PROELIANS

PROACTIVE CYBER SECURITY

Purple Team Assessment

Purple Team assessments are designed to test your internal infrastructure resilience against controlled and realistic cyber attacks.

During Purple Team assessments **Proelians** will perform common Tactics, techniques, and procedures (TTPs) in order to assess detection and response capabilities of your Blue Team.

Why would you benefit from a Purple Team assessment?

The main benefits of conducting a purple team assessment are:

- Test your Blue Team to detect common TTPs in a controlled and methodical way.
- Tune and refine your alerting mechanisms to minimise false positives.
- Understand whether the current level of security controls are sufficient to contain the attacks carried out by an internal malicious actor.

Our Methodology

Scoping

Proelians will define with you the rules and the boundaries of the Purple Team assessment, also ensuring all your requirements are carefully considered.

Execution

Proelians will execute agreed TTPs and provide feedback.This will give the opportunity to your Blue Team to tune and refine your detection controls. Examples of common TTPs are listed below:

- Process Injection (T1093)
- Steal or Forge Kerberos Tickets: Kerberoasting (T1558.003)
- Use Alternate Authentication Material: Pass the Hash (T1550.002)

Each activity is mapped to the Mitre ATT&CK framework. The Mitre ATT&CK framework is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

Delivery

When the Purple Team Assessment is complete, Proelians will provide a report containing the following sections:

- Executive summary for directors, senior-level management or stakeholders
- Technical recommendations for fixing discovered vulnerabilities
- Strategic recommendations for long-term improvement
- Indicator of compromises mapped to the ATT&CK framework for Blue Team investigation

In addition to the above, Proelians will provide the Blue Team access to the Red Team's Security Information and Event Management (SIEM) console. Unlike the report, this SIEM console would give much more visibility to the Blue Team when auditing logs of all activities performed during the red team assessment.

Proelians can also assist Blue Team with the following tasks:

- Review of the audit logs and alerts to check if there are any trace of the activity performed by Proelians Purple Team
- Assist your SOC or Blue Team to configure alerts in order to detect these attacks
- Test the newly configured alerts by re-running the attack scenarios of the Purple Team assessment

Why Proelians ?

We are not just another independent security firm. With more than 10 years of experience in Cyber security our commitment is to provide top-quality services that meet your expectations. If you are willing to try us, feel free to contact us and we will get back to you as soon as possible.

Flexible - Trusted - Secure - Unconventional