# Purple Team

## WHITE PAPER

May 2023

VERSION: 1.0

TABLE OF CONTENTS

## Why implement purple teaming?

Martin Walsham from AMR CyberSecurity discusses the benefits of implementing a purple team assessment process and provides a high-level structured approach to implementation.

Before going any further, it's worth highlighting what we mean by red, blue and purple teams.

Red teams assess security by simulating attacks, blue teams focus on defence and incident response, while purple teams facilitate collaboration between the two to enhance security measures.

These teams collectively contribute to strengthening organisational cybersecurity defence and reduce vulnerability to potential threats.

Purple teaming is valuable because it brings:

**Enhanced Collaboration**: Purple teaming fosters collaboration and communication between the red and blue teams. It breaks down silos and encourages knowledge sharing, enabling both teams to work together towards a common goal. This collaborative approach improves the overall understanding of threats, vulnerabilities, and defensive strategies -- leading to more effective security practices.

**Realistic Testing**: Purple teaming provides a realistic testing environment by combining offensive red team tactics with blue team defensive capabilities. This approach allows organisations to assess their security controls and response capabilities in a controlled but authentic scenario. It provides a practical assessment of how well the organisation can detect and respond to simulated attacks, uncovering potential gaps and areas for improvement.

**Proactive Defence:** By engaging in purple team exercises, organisations can take a proactive approach to security. Rather than simply reacting to incidents, red and blue team collaboration enables them to proactively identify and address vulnerabilities. This proactive defence posture helps organisations stay one step ahead of potential attackers and reduce their overall risk exposure.

**Continuous Improvement:** Purple teaming promotes continuous improvement in an organisation's security practices. Through regular assessments, feedback and joint exercises, teams can iterate and refine their defensive strategies and tactics. This iterative process enables organisations to adapt to evolving threats, enhance their incident response capabilities and strengthen their overall security posture.

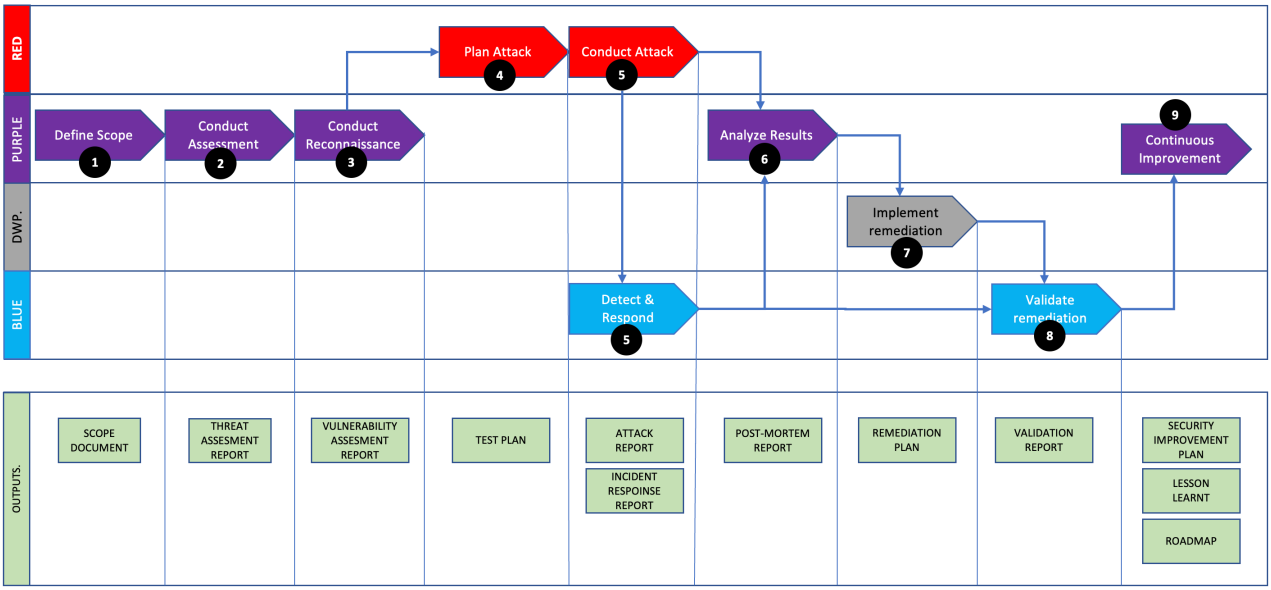
**Skill Development:** Purple teaming provides a valuable learning opportunity for both red and blue team members. The exchange of knowledge and experiences between the teams helps improve their skills and expertise. Red team members gain insights into defensive techniques and considerations, while blue team members acquire a deeper understanding of attack methodologies. This cross-training enhances the capabilities of individual team members and strengthens the organisation's overall cybersecurity skillset.

These advantages make purple teaming a valuable practice for enhancing an organisation's security posture and resilience against cyber threats.

## Identifying the best framework for purple team assessments

It is important to have an overview of the key steps of an effective purple team assessment. These steps must align with industry best practice red, blue and purple team assessment frameworks such as CREST STAR, CBEST, TBEST, TIBER-EU and GBEST.

The diagram below shows the main steps in the purple teaming process. Each step is clearly signposted, along with the outputs created.




## The Steps Explained

### 1. Define the Scope

The first step is to define the scope of the exercise, including assets to be protected, potential threats, and the goals.

This should be documented in a scope document or Statement of Work (SOW).

The scope should include the:

- Critical assets in scope of testing
- Legal and regulatory requirements for the test and any limitations
- An operational risk assessment for the test, to allow it to be carried out in a realistic manner while managing any risks that could cause unacceptable disruptions to the organisation.

### 2. Conduct Threat Assessment

It is essential to conduct a threat assessment to identify the threat actors targeting the critical assets in scope, the organisation and the sector, and to identify the tactics, techniques and procedures (TTPs) that these threat actors use to identify potential vulnerabilities and weaknesses.

These include reviewing publicly available information, conducting network scans, and performing social engineering attacks.

The results of the threat assessment should be documented in a threat assessment report.

### 3. Conduct Reconnaissance

Conducting reconnaissance will help identify potential vulnerabilities and weaknesses.

This includes reviewing publicly available information, conducting network scans, and performing social engineering attacks.

The results of the reconnaissance should be documented in a report or vulnerability assessment.

### 4. Plan the Attack

Based on the results of the reconnaissance and the threat assessment, the Red Team will plan the attack.

This includes techniques and tools they will use to exploit the identified vulnerabilities.

The plan should be documented in a test plan.

**5. Conduct the Attack**

The Red Team conducts the attack, attempting to breach the organisation's defences.

The Blue Team's role is to detect and respond to the attack, following their incident response plan.

The results of the attack should be documented in an attack report.

Any response from the blue team will be documented in the incident report.

**6. Analyse the Results**

The Purple Team analyses the results of the attack, including the techniques used by the Red Team and the effectiveness of the Blue Team's response.

They should identify areas for improvement and develop recommendations for enhancing the organisation's security posture.

The results of the analysis should be documented in a post-mortem report.

**7. Implement Remediation**

Based on the recommendations of the Purple Team, the organisation should implement remediation measures to address the identified vulnerabilities and weaknesses. These measures should be documented in a remediation plan.

**8. Validate the Remediation**

The Blue Team validates the effectiveness of the remediation measures. They should conduct tests to ensure the vulnerabilities identified have been addressed and that the organisation's defences are effective.

The results of the validation should be documented in a validation report.

**9. Continuous Improvement**

It is important that the Purple Team continuously monitors and evaluates the organisation's security posture to identify areas for improvement.

A roadmap for implementing new security measures and enhancing existing ones needs to be developed.

This roadmap should be documented in a security improvement plan.

Overall, an industry best standard Red and Blue Team with advanced Purple Team capability should function through a well-defined operating model or process map that enables effective collaboration and communication between the teams, continuous improvement, and enhanced security posture.

The documentation accompanying each area should include scope documents, SOWs, vulnerability assessments, test plans, attack reports, post-mortem reports, remediation plans, validation reports and security improvement plans.

## Benefits of Implementing a Purple Team Assessment Process

The key to an effective high quality purple team capability -- and to demonstrate its value -- is that it is intelligence-led.

This is recognised by recognised, structured red and purple team assessment frameworks such as the CREST STAR Scheme, the Bank of England CBEST Scheme and the European Central Bank TIBER EU Scheme.

**The main benefits of an effective purple team are:**

- A clear view of the threats that similar organisations face, along with the tools, techniques and processes that threats actors use.
- The ability to test your organisation to understand its ability to defend against attacks and identify weakness.
- Greater communication and collaboration between red and blue teams – resulting in better processes and capabilities.
- The ability for your organisation to better test its capabilities to detect, identify areas of weakness, and respond to cyber-attacks.
- The ability to test effectively while complying with legal and regulatory requirements and ensuring risks to operational functionality are managed during the testing period.
- The ability to report a clear view of the cyber resilience of the organisation at a board level.
- The ability to make informed decisions on risk acceptance and security spending priorities and amount.

This can be summarised in terms of gaining greater risk transparency and the ability to effectively detect, defend against and respond to cyber-attacks.

**Metrics**

To demonstrate value of the purple team it is essential to have measurable and meaningful metrics and appropriate reporting, tailored appropriately to relevant audiences (e.g. security teams, senior management).

Examples of metrics include:

- The key threats and threat levels.
- The percentage of critical assets tested during a. given period.
- The percentage of critical threat actor scenarios tested during a given period.
- The percentage of attack scenarios defended against.
- The percentage of attack scenarios detected.
- The percentage of attack scenarios successful.
- The number and severity of vulnerabilities identified.
- The number and severity of vulnerabilities remediated in a given period.
- The maturity of the purple team capability (split between threat intelligence; red team and blue team capabilities).

**Improving your security posture and enabling further innovative security practices**

The purple team will improve the security posture of your organisation.

It is threat led, so your organisation will gain greater understanding of its threats, and its ability to detect, defend and respond to them.

The nature of the output of the purple team activity will demonstrate organisational risks that should be consumed, tracked and managed at the senior level within the organisation.

This visibility will help improve security by helping senior leadership make informed decisions to fund security improvement activities.

The development of purple team capability also improves an organisation’s ability to detect and respond to cyber-attacks through the development of blue team capabilities and processes, and the testing and continual improvement of these through purple team exercising.

Red team testing helps identify areas of vulnerability requiring priority improvement and additional controls.

The continual improvement and tracking of this will ensure the overall continual improvement of your organisation’s security posture in a prioritised manner.

The implementation and tracking of controls can be built into existing compliance frameworks such as Gov Assure, 27001, internal HMG accreditation frameworks, NIST Frameworks and the NCSC CAF framework.

The purple team approach allows for innovation in security controls as the threats are being tested against the ability to detect, defend and respond.

This means controls can be tailored specifically to address these rather than just applying a baseline set of controls hoping these will address the threat.

By blending and continuously improving defensive, detection, and response measures, this approach enables the creation of hybrid controls that effectively counter threats.

## Implementation Considerations

As part of an implementation strategy, an organisation should consider the maturity of its current security testing regimes and red and blue testing capabilities.

There are benefits in having an established blue team capability and standard penetration testing function established ahead of carrying out a purple team assessment.

This ensures you have an appropriate baseline level of security in place, prior to engaging in more advanced assessment techniques.

However, running an early purple team assessment could enable you to identify and escalate deficiencies across your organisation.

To assess the maturity of your organisation, CREST has several free maturity assessment tools that can be used to assess your maturity levels across areas such as testing, threat intelligence and incident response.

To support your purple team assessment, there are a number of options regarding the use of specialist third parties to support parts of the capability or to lead the overall service.

When using a third party, an organisation must consider the accreditation of the third party to ensure they have the required skills and competencies, and to gain assurances that it has the appropriate insurance, internal security, vetting and robust methodologies.

The CREST STAR Scheme provides an example of a recognised industry best practice accreditation scheme for red and purple team engagements.

Using an accredited third party to carry out the red team element of a purple team engagement ensures you have an objective, independent robust assessment of your threats and ability to defend and detect.

Using an accredited third party to lead the purple team assessment ensures you have better overall outcomes and ensure blue teams are properly engaged and end-to-end processes are assessed and continually improved.

## Further Support

If you need assistance in designing and implementing a purple team capability or carrying out a purple team assessment then the specialists at AMR CyberSecurity can support you. Specific areas where we can assist include:

- Maturity Assessments
- Threat Assessments
- Red, Blue and Purple Team Assessments

Please contact enquiries@amrcybersecurity to speak to one of our consultants.