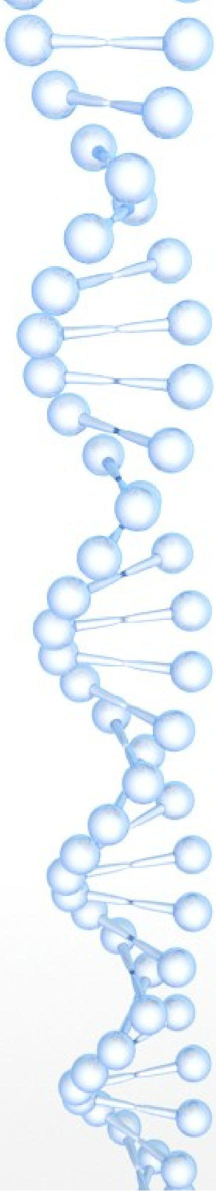
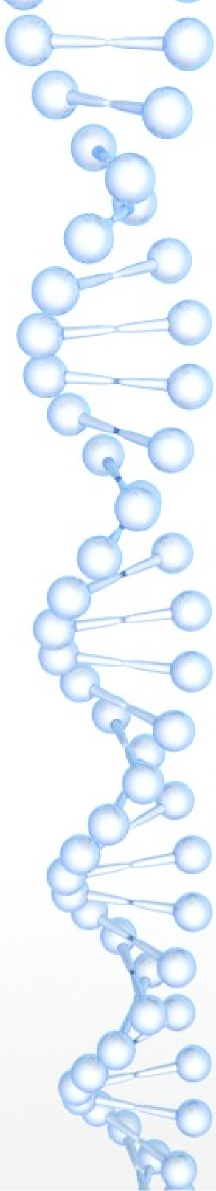
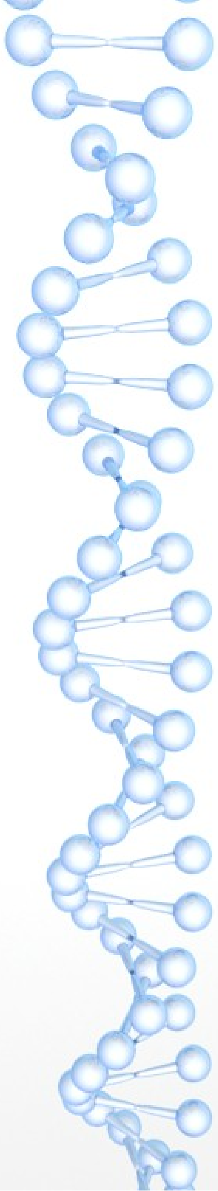


Purple Team assessment



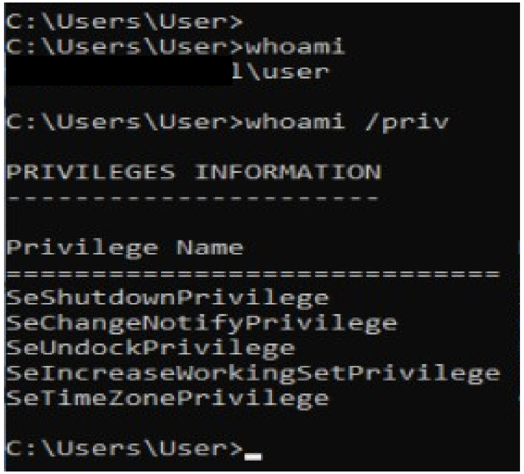
Agenda

- 3 whoami
- 4 BAD pyramid
- 5 Introducing the BAD pyramid
- 6 Definitions
- 7 Frameworks and regulations
- 8 Purple Team – methodologies and frameworks
- 9 Purple Team – assessment life cycle
- 10 The kill chain
- 11 Red Team assessment vs Purple Team assessment
- 12 Which assessment is appropriate



whoami

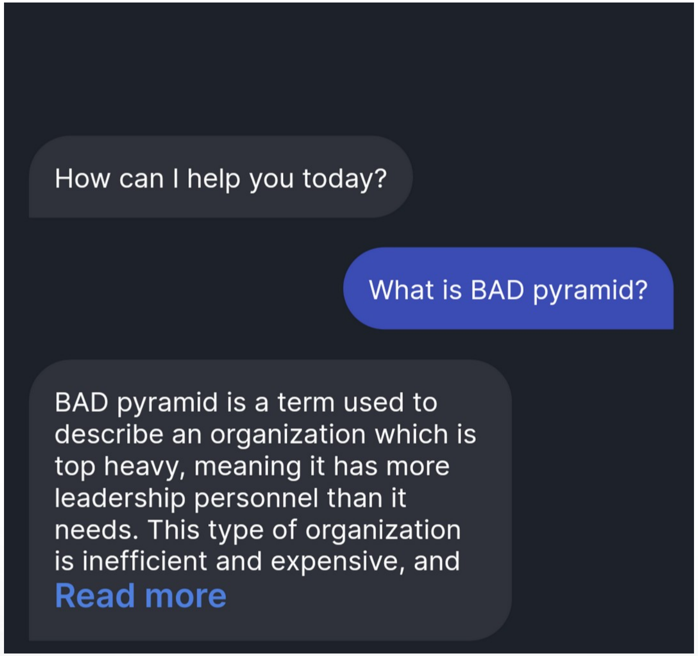
- How I recharge
  - Like running and hiking
- My professional expertise
  - More than 10 years professional experience most of which was gained in the UK
  - BSc Computer Network Security
  - MSc Information Security
  - ISC2 CCSP etc.



```
C:\Users\User>
C:\Users\User>whoami
[redacted]l\user

C:\Users\User>whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name
=============================
SeShutdownPrivilege
SeChangeNotifyPrivilege
SeUndockPrivilege
SeIncreaseWorkingSetPrivilege
SeTimeZonePrivilege

C:\Users\User>_
```

BAD pyramid

- CHAT GPT



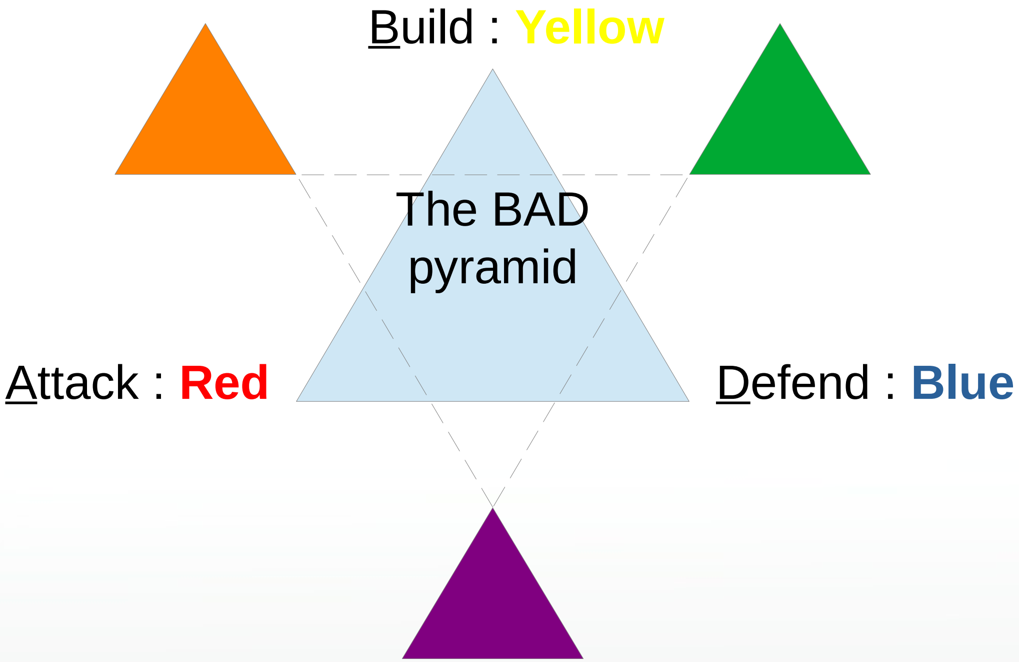
How can I help you today?

What is BAD pyramid?

BAD pyramid is a term used to describe an organization which is top heavy, meaning it has more leadership personnel than it needs. This type of organization is inefficient and expensive, and

Introducing the BAD pyramid

- Build Attack Defend (BAD)



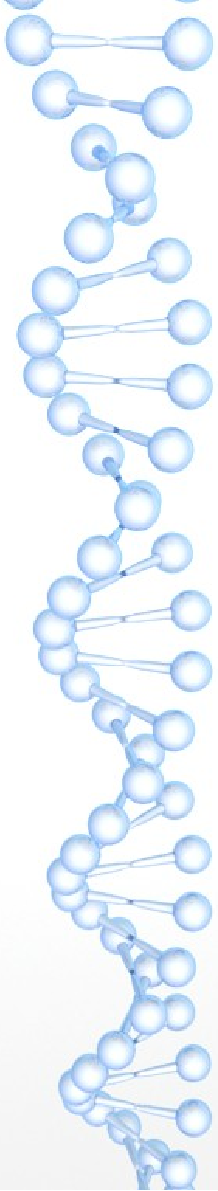
Build : Yellow

The BAD pyramid

Attack : Red

Defend : Blue

* PTP: https://www.pentestpartners.com/security-blog/bridging-the-gaps-between-red-and-blue-teaming/

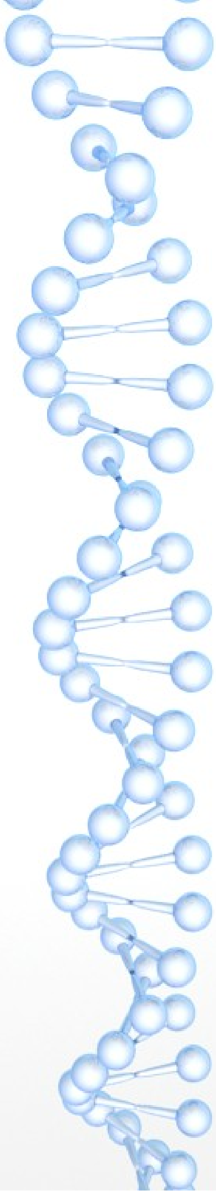


Definitions

Red Team and Blue Team

- The Red Team’s objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment.
- The blue team is responsible for defending an enterprise’s use of information systems by maintaining its security posture (i.e., the Red Team).
- Typically the Blue Team and its supporters must defend against real or simulated attacks
  - 1) over a significant period of time,
  - 2) in a representative operational context (e.g., as part of an operational exercise), and
  - 3) according to rules established and monitored with the help of a neutral group refereeing the simulation or exercise (i.e., the White Team).

* NIST: https://csrc.nist.gov/glossary/term/red_team_blue_team_approach



Regulations

- TIBER - Threat Intelligence-Based Ethical Red Teaming Framework (ECB in the European Union)
- CBEST - Intelligence-led penetration testing framework (BoE in the UK)
- FEER - Financial Entities Ethical Red Teaming (Saudi Arabian Monetary Authority in Saudi Arabia)
- AASE - Adversarial Attack Simulation Exercises (Association of Banks in Singapore in Singapore)
- ICAST - Intelligence-led Cyber Attack Simulation Testing (Hong Kong Monetary Authority in Hongkong)

* ECB - TIBER: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.htm

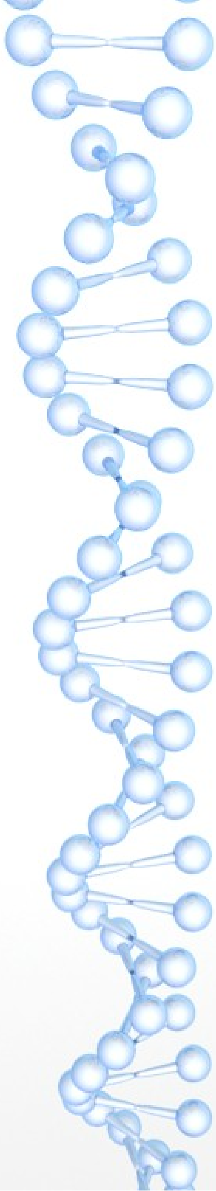
* BoE - CBEST: https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/

cbest-threat-intelligence-led-assessments-implementation-guide

* SAMA - FEER: https://www.sama.gov.sa/en-US/Laws/BankingRules/Financial%20Entities%20Ethical%20Red%20Teaming%20Framework.pdf

* ABS - AASE: https://abs.org.sg/docs/library/abs-red-team-adversarial-attack-simulation-exercises-guidelines-v1-06766a69f299c69658b7dff00006ed795.pdf

* HKMA – ICAST: https://www.crest-approved.org/membership/icast/



Purple Team – methodologies and frameworks

- Lockheed Martin’s – The kill chain
- Mitre’s - ATT&CK framework
- Mitre’s - Engenuity
- Scythe - Purple Team Exercise Framework (PTEF)
- Pan-Unit42’s - Playbooks
- etc.

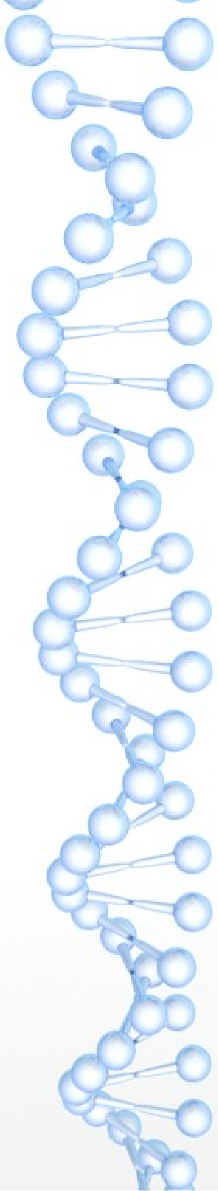
* Lockheed Martin: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

* MITRE: https://attack.mitre.org

* MITRE: https://attackevals.mitre-engenuity.org/methodology-overview

* Scythe: https://github.com/scythe-io/purple-team-exercise-framework

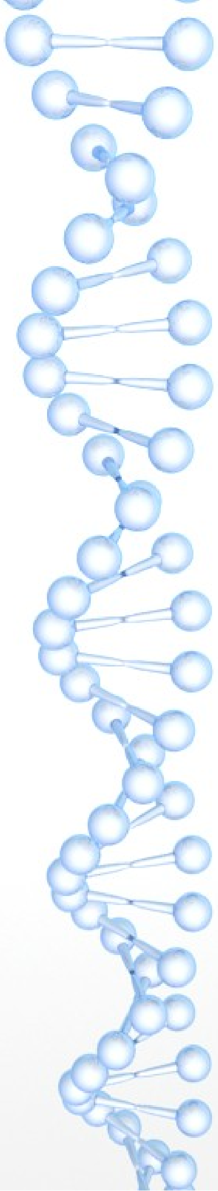
* Pan-Unit42: https://pan-unit42.github.io/playbook_viewer



Purple Team – assessment life cycle

- Cyber Threat Intelligence (done by the Organisation A and the Client)
  - An organisation (could be other organization not the one that will execute the purple team assessment) performs threat intelligence activities to identify threat actors and threats applicable to the Client
  - An organisation delivers a threat intelligence report to the Client that the Client can forward to the organization that will execute the assessment
- Preparation (done by the Organisation B and the Client)
  - Plan and agree the details of the cyber attack simulation with key Client stakeholders
  - Clarify the communication chain
- Exercise Execution (done by the Organisation B and the Client)
  - Execute the agreed cyber attack simulation
  - Keep key Client stakeholders informed about the process as agreed
- Lessons Learned (done by the Client)
  - Analyse the attack simulation outcome
  - Analyse the alerts raised by the detection tools
  - Improve tools, documentation and processes

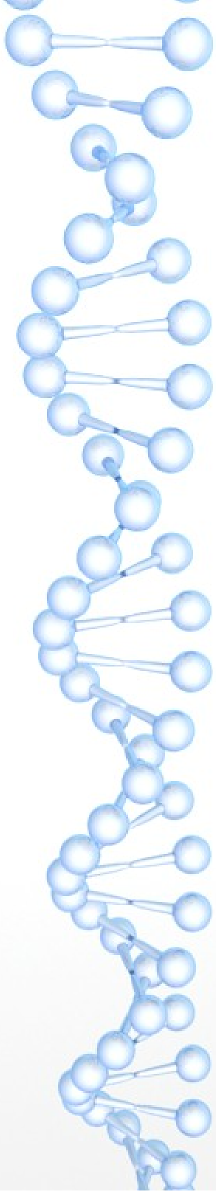
* SANS: https://www.sans.org/blog/cyber-kill-chain-mitre-attack-purple-team/



The kill chain

- Reconnaissance
- Weaponisation
- Delivery
- Exploitation
- Installation
- Command and Control (C2)
- Actions on objectives

* Lockheed Martin: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

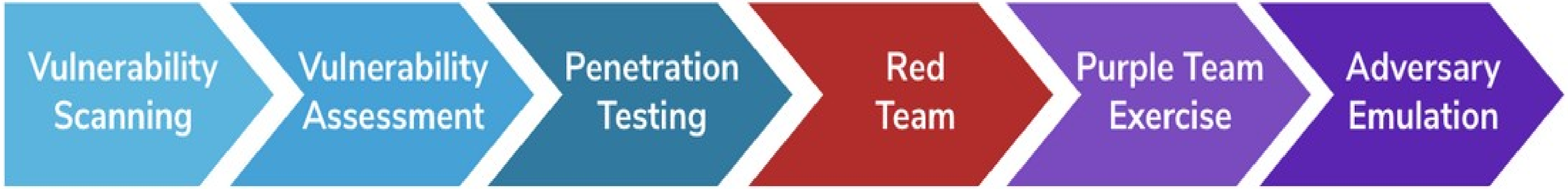


Red Team assessment vs Purple Team assessment

- One
  - Purple Team: The assessment is executed to simulate specific attack(s)
  - Red Team: The assessment is executed to try to reach objectives agreed with the Client (i.e., it is not limited to specific tactics, techniques and procedures)
- Two
  - Purple Team: The assessment could require the Client to engage a dedicated organisation that is to perform the threat intelligence (i.e., the Client needs to engage two organisations to have the assessment completed)
  - Red Team: The assessment could be executed by one organisation that will perform the threat intelligence and the attack simulation (i.e., the Client could engage one organisation to have the assessment completed)
- Three
  - The Purple Team: The key communications with the Client could help to improve the Client threat detection during the assessment execution
  - Red Team: The key communications with the Client could help to improve the Client threat detection after the assessment execution

In short, purple team assessments are special assessments performed by the red team and the blue team that help organisations improve their defence capabilities.

Which assessment is appropriate



Vulnerability Scanning

Vulnerability Assessment

Penetration Testing

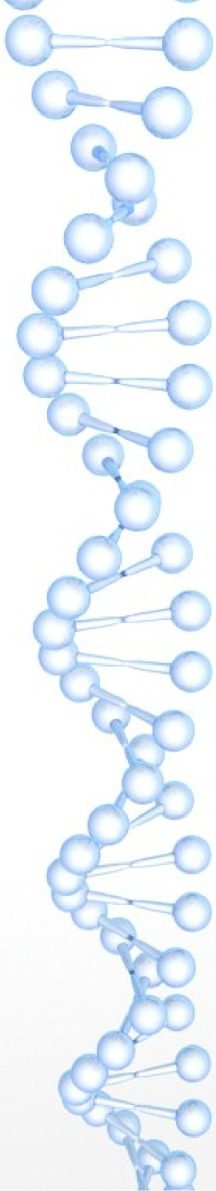
Red Team

Purple Team Exercise

Adversary Emulation

* NIST: https://csrc.nist.gov/glossary/term/red_team_blue_team_approach

* SCYTHE: https://scythe.io/library/scythes-ethical-hacking-maturity-model



Thank you

Your questions ...