2021

HEFESTIS

STOic TTX Certification

JORDAN SCHROEDER

HEFESTIS LTD. | Unit 27, Stirling Business Centre, Stirling FK8 2DZ

Contents

Purpose

Organisations need to be able to provide assurance that their TTX programme is progressing, is meeting objectives, and that the organisation is better able to respond to cyber incidents. STOic TTX includes a high-level, self-certification path that can provide this assurance.

Having a certification path and goals help to the organisation as to what to exercise/tackle next.

Scope

The scope of the certification is determined by the organisation. Having layers of certification allows the organisation to decide on the scope which best suits them. This may be across the entire organisation or limited to one department.

Organisation's having decentralised IT may choose to gain certification for certain business units only, or for organisations with a central IT dept, they may choose to only certify the Incident Response Team.

The scope can be defined in the way which makes most sense for the organisation in line with their goals and objectives. It must be made clear, however that should an organisation choose to limit the scope of certification, to certain areas/departments, they will be potentially missing the opportunity to improve their ability to respond to an incident as an organisation.

Certification Levels

Within each agreed scope, to achieve each STOic certification stage, Bronze, Silver & Gold, all of the three levels Strategic, Tactical and Operational, must be exercised. To confirm, to achieve STOic TTX Bronze certification the organisation would need to perform at least twelve TTX, four Strategic, four Tactical and four Operational. As the framework provides all the information required for a facilitator to arrange and deliver these exercises, it is not envisaged that this will be overly onerous for an organisation. In fact, it is hoped that participating in a STOic TTX event will be an enjoyable way to learn and address the more serious topic of a cyber attack.

Below is sample template to assist organisations in keeping track of TTX's which have been performed. There is a tracking document for each level, Bronze, Silver and Gold. Tracking documents should also be completed by organisations for each scope exercised.

Full copies of tracking documents have been included as attachments at the end of this paper.

Objectives

The typical objectives of a tabletop exercise are listed in the table below. The levels associated with each objective relate to the expected STOic TTX certification path levels. However, an organisation can set their own objectives no matter what certification level the organisation might be.

Objectives of TTX	Level
Test effectiveness of the organization's incident response plans	Bronze
Test the effectiveness of communications processes during an attack	Bronze
Determine what enhancements or capabilities are needed to protect an information system and provide for operations in a hostile environment	Bronze
Determine the effectiveness of cyber training provided to staff	Bronze
Test the organization's capability to respond to uncertain and complex incidents and attacks	Gold
Test ability to detect and properly react to hostile activity	Silver
Test the organization's capability to determine operational impacts of cyber attacks and implement proper recovery procedures	Silver
Understand the implications of losing access to IT systems and test the workarounds for such losses	Silver
Expose and correct weaknesses in cyber security systems, policies and procedures	Silver
Enhance cyber awareness, readiness, and coordination	Silver
Develop contingency plans for surviving the loss of some or all IT systems	Silver

Core Scenarios

The table below lists the STOic TTX Core Scenarios. These represent the largest threats to the average organisation at the time of this writing as identified by MITRE.

Scenario	Description
Virus	A user has clicked a link in a spear phishing email, This has installed malicious software on the device.
Denial of Service (DoS)	An abnormally high amount of network traffic is being experienced and is visible in system performance statistics and volume of log data. Additional notification from users about reduced network capability or inability to access website has been received.
Unauthorized computer on network	An attempt is made to connect an unauthorized laptop to the organisation's network.
Malicious external scanning	An in-depth, long-running external scan of the organisations network is being performed.
Malicious internal scanning	A device on the network is performing scans on the internal network.
Computer compromise	Unattended computers with no password screensaver lock have notes in the on-screen text editor that the computer has been compromised.
Phishing via email	A phishing email is sent to multiple employees attempting to capture credentials.
Ransomware	Core servers and many end points have been infected with ransomware and are non-functional.

Certification Path

The requirements for each of the STOic TTX certification levels are explained in the table below.

Please note certification must be completed for each scope to be exercised within the organisation, as explained in the Scope section of this document.

Level	Description
Bronze	Participated in four Core Scenarios
Silver	Participated in four Core Scenarios, three of which included two additional injects
Gold	Participated in any four scenarios with an expert Cyber Professional in attendance to present adaptive injects