Purple Team Strategies

Enhancing global security posture through uniting red and blue teams with adversary emulation

David Routin
Simon Thoores
Samuel Rossier

Purple Team Strategies

Enhancing global security posture through uniting red and blue teams with adversary emulation

David Routin

Simon Thoores

Samuel Rossier

Packt

BIRMINGHAM—MUMBAI

Purple Team Strategies

Copyright © 2022 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the authors, nor Packt Publishing or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

Group Product Manager: Vijin Boricha
Publishing Product Manager: Vijin Boricha
Senior Editor: Tanya D'cruz
Content Development Editor: Yasir Ali Khan
Technical Editor: Arjun Varma
Copy Editor: Safis Editing
Project Coordinator: Shagun Saini
Proofreader: Safis Editing
Indexer: Tejal Daruwale Soni
Production Designer: Shyam Sundar Korumilli
Senior Marketing Coordinator: Hemangi Lotlikar
Marketing Coordinator: Sourodeep Sinha

First published: May 2022

Production reference: 1190522

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham
B3 2PB, UK.

ISBN 978-1-80107-429-2

www.packt.com

Contributors

About the authors

David Routin became interested in computer security at a young age. He started by learning about old-school attack methods and defense against them in the 1990s with Unix/Linux systems. He now has over two decades of experience and remains passionate about both sides of security (offensive and defensive). He has made multiple contributions to the security industry in different forms, from the MITRE ATT&CK framework, the SIGMA project, and vulnerability disclosures (Microsoft) to public event speaking and multiple publications, including articles in the French MISC magazine.

As a security professional, he has held multiple positions, including security engineer, open source expert, CISO, and now **security operations center** (**SOC**) and Purple Team manager at e-Xpert Solutions. Over the last 10 years, he has been in charge of building and operating multiple SOCs for MSSPs and private companies in various sectors (including industry, pharma, insurance, finance, and defense).

His domains of expertise are SOC creation, SIEM technologies, use case development, Blue teaming, incident response for large-scale critical incidents, and forensic (SANS GCFA/GCIH certifications) and applied norms (ISO 27001 and PCI-DSS company certifications).

Special thanks to my co-authors and friends for taking up this challenge.

To my bosses, Cédric and Christian @e-Xpert Solutions, thank you for your trust and your support.

This book is dedicated to my family for their love, patience, and flawless support. Thank you, Marie, Elisa, and Alexandre.

Simon Thoores is a cybersecurity analyst who specializes in forensics and incident response. He started his career as a security analyst after obtaining an engineering diploma in information system architecture with a focus on security. He built his forensics and reverse engineering skills during large-scale incident responses, and he finally validated these skills with GCFA. Then, he moved to the threat intelligence field to better understand and emulate attackers in order to improve infrastructure security.

I want to thank my wife, Alix, for her boundless support and trust, and I also want to thank my family for their encouragement and help. Finally, I want to thank my former and current colleagues for their help and our late-night discussions about our common passion.

We would also like to thank Dimitri Cognet for his contribution to the book as a DevOps specialist.

Samuel Rossier is currently SOC lead within a government entity where he focuses on detection engineering, incident response, automation, and cyber threat intelligence. He is also a teaching assistant at the SANS Institute. He was previously responsible for a private bank group CIRT, and also worked as an SOC manager within an MSSP. He also spent several years within a consulting cybersecurity practice.

Samuel currently holds a master's degree in information systems and several information security certifications, including GRID, GMON, eCIR, eCTHP, eCRE, eNDP, and eJPT.

He is also a contributor to the MITRE D3FEND and SIGMA frameworks and likes to speak at conferences and analyze malware. He values a strong emphasis on the *people* dimension of cybersecurity by sharing knowledge.

Thanks to my family, friends, and colleagues for their guidance and support.
Thanks to my two sons, who are challenging me every day to be a better father.
Thanks to my friends and co-authors for this amazing cybersecurity journey we are sharing together.
Finally, I'd like to thank my beloved wife for her love, patience, and encouragement, and for always believing in me.

2

Purple Teaming – a Generic Approach and a New Model

Purple teaming is an under-documented process; indeed, there is no official documentation for this – even Wikipedia doesn't have any official article on this process (at the time of writing). The problem is also amplified as many vendors try to explain and develop their own vision of purple teaming activities based on the product they market.

This global issue leads to a situation where a vendor-agnostic approach based on financially interested parties and researchers is required to help people understand and implement purple team strategies in their companies.

In this chapter, we are proposing our own purple teaming vision; we don't pretend it is the best or the *official* one, but our vision is result-centric, based on our various purple teaming experiences using different scopes and approaches. We have also tried to leverage existing efforts that the community has made to help the industry mature the purple teaming process. We wanted to offer you practical processes and models that are as generic as possible, with documentation, collaboration tools, and continuous improvement capabilities in mind.

In this chapter, we will cover the following topics:

- A purple teaming definition
- Roles and responsibilities
- A purple teaming process description
- The purple teaming maturity model
- Purple teaming eXtended
- Purple teaming exercise types
- Purple teaming templates

A purple teaming definition

You might have noticed that we didn't define purple teaming in the first chapter. Therefore, let's start this chapter by defining what purple teaming is and what it is not.

First of all, purple teaming is not a dedicated team. So, be reassured that you don't need to hire additional, hard-to-find security experts to build a new team. In fact, *teaming* is simply the act of working together as a team. As we've seen in the previous chapter, there are issues currently faced by the traditional approach to red (offensive) and blue (defensive) concepts around security. Purple teaming joins both the red and the blue teams toegther to act as a virtual team during an exercise called purple teaming. This will ensure that both teams' goals are aligned and that both teams have incentives to help each other.

Purple teaming solves the issue with the *success of one means the failure of the other* mindset and helps an organization to optimize its security efforts in a common direction. It is a collaborative approach that creates a bond between red and blue members to, of course, enhance an overall organization's security posture but also to improve people's skills and communication.

This historical approach can also be enhanced thanks to purple teaming technical solutions. The *purple teaming activities flower* was eventually introduced, which describes the different components of purple teaming:

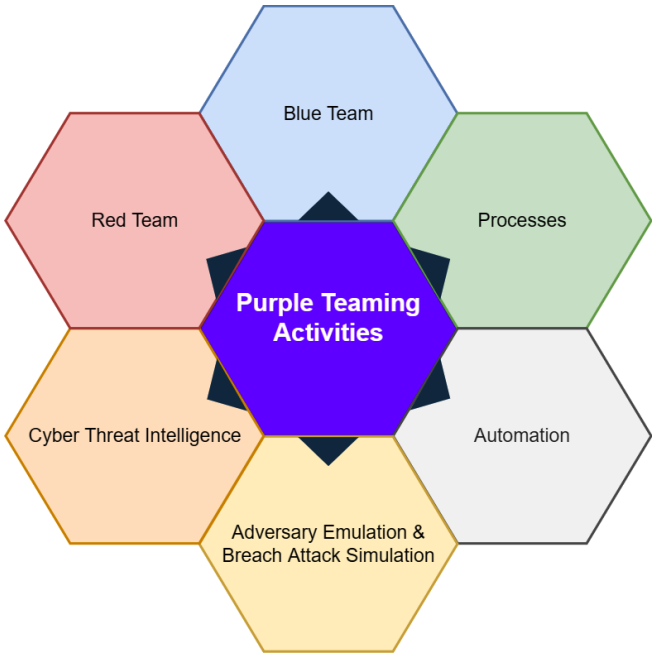

Figure 2.1 – A purple teaming activities model

From the previous figure, we can see that the activity is not limited to human interactions with blue and red teams and can also involve the following:

- **Processes**: Different processes are involved in the activity to provide a continuous improvement life cycle, including activity logs, reporting, and change management.
- **Automation**: Custom development of continuous security controls based on attacks.
- **Breach Attack Simulation (BAS)**: An operation consisting of replaying one or multiple existing attack techniques manually or relying on an existing tool.
- **Adversary Emulation**: Identifying different techniques used by a specific attacker, leveraging CTI, then building a plan to replay them in order to be able to test the organization's defenses.

Before digging into the purple teaming process, we need to describe the overall organizational structure encountered during a purple teaming exercise.

Roles and responsibilities

As usual in security, organization is key, especially for purple teaming success. Roles and responsibilities have to be clearly defined to avoid confusion, failure, and tension between teams and to optimize the success of the exercise.

A standard structure would look like this:

Roles	**Responsibilities**
Purple teaming manager/project coordinator	The person in charge of the whole purple teaming process, including planning with other managers, data centralization, exercise coordination, gaps analysis and reports, and purple suggestions for tools. Depending on the resources available internally, an external third party can also take over this role. This might be relevant in terms of independence.
Cyber Threat Intelligence (**CTI**) team/function	Responsible for identifying a threat actor relevant to the organization, extracting its **Tactics**, **Techniques**, and **Procedures** (**TTPs**), and helping the red team to build the attack campaign.
Red team/function	Receives the emulation/simulation plan from the CTI team, and lists and controls the correct executions of the assessments. In charge of preparing and executing the attack scenario, and research and development around new attack TTPs.
Blue team/function	Often, the blue team manager is the SOC manager and is responsible for the various security controls in place that will be tested. They are responsible for identifying the success and failure for each control. They are also in charge of implementing the improvements identified at the end of the exercise. They can also, in some cases, take the role of the purple teaming manager. The team oversees the security controls in place, whether it's a preventive, detective, or responsive control. Usually, SOC analysts are also involved in the detection engineering tasks necessary to implement identified improvements. The team can also oversee the running of purple teaming tools (such as continuous tests, BAS, and adversary emulations), depending on the organization size.

Table 2.1 – Purple teaming roles and responsibilities

Of course, the structure may be adapted according to an organization's resources, needs, and objectives.

Indeed, it is common to see companies where a purple team manager or dedicated project manager is missing or merged with other roles. Most of the time, the blue team manager will take the lead on a purple teaming activity; this will ensure that the incident response is not disproportionate and not blocking production assets. On the other hand, we might want to introduce independence for the assessment; in that case, it can be necessary to hire an external consultant that will lead the exercise as a coordinator and for the reporting activities.

In addition, it is also common to see companies that do not have a red team in place (or at least use external resources for scheduled activities).

We may think that the purple teaming process cannot be implemented if no internal red team exists. This is not correct. Leveraging external resources can still be used collaboratively on one hand and also completed with internal developments and solutions (open source or commercial) for continuous controls and improvements on the other hand.

The same applies to a **Cyber Threat Intelligence** (**CTI**) team, which most organizations don't have. Leveraging external third-party companies and resources is a must-have. Some might still be able to dedicate a **Security Operations Center** (**SOC**) analyst to perform this duty.

Now that we have a good understanding of the roles necessary for performing a purple teaming exercise, let's see how the process works.

A purple teaming process description

As we have seen previously, the purple teaming process combines red and blue activities across a joint-venture exercise supported by the CTI team and an exercise coordinator. This combined approach allows global company security to be improved thanks to failure and gap identification.

The Prepare, Execute, Identify, and Remediate approach

Everyone should be familiar with the **Plan-Do-Check-Act** (**PDCA**) process, also called the **Deming wheel**, which is a generic management tool used to verify and continuously improve processes and products over time. This seems to perfectly fit what purple teaming is trying to achieve, and that is why we have based the purple teaming process on this method, resulting in a more tailored **Prepare, Execute, Identify, and Remediate** (**PEIR**) model.

This high-level process is represented in the following figure:

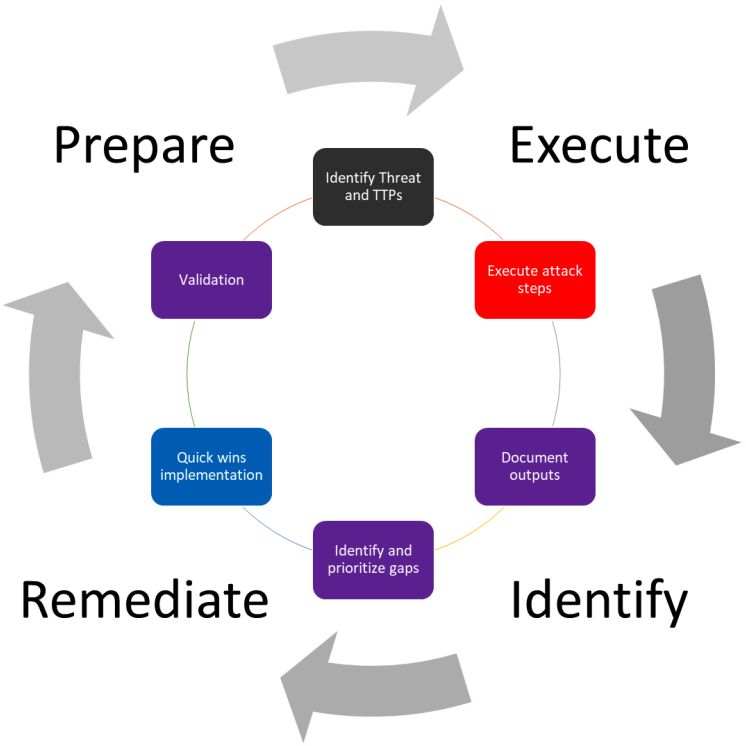

Figure 2.2 – The PEIR process of purple teaming

This scheme represents a high-level purple teaming approach where both blue and red team managers are involved. In such a situation, blue team members may or may not be informed about the exercises. Without crossing the boundaries of red teaming, whose goal is to be stealthy and assess response capabilities, a purple teaming exercise can still be performed in a blind way where most of the blue team members are not informed in order to also assess detection and response capabilities. Indeed, it is possible to simulate red team activities such as injecting logs or deploying unweaponized techniques to evaluate the blue team's overall capabilities and controls, especially investigation, escalation, and response.

Let's now see in a bit more detail each step of the process:

1. **Prepare**: The purple process is initiated by a plan to run security tests (offensive actions, attacks, and scans) on a predefined scope and security controls. This plan can be manually defined (at least for the first iteration) or automated using advanced implementation or solutions (**Breach Attack Simulation** (**BAS**), custom developments, adversary emulation, and so on).

The following is a workflow example of this process step:

A. All members sit at the same table for this phase.
B. The CTI team starts by selecting a threat actor and the TTPs of the attack that are relevant to the organization, depending on its context and environment.
C. The CTI team presents the TTPs that the red team will prepare to perform the selected scenario.
D. The CTI and the red team present the detailed TTPs to the blue team, which documents and identifies expected security controls (prevention, detection, and hunts) for each presented TTP. This step can be skipped if the blind approach is selected.

2. **Execute**: Attacks are executed in person by a red team or emulated with a tool (continuously or temporarily). The current active defense systems are expected to detect TTPs partially or totally to provide security-related information.

The following is a workflow example of this process step:

A. The red team starts executing the selected attack scenario.
B. The blue team will detect and respond to these TTPs.
C. The blue team manager will report the findings to the purple team manager.

3. **Identify**: Gap detection and prioritization are performed. All related information will be reported to the purple teaming process owner (the project manager or SOC manager) or to a technical solution that will identify detection gaps and new unseen security risks.

The following is a workflow example of this process step:

A. All members sit at the same table for this phase.
B. All teams go through each step of the attack and describe all issues, successes, and failures to document the efficiency of all security controls identified at the beginning of the exercise.
C. The purple team manager documents all findings.
D. All members assess and prioritize improvements according to the risk reduction and the implementation effort.

4. **Remediate**: Implement and validate improvements. Prevention and detection gaps will be identified and then transmitted to the blue team manager to prioritize the implementation of a corresponding remediation. The blue team will perform detection engineering in accordance with the identified risks and then implement new detection rules or change existing configurations. As a continuous improvement process, detection will be checked afterward to ensure it is implemented and working properly.

The following is a workflow example of this process step:

A. The blue team implements the quick wins.

B. The red team replays TTPs related to the newly implemented quick wins to ensure immediate efficiency.

C. The blue team together with the purple team manager document and plan the rest of the identified improvements on a roadmap.

This workflow is vendor-independent and can cover any type of purple teaming activities. It can be used as a generic purple teaming workflow approach.

For the veterans among you, in 1993, a document called *Improving the security of your site by breaking into it* published by *D. Farmer* suggests various attack methods to defend by thinking like an attacker. It could be the first public resource describing an approach for purple teaming, even if the team, in that case, was composed of one person only.

Purple teaming exercises can be considered as a continuous security improvement process by mixing offensive and defensive skills. This exercise is not purely focused on technology but can also be shaped in different forms to improve the overall security posture (that is, people and processes too).

The foundation of cybersecurity is often described with three pillars, which are the people, the processes, and the technology (or products). Let's now see how purple teaming can address each of them.

Improving the people

Improving the people with purple teaming is a must. Regardless of the types and goals of the purple teaming exercise, people will always benefit from it because it gives them the opportunity to see the other side of security. The red team will learn and understand what kind of security controls are in place within their organization, how they can bypass it, and therefore think about ways to strengthen it to increase the overall security posture of the organization. On the other hand, the blue team will learn and understand how the red team, and therefore adversaries, approaches and operates during an attack scenario, as well as better understanding the strengths and weaknesses of their controls, again to improve the defense strategy.

Nevertheless, it can be useful to assess how people react and handle security alerts and incidents within an organization.

Even if it is not *pure* purple teaming, some professionals may also implement a blind approach where the blue team is not initially informed. It can be interesting for the blue team manager to determine whether all the members of its team can investigate and handle alerts and incidents in a consistent manner and not depend on people's interests, skills, and experience.

The following criteria should be taken into account:

- **Mean Time to Detect** (**MTTD**), which starts from the beginning of the attack until the first event or alert being handled by the blue team.
- **Mean Time to Respond** (**MTTR**), which starts from the beginning of the attack until the full containment of the attack by the blue team. This one can be tricky, as it might lead the team to select alerts and incidents that they are most comfortable with. Other key points can be monitored, such as the fact that blue team analysts have effectively followed the steps described in **Standard Operating Procedures** (**SOP**) and/or incident response playbooks.

Then, the purple team manager can use those **Key Performance Indicators** (**KPIs**) to create charts in order to identify improvements and benchmark against other purple teaming exercises over time. This approach is fully described in *Chapter 14*, *Exercise Wrap-Up and KPIs*.

When considering assessing people, other parameters must be considered, such as the following:

- Analyst skills
- Adequate resources to incident response

Thus, to evaluate those points, a purple approach would be to open critical cases and measure whether the blue team (especially level 1) is able to manage and respond to cases in a timely and effective manner (using a service-level agreement or an average handling time).

The capacity to adapt to TTP variations is also important; perhaps your blue team is highly trained to handle specific incidents, but what if slightly different TTPs are applied or, even worse, a different threat actor with radically different TTPs starts considering your business a potential target? This is exactly why simulation is also a key concept that need to be applied and developed. Testing your organizations controls against non-related threat actors may add value in case threat actors decided to shift targets or motivations.

Improving the processes

In addition to people, processes are the second key pillar of any organization's cybersecurity practice; for this reason, it is important to assess several aspects, such as the following:

- **Creating defense from newly tested attackers' tools using a shared methodological approach**: This is maybe one of the best examples of a powerful collaboration between the red and blue teams thanks to purple teaming. The concept is quite simple – new tools and TTPs are published every day and evaluated by the red team to improve their internal knowledge, but the same TTPs are also reviewed by the blue team to implement security controls.
- As the purple team is focused on collaboration, both team members should work together to evaluate TTPs to create not only new attack methods but also new security controls (or validate existing ones) to detect and mitigate these methods.
- Reducing the amount of work with automated controls.
- **Assessing incident response processes**: Performing purple teaming exercises can help measure the efficiency of your whole **Incident Response** (**IR**) process; you can review reports generated from these exercises and assess the quality of your IR at each point (analysis, containment, remediation, recovery, and lessons learned)

All these aspects should be taken into consideration when improving the processes around cybersecurity within an organization.

Improving the technology

Technical solutions are implemented at different layers; therefore, being able to assess them is an absolute requirement to ensure the safety of your data. Purple teaming can help us with the following:

- Improving perimeters and endpoint security.
- Continuously testing **Security Information and Event Management** (**SIEM**) detection rules to ensure system's health.
- *Diffing* security tools that generate reports at different periods in time to monitor and alert on evolutions and changes. This topic will be discussed in *Part 4*: *Assessing and improving* of the book.

  Generating automated reports from security tools such as vulnerability scanners, Active Directory security audits, and network port scanners frequently, and making the *diffing* automatically between the previous and current report to generate alarms and insights from this intelligence. These technical implementations will be covered in *Chapter 12*, *Purple Teaming eXtended*, to provide practical usage examples.
- Being able to answer the C-level question, "Are we prepared for a `New_Strange_Name` attack?"

So, clearly, the old approach of red versus blue, even if still applicable, can be greatly improved. This book was created for that purpose – giving us new concepts, tools, opportunities, and ideas to leverage purple teaming in order to improve our overall security posture.

Each of us co-authors has had experience in different environments with multiple positions, providing various visions and tried-and-tested methods of purple teaming for multiple layers of security.

Now that we understand the standard purple teaming process, the next obvious question to ask ourselves is, where do we start? That's why we believe that a maturity model is key to enabling all organizations, whether Fortune 100 or small-to-medium businesses, to start applying purple teaming within.

The purple teaming maturity model

Whether our blue team is composed of one person or a full SOC and **Computer Security Incident Response Team** (**CSIRT**), the maturity model should give us a place to start and help us make our way up to the top.

We, humbly, tried to develop a new approach while having in mind that the industry is overwhelmed with new tools, acronyms, frameworks, and models every day. So, we tried to stick to something simple and applicable to any kind of organization. We strongly believe that this practical model to purple teaming will help anyone succeed:

The purple teaming maturity model			
	CTI	**Red**	**Blue**
Level one – initial and manual	Collect top TTPs from public sources.	Execute TTPs as described with the exact same tools and procedures.	Focus on the validation of existing and identified security controls.
Level two – defined and semi-automated	Collect TTPs and adversary emulation plans from public sources for threats tailored to an industry and/or region.	Execute the same procedures with other public tools.	Train the blue team to defend and hunt but also focus on ensuring the visibility of red team activities (data sources and logs).
Level three – optimized and mainly automated	Produce TTPs and emulation plans for threat actors tailored to an organization.	Develop custom tools and procedures to test slight deviations.	Detection engineering and hardening prioritization.

Table 2.2 – The purple teaming maturity model

As we can see here, the model is meant to fit any organization's size. Of course, third-party tools or services can help in fulfilling a role, as stated previously. Maturity levels are not meant to be aligned between all teams. It is also important to keep in mind automation as we mature; repeated activities must be automated as much as possible to ease the repetition of exercises.

As an example of maturity levels, we can rely on our CTI inputs on public reports describing the most used TTPs as a start (level one), having a red team executing the TTPs exactly as described in the provided CTI report (level one), and having the blue team already looking at improving and developing new alerts (level three).

But how can collaboration work between the three teams? We will suggest a tool in the next section. Let's introduce here the purple teaming templates.

PTX – purple teaming extended

We strongly believe that the purple teaming mindset could benefit organizations by being extended for broader use. The approach remains the same and follows the PEIR process, but it could be applied not only for adversary emulation but also for various types of exercises, as we will see later in this chapter. Indeed, any offensive activity that builds on the attack, audit, or scan steps can be automated to perform continuous testing to assess, measure, and control security controls based on active detections or blocking mechanisms at any layer of an infrastructure. This approach will be detailed more in the next section, and multiple examples of this approach will be covered in *Chapter 12*, *PTX – Purple Teaming eXtended*.

Let's now see some types of exercise that can be performed based on the generic purple teaming process and the **Purple Teaming eXtended** approach.

Purple teaming exercise types

In the previous sections, we have seen the official operation of what a purple teaming exercise is, but we have also seen that the concept of purple teaming could and should include a broader usage of PTX to benefit organizations. We will now see different exercise types that can be defined using the five Ws and 1 H framework:

- **Who**: The *who* defines the functions during the exercise; it could be in-person (teams, managers, or coordinators) or automated (for example, with a breach attack simulation tool). We must think about filling the following functions:
  - The defensive function
  - The offensive function

    - The CTI function
    - The purple coordinator

- **What**: The *what* defines the threat(s) that will be tested, such as the **Advanced Persistent Threat** (**APT**) group, vulnerability exploitation, specific TTP, and threat campaign.
- **Where**: The *where* defines the scope of controls to be assessed, such as people, processes, products, and technologies.
- **When**: The *when* defines the planification and frequency of the exercise; it can be scheduled or continuous.
- **Why**: The *why* defines the reason to perform this control – for example, is it to prevent an existing risk, a future risk, or check the health of existing controls?
- **How**: The *how* defines the methodology and approach, such as informed-based exercises and an emulation plan.

Next, we'll describe some exercises and the processes linked to them.

Example one – APT3 emulation

Let's start by defining the five Ws and one H of the emulation of the threat actor APT3:

Who	In-person, the blue team, the red team, the CTI team and the purple manager
What	APT3 emulation
Where	Technical controls, incident response process, and collaboration
When	Scheduled
Why	Evaluating cyber-resilience of the organization against the APT3 threat actor
How	An informed approach and APT3 emulation plan

Table 2.3 – The five Ws and one H for the APT3 emulation

Adversary emulation is probably the most common purple teaming exercise with the collaboration of red and blue teams. So, how do we handle such an exercise?

To make it easier with a concrete example, we suppose that after producing our CTI, which will be described in the next chapter, we can select the APT3 threat actor as a potential adversary to our organization. Let's assume we have both a red and a blue team internally, and that we need to make them work together to run a purple teaming exercise in order to assess our cyber-resilience against this threat actor.

Step one – preparation

The process begins with the *preparation* phase; at this stage, we will use available information and intelligence regarding this adversary.

An initial approach would be to use the MITRE ATT&CK framework, `https://attack.mitre.org/groups/`, to gather initial information on the adversary. Indeed, this would be faster than reading and aggregating multiple threat intelligence reports:

Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1087	.001	Account Discovery: Local Account	APT3 has used a tool that can obtain info about local and global group users, power users, and administrators.[4]
Enterprise	T1098		Account Manipulation	APT3 has been known to add created accounts to local admin groups to maintain elevated access.[7]
Enterprise	T1560	.001	Archive Collected Data: Archive via Utility	APT3 has used tools to compress data before exfilling it.[7]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	APT3 places scripts in the startup folder for persistence.[3]
Enterprise	T1110	.002	Brute Force: Password Cracking	APT3 has been known to brute force password hashes to be able to leverage plain text credentials.[3]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	APT3 has used PowerShell on victim systems to download and run payloads after exploitation.[3]
		.003	Command and Scripting Interpreter: Windows Command Shell	An APT3 downloader uses the Windows command `"cmd.exe" /C whoami`. The group also uses a tool to execute commands on remote computers.[3][4]
Enterprise	T1136	.001	Create Account: Local Account	APT3 has been known to create or enable accounts, such as `support_388945a0`.[7]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	APT3 has a tool that creates a new service for persistence.[3]
Enterprise	T1555	.003	Credentials from Password Stores: Credentials from Web Browsers	APT3 has used tools to dump passwords from browsers.[4]
Enterprise	T1005		Data from Local System	APT3 will identify Microsoft Office documents on the victim's computer.[7]
Enterprise	T1074	.001	Data Staged: Local Data Staging	APT3 has been known to stage files for exfiltration in a single location.[7]
Enterprise	T1546	.008	Event Triggered Execution: Accessibility Features	APT3 replaces the Sticky Keys binary `C:\Windows\System32\sethc.exe` for persistence.[7]
Enterprise	T1041		Exfiltration Over C2 Channel	APT3 has a tool that exfiltrates data over the C2 channel.[8]
Enterprise	T1083		File and Directory Discovery	APT3 has a tool that looks for files and directories on the local file system.[8][9]
Enterprise	T1564	.003	Hide Artifacts: Hidden Window	APT3 has been known to use `-WindowStyle Hidden` to conceal PowerShell windows.[3]
Enterprise	T1574	.002	Hijack Execution Flow: DLL Side-Loading	APT3 has been known to side load DLLs with a valid version of Chrome with one of their tools.[8][10]
Enterprise	T1070	.004	Indicator Removal on Host: File Deletion	APT3 has a tool that can delete files.[8]

Figure 2.3 – MITRE ATT&CK showing the APT3 adversary techniques used

Another interesting feature is the MITRE ATT&CK Navigator; this web application allows an analyst to clearly view the attack steps (tactics) and techniques used:

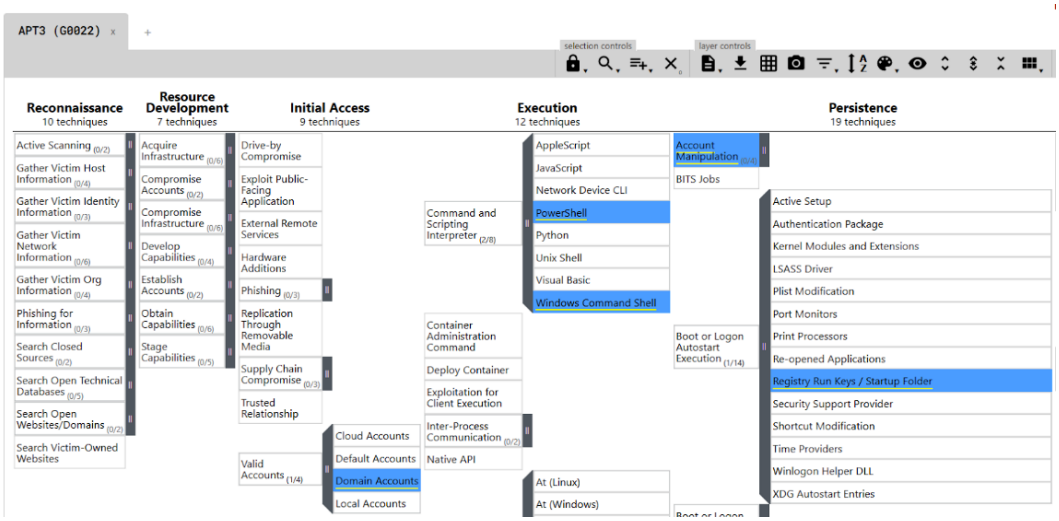

Figure 2.4 – The MITRE ATT&CK Navigator for APT3

Each technique is detailed and usually has an interesting detection section. It will provide a generic approach to detect each specific technique. It requires detection engineering skills to be converted into practical usage – for example, monitoring `net.exe` or `net1.exe` usage, which can be technically translated to the following:

- The required data source: Sysmon
- Sysmon `EventID` to collect: 1
- Specific fields to analyze: `Image` or `CommandLine`
- Pattern match (pseudocode): `Image == "*\net.exe*"` or `Image == "*\net1.exe*"`

As we can see, *detection* recommendations require additional work to be effective.

From this pre-analysis, an adversary emulation plan can be defined. This document should contain details on all identified techniques and how to reproduce them. A sample of such a document is provided by MITRE at `https://attack.mitre.org/docs/APT3_Adversary_Emulation_Plan.pdf`.

Obviously, to be able to create reports from this adversary emulation, we need to have an overview of all the actions to perform. For this, multiple approaches can be used, usual spreadsheets, or dedicated tools for collaboration. (This option will be described later in *Chapter 9*, *Purple Team Infrastructure*.) For a first-time scenario, we will rely on an existing spreadsheet provided by MITRE for this specific APT group.

We modified it a little bit to add additional columns, test results, and reasons/comments. Ideally, tests should not be performed on a production environment. A cyber range infrastructure or a *pre-production* environment similar to the real *production* environment should be used to prevent disruptions that may be caused by an attack. While riskier, executing the TTPs in the production environment would gives the most accurate results.

It is also important to schedule operations with both blue and red teams to have dedicated resources working simultaneously on the exercise.

So, the global output of this phase is as follows:

- Define the adversary TTPs.
- Create the emulation plan.
- Create a spreadsheet to be filled with expected attack results
- Define the scope of the tests.
- Schedule operations with both teams.

Once everything is prepared, the next phase can be applied – execution.

Step two – execution

This step will be the starting point of the attack scenario. Both teams start the exercise.

The red team plays the TTPs one by one corresponding to the emulation plan defined previously. In the meantime, the blue team checks the expected security controls (prevention, detection, and hunting) in tools such as **SIEM**, **Endpoint Detection and Response** (**EDR**), and **eXtended Detection and Response** (**XDR**) to ensure that each technique is properly prevented, detected, or at least logged.

The blue team will have to fill in the emulation plan results.

The output is as follows:

- Emulation plan results
- Results sent to the purple team manager

Now, we can move on to the next step – identification.

Step three – identification

The emulation plan will be analyzed to determine gaps, failures, and improvements on each expected security control. A remediation plan will be created with prioritized actions based on implementation effort and risk reduction.

Once done, this information will be transmitted to the blue team to improve prevention, detection, and logging capabilities.

The output is as follows:

- A remediation plan with prioritized improvement actions

Let's move on to the final step – remediation.

Step four – remediation

Once received, the blue team manager asks detection engineers, SOC analysts analysts, or SIEM/SOC engineers to implement new detection rules and/or change the existing configuration to close identified gaps.

As a continuous improvement process, once implemented, these failed detections should be tested again with the same tests to ensure newly modified security controls work properly.

Some KPIs and reports of the operation will be provided to different managers to show the process relevance and demonstrate the security improvements.

The output is as follows:

- Configuration changes and/or new use cases
- Reporting
- A new iteration of the process to ensure everything was implemented correctly

As discussed previously, different types of exercise can be performed to leverage the purple teaming approach. We will describe other common and uncommon exercises next.

A breach attack simulation exercise

Let's define the five Ws and one H for a BAS exercise:

Who	Automated for the red team, the blue team, and the purple manager
What	A set of TTPs
Where	Technical control validation
When	Continuous or repeated
Why	Evaluate current security control efficacy
How	An informed approach and a selection of TTPs from the BAS library

Table 2.4 – The five Ws and one H for the BAS exercise

An approach using existing BAS solutions is common nowadays; indeed, attackers' techniques are mapped in the MITRE ATT&CK framework in a standardized way.

From this postulate, it becomes possible to apply a model similar to the previous one.

Step one – preparation

Even if part of a job is automated, the preparation phase remains a success key.

In such a situation, multiple elements have to be considered and configured.

Once again, you have to define your tests (if not defined by default in the BAS solution), based on CTI or the most common trends (see next chapter).

From there, you will build your emulation plan and pay special attention to technique tags that can be extracted from the MITRE ATT&CK framework.

In this specific configuration, the red team will be potentially involved only in the last step (remediate); instead, the blue team will work by itself with the BAS tool.

As usual, a test machine using the same production conditions (such as audit policies and log collection) will have to be used.

The output is as follows:

- The simulation plan (based on the same model as the emulation plan)
- The simulation results spreadsheet (for results analysis)
- The test machine (ideally virtual and snapshotted for reuse later on)
- BAS software installation on a dedicated machine (such as Atomic Red Team)

Let's now go to the execution step.

Step two – execution

In this situation, the blue team will work by itself and will run tests locally to ensure security detection.

For each test, the blue team will check on required security devices (SIEM, EDR, and so on) to ensure prevention and detection happens correctly.

All elements will be reported on the simulation results spreadsheet at the identification phase.

The output is as follows:

- The simulation results spreadsheet (updated)

Once the execution has been performed, we need to document the results and identify necessary remediations.

Step three – identification

At this step, the purple team manager (or, more generally, the blue team manager) will analyze the simulation results spreadsheet and identify gaps. These gaps will be output for the last step – remediation.

The output is as follows:

- A summary of the simulation plan results with identified gaps and possible improvements

Now we move on to the last step, remediation.

Step four – remediation

At this stage, remediations will be handled by the blue team to add new detection capabilities. To follow the control process, the red team can then be included in the process to perform collaborative tests with exact techniques and small variations to ensure the detection of identified gaps.

The output is as follows:

- Implemented changes
- A request for a new human-based control with the red team to ensure the correct detection (a new purple teaming exercise loop)
- Reports to management

We will now see another type of exercise that slightly deviates from the original definition but still retains the purple mindset. It is not an exercise anymore but rather a continuous assessment.

Continuous vulnerability detection

Let's now see the five Ws and one H of continuous vulnerability detection:

Who	Automated for the red team and the blue team
What	Exploit of an internal or external facing application
Where	The vulnerability management process
When	Continuous/Repeated
Why	Evaluating cyber-resilience of the organization against known vulnerabilities and preventing intrusions from exploited vulnerabilities
How	Continuous external and internal vulnerability scans and *diff* analysis

Table 2.5 – 5 Ws and 1 H for continuous vulnerability detection

This specific use case will be fully described in the next chapters; the global concept we will introduce is **vulnerability diffing** (also known as a **purple scan**).

This is the same concept as patch diffing where a reverse engineer will try to find the differences between an existing portion of reverse-engineered code before and after an applied patch to discover a zero-day vulnerability. This same *diffing* approach can be applied to an infinite number of security solutions (such as vulnerability scanning, AD audits, and network scans).

In this specific scenario, a vulnerability scanning solution is implemented, reports are collected automatically and normalized, and then an algorithm is applied to detect differences between previous and current vulnerability scans. These differences are considered as new vulnerabilities to investigate and will generate an alert to the blue team.

This approach can be implemented without the red team.

Step one – preparation

The interesting part of this scenario is that thanks to automation, human activity and document handling are strongly limited.

Basically, the main requirement is to set up the correct technical components – a vulnerability scanner, a scheduled scan on a specific scope, and a script run for data collection and diffing (which can be done thanks to a SIEM with *real* analytic capabilities).

The output is as follows:

- A configured vulnerability scanner (scheduled scans)
- Data collection, normalization, and a *vulnerability diffing* algorithm implementation thanks to a custom script
- Alerting, email, **instant messaging** (**IM**), and so on

Let's now go to the execution phase.

Step two – execution

Contrary to the other scenarios presented previously, execution is automated and repeated (scheduled once a week, for example). This frequency allows us to greatly reduce the attack window risk.

Once executed, reports are generated and then collected by a SIEM or using custom code.

The purple scan code or the SIEM will handle the identification step.

The output is as follows:

- Generated reports

Now let's move on to the identification step.

Step three – identification

As already shown, the main idea of this step is to be able to perform an automated analysis between a previous and a new scan. This difference can be applied using a previous reference of the vulnerability name and the impacted host tuple.

Once a difference (diff) is identified by the detection algorithm, an *alert* event is generated to the SIEM, which is analyzed by the blue team as a *newly identified vulnerability* and handled as a security threat.

Whether it produces positive or `null` results, the new report is considered as the new *reference* model.

The output is as follows:

- SIEM alerts that contain the result of vulnerability diffing (only if positive)

Finally, let's tackle the remediation step.

Step four – remediation

Once the blue team receives this alert the internal vulnerability management process will begin for prioritizing patching.

The output is as follows:

- Vulnerability identified
- Applied patches
- A new manual scan after a patch to ensure that it is correctly patched
- Automatic updates of dashboards, reports, and KPIs

The next section requires the collaboration of both attack and defense teams to protect the company from new hackers' TTPs.

A new TTP or threat analysis

Let's now see the five Ws and one H for an exercise focusing on a new TTP:

Who	In-person, the blue team, the red team, and the purple team manager.
What	New TTP used by attacker
Where	Technical controls, incident response process, and collaboration.
When	Scheduled.
Why	The objective is to prepare the company for detecting and preventing attacks against a newly used TTP.
How	The red team and the blue team will work closely using the *purple teaming analysis collaboration template* to provide continuous improvements in detection engineering for this new TTP.

Table 2.6 – The five Ws and one H for the new TTP exercise

In this scenario, the company is facing another problem – they need to create detection from an existing public threat, TTP, or offensive software. This same model can be applied to published exploits without a patch provided for the vulnerability or no available team to patch quickly. The red and blue teams will be involved together to build detection rules collaboratively.

Let's take a practical example.

The red team, as part of their research and development, analyzed a threat report to discover a new potential TTP to use. This report disclosed the fact that **Ping Castle** is used by an attacker group to perform malicious operations. PingCastle is a tool developed by Vincent Le Toux (who is also the famous Mimikatz co-author), which allows any domain user to get an exhaustive overview of Active Directory security risks and exploitation possibilities. It has the main advantage of being trusted by antivirus/EDR vendors and can be run on the command line. A quick search on the internet did not reveal any technique that could be used for the detection of such a tool.

This issue is very common because most of the time, attackers will try to use TTPs that are as stealthy as possible to evade detection.

Now that we've understood the overall process and some practical applications of purple teaming, let's talk about about purple teaming analysis collaboration template.

Purple teaming templates

Purple teaming is an amazing example of collaboration across teams that usually compete with each other. This is where a need for a standardized collaborative approach and methodology is necessary. Let's introduce the purple teaming templates. Here, two templates are proposed. One purple teaming report template which contains the intelligence overview, the emulation plan and can validate security controls and identify improvements and gaps a low level version of this template can be found inside the *Chapter 14*, *Exercise Wrap-up and KPIs*. The collaboration engineering template aims to provide a standardized methodology to guide red and blue teams through a detection engineering process.

Both can be leveraged as inspiration for a custom template that better suits everyone's needs.

Report template

This template example is intended to be a complete log of a purple teaming exercise. It describes its objective, the intelligence overview of the threat being emulated as well as the adversary emulation plan. This plan lists the techniques identified by the CTI team. The red team can then explain the procedure of how the technique will be executed. The blue team can then identify and document each of its security controls following the four key dimensions – prevention, visibility, detection and remediation.

Throughout an exercise, each successful and failed control can be highlighted with a dedicated color. Upon completion, the purple teaming manager can synthesize the results before all three teams sit together to discuss the priority concerns of the gaps and improvement opportunities identified:

Purple teaming analysis collaboration template						
Version	1.0	**TLP**	12.12.2012	**Date**	AMBER	
Teams and roles	John - Coordinator Alice - Red Team Bob - Blue Team Mario - CTI Team					
Purple teaming objective	Objective of this exercise is to evaluate defenses against threat X					
CTI overview						
Name	Threat X					
Type	Malware/Threat actor					
Overview and relevance to organization	Threat X is a malware known to be used by initial access brokers before selling accesses to ransomware operators. Threat X is relevant to our organization because we've seen it in previous incidents.					
Objective	Threat X main goal is financial					
Victimology	Various and opportunistic					
Tools and malware	Malware Y					
Attribution theory	Threat actor Z is behind the threat X					
TTPs – ATT&CK Navigator	<Link or screenshot of the ATT&CK Navigator map of the TTPs of threat X					
Emulation Plan						

CTI Team		Red Team		Blue Team			ALL
Tactic	Technique	Procedure		Control	Type	Effectiveness	Comment
		Description	Execution				
<Reference to MITRE tactic>	<Reference to MITRE technique>	<Description of the procedure>	<Command line execution> <Control 2>	<Control 1>	Preventive / Telemetry / Detection / Remediation	Effective / Partially effective / Ineffective	Expected, not expected
				Preventive / Telemetry / Detection / Remediation	Effective / Partially effective / Ineffective	Expected, not expected	

Table 2.7 – The basic collaboration template

Now let's see another type of template useful for collaboration engineering.

Collaboration engineering template

This template can be used for multiple analysis activities requiring both red and blue teams' work and analysis. We have tried to make it as standard as possible and respect the PEIR approach to ensure security improvements and controls throughout the collaboration. The detection logic relies on pseudo-code to be *product-agnostic*. All the gray parts have to be filled. Please note that interaction should still be coordinated by a manager:

<table>
<tr><td colspan="2">Purple analysis collaboration template</td><td>Version and date</td><td>Coordinator(s):</td></tr>
<tr><td colspan="4">Generic comments and exercise description
APTxx is using PingCastle as an offensive tool for privilege escalation assistance; detection of this activity is required.</td></tr>
<tr><td colspan="4">Step one – preparation</td></tr>
<tr><td>Red team references</td><td>Blue team references</td><td colspan="2">Exercise type</td></tr>
<tr><td>Articles and tools</td><td>Links related to detection/risk control</td><td colspan="2">New TTP analysis
Exploit/vulnerability
Hacking tools
Others – specify</td></tr>
<tr><td>Red team members</td><td>Blue team members</td><td>Involved red team infrastructures</td><td>Involved blue team infrastructures</td></tr>
<tr><td>Name one, name two, and so</td><td>Name one, name two, and so</td><td>Attack on the server IP address,
username, and so on</td><td><code>Cyber_ranges</code>, <code>test_vlan</code>, and <code>endpointNN</code></td></tr>
<tr><td colspan="2">MITRE ATT&CK tactics
Initial access
Execution
Lateral movement
Privilege escalation</td><td colspan="2">MITRE ATT&CK techniques
List of techniques should be listed here</td></tr>
<tr><td colspan="4">Execution schedule – from 19.07.2021 09:00 to 19.07.2021 18:00</td></tr>
</table>

Step two – execution			
Red team		**Blue team**	
Initial runtime (first run)	19.07.2021 09:25	Triggered alerts at the first run from systems List all alerts triggered by the red team execution (`Alert_reference`, alert title, and data source(s) involved)	
Red team comments Examples – partially detected and can be easily bypassed (improvements required)		Blue team comments	
Blue team capabilities		Detect/block/no detection/partial	
Blue team capacity validated (even with variations) ?		YES (the process stops)/NO	
Step three – identification			
Red team threat replay	List each iteration timestamps	Specify additional information (variations)	
Threat source code available ?	Red team Indicator Of Compromise/ TTP information List the IOC provided by red Team	Blue team IOC/TTP information List IOC provided by the blue team	External information
Complementary analysis			
Activity	Blue team data source and event type	Pattern(s) to match or pseudo-code logic	Number of matches for 7 days (in SIEM)
Execution	Sysmon EventID 1	Image, ParentImage, CommandLine, and Products	
Network connection	Sysmon EventID 3	List domain, IP, and ports	
Driver loaded	Sysmon EventID 6	List of loaded drivers	

File creations	Sysmon EventID 11/15	Filename and paths	
Registry modifications	Sysmon EventID 12/13/14	Registry path and actions	
Pipe events	Sysmon EventID 17/18		
WMI activities	Sysmon 19/20/21		
Network behaviors	Intrusion Detection System logs Firewall IPS Other devices	Locally opened ports Outbound IP connection Outbound domain connection Used protocols Covert channel based on third party protocols such as DNS Other recognizable activities	
Network packet captures	IDS	Precise patterns to match using the IDS rule. You could use Wireshark to extract hexadecimal signatures	
EDR/detection devices alerts	EDR	Alarm name	
Other events of interest	Authentication Groups management Sensitive privileges File access (monitor) Sensitive objects access	Example: EventID = 4624 and Logon type 3 Activate audits on specific objects	

Detection logic (pseudo code-based) and comments, here we suggest two different aproaches:

First approach:

```
(src_ip in [HOME_NET]) AND

(dest_ip in [HOME_NET] ) AND

dest_port=389 AND protocol=389 AND

packet.match("43 4e 3d 57 69 6e 64 6f 77 73 32 30 30 33 55 70
64 61 74 65" OR "43 4e 3d 6d 73 2d 4d 63 73 2d 41 64 6d 50
77 64") | group by distinct_count(packet_match) by src_ip |
where distinct_count(packet_match) > 1)
```

Second approach:

Enable object audits (Event 4662) on non-existing computer objects (honeytokens)

Additional data source to collect	IDS	**Number of SIEM hits with this detection logic (history of the last 7 days)**	

List of changes required for implementation:

Here, you list every required change:

- A new data source/scope to monitor
- EDR rule for blocking
- IDS rule
- SIEM rules for detection
- Sigma/YARA rule in the catalog
- Change request ID (if change management is implemented)

Changes implemented in the test environment	Date of implementation by name one	Ready for a new test by the red team	YES/NO

Red team		**Blue team**
New run	21.07.2021 10:25	Attacks correctly detected and/or blocked List all alerts triggered by the red team execution (`Alert_reference`, the alert title, and data source(s) as proof of success)

Confirmation that the threat was correctly handled (blue team)		YES (detect/block)/NO (no detection/partial)	
Red team comments: Recommendations provided by the red team		Blue team comments: Other risks identified or improvement opportunities	
Step four – remediation			
Change validated for production	YES/NO	**Implementation date:** 21.07.2021 10:25	**By**: Name X
Red team recheck **(on real production if possible)**	**Check date**: 21.07.2021 10:25	**Blue team results** **Date of detection:** 22.07.2021 8:42	OK/NOK (Not OK)/partial Alert reference
If results are NOK/partial, restart at step two.			

Now that you have understood the concepts of how to plan, execute, identify, and remediate, the next chapter will focus on the usage of CTI as a main input for your purple teaming exercise preparation.

Summary

In this chapter, we saw that purple teaming is a process that can be applied in different kinds of assessments; nevertheless, we strongly believe that purple teaming is also a mindset that must be incorporated into an organization's culture. Purple teaming exercises help to build human cross-collaboration between red and blue teams. This is exactly what purple teaming enables within an organization – a common and shared objective: improving the organization's security. After all that, does this mean that red teaming exercises don't make sense anymore? Not at all – they do serve a purpose to test responsive capabilities in a realistic scenario where the blue team is not informed, and the red team performs actions with stealth in mind.

In the next chapter, we will introduce CTI and what it implies, as well as defining how it should be leveraged as an input for purple teaming.