ART Purple Team Guide

for the financial sector

DeNederlandscheBank

EUROSYSTEEM

Contents

1 About this guide

This purple team (PT) guide gives guidance to the control team (CT), the control team lead (CTL) and the red team provider (RTP) on the steps for preparing the PT phase and its two variants, PT foundation and PT full. For a list of abbreviations, see annex A.

1.1 Purpose of this guide

The purpose of this document is to provide the relevant stakeholders such as the CT and the RTP with information on the requirements[1] for conducting one of the PT variants.

This guide is part of the ART framework as published by De Nederlandsche Bank (DNB) on ART-NL | De Nederlandsche Bank | De Nederlandsche Bank (dnb.nl). For enquiries about ART, please contact the DNB Test Cyber Team (TCT) at tct@dnb.nl.

1.2 Target audience

This ART guidance is primarily intended for the CT(L), BT and the RTP conducting the PT phase. In addition to these primary users, it may also provide the other stakeholders of an ART test with useful information.

1.3 Legal disclaimer

This document is intended for institutions within the scope of an ART test. Nothing in this guide should be construed as legal or professional advice. This guide is an underlying document of the ART-framework. For information on copyrights and creative commons, please refer to section 1.3 of the ART framework.

1.4 Role of the TCT, minimum requirements and attestation

The purple teaming (PT) phase is an essential and mandatory part of each ART test. It is strongly connected to the red team (RT) module. To ensure the quality of the test meets the ART standards, the DNB Test Cyber Team (TCT) consults with the CTL and RTP to plan the PT sessions within the institution. The form of the PT sessions depends on the outcome of the RT phase and the PT variant to be planned. Optionally, the TCT can be present during the PT sessions at the institution. The PT sessions are mainly of a technical nature and aimed at the specific teams and/or department forming the BT.

The TCT will work in close collaboration with the CTL and RTP. Next to the quality assurance (QA) role, the TCT is a neutral sparring and guiding partner for the CTL who holds the ultimate responsibility for the ART test within the institution, and for the RTP.

If the test has been carried out in accordance with the requirements of the ART framework, the TM will provide the institution on behalf of the TCT with a DNB attestation document concluding the test.

[1] This document also includes operational ART guidance based on best practices, knowledge and experience from numerous previous tests.

2 Introduction

2.1 What is PT?

Purple teaming (PT) is a cybersecurity methodology that combines the strengths of red team and blue team into a collaborative activity after the RT phase. It combines both the red team provider (RTP) and the blue team (BT) and their corresponding offensive and defensive actions. In general, PT can be done as a standalone test. However, in the context of the ART framework it is a mandatory step during the test, to be performed after the RT phase if there was no detection during the RT phase.

The ART framework describes two variants for PT: 1) the 'PT fundamentals' variant and 2) the more extended 'PT full' variant which are explained in Chapter 4.

2.2 What is the purpose of PT?

The primary purpose of PT is to maximise the effectiveness of an organisation's cybersecurity defence by fostering collaboration between the offensive RT and defensive BT. Purple teaming ensures that every simulated attack directly improves detection, response, and resilience.

2.3 What are the goals of PT?

In line with the purpose, the goals of PT are to gain insight into the institution's current cyber resilience posture and to learn where additional measures can be taken to increase the institution's cyber resilience.
These insights can be gained in various fields, such as:

- Improving detection and response
  - Ensuring defensive tools (SIEM, EDR, NDR, IDS) can detect real-world attack techniques.
  - Validating alerting and incident response workflows.
- Validating and strengthening security controls
  - Assessing whether existing controls (rules, use cases, firewalls, endpoint protection, MFA etc.) work as intended
  - Identifying gaps and misconfigurations that attackers could exploit.
- Enhancing the use of threat intelligence
  - Mapping attacks to frameworks such as MITRE ATT&CK
  - Teaching the BT how to recognise indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs).
- Fostering continuous learning and collaboration
  - Breaking down silos between red and blue teams
  - Sharing knowledge in real time to accelerate security maturity.
- Prioritising risk-based remediation
  - Focusing on vulnerabilities and detection gaps that cause the highest risk
  - Aligning improvements with critical functions and underlying systems and services.

2.4 Who is PT for?

PT is intended for:

- Security operations teams
  - Blue Teams gain real-time insight into attack techniques and improve detection and response
  - Red Teams (attackers) get feedback on how their tactics, techniques, and procedures (TTPs) are detected, helping refine realistic scenarios.
- Threat hunting and incident response teams
  - They learn new indicators of compromise (IOCs) and TTPs after red team testing.
- The organisation's security management (CISO, SOC Managers, IT and Facility Management)
  - They gain insight into the extent to which the organisation is prepared for cyber attacks
  - Provides measurable improvements in security posture
  - Demonstrates ROI for security investments and compliance readiness.
- Organisations with compliance or high-risk requirements
  - Financial institutions and critical third parties for which proactive defence is essential.
- Any organisation preparing for red team testing or testing the latest TTPs.
  - Organisations that already conduct red team testing but want continuous improvement instead of one-off tests.

3 Core principles of purple teaming

This chapter describes the core principles of purple teaming in an ART test. These core principles provide the reader with a clear understanding of the key notions, ideas and concepts that are essential for conducting the PT module.

3.1 Safety and a safe learning environment

For all ART modules, the most important rule is that safety and a safe learning environment come first. The PT module may involve elements of stress, which can challenge the resilience of your staff and team. Collaboration over competition is important: PT is a learning exercise.

The RTP and BT are open and transparent in sharing their insights. The CT and TM must have sufficient confidence in safety, capacity and expertise throughout the PT module. When in doubt, the CT and the TM will discuss how to enable this safe and capable learning environment.

3.2 Based on learning goals and sufficient planning

The objectives or learning goals of the overall test – as defined in the preparation phase – continue to run as a common thread throughout the PT phase. Objectives depend on an institution's current level of maturity and cyber resilience. Just as for the RT, the PT is deliberately planned. The more hours available (depending on the variant selected), the more extensive the PT plan and planning.

3.3 Confidentiality

Confidentiality is of vital importance during all ART modules, including PT. All observations are highly confidential and only known by the CT, RTP and TCT.

4 PT variants

Purple teaming (PT) is a form of a technical collaborative activity that involves both the red team provider (RTP) and the blue team (BT) and their corresponding offensive and defensive actions. Purple teaming is part of the ART test and is planned after the RT activities.

The output of the RT phase is a RTTR produced by the RTP and delivered to the institution. The RTTR is the input for the PT phase. A draft RTTR should be delivered within two weeks of the test's completion and contain all required information as described in the RT guide.

Based on the information described in the RTTR and the notes taken during the RT phase, the CT will decide which key members of the institution's BT are to be informed about the test and should be involved in the PT phase. This not only includes people responsible for security monitoring, detection and response (SOC analysts). Depending on the executed scenario(s), key members of the institution's BT could be business process or system owners, people from facility management, HR, targeted end users, database administrators or other people responsible for managing ICT infrastructure components. People from the BT (usually from the SOC) should share their own observations ahead of purple teaming.

The ART framework describes two PT variants:

- PT fundamentals
- PT full

Both variants give the BT insight into what has been done during the RT phase and its attack phases, detections, defensive actions and the red team test report (RTTR). PT helps to expand knowledge on the threat actors' TTPs, mitigate certain risks linked to red teaming, and identify areas and actions that can be improved in the areas of people, process, technology level and physical properties. It also helps to identify weaknesses in protection and detection capabilities so that these can be addressed and incorporated in the remediation plan. As such, PT is a required component of every ART test to promote learning and strengthen cyber resilience efficiently.

Both PT variants focus on selected topics jointly identified by the BT and RTP.

4.1 PT fundamentals

The PT fundamentals variant is a one-day PT exercise which can be split into different sessions. During these sessions, the RT and BT (at least the SOC analysts) share intelligence based on the selected scenario(s) and RTTP, replay the simulated attack(s) and analyse the observations and the RTTR. The requirements for this variant can be found in Chapter 6.

4.2 PT full

The PT full variant is a multi-day exercise, and more PT sessions could be planned with other departments or teams forming the BT (defence of the institution). In addition to replaying the simulated attack(s) and analysing observations as mentioned in the PT fundamentals, the RT and BT share other relevant threat intelligence (for example extracted from the TIR and non-selected scenarios). More 'what if' scenarios (TTPs) and protection and detection capabilities are tested to enhance the learning experience and technical skills of the BT. The requirements for this variant are described in Chapter 6.

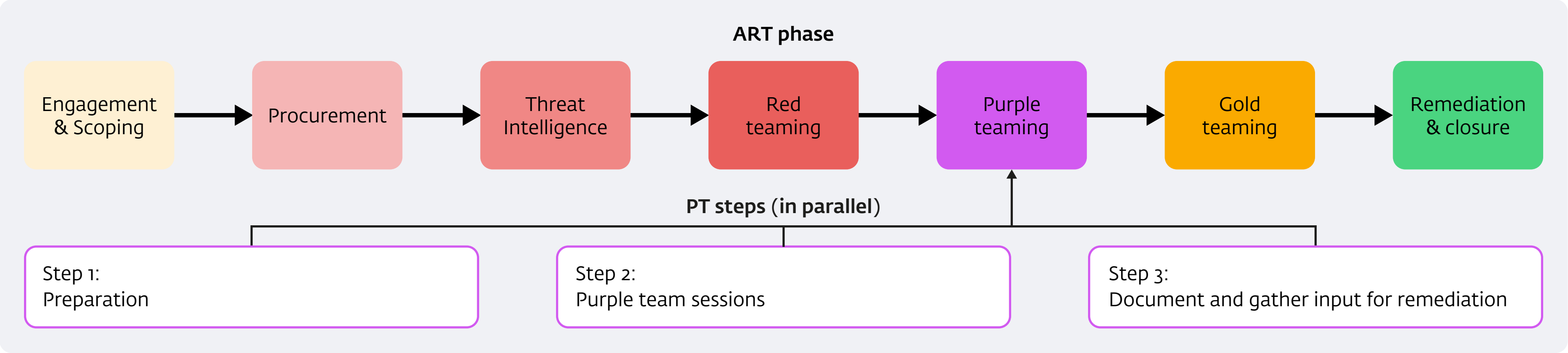
5 Description of the purple teaming steps

The PT phase starts after the RT phase. The CTL takes the lead in planning and preparing the agreed purple team sessions with the departments or teams forming the BT (the defence of the institution). After the PT sessions, the CTL gathers documented input for remediation.

For a successful PT phase, the following steps must be taken:

- Step 1: Preparation
- Step 2: Purple team sessions
- Step 3: Document and gather input for remediation.

As explained in Chapter 4 the PT fundamentals variant is a one-day PT exercise (about eight hours) while the PT full variant may take multiple days (in practice often two to three days physically on location with different teams). These lead times only relate to the PT sessions and do not cover preparation, documentation or gathering input for remediation.



Step 1: Preparation

- Define scope and objectives: what do you want to achieve? Which teams and which experts are to be involved? Examples: improving detection, validating response processes, testing specific TTPs, involving SOC analysts, (business) process owners, product owners for example from IAM
- Plan PT sessions with the teams that should be involved based on the RTTR
- Agree on rules of engagement: boundaries, systems in scope, timelines
- Identify critical assets and (additional) 'what if' threat scenarios based on the RTTP and TI report
- Ensure communication channels (including the BT) and safeguard are in place.

Step 2: Purple team sessions

- RTP actions: Replay the simulated attack(s) step-by-step, share TTPs transparently
- Blue Team actions: detect, analyse and respond in real time; tune detection rules
- Continuous feedback loop: both teams collaborate during the exercise to close gaps immediately or to document them
- Review which TTPs were detected, how quickly alerts were triggered and response effectiveness
- Document blind spots, missed detections and process weaknesses.

Step 3: Document and gather input for remediation

During PT sessions, observations and issues to be resolved should be documented and gathered centrally. Documented improvements will be used as input to:

- Develop the remediation plan after the PT phase: improving use-cases and rules for detection, response playbooks, and security controls
- Share lessons learned across teams to strengthen collaboration and resilience and increase awareness on each level within the organisation
- Replay attacks steps and TTPs to validate improvements (optional).

< Back to overview purple teaming steps

6 Requirements for each PT variant

Apart from the required steps set out in Chapter 5, the following topics must be included in the PT fundamentals and PT full variants.

6.1 Requirements for PT fundamentals

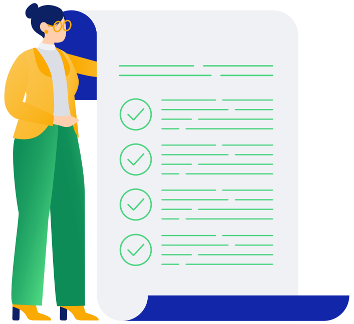
The PT fundamentals must at least include the following topics based on the RTTR, as identified by the RTP and CT:

- replay of the performed attack scenario(s)
- substantiation of why an assumed compromise or provided leg-up could have occurred in real life
- vulnerabilities identified during the test
- issues that could not be tested during the active red team testing phase (like in the PT full variant)
- discussion of anticipated remediation measures.

6.2 Requirements for PT full

The PT full variant must at least include the topics mentioned under the PT fundamentals variant, and in addition:

- alternative (what if) scenarios and their potential consequences
- other applicable threat actors and their TTPs, for example selected from the TI report
- forward-looking, outside-the-box scenarios or TTPs
- other steps which could have been taken by the RTP and potential BT responses to prevent other TTPs to be successful or lower their impact.
- demonstration of tools to improve security monitoring, detection, and response capabilities.



7 General considerations

7.1 Rationale

PT, whether being PT fundamentals or PT full, helps to optimise RTP and BT collaboration and maximises learning opportunities, defence capabilities, situational awareness and ultimately the return on investment of the whole test.

Well-executed PT can provide the institution with a comprehensive review of the effectiveness of its cyber security at each layer of its infrastructure in scope. Moreover, it aims to improve the detection controls that are crucial to shed light on suspicious activity.

7.2 Planning

PT should be scheduled close to the delivery of the final RTTR and optional BT Test Report. This timeline ensures that PT is carried out while the details and observations noted during the testing phase are still fresh in the minds of the BT and RTP. It is advisable to agree in advance on expectations regarding the outcome, communication channels, response and recovery activities, confidentiality boundaries, start and end, escalation paths, allocated resources (including budget) and reporting formats.

7.3 Communication channels

Communication channels (including the BT) and safeguards must be in place before the PT session(s) can start.

A dedicated communication channel is then set up between the RTP, BT, CT and TM. In the event of any further detection within well-defined boundaries (e.g. certain machines or subnets), the BT uses this channel to report the detected Indicators of Compromise (IoC) to the RTP, which confirms or refutes them as being part of their test.

Note that the CT should take special care to ensure that the BT blocks out confidential information that might not be related to the test. Should the identified IoCs indeed be part of the ART test, the BT will then perform the agreed measures to allow the test to continue. If this involves releasing an isolated machine or account, this is also referred to as 'catch and release'. Alternatively, other previously agreed actions might also be taken, such as shutting down a machine, escalating the incident or starting a forensic investigation with the aim of evaluating these processes as part of the test.

7.4 Results

PT allows direct leverage of the expert knowledge of the RTP and BT to revisit and address specific areas deemed important by the tested institution.

PT can therefore result in a deeper understanding of the interconnections and implications of the most relevant offensive and/or defensive measures for the tested institution. It might help to demonstrate and highlight the potential consequences from both a technical and a business perspective (e.g. remediation, recovery time/point-, business continuity, etc.) and hence inform considerations beyond the technical realm. As a result, PT may facilitate a better understanding of the consequences of an attack, further proliferation of an attack and alternative ways to enhance protection and detection. Observations made during the test and threat actor behaviour are to be used as input for Gold Teaming.

The results of PT will greatly benefit the further refinement of recommendations and remediation planning, which will in turn enhance the institution's cyber resilience. In addition, the results can be used in other operational resilience exercises and improve the institution's operational risk and information security/cyber resilience programme or framework. It is important to ensure that the PT results are clearly documented and used as input for the remediation and closure phases.

7.5 Scope and objectives

For both PT variants to be successful, the key members involved must clearly define the scope, goals, objectives, timing and rules of engagement for the actual PT activities. It is important to consider risks, since attack scenarios and TTPs can be tested under PT.

The PT full variant can have a forward-looking, outside-the-box perspective that is extreme but plausible and should simulate attacks which could occur in the (near) future. The CT should approach PT with an exploratory mindset to delve deeper into the attack scenarios and examine additional techniques and possibly additional attack scenarios. This could be done based on the TI report describing other relevant threat actors, scenarios and TTPs.

7.6 Cooperation among stakeholders

PT is planned by the CTL. The objective is to consistently achieve maximum learning outcomes. The CTL should connect the observations described in the RTTR and documented during the test to the departments and teams that make up the institution's BT, assigning responsibility to them for resolving these issues.

For the PT to be successful, the BT and RTP are expected to forge a working relationship and maximise their collaboration, to create a unique learning experience and enhance each other's understanding of the test activities. To ensure effective communication between the various teams, it is important to agree on clear definitions, so that all stakeholders have a common understanding. To promote effective cooperation, the RTP should set a positive example by clearly and thoroughly explaining their strategies and objectives to the BT, acknowledging areas of strength, and addressing the areas that require further improvement. This can be done for example by conducting remediation to refine existing controls or implementing new ones.

Close cooperation between the CT, RTP and BT is essential for successful PT. Regular checkpoints should be established to ensure the RTP and BT understand each other's actions. The CT should clearly define the roles and responsibilities in the PT setting and specify the TCT's role during the test to support effective collaboration.

Note that right after the RT phase, it may be difficult for the BT to shift from a defensive to a more cooperative attitude, particularly if its required actions are unclear. The CT should regularly communicate with the BT members to ensure the constructive nature of PT is maintained.

7.7 Roles and responsibilities

7.7.1 The TCT test manager

The TCT test manager (TM) acts as an adviser for all parties and especially the CTL during PT preparation. In particular, the TM is responsible for upholding and adhering to the spirit, principles and processes outlined in the ART framework. In some cases, the TM joins the PT sessions' kick-off meeting to explain the ART process and the TCT's role to the BT and to emphasise that ART is first and foremost a learning experience. The TM should also emphasise that they are not a supervisor, and that all observations will be treated confidentially (and not shared with the supervisor).

7.7.2 The control team

The control team (CT), and especially the control team lead (CTL), is responsible for making the necessary decisions as circumstances arise and for ensuring that proper risk management controls are in place for the test to be conducted in an appropriate manner. The CTL prepares the PT sessions and makes sure improvements are collected and documented from each purple team session. Risk management controls that apply to PT testing must remain effective.

7.7.3 The threat intelligence provider

The threat intelligence provider (TIP) can provide expert judgement on the (alternative) scenarios and TTPs to be used during PT. These can be derived from the TI report. Additional and more advanced scenarios or TTPs may be added, depending on the PT variant, planning, resources and timing.

7.7.4 The red team provider

The red team provider (RTP) can also provide expert judgement when considering and planning PT. Based on the observations documented by the RTP in the (draft) RTTR, the CT can invite people from different departments responsible for resolving them. The RTP could validate the planned sessions and provide a list of new and alternative TTPs to be used during PT. These could be based on the alternative scenarios set out in the TI report.

7.7.5 The blue team

The blue team (BT) is responsible for the defensive aspects of all scenarios that are executed. The BT may also contribute to additional scenarios and/or variations by providing interesting leads and feeding information back to the RTP during PT. Before starting the PT phase, the BT will be asked to respond to the RTTR, for example in an optional BT Test Report. The CT should ask the BT to document the following:

- for each applicable attack step described by the RTP in the RTTR:
  - a list of detected attack actions
  - log entries corresponding to these attack steps or detections (if any)
  - a timeline mapped with RTP and BT actions
- remaining RTP artefacts found by the BT, including information on when and where they were found and if the BT was informed about the artefact by the RTP (if applicable)
- an assessment of the findings and recommendations of the RTP
- evidence of the RTP attack collected by the BT
- BT root cause analysis of successful attacks executed by the RTP
- a list of lessons learned and identified areas of improvement
- a list of topics to be addressed in the PT exercise.

Annex: List of abbreviations

ART	advanced red teaming
BOD	board of directors, also referred to as executive board
BT	blue team
CIFs	critical or important functions
CMT	crisis management team
CT	control team
CTL	control team lead
GT	gold teaming
GTL	generic threat landscape
GTP	gold team provider
GTTP	gold team test plan
LPT	limited purple teaming
NDA	non-disclosure agreement
OSINT	open source intelligence
PT	purple teaming
RFP	request for proposal
RT	red teaming
RTP	red team provider
RTTP	red team test plan
RTTR	red team test report
SME	subject matter expert
SOC	security operations centre
SSD	scope specification document
TCT	test cyber team
TI	threat intelligence
TIBER	threat intelligence based ethical red teaming
TIP	threat intelligence provider
TIR	threat intelligence report
TM	test manager
TPSP	third party service provider
TTP	tactics, techniques and procedures

De Nederlandsche Bank N.V.
PO Box 98, 1000 AB Amsterdam
+31 (0) 20 524 91 11
dnb.nl/en

Follow us on:
Instagram
LinkedIn
X

DeNederlandscheBank
EUROSYSTEEM