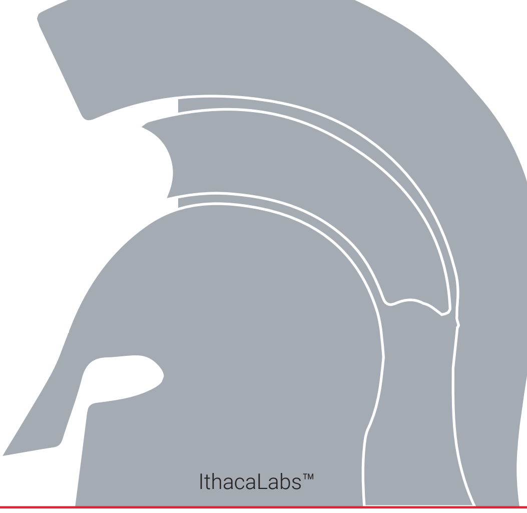
ODYSSEY™
cybersecurity



Odyssey IthacaLabs™ Red Team Services

Uncover your technological and procedural weaknesses before they are spotted by real threat actors.

Service Overview

A Red Teaming engagement simulates realistic cyberattack campaigns targeting your organization in an effort to assess its readiness, resilience and response capabilities, on a technological and premises accessibility level, under real-world attack scenarios (i.e. data theft, espionage, extortion, sabotage).

During this engagement, our specialists act as threat actors attempting to circumvent your digital and/or physical security defenses with the aim of causing harm and/or gaining access to your organization's information assets as well as premises.

In doing so, our specialists orchestrate and execute multi-layered pre-agreed attack scenarios against your organization's digital and physical resources, in a controlled and transparent manner.

The outcome of this engagement aims to improve your organization's readiness, resilience and response capabilities against risks posed by people, processes and technology.

All weaknesses identified during this engagement are presented in a detailed report accompanied by specific recommendations to help you with your overall security objectives based on your organizational risk appetite, this way significantly improving your defenses and processes.

Acquire Odyssey's Red Teaming engagement to help improve the effectiveness of your resilience, readiness and response capabilities against the constantly evolving cyber-threat landscape.

How Red Teaming works

Red Teaming services expose security weaknesses in areas related to people, processes and technology that can be further improved to minimize the impact of a potential security breach, either technological or physical.

These engagements, conducted from the perspective of cybercriminals, challenge your technological and procedural defenses, as they consist of a number of tailor-made exercises which complement each other to match your organization's risk objectives.

During a Red Teaming engagement, the following services are conducted:

- Wireless & Wired Network Penetration Testing
- Vulnerability Assessment,
- Host Penetration Testing,
- Web Application Penetration Testing,
- Passive & Active Information Gathering,
- Social Engineering, and
- On-Premises Access Control Risk Assessment.

Key Benefits

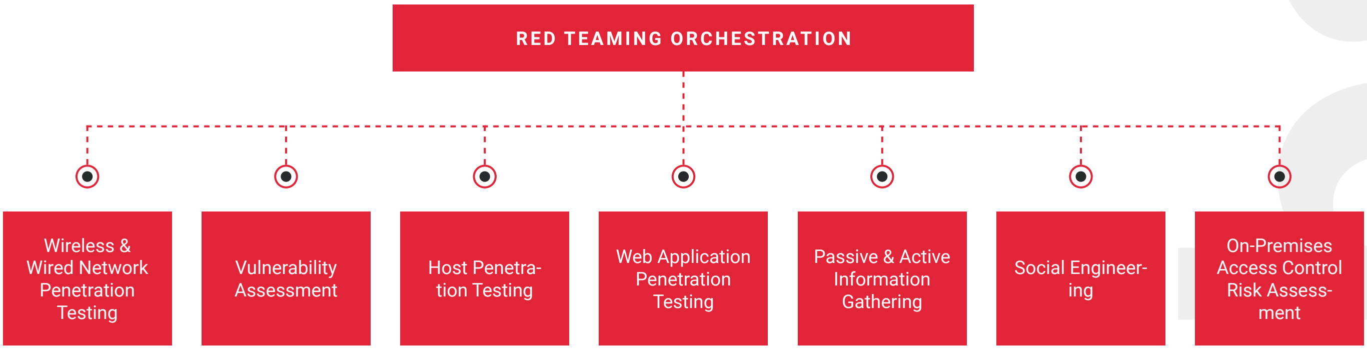
- Identify your organization's security and procedural weaknesses before others do
- Assess the effectives of your digital and physical security controls and processes

Key Features

- TIBER-EU & SAMA compliant process/methodology
- Top-of-the-range Red Teaming best practices
- Complete confidentiality through task compartmentalization
- Close communication and transparency before, during and after the Red Teaming engagement
- Tailor-made pre-agreed attack scenarios relevant to your industry specifically

Why chose us

1. Expertise, experience and intelligence
2. Happy clientele that keep returning
3. Proven and effective methodology
4. Attention to detail



RED TEAMING ORCHESTRATION

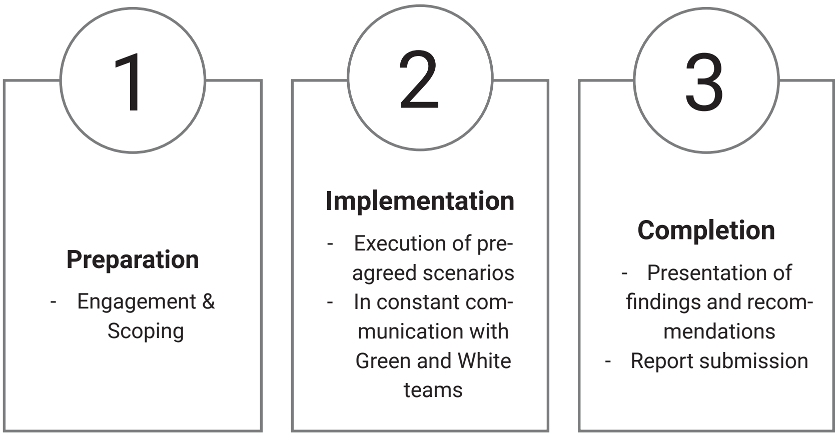
- Wireless & Wired Network Penetration Testing
- Vulnerability Assessment
- Host Penetration Testing
- Web Application Penetration Testing
- Passive & Active Information Gathering
- Social Engineering
- On-Premises Access Control Risk Assessment

Depending on the scenario to be executed, we orchestrate a multi-blended combination of exercises that aim to ethically breach your organization's security defenses in an effort to identify its level of readiness, resilience and response capability.

Identify your weak spots before motivated Threat Actors find them first.

Red Teaming Methodology

Our Red Teaming methodology is in line with TIBER-EU and the Saudi Arabian Monetary Authority (SAMA) Financial Entities Ethical Red Teaming processes, as shown below.



1

Preparation

- Engagement & Scoping

2

Implementation

- Execution of pre-agreed scenarios
- In constant communication with Green and White teams

3

Completion

- Presentation of findings and recommendations
- Report submission

This means, that during this exercise, we provide full transparency to your relevant regulatory authority (Green Team), if required, as well as those in your organization who must be aware of this engagement (White Team). Throughout this process, the Red, Green and White teams are involved in a constructive and mutually beneficial back-and-forth regarding the progress of the pre-agreed scenarios as they unfold.

Proven methodology that provides full transparency to involved stakeholders.

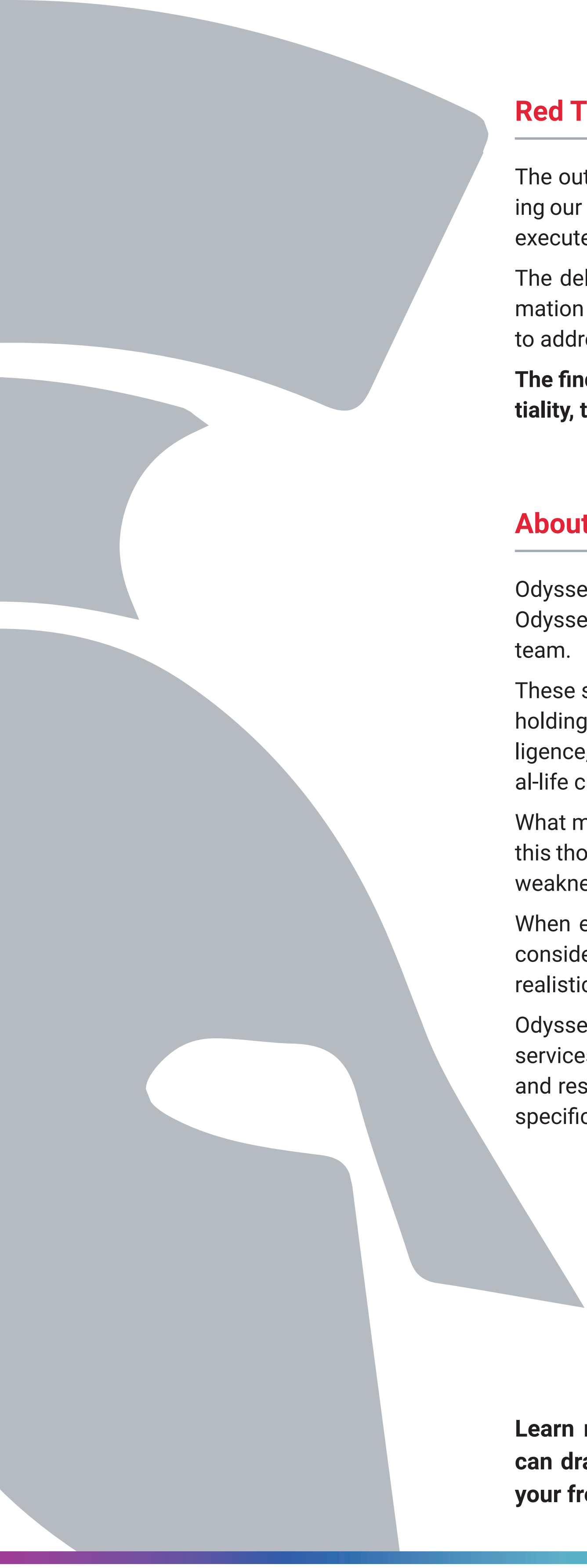
Real-life Examples of Red Teaming Orchestrated by IthacaLabs™

Managed to remotely gain access to the internal network of a large organization, and escalated access privileges from within. From this point onward, a real threat actor could have had access to the entire organizational network, and then engage in espionage, sabotage, undermining of business operations, the obstruction of operations and the leaking of sensitive information, resulting in irreparable costs in punitive measures, loss of business and reputation damages.

Gained access to an organization's email servers by employing Social Engineering methods. Used the intercepted information to execute more sophisticated cyberattacks by incorporating latest tactics, techniques and procedures (TTPs). Under real-life circumstances, cybercriminals could have used this advantage to conduct major financial fraud, information leaks and data theft that could have damaged the organization's viability.

Compromised user workstations remotely as well as by using onsite Social Engineering to perform lateral movement to retrieve "flags". If this were a real cyberattack, it could have resulted in the interception and theft of valuable data, such as patents and proprietary software, causing immense losses to the organization's critical digital assets.

And many more...



Red Teaming Deliverables

The outcome of this engagement is presented to relevant stakeholders, providing our findings and recommendations related to the simulated attack scenarios executed.

The deliverables also include a comprehensive report providing detailed information regarding our findings, recommendations, tools and guidelines needed to address these weaknesses.

The findings identified during this exercise are treated with absolute confidentiality, transparency and privacy considerations.

About IthacaLabs™

Odyssey's Red Teaming services involve world-class security specialists from Odyssey's IthacaLabs™ Risk Assessment & Mitigation professional services team.

These seasoned and experienced professionals with many years of experience, holding several globally recognized certifications, employ the knowledge, intelligence, tools and techniques to assess your defenses and processes under real-life circumstances.

What makes IthacaLabs™ Red Teaming stand out is our attention to detail. With this thorough approach, our Red Teaming professionals will be able to recognize weakness that would otherwise go unnoticed.

When engaged in Red Teaming services, our people acknowledge the special considerations and uniqueness of your organization and industry for designing realistic attack scenarios.

Odyssey's Red Teaming by IthacaLabs™ combines a range of Risk Assessment services that converge into one main goal: to assess your readiness, resilience and response capabilities using pre-agreed real-life controlled attack scenarios specific to your industry.

Learn more about how Odyssey's Red Teaming services by IthacaLabs™ can drastically improve your security posture. Contact us now to reserve your free and confidential consultation.

HEADQUARTERS

CYPRUS
1 Lefkos Anastasiades Str.
2012 Strovolos, Nicosia

T +357 22463600
F +357 22463563
E info@odysseycs.com

www.odysseycs.com

ODYSSEY™
cybersecurity

OFFICES CYPRUS | GREECE | USA | UK | KSA