

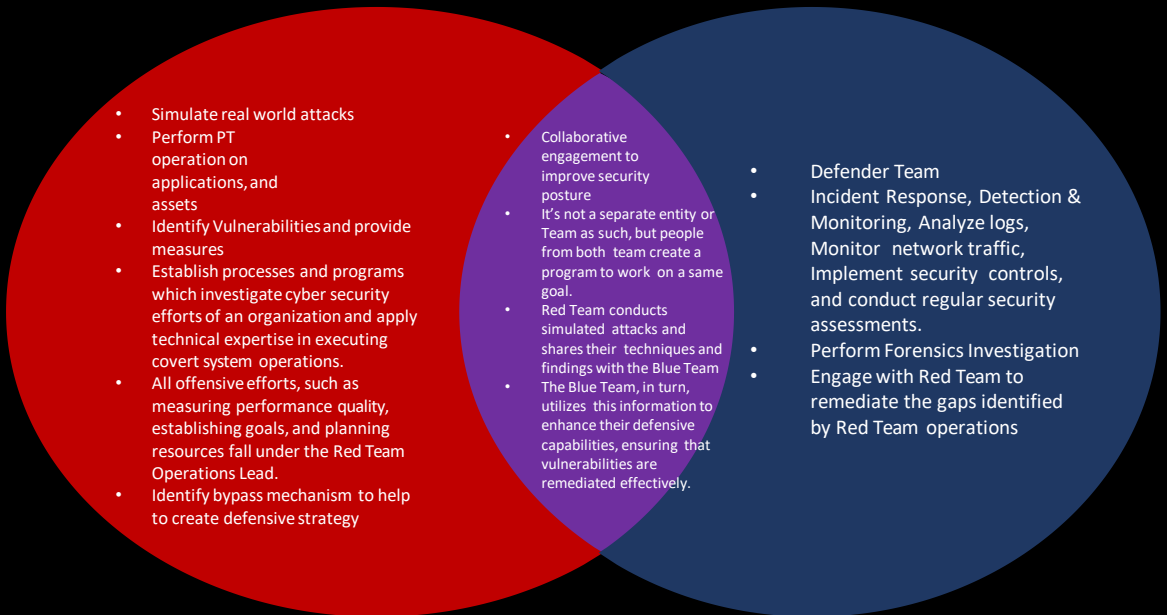


Purple Teaming Cheat-sheet

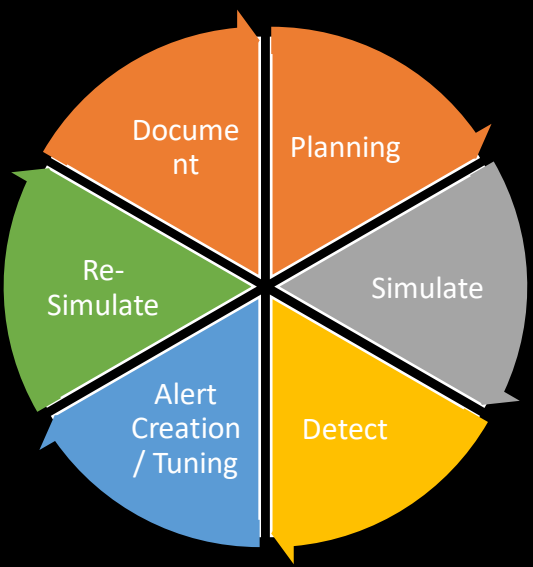
Purple Team: Purple Teaming is a collaborative approach that combines offensive (Red Team) and defensive (Blue Team) security practices to enhance an organization's overall security posture.



Short discussion about Red VS Purple VS Blue Teams :



Process of Purple Teaming:



Purple Team Activities

Threat Scenario Simulations	Attack Path Mapping	Vulnerability Assessment and Validation
Phishing Campaigns	Penetration Testing	Incident Response Drills
Red Team Feedback Loop	Security Tool Evaluation	Threat Intelligence Sharing

Purple Team Resources (Blue Team Resources) :

URL Check

URLHaus - <https://urlhaus.abuse.ch/browse/>

URLScan - <https://urlscan.io/>

InQuest Labs - <https://labs.inquest.net/iocdb>

Threat Fox - <https://threatfox.abuse.ch/browse/>

MalwareURL - <https://www.malwareurl.com/listing-urls.php>

RedirectDetective - <https://redirectdetective.com/>

RedirectTracker - <https://www.redirecttracker.com/>

Bulkblacklist - <https://www.bulkblacklist.com/>

Cyber Threat Intelligence

Vulldb - <https://vulldb.com/>

Alien Vault OTX - <https://otx.alienvault.com/browse/global/indicators>

IBM X-Force Exchange- <https://exchange.xforce.ibmcloud.com/>

Risk IQ Community - <https://community.riskiq.com/home>

Feedly - <https://feedly.com/>

Mandiant Threat Intelligence - <https://www.mandiant.com/advantage/threat-intelligence/free-version>

VmWare Carbon Black - <https://community.carbonblack.com/>

Malware Bazaar - <https://bazaar.abuse.ch/browse/>

Ransom Wiki - <https://ransom.wiki/>

PulseDive Ransomware Feed - <https://pulsedive.com/threat/Ransomware>

PulseDive Threat Feed - <https://pulsedive.com/explore/threats/>

Threat Simulations

Infection Monkey - <https://github.com/guardicore/monkey>

MITRA Caldera - <https://github.com/mitre/caldera>

APT Simulator - <https://github.com/NextronSystems/APTSimulator>

APT Simulator - <https://github.com/soprasteria/cybersecurity-APTSimulator>

MITRE ATT&CK® framework - <https://github.com/redcanaryco/atomic-red-team>

Car Analysis Repository of MITRE - <https://car.mitre.org/>

For Detection Purpose

Sigma Rules - <https://github.com/SigmaHQ/sigma>

SIEM Query - <https://www.linkedin.com/feed/update/urn:li:activity:7099679815934377984>

EDR Tools:

The Hives Project - <https://thehive-project.org/>

Zeek – <https://github.com/zeek/zeek>

Mozilla Mig – <https://github.com/mozilla/mig>

Osquery – <https://osquery.io/>

Cuckoo – <https://github.com/cuckoosandbox/cuckoo>

Google GRR – <https://github.com/google/grr>

Wazuh – <https://github.com/wazuh/wazuh>

Purple Team Resources (Red Team Resources) :

OSINT

OSINT Framework - <https://osintframework.com/>

OSINT Cheatsheet - <https://www.cheatsheet.wtf/osint/>

DNSdumpster - <https://dnsdumpster.com/>

cqcounter Whois - <http://www.cqcounter.biz/whois/>

Subdomain Finder - <https://subdomainfinder.c99.nl/>

DNStwister - <https://dnstwister.report/>

Blackbird - <https://blackbird-osint.herokuapp.com/>

Pentest References and CheatSheets

Hack Tricks - <https://book.hacktricks.xyz/>

Hacking Articles - <https://www.hackingarticles.in/>

Cloud Hack Tricks - <https://cloud.hacktricks.xyz/>

Pentest Book - <https://chryzsh.gitbooks.io/pentestbook/content/>

Payload Box - <https://github.com/payloadbox>

Steganography Tools - <https://0xrick.github.io/lists/stego/>

Metasploit Unleashed - <https://www.offensive-security.com/metasploit-unleashed>

Mobile Security Testing Guide - <https://mobile-security.gitbook.io/mobile-security-testing-guide/overview/0x03-overview>

Total OSCP Guide - <https://sushant747.gitbooks.io/total-oscp-guide/content/>

Hack The Box OSCP Preparation - <https://rana-khalil.gitbook.io/hack-the-box-oscp-preparation/>

Steflan Security - <https://steflan-security.com>

HighOnCoffee - <https://highon.coffee/blog/>

/home/six2dez/.pentest-book - <https://pentestbook.six2dez.com/>

0xffsec Handbook - <https://0xffsec.com/handbook/>

golinucloud - <https://www.golinucloud.com/kali-linux-bootable-usb/>

Pentest Monkey - <http://pentestmonkey.net/>

Web App Testing Guide - <https://owasp.org/www-project-web-security-testing-guide/stable/>

XSS CheatSheet -

https://cheatsheetseries.owasp.org/cheatsheets/XSS_Filter_Evasion_Cheat_Sheet.html

Exploit Development Resources & Articles

Exploit Development - Everything you need to know:

<https://null-byte.wonderhowto.com/how-to/exploit-development-everything-you-need-know-0167801/>

How to create a Metasploit Exploit in a few minutes:

<https://null-byte.wonderhowto.com/how-to/create-metasploit-exploit-few-minutes-0168445/>

Metasploit - Building a Module:

<https://www.offensive-security.com/metasploit-unleashed/building-module/>

The art of creating backdoors and exploits with metasploit:

<https://www.thesecurityblogger.com/the-art-of-creating-backdoors-and-exploits-with-metasploit/>

Cracking Hashes

Hashes.com - <https://hashes.com/en/decrypt/hash>

CrackStation - <https://crackstation.net/>