Bank of England PRA

STAR-FS Threat Intelligence Report Specification

Simulated Targeted Attack & Response Assessments for Financial Services

Contents

Executive Summary

This document presents the specification for the Threat Intelligence Report deliverable developed by the Threat Intelligence service provider (TISP) during the Threat Intelligence phase of a STAR-FS assessment.

It should be noted that the specification presented in this report represents the minimum standard expected. There is an expectation that TISP will extend the template so they can offer additional value to the commissioning firm/FMI.

Comments and feedback on this document are welcome from all parties and should be sent to **STAR-FS@crest-approved.org**. Please place "[STAR-FS THREAT INTELLIGENCE REPORT FEEDBACK]" in the subject line of the email.

This document should be used in the Threat Intelligence phase, as described in section 6 of the **STAR-FS implementation guide**.

Legal Disclaimer

The information and opinions expressed in this document are for information purposes only. They are not intended to constitute legal or other professional advice, and should not be relied on or treated as a substitute for specific advice relevant to particular circumstances. The sponsors and authors of this document shall accept no responsibility for any errors, omissions or misleading statements in this document, or for any loss that may arise from reliance on the information and opinions expressed within it.

Copyright notice

1. Introduction

Purpose of this document

This document presents the specification for the Threat Intelligence Report deliverable developed by the TISP during the Threat Intelligence phase of a STAR-FS assessment. It is aimed at the following audiences:

- STAR-FS TISP — to show what kind of threat intelligence the commissioning firm/FMI (Financial Market Infrastructure) will require as a minimum.
- STAR-FS Penetration Testing service provider (PTSP) — to show what kind of intelligence will be provided for the purpose of configuring their penetration tests.

As described in the **STAR-FS implementation guide**, during the Threat Intelligence phase of a STAR-FS assessment the TISP collects, analyses and disseminates a body of threat intelligence using sources such as OSINT, TECHINT and FININT. This process is guided by the key systems and services information contained in the STAR-FS Scope document together with any other relevant organisational and technical information provided by the commissioning firm/FMI.

The output of this activity is a Threat Intelligence Report as specified by this document. The Threat Intelligence Report aims to gain a credible picture of the current threat situation by presenting threat profiles and threat scenarios relating to the commissioning firm/FMI. It also provides, crucially, evidence of real attack behaviour — what is probable rather than theoretically possible — to support the penetration testing service provider in justifying the approach it plans to take.

Equipped with this report, and the Targeting Report, the PTSP will have an evidential basis for designing and justifying a realistic and effective penetration test.

For the purpose of clarity, the definitions of “threat” and “intelligence” are set out below:

Threat

- an expression of intent to do harm, i.e., deprive, weaken, damage or destroy.
- an indication of imminent harm.
- an agent, in pursuit of its goals, that is regarded as harmful.

- a harmful agent’s actions comprising of tactics, techniques, and procedures (TTPs).

Intelligence

- Information that provides relevant and sufficient understanding for mitigating a potentially harmful event.

2. Report Structure

Overview

The Threat Intelligence Report is a bespoke report generated during the Threat Intelligence stage of a STAR-FS assessment. It aims to gain a credible picture of the current threat situation by presenting threat profiles and threat scenarios relating to the commissioning firm/FMI.

A key aspect of the report is the prediction of a future status derived (or implied) from a comprehension of the current situation. This may include, where appropriate, geopolitical-level information.

The Threat Intelligence Report also makes use of information contained in the Targeting Report developed by the TISP. Equipped with this report, and the Targeting Report, the penetration testing service provider will have a firm evidential basis for designing and justifying a realistic and effective penetration test. Three outputs from the Threat Intelligence Report are particularly relevant in this respect:

- tailored scenarios that support the formulation of a realistic and effective penetration test plan and are the basis for handover discussions with the PTSP.
- threat actor goals that provide a set of “flags” that the PTSP must capture.
- validated evidence that underpins the business case for penetration testing and post-test remediation.

The Threat Intelligence Report document is not an HM Government-produced document and therefore should carry a protective marking that is mutually enforced by the commissioning and delivery parties. For example: “COMMERCIAL IN CONFIDENCE”.

Production of this report is mandatory and the STAR-FS templates will be assessed regularly to ensure standards remain high.

The structure and content of the Threat Intelligence Report is summarised below.

Ref.	Title	Content
1	Scope	Overall scope of the intelligence research
2	Threat Profiles	Threat profiles of one or more threat actors (specific individual/group or generic class) that are targeting the commissioning Firm/FMI
3	Threat Scenarios	Threat scenarios for those threat actors (specific individual/group or generic class) who exhibit the highest threat severity scores or satisfy other selection criteria derived from commissioning Firm/FMI’s requirements.

Scope

This section defines the overall scope of the intelligence research.

Objectives	Objective of the intelligence research as determined by the commissioning Firm/FMI, bearing in mind that the overall objective of a STAR-FS assessment is to establish the resilience of an Important Business Service (IBS) to attack.
Important Business Services (IBS)	Details of the IBS’ agreed to be tested by the commissioning Firm/FMI. This will include: • geographies concerned with the delivery and use of the IBS

	• languages in use • brands of the operating company involved • third parties involved in the delivery of the IBS Depending on the organisation, the IBS' under test will vary and a sub-set may be selected.
Research Methods	Summary of the research methods used. This will include intelligence sources such as OSINT, TECHINT and FININT as well as activities such as research, monitoring and forensics.
Time Period	Period of time over which the intelligence was gathered and processed.
Ethical Standard Statement	A statement of confirmation from the threat intelligence service provider that they have observed an appropriate ethical standard for conducting threat intelligence activities.

Threat Profiles

This section presents profiles of one or more threat actors that are targeting the commissioning firm/FMI.

Note that, according to the derived intelligence, a threat actor may be a specific individual/group or a higher-level class of threat actors. Either way, the intelligence will be bespoke and tailored to the commissioning firm/FMI.

For each threat actor identified, the following sections will be filled in and repeated as appropriate. They should be presented in highest-to-lowest order of severity.

Threat Summary

This summarises the kay characteristics of the threat.

Identifier	An appropriate identifier for this threat profile. This will be derived from the Name and/or Class fields in Threat Actor below.
Threat Summary	A high-level summary of the threat actor derived from the fields below: Active since, Source geography, associated groups, Motivation, Intended effect.
Threat Severity	A summary of the overall severity of this threat in terms of its capability to compromise the resilience of a CBS. Based on the Capability Score and Activity Score fields below.
Grading	An appropriate grading system should be used to classify the intelligence on this threat. For example, the UK National Intelligence Model, informally known as “5x5x5”, allows intelligence to be evaluated where the original source is not made known to the recipient (NCIS, 2000)[1]: Source: A: Always reliable B: Mostly reliable C: Sometimes reliable D: Unreliable E: Untested Information: 1: Known to be true without reservation 2: Known personally to source by not to collector 3: Not personally known to source but corroborated 4: Cannot be judged 5: Believed to be false or malicious

[1] NCIS (2000). The National Intelligence Model. National Criminal Intelligence Service.

	Handling: 1: Open source no restrictions 2: Restricted to clients only 3: Restricted to specific clients 4: Restricted to specific clients with conditions 5: No dissemination without authority

Threat Actor

Key details of the threat actor. Note that, according to the derived intelligence, this may be a specific individual/group, or it may be a generic class of threat actors.

Name	Name of threat actor. If only a class of threat actor has been identified rather than a specific named entity, then this field can be left blank.
Class	Class of threat actor, e.g.: • Hacker • Hacktivist • Organised Crime Group • Nation State Proxy (acting on behalf of a specified country) Nation State (specified country)
Active since	Date when the threat actor commenced activity
Source geography	Country(-ies) where the threat actor is based
Primary language	Language(s) primarily associated with the threat actor
Associated actors	Other threat actors with whom the threat actor is associated

Goal Orientation

This section describes what motivates the threat actor and what effect they intend to have on the target. This explains the existence and potential seriousness of the threat actor.

PTSP will already be familiar with the technical methodology behind an attack, e.g., reconnaissance of network assets, social engineering to spearphish a user, initial execution, and entrenchment. If there is an opportunity to understand more about the person or organisation behind the attack and why they are doing it, then this will enrich and justify their testing as well as help to improve existing security countermeasures. "Who attacked us and why" is also a particularly important question that senior management will ask in the aftermath of a cyber attack.

Motivation	Motivation behind the cyber attack, e.g.: • Ideological - Anti-Corruption • Ideological - Anti-Establishment • Ideological – Environmental • Ideological - Ethnic/Nationalist • Ideological - Information Freedom • Ideological – Religious • Ideological - Security Awareness • Ideological - Human Rights • Egotistical • Financial or Economic • Military • Political • Opportunistic
Intended effect	Actor's intended effect on the target, e.g.: • Loss of Competitive Advantage – Economic • Loss of Competitive Advantage – Military • Loss of Competitive Advantage – Political • Theft - Intellectual Property • Theft – Credential • Theft – Identity • Theft - Proprietary Information • Fraud

	• Extortion • Bad Debt • Money Laundering • Degradation - Brand or Image • Degradation – Service • Degradation – Operations • Regulatory Non-Compliance • Law Breaking • Harassment • Destruction of Assets

Target

Characteristics of the threat actor's target.

Target geography	Country where the threat actor's target typically resides
Target sector	Sectors within which the threat actor's target typically operate
Target areas	With respect to the commissioning firm/FMI, details of any specific people, processes or systems that are being targeted

Capability

The capability the threat actor has to pursue its goals. This explains the threat potential exhibited by the threat actor (the opponent's size and strength).

Resources	Resources available to the threat actor, e.g. People, Technology, Finance
Skills	The strategic and tactical skills possessed by the threat actor (the opponent's cunning and maturity)
Resolve	How much danger or harm the threat actor can incur while still maintaining its hostile activity

Access to target	The threat actor's ability to gain entry to a restricted system by cyber or kinetic means, e.g., access to supply chain and adjacent targets, privileged relationships with insiders, coercion or bribery of insiders, exploitation of an under-protected network or computer system, extent of previous success in infiltrating target
Risk sensitivity	How much potential danger or harm the threat actor will risk facing in order to achieve its goals
Capability score	An assigned capability score of High, Medium, Low

Modus Operandi

The threat actor's tools, tactics, techniques and procedures that explain how malicious activity unfolds and what forensic remnants of malicious code may be identified and, crucially, used as supporting evidence.

Modus operandi should be structured around the following generic variant of the "kill chain" that enumerates the successive stages of a cyber attack[2].

Reconnaissance	Initial research, reconnaissance, and target selection
Preparation	Prepare attack components: • develop malicious code • acquire vulnerability exploits • instantiate threat infrastructure prepare delivery vehicle
Infiltration	Gain access to an office-based or mobile endpoint computing device via exploitation, deception, or force

[2] Hutchins, E., Cloppert, M., & Amin, R. (2011). Intelligence-driven computer network defence informed by analysis of adversary campaigns and intrusion kill chains. In proceedings of 6th Annual International Conference on Information Warfare & Security. Lockheed Martin Corporation.

Entrenchment	Entrench, reinforce, and maintain persistence: • pivot laterally from initial foothold to other parts of the system deploy persistence enhancements (e.g., backdoors)
Compromise	Weaken or destroy CBS: exfiltrate data, corrupt or delete data, disrupt, or deny service, install botnet
Exploitation	Exploit results of compromising target

Activity

This indicates how active the threat actor has been in recent times. At a minimum this should be over the past two months.

Activity score	Summary score indicating degree of activity based on the date of the last incident, e.g.: • < 30 days: Very Active • 30-60 days: Newly Active • >60 days: Inactive No incidents: No Activity

For each known incident involving this threat actor, the following intelligence should be provided in the form of an ordered timeline:

Date	Date of incident
Description	Description of incident
Impact effect	Impact effect of the incident
Severity	Score indicating the severity of the incident, e.g. Low, Medium, High

3. Threat Scenarios

Background and Purpose

This section presents threat scenarios for those threat actors (specific individual/group or generic class) who exhibit the highest threat severity scores or satisfy other selection criteria derived from commissioning firm/FMI's requirements.

A threat scenario presents a high-level story that narrates the flow of interaction between threat actors and their targets. It is based largely on the intelligence contained within a threat profile. Each threat scenario should relate to one of the following:

- a specific threat against an IBS that, if faced with loss in confidentiality, integrity, or availability, would seriously disrupt the organisation's ability to function.
- a required mitigating capability to assure the resilience of an IBS to cyber attack.

Scenario design should combine a realistic technical attack with a plausible storyline. The storyline should cover every stage of the cyber attack and at a level of detail that will elicit the desired penetration tester responses[3].

Based on the highest-scored threat actors, plus the people, process and infrastructure targets identified in the Targeting Report, threat scenarios are a key input from threat intelligence into the penetration test planning process. The PTSP should align its planning with the goals of each of the actors and draw upon the evidence to justify the actions taken during the test. The scenarios provide background to the tradecraft employed by each threat and the penetration testing service provider may additionally draw upon the Targeting Report that enumerates part of the attack surface of the commissioning firm/FMI. Threat scenarios are also a valuable means of presenting the results of a STAR-FS penetration test in terms of demonstrating how far a threat actor managed to progress through a particular scenario.

To quote An Introduction to Cyber Threat Modelling[4]:

"…penetration testers will use these scenarios to prioritise their plans for penetrating participants' networks, specifically by allowing them to determine what systems most

[3] Guerber, A., Fogle, C., Roberts, C., Evans, C., MacDougald, B. & Butkovic, M. (2010). Methods for enhanced cyber exercises. Delta Risk LLC, US Department of Homeland Security/National Cyber Security Division/Cyber Exercise Program Support and the Software Engineering Institute of Carnegie Mellon University.

[4] CBEST Intelligence-Led Testing: An Introduction to Cyber Threat Modelling v2 2016

easily are more important than others, given the objectives and capabilities of actual threat entities. In this way, some penetration testing activities can be safely discarded for some exercises, while others will feature as essential, and others still can be listed as optional or conditionally preferable.

“For example, a threat scenario may narrate how a major nation state’s intelligence services will seek to infiltrate a UK bank’s high-frequency trading algorithm platforms in order to cause maximal disruption in the event of a future crisis. The threat actor prefers to coerce the UK government by threatening to cause the disruption without actually having to execute it. Therefore, the threat will prioritise multiple, redundant, highly undetectable points of access into the targeted system and the threat actor will seek to maintain such channels of access over time.

“This scenario, in turn, specifies that the foreign threat actor’s cyber espionage operators will prefer some methods of infiltration and access reinforcement over others. For instance, they may prefer not to exploit existing infiltrations and may target legal staff attached to the high-frequency trading operations rather than the bank’s general help desk or customer information database administrators”.

Narrative Structure

A threat scenario should employ a narrative structure for the following reasons:

- narrative employs an intuitive structure which increases engagement and memory retention.
- a story-based structure allows for easier arrangement of fixed information and demarcated spaces for improvisation.
- narrative reflects the “real” salience of an event, i.e., it conveys more “meaning” than “fact”.

The classic narrative structure used as the basis for story telling in novels, theatre, films, and computer games is summarised in Figure 2.1 together with some STAR-FS-specific annotations[5]:

[5] Freytag, G. (1863). Die technik des dramas (Technique of the drama). Retrieved from http://www.matoni.de/technik/tec_inh.htm. Hirzel.

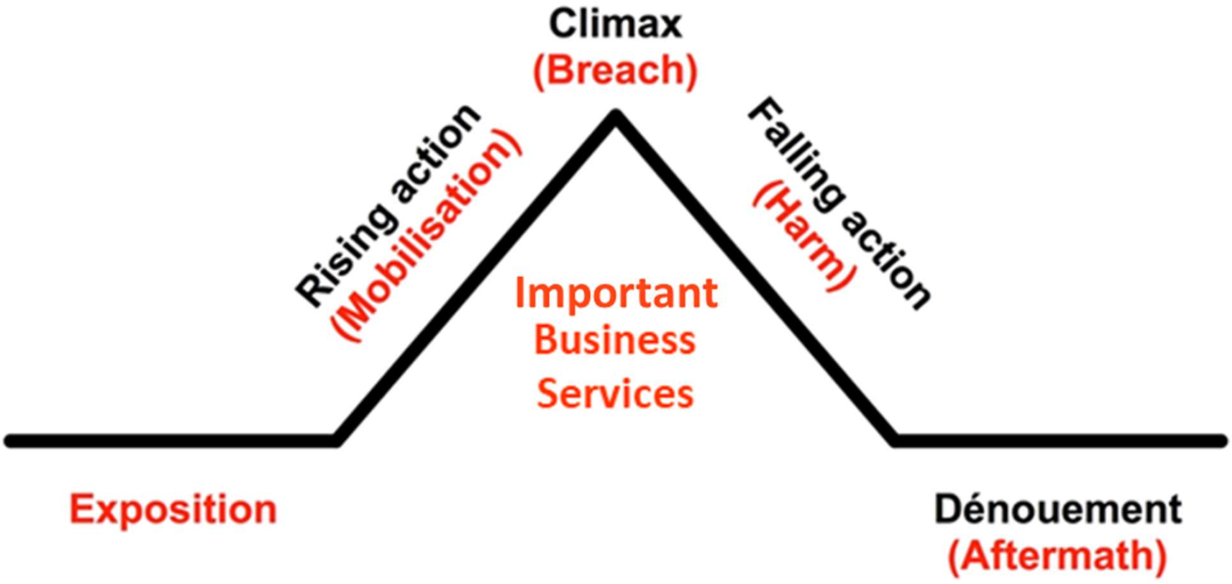

Figure 2.1: Classic narrative structure with STAR-FS-specific annotations

As Figure 2.1 shows, there are five key stages of a narrative:

Exposition

During the exposition all the key elements are introduced: the characters, the setting, the time, the place, etc. In addition, and crucially, a complication (problem, conflict or other inciting incident or decision) is introduced which disturbs the equilibrium and hooks the audience as they yearn for a resolution.

In STAR-FS terms this equates to the “back story” behind the targeted cyber-attack.

Rising action

In the rising action, a series of events, stemming from the complication, escalate towards the point of greatest interest (the climax). These events are generally the most important parts of the story since the entire plot depends on them to set up the climax and ultimately the satisfactory resolution of the story itself. This part tends to be dramatic and suspenseful as it builds a sense of tension.

In STAR-FS terms this equates to the mobilisation of the threat actors, namely reconnaissance and preparation.

Climax

The climax is the highest point of tension in a story and the turning point that changes the protagonist’s fate. If the story is a comedy, things will have gone badly for the protagonist up to this point; now, the plot will begin to unfold in the protagonist’s favour, often requiring them to draw on hidden inner strengths. If the story is a tragedy, the opposite state of affairs will ensue, with things going from good to bad for the protagonist, often revealing the protagonist's hidden weaknesses.

In STAR-FS terms this equates to threat actors breaching defences, namely infiltration and entrenchment.

Falling action

During the falling action, the conflict between the protagonist and the antagonist unravels, with the protagonist winning or losing against the antagonist. The falling action may contain a moment of final suspense in which the final outcome of the conflict is in doubt. The story moves towards closure with the actions and decisions being made leading to a resolution and a new equilibrium.

In STAR-FS terms this equates to the threat actors causing harm, namely compromise and exploitation.

Dénouement

The French word dénouement refers to the unravelling or untying of the complexities of a plot. During dénouement the original complication (conflict) is resolved, creating normality for the characters and a sense of catharsis, or release of tension and anxiety, for the reader. A comedy ends with a dénouement in which the protagonist is better off than at the story's outset. A tragedy ends with a catastrophe, in which the protagonist is worse off than at the beginning of the narrative.

In STAR-FS terms this equates to the conclusion of the scenario, namely post-attack impact on target and any further actions taken by the threat actors.

STAR-FS Scenario Structure

The narrative structure described above provides useful guidelines for developing a compelling scenario for the penetration testing service provider to exploit. As Figure 2.2 shows, the classic narrative structure maps conveniently against the threat intelligence/cyber kill chain structure presented in Section 2.

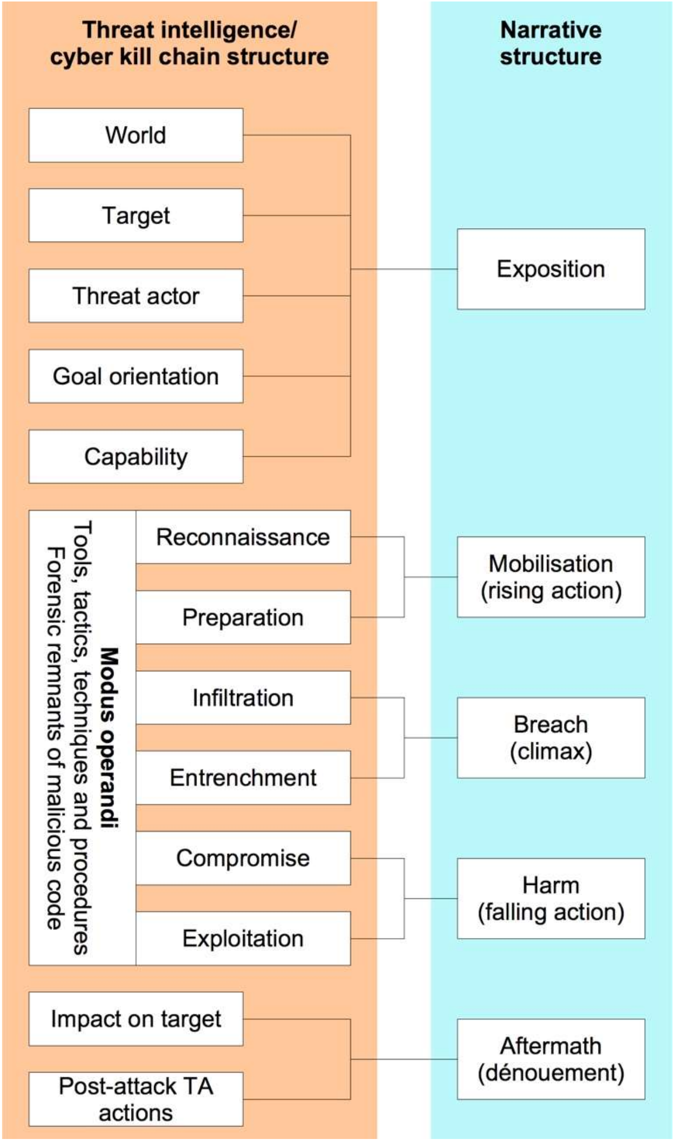

Figure 2.2: Mapping from threat intelligence/cyber kill chain structure to narrative structure

Given the above discussion on narrative structure, the structure for the threat scenario is shown below.

Exposition	Introductory section describing the current state of affairs and general context within which the scenario takes place, i.e., the setting, the threat actor, and the target. This provides essential scene-setting context or the "back story".
Mobilisation (Rising action)	Sequence of tension-building events, setting out threat actor's modus operandi, as threat actor undertakes: • reconnaissance: initial research, reconnaissance, and target selection.

	• preparation: prepare attack components.
Breach (Climax)	Sequence of climatic events, setting out threat actor's modus operandi, as threat actor undertakes: • infiltration: gain access to an office-based or mobile endpoint computing device. • entrenchment: entrench, reinforce, and maintain persistence.
Harm (Falling action)	Sequence of resolving events, setting out threat actor's modus operandi, as threat actor undertakes: • compromise: weaken or destroy IBS. • exploitation: exploit results of compromising the target.
Aftermath (dénouement)	Conclusion of the scenario in terms of: • post-attack impact on the target. • post-attack actions undertaken by the threat actor.