Bank of England PRA

STAR-FS Detection & Response Assessment Guide

Simulated Targeted Attack & Response assessments for Financial Services

Executive summary

Within the STAR-FS framework, the firm/FMI has the option to complete a Detection & Response Assessment. This assessment is completed by the Penetration Test service provider (PTSP).

The Capability Indicators (CIs) presented in this document measure the capability of a firm/FMI's detection and response to, intelligence-led penetration testing.

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 DETECTION & RESPONSE ASSESSMENT GUIDE FEEDBACK]" in the subject line of the email.

This document should be used in the penetration test phase, as described in section 7.5 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.

Introduction

Purpose of this document

This document presents CIs for the penetration testing component of a cyber security capability assessment exercise. It is aimed at the following audiences:

- accredited STAR-FS penetration testing service providers — to enable them to conduct a benchmark assessment of firms/FMIs participating in STAR-FS assessments;
- supervised firms/FMIs.

STAR-FS cyber security CIs may be used at the conclusion of a STAR-FS assessment to provide:

- an objective assessment of the Firm/FMI's cyber security capability (to the extent that STAR-FS can be used for such an assessment);
- a data point for a broader understanding of the financial sector's cyber security capability.

The ultimate objective of the Detection and Response assessment is to promote transparency and demonstrate that STAR-FS is delivering benefits to firms and the sector as a whole.

Capability Indicators

The following CIs are used by an accredited STAR-FS penetration testing service provider to assess a Firm/FMI's detection and response capability during a STAR-FS assessment.

The CIs are divided into two tables. The first is quantitative, with low, medium and high scores, and provides a means to assess monitoring and incident response team capability. The second is qualitative in order to allow both the Firm/FMI and the service provider to give expanded details on the perceived success or failure of the penetration test.

Quantitative SOCassessment: monitoring and incident response team			
Measurement			
CI	Low	Medium	High
1. Security Operations Centre			
	No	Yes, although limitations reduced the ability to analyse system logs	Yes, all activity is monitored and the Firm/FMI possesses sufficient capacity to analyse all alerts and logs

Qualitative assessment: intrusion detection and incident response	
CI	Supporting evidence
1. Detection of targeting	
1.1 On what dates and at what time did the client detect targeting of its network by the vendor?	DTG of each detected targeting attempt
1.2 What action did the client take following detection of targeting against its network by the vendor?	Provide details of action taken

2. Intrusion detection	
2.1 On what dates and at what time did the client detect intrusions of its network by the vendor?	DTG of each detected intrusion
2.2 What actions did the client take once intrusions into its network were identified?	Provide details of action taken
2.3 What method did the client use to detect each network intrusion by the vendor?	Active (active security processes)/passive (detected by non-security processes such as resource utilisation)/externally informed (by STAR-FS penetration tester) — provide supporting details
2.4 What root cause did the client attribute to each vendor-identified breach?	Provide details for each identified intrusion
3. Incident response	
3.1 For each vendor identified security breach, what date and time did the client effectively contain the malicious activity?	Provide details for each intrusion
3.2 What method was used by the client to effectively contain each vendor-initiated breach?	Provide details of methods utilised
3.3 What members of staff within the client Firm/FMI were informed of STAR-FS testing?	Provide names, positions, and dates informed, of all persons with knowledge of STAR-FS testing
3.4 Was any detail of STAR-FS testing circulated internally within the client organisation to either the monitoring or incident response team?	Yes/no — provide reasons why if answer is yes
4. Testing success	
4.1 Did the client suffer any system outages that could be attributed to STAR-FS testing?	Yes/no – provide details of any STAR-FS attributable outages

4.2 Within the parameters of the STAR-FS scope, how many client non-critical systems were compromised?	Provide details of systems compromised
4.3 Within the parameters of the STAR-FS scope, how many client critical systems were compromised?	Provide details of systems compromised
5. Lessons learned	
5.1 What additional security controls would have allowed the client to detect each vendor initiated network intrusion?	Client to provide assessment for each intrusion based on information provided by vendor post-testing
5.2 What changes have been implemented to prevent each successful intrusion being repeated? If not yet implemented, when will these changes be fully in place?	Provide details of each change