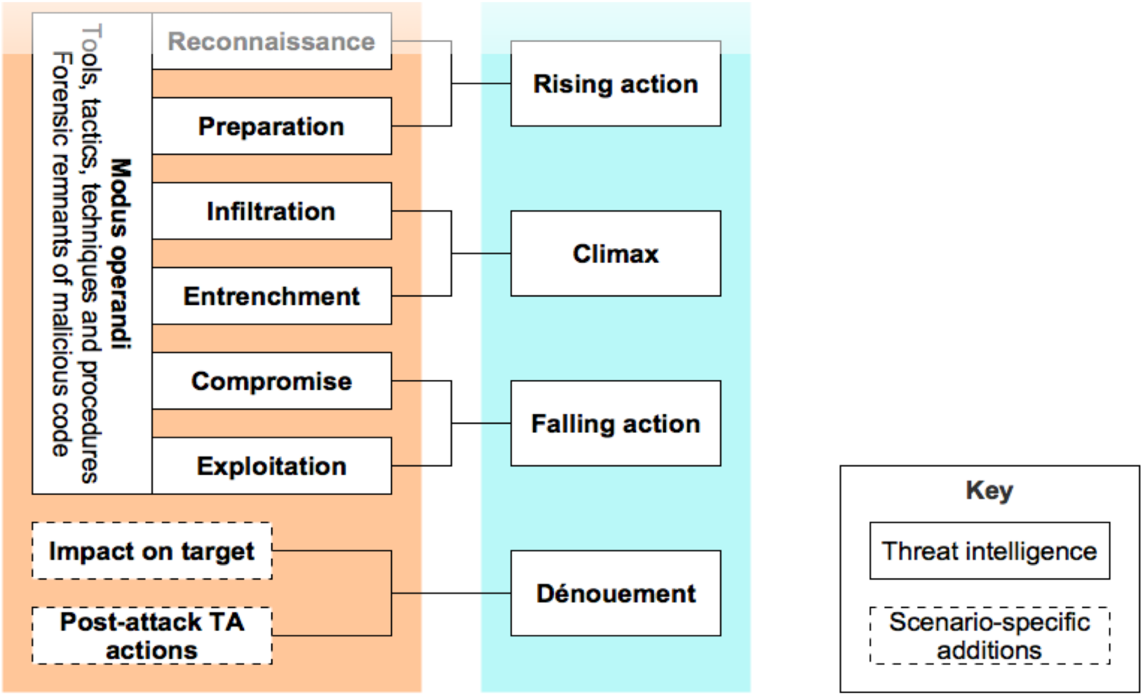
Preparation

Narrative structure

Exposition

Rising action

Mapping to a storyline



CBEST - What Went Well

- Created an evidence backed business case for a broad end to end test of resilience/red team where hard to justify previously
- Created useful discussion on what is ‘critical & economically important’ separate from tech change.
- Forced organizations to prove IR playbooks were really working to regulators
- Genuinely got the board to take the test seriously and helped understand the challenges
- Created discussion about what is probable and linked to other risk assessment
- Took business stakeholders end to end through process helping to justify existing investments in defenses and Detection and Response capabilities

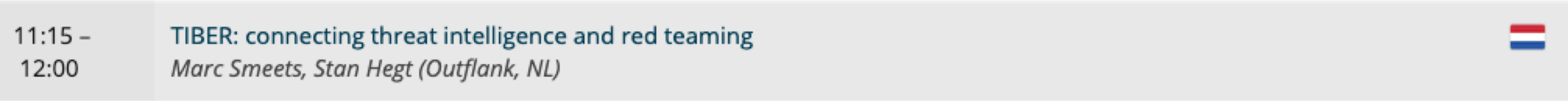
CBEST – Even better if.. Common observations/complaints/comments

Observation	Comment
National Bank X and National Bank Y have pretty much the same threats – often a validation of what was already known	Shared threat models better where this is shared - but ”opportunities” for attackers different due to varying tech stack – need a common threat model and shared labour. Also only true for sub-types. Infrastructure, Investment Banking vs. Retail Banking.
The Red Team still carried out the same test	Not intended to dictate red team, but help justify actions.
The scenarios would benefit from being more specific	Tools such as MITRE ATT&CK give us increased specificity now we would have benefited from that then
It was labour intensive	Yes – components should be made generic and shared x-industry where possible.
After the Red Team made initial intrusion discoveries were made that did not relate to the scenario	Yes – should be an interactive continuous process
After initial intrusion scenarios written in absence of internal recon needed updating	Both Scenarios and test plans should only be finalized after initial intrusion.

Phase II – The TIBER(s)

digital shadows_

TIBER (Phase II)



11:15 – 12:00

TIBER: connecting threat intelligence and red teaming

Marc Smeets, Stan Hegt (Outflank, NL)

- Progressive approach – learnings from tests quickly integrated into approach and standards
- Created a shared ‘Threat Landscape’ document on which tailored threat scenarios can be developed, greatly reducing the labour required during the threat phase – more cost effective
- Better handover and collaboration between threat intelligence and testing provider updating test plans and scenarios in light of findings during test

Summing up – Where should this go?*

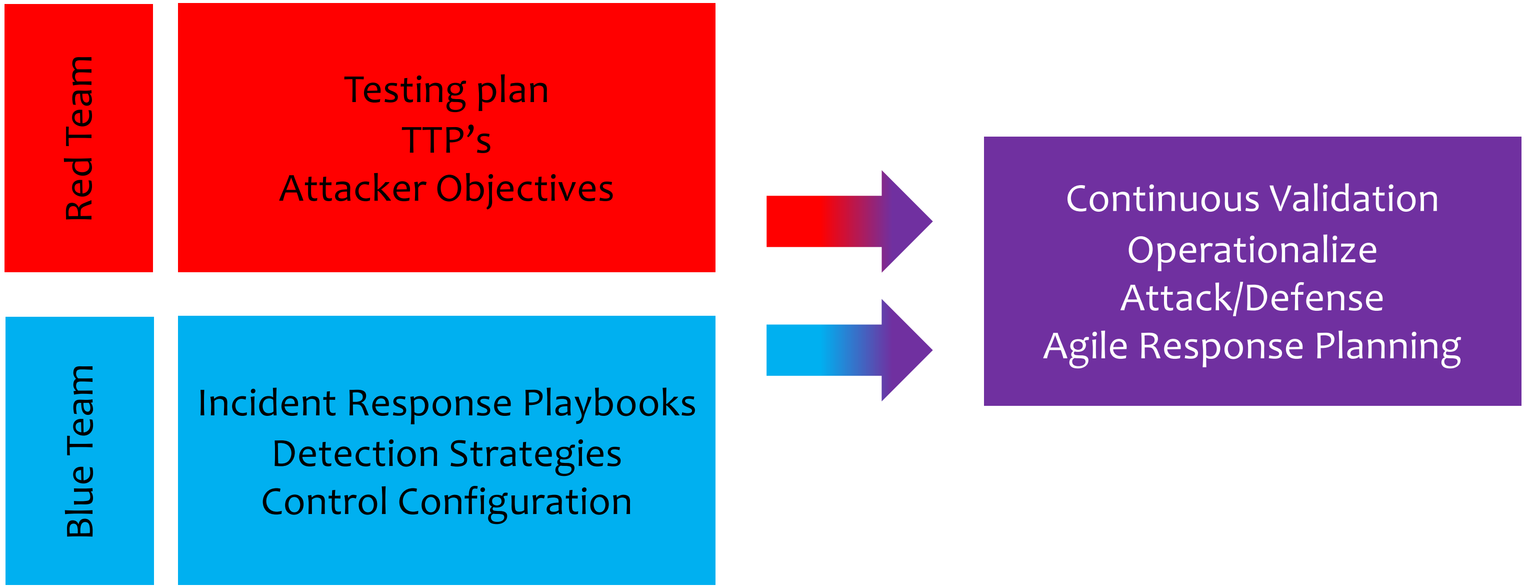
* In my humble opinion

digital shadows_

MAKE IT

PURPLE

Combining outputs



Red Team

Testing plan
TTP's
Attacker Objectives

Blue Team

Incident Response Playbooks
Detection Strategies
Control Configuration

Continuous Validation
Operationalize
Attack/Defense
Agile Response Planning

Biggest takeaways

- **Make it Purple:** Instead of passing threat reports over, continually update and validate throughout the test. Make Red Teams inform the Blue Team and vice versa. Make it a continual test of the IR playbooks, make regulatory test a snapshot of this embedded process.
- **Operationalize this:** Threats change constantly – Should not be a one-off test: Embed threat modelling into Incident Response, and Preparedness planning on a continuous basis – demonstrate on ongoing basis and then pick examples once a year.
- **Involve the business throughout:** No better model of a threat than an incident (a threat/risk that came to pass). Businesses know their critical assets from an internal perspective better than anyone – this is all valid input.
- **MITRE ATT&CK Adversary Emulation Plans** – A threat model with real purpose and community collaboration, A common language for Threat Intelligence and Red Teams to talk to each other but also increasing utility across the board
- **Share and Share-a-like:** Shared Threat Landscapes and Efficient Collaboration tailoring for just the efficient.

The Future

- Automation in Vulnerability Management – Platforms such as ATTACKIQ, SafeBreach etc taking real scenarios and including them in routine testing
- MITRE ATT&CK provides a very helpful model which should exist throughout these tests and be the center for them, adversary emulation.
- Pen Testing Frameworks:
  - Cobalt Strike (C2 emulation and in memory artefacts)
  - Caldera (open source framework)
  - APT Simulator
  - Metta
  - Blue Team Training Toolkit (BT3)

Great resource list here: http://pentestit.com/adversary-emulation-tools-list/

Does Threat Intelligence have a valid role in testing security resilience?

YES

- A justification for a broad test
- A live measurement of the ‘playbook’ in realistic circumstances
- A way of ‘trying out’ threat intelligence, or comparing it to existing feeds or capability
- Validation of existing thinking and controls, risk and response plans
- Evidence to support business cases

Use a regulatory driver to support a business case – to achieve the things you wanted to do anyway www.digitalshadows.com

James Chappell
Co-Founder & Chief Innovation Officer
James [at] digitalshadows.com

@jimmychappell

London

6th floor, 7 Westferry Circus, London, E14 4HD
T: +44 (0)203 393 7001

San Francisco

332 Pine St. Suite 600, San Francisco, CA 94104
T: +1 888 889-4143

Dallas

5307 E. Mockingbird Ln, Suite 915
Dallas, TX 95206

✉ info@digitalshadows.com

digital shadows_