



## T.E.R.R.A Framework

T.E.R.R.A is a comprehensive approach to securing systems and data from the constantly evolving threat of cyber attacks.

By testing for vulnerabilities, evaluating current security measures, reviewing results, and responding to potential threats, **Proelians** will help your organization stay ahead of adversaries and ensure the smooth operation of their business. With T.E.R.R.A, you can trust that your organization is well-equipped to face the challenges of the digital age.

## T.E.R.R.A Phases

The phases of the TERRA framework have been carefully crafted to provide the most comprehensive protection against cyber threats. These are highlighted below:

- **Test:** The test phase involves actively searching for vulnerabilities in your systems and data, using techniques such as penetration testing and vulnerability assessments. These tests may be performed internally or externally, and are designed to identify areas that need improvement in order to better protect against cyber threats.
- **Educate:** The educate phase involves performing social engineering tests such as phishing simulations and providing social engineering training to employees. This will help your organization to better understand and defend against common tactics used by adversaries, such as phishing and vishing attacks.
- **Review:** After the test and educate phases have been completed, the review phase involves taking a close look at the findings and determining what changes need to be made to improve security. This may include updating policies and procedures, implementing new security technologies, or providing additional training to employees.
- **Respond:** The respond phase involves providing a "purple team" service, in which we test your incident response capabilities and identify areas for improvement. This may include simulating common attacks and tactics, techniques, and procedures (TTPs) used by adversaries and working with the security operations center (SOC) and security team to educate them on how to effectively defend against these threats. By proactively testing and improving their incident response capabilities, you can be better protected against the ever-evolving threat of cyber threats.
- **Adversary:** The adversary phase involves staying up to date on the latest cyber threats and tactics used by adversaries. This includes conducting real-world simulations of attacks, in which you can test your incident response capabilities and identify areas for improvement. By proactively defending against potential attacks, organizations can better protect themselves against the ever-evolving threat of cyber threats.

## Why would you benefit from following T.E.R.R.A?

The main benefits of following our framework are:

- Identify whether your most critical asset is vulnerable to cyber attacks.
- Test your Blue Team to detect common TTPs in a controlled and methodical way.
- Uncover unconventional vulnerabilities that would not be typically identified with traditional testing only.
- Understand whether the current level of security controls are sufficient to contain the attacks carried out by an internal malicious actor.
- Test your members of staff against phishing attacks.
- Provide an evidence-based risk report to directors, senior-level management or stakeholders.

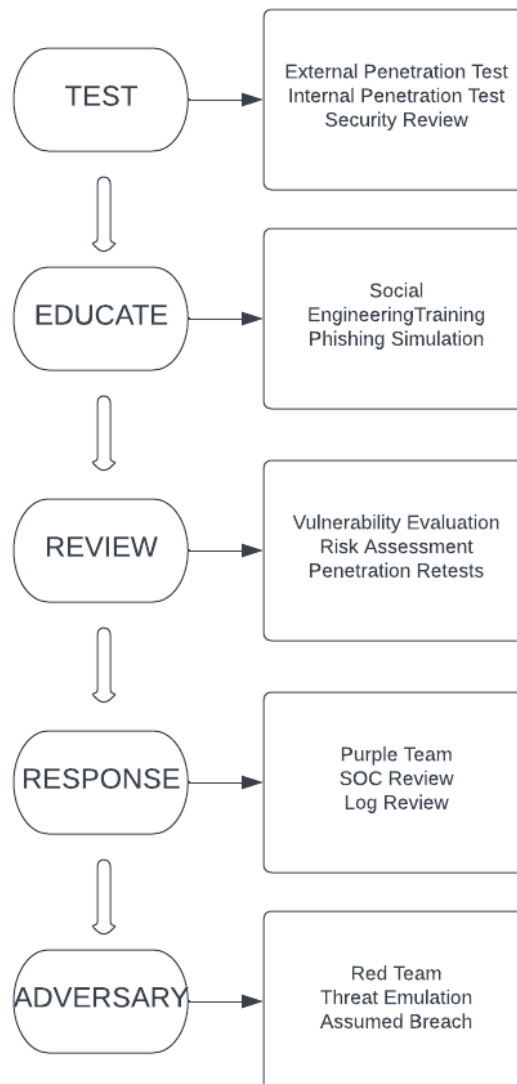
## Our Methodology

### Scoping

Proelians will define with you the scope for each phase of the T.E.R.R.A framework, also ensuring all your requirements are carefully considered.

## Execution

Proelians will execute each phase of the assessment based on the agreed scope. An example of a sample execution of the framework is shown below:



## Delivery

For each phase of the assessment, 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

The scope and deliverables for each phase of the TERRA framework may vary. For more information on the execution and delivery of these phases, please refer to our other services page.

## 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