|  |
| --- |
| ​ |
|  |
| ART Test Summary [Code name test][dd-mm-yyyy] |
|  |

Version management Format

|  |  |  |
| --- | --- | --- |
| **#** | **Date** | **Updated information** |
| 1.0 | May 2024 | Delivery ART Test Summary Format, based on the TIBER-NL Test Summary Format |
|  |  |  |

Version management Test Summary [Code name test]

|  |  |  |
| --- | --- | --- |
| **#** | **Date** | **Updated information** |
| [x.x] | [dd-mm-yyyy] |  |
|  |  |  |
|  |  |  |
|  |  |  |

Table of contents

Table of contents 3

Format instructions 4

Format development and version updates 4

Purpose 4

Audience 4

Delivery process and responsibilities 4

Level of detail and pseudonymisation 5

Legal disclaimer and confidentiality 5

1. Document structure and required information 6

2. General information 7

2.1 Chosen ART-modules and project timelines 7

2.2 Parties involved in the test 7

3. Overview of the test 8

3.1 Scope 8

3.2 Targeted Threat Intelligence 8

3.3 Attack scenario’s, actors and flags 8

3.3.1 Selected attack scenarios 8

3.3.2 Executed attack scenarios 8

3.4 High level objectives and learning goals Gold teaming 9

4. Observations, follow up actions and recommendations 10

4.1 Main observations and (proposed) remediation actions 10

4.2 Key learnings and recommendations 10

Format instructions

Format development and version updates

The Test Cyber Team (TCT) from De Nederlandsche Bank (DNB) has developed this ART Test Summary format based on the TIBER-NL Test Summary format and is adjusted to fit the requirements as set out in the ART framework. The document will be periodically updated with the latest insights.

This chapter provides background information on why and how to use this ART Test Summary format. All text that needs to be provided by the entity in order to complete this Test Summary, is indicated with […]. Once chapters 2 to 4 have been completed, the pages describing the ‘Format instructions’ can be deleted, for they are only intended to give guidance on the information to be shared.

This format is dated May 2024 (version 1.0) and provided to support the requirements as set out in the ART framework.

Purpose

The purpose of the Test Summary is to serve:

* as a comprehensive overview of performed test, its scope, main findings and key learnings to be shared with relevant stakeholders in the entity and their supervision authority;
* as an overview of the test (performed ART modules and outcomes of the test) for later reference by the entity;
* to facilitate analysis by the TCT on sector trends, learnings and best practices as a means to facilitate learning.

Audience

The Test Summary is primarily aimed at the stakeholders on strategical/tactical level in the entity undertaking the ART test (eg. CISO, CIO, Board members of the entity).

This Test Summary can be shared by the entity with:

* the Threat intelligence provider (TIP), if any, the Red team provider (RTP) and Gold team provider (GTP), if any;
* Test Cyber Teams (TCTs) involved in the TIBER test (applicable in multi jurisdiction tests only);
* The entity’s supervision authority.

Delivery process and responsibilities

The ART Test Summary summarizes the outcomes of the executed ART test process and builds upon the delivered documentation such as the Scoping Document, the Targeted Threat Intelligence (TTI) report, the Red Team and Blue Team reports, the Gold Team report (if executed) and the remediation plan(s).

The Control Team Lead (CTL) is responsible for providing the Test Summary as soon as possible after the delivery of the former mentioned reports and remediation plan.

Level of detail and pseudonymisation

This format aims to provide a standardised approach and structure for the ART Test Summary to entities undertaking an ART test and to provide a high level overview of the ART test undertaken[[1]](#footnote-2).

The information in this Test Summary should be drafted in wording that is accessible to senior management, providing an adequate account of the end-to-end test, its conclusions and the recommendation for the tested entity to improve their cyber resilience. As is the rest of the documentation on the test, the information should be pseudonymized as much as possible (e.g. using the code name for the test).

Legal disclaimer and confidentiality

The information and opinions expressed in this document are for information purposes only. They are not intended to constitute legal or other professional advice.

1. Document structure and required information

The ART Test Summary consists of the following chapters:

**Chapter 2 General information**

In this chapter an overview of the performed ART modules, the timelines and all parties involved is presented.

**Chapter 3 Overview of the test**

This chapter provides a high level overview of the entity’s attack landscape, the performed threat intelligence and proposed test scenarios. It also provides information on the objectives and learning goals of the optional Gold Teaming exercise – if performed. The information included in this chapter is based on the final versions of the Scoping Document, Targeted Threat Intelligence report, the Test Plan and Gold Teaming plan and consists of:

* An overview of the attack landscape and possible flags of this entity as described in the Scoping Document;
* The outcomes of the Targeted Threat Intelligence;
* The selected and executed attack scenario’s and targeted flags;
* The objectives and learning goals of the Crisis Management exercise as performed during the Gold team steps.

**Chapter 4 Observations, actions, learnings and recommendations**

In this chapter the high level observations and outcomes of the performed test are presented together with the (proposed) actions to be taken as presented in the remediation plan. It also aims to give insight in the key learnings and recommendations to enable the increase of the cyber resilience in the entity itself and possibly other entities in the sector.

This chapter is based on the details as presented in the final Red Team Report, the Blue Team Report, the Remediation Plan and the optional Gold Team Plan. If applicable, the entity should also include information on:

* Positive observations from the test, notably any strong control areas that the RT provider was unable to circumvent;
* Insights into the main categories of recommendations to address the observations and their root causes;
* Significant observations and deviations from the threat intelligence, test plan and/or the gold team plan;
* Any other insight from the TI/RT/GT provider on the cybersecurity posture of the entity that can also be valuable for other entities in the sector.
1. General information
	1. Chosen ART-modules and project timelines

This test has been performed in line with the ART framework as provided by TCT-NL. For this specific test, the following modules were chosen and performed:

|  |  |
| --- | --- |
| **Module** | **Performed Y/N** |
| Threat intelligence |
| Internal TI team + GTL |  |
| Optional: internal TI team + old TI report + GTL |  |
| Optional: limited TI report by RT provider |  |
| Optional: full TI report by TI provider |  |
| Red teaming |
| 1 scenario, assumed compromise |  |
| Optional: 2 scenarios |  |
| Optional: end-to-end simulation |  |
| Optional: scenario X |  |
| Purple teaming |
| PT fundamentals |  |
| Optional: PT full |  |
| Gold teaming |
| Optional: walkthrough |  |
| Optional: tabletop exercises |  |
| Optional: simulation |  |

The test ran over a period of **[xx months/weeks] in total** and has been executed during the following timelines:

* Engagement and scoping: [dd-mm-yyyy to dd-mm-yyyy]
* Procurement: [dd-mm-yyyy to dd-mm-yyyy]
* Threat intelligence: [dd-mm-yyyy to dd-mm-yyyy]
* Red teaming: [dd-mm-yyyy to dd-mm-yyyy]
* Purple teaming: [dd-mm-yyyy to dd-mm-yyyy]
* Gold teaming: [dd-mm-yyyy to dd-mm-yyyy]
* Remediation planning and closure: [dd-mm-yyyy to dd-mm-yyyy]
	1. Parties involved in the test

During the execution of the performed test, the following parties and their representatives were involved:

* CT, consisting of [names and roles of the members]
* The TIP [internal or external], consisting of [names and roles of the members]
* The RTP, consisting of [names and roles of the members]
* The GTP, consisting of [names and roles of the members]
* The TCT, consisting of [name: lead test manager, name: backup test manager and name: TI manager]
* [other parties, names and roles]
1. Overview of the test
	1. Scope

In this paragraph a short description of the entity’s critical functions (CF’s), subfunctions and underpinning systems are presented as well as the possible flags. The information from the Scoping Document is reused and provides insight in the entity’s attack landscape.

[Please present the information from the Scoping Document.]

* 1. Targeted Threat Intelligence

This paragraph gives an overview of the outcomes of the Target Threat Intelligence (TTI) activities and findings. Also this paragraph gives a reflection of the high level scenarios and most likely threat actors as produced by the TIP.

[Please present in this paragraph:

* the threat actors deemed most relevant and a justification of why they are most relevant for your entity;
* the most likely used attack scenario’s, based on the entity’s attack landscape and TTI;
* other significant findings on the digital presence.]
	1. Attack scenario’s, actors and flags

Both the Scoping Document and the Targeted Threat Intelligence Report have provided the information on which attack scenario’s, actors and flags were most relevant and were selected to use and described in the Red Team Test plan.

* + 1. Selected attack scenarios

Based on the ART framework the following scenario(s) have been selected and described by the Red Team Provider using the MITRE ATT&CK Framework.

[Please present the planned scenario(s) (threat actors, attack techniques, systems and objectives/flags) from the RT Test Plan in this paragraph.]

* + 1. Executed attack scenarios

This paragraph highlights the scenarios as executed during the RT test. The executed test scenarios differed from the planned test scenarios, for example the planned techniques, tools or procedures (TTPs), a leg up could have been given or other unforeseen deviations which can be found in the Red Team Test Report.

[Please copy the executed attack scenarios from the Red Team Report in this paragraph and provide background information on when and why there was a deviation from the planned attack scenarios. Please also include the captured and non-captured flags.]

* 1. High level objectives and learning goals Gold teaming

This paragraph describes the objective and learning goals as were intended to be achieved with the performed Gold Team variant. This paragraph is only applicable when the GT module is performed during this ART test.

[Please present the planned GT variant, the high level objectives and their learning goals.]

The following persons, including their respective roles, have participated in the chosen the GT variant:

* [name, role]
* [name, role]
* [name, role]
1. Observations, follow up actions and recommendations

In this chapter of the ART Test Summary the observations and findings, (proposed) follow up actions, key learnings and recommendations to the entity are presented on a strategical/tactical level. The operational and more detailed technical findings, learnings and recommendations are presented in the Red Team Report, the Blue Team Report and the Remediation Plan.

When a GT module was chosen, a different level of reporting is required for each different GT module. The strategical/tactical observations as presented in that report are also highlighted in this chapter of the ART Test Summary, when applicable.

* 1. Main observations and (proposed) remediation actions

The following observations and proposed follow up actions are advised on a strategic and tactical level.

| **Observations and follow up actions** |
| --- |
| [**Observation]** – [Follow up actions] |
| [**Observation]** – [Follow up actions] |
| [**Observation]** – [Follow up actions] |
| [**Observation]** – [Follow up actions] |
| [**Observation]** – [Follow up actions] |
| [**Observation]** – [Follow up actions] |

* 1. Key learnings and recommendations

[In order to facilitate learning within your own organization but also potentially for other entities in the sector, please share the general key learnings and recommendations you have to other entities regarding general mitigating actions, best practices etcetera in addition to what is mentioned in the former chapters. For your audience think of other CT’s, CISO’s, Blue Teams and intelligence teams.]

1. It should *not* contain detailed technical information and findings regarding weaknesses and vulnerabilities as information at that level of detail is highly sensitive and intended for the tested entity only (i.e. documented in the Red Team Report, Blue Team Report and Remediation Plan). [↑](#footnote-ref-2)