Cyber Intelligence Led Penetration Testing (ILPT): Service Description

The service ILPT bases on various processes and activities. It consists of three main steps, which can be offered as a package or individually. Those service components are described in the following sections.

SAMA PARTNERS ILPT and its components follow the CBEST and CREST frameworks, known in the financial industry, and are carefully adapted to a wider range of profit and non-profit organizations.

SAMA PARTNERS
THE SECURITY INTELLIGENCE COMPANY

1 Service Components

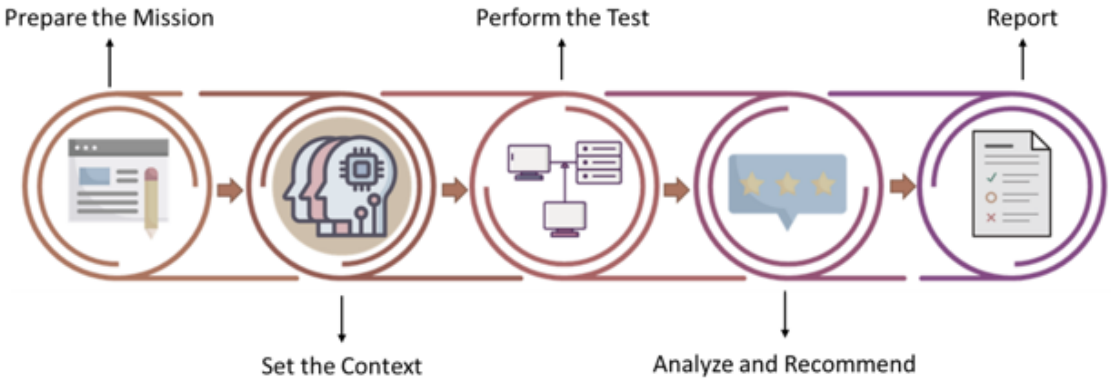

Figure 1: ILPT Methodology

1.1 Prepare the Mission

A penetration testing mission is a project that needs good preparation, in both the technical and organizational aspects.
Understanding the requirements and the end objective of what to be achieved from our customers is essential to align the activities and deliverables with the goals.
Defining the scope, nature (black, white box, or grey box), roles, time windows, milestones and risks are essential part of the mission. A good preparation is not only helpful but also necessary to avoid any unwanted interruption of the services tested.

1.1 Set the Context

The foundation for ILPT is a deep knowledge about contemporary threats and threat actors that your organization is faced to. While proceeding this basic step we will figure out most likely attack scenarios including corresponding actors and their capabilities. Aiming to provide an efficient and effective ILPT we will evaluate your business systems from an external attacker's point of view, too. This allows us to understand the motivation of possible attacks. To be able to bring both parts, i. e. the motivation of possible attackers as well as attack scenarios, together, checking your digital footprint is an additional part of our service. An investigation of your network, infrastructure and processes based on your public presence in social and print media as well as checking your organizations announcements will be used as source of information.
This external point of view comes along with an internal review of your current compliance requirements as well as understanding how you manage risk.

1.3 Perform Penetration test

During this stage we will use our skills, experience and resources within the context of your organization, to perform realistic attack scenarios. However, don't worry: Our ILPT is strictly conform with current law and we will agree with you on a pre-set level of access into your organization and corresponding systems. We won't do anything without your permission. Customers trust is one key of our long-term success.
Possible elements of ILPT are evaluating the network architecture, checking the technical implementation of security controls, assessing your capability to detect and respond to attacks and figure out the activities and behaviour of people and processes responsible for security.

While proceeding with ILPT we will create a report, that allows you to remediate the detected vulnerabilities, weaknesses and other issues, directly.

1.4 Analyse and Recommend

One of our key strength is that we are transparent throughout the whole process. Therefore, we will deliver you all reports and documents at the time of creation. That means: While starting the Analysis and Improvement step the Threat Intelligence Report–which covers mainly the context of your organization and realistic attacking scenarios–and the results of the ILPT are in your hands, already.
After finishing the step of "Analysis and Improvement" we will present you the conducted process and the gained results of the whole ILPT. Furthermore, we will come up with a Security Improvement Plan that includes recommended remedial security enhancements. Of course, if you need further support while realizing those improvements our consultancy services will be with you.

1.5 Report

Depending on the target audience of the penetration test, several reports may be produced and provided. In the reports, we document all findings found during the assessment period as well as the review of the performance and overall capacity of the organization.

2 Typical Deliverables

2.1 Penetration Testing Report

A report will document the observations we made, while determining the context of your organization. This includes on one hand the external (e. g. your organizations announcements and digital footprint) and internal perspective (e. g. compliance requirements and risk management) on the other the evaluation and motivation of possible attackers. All that information serve to derive realistic scenarios, which are needed for step 2 "Perform Penetration test" by supporting the definition of suitable and realistic attacking vectors, including utilisation of tools and tactics applied by real-life attackers.

2.2 Remediation Action

After finishing the penetration test we will hand over a corresponding report. It includes a comment on each component that has been tested within the context of your organization. Furthermore, it describes the progress made by the penetration testers in terms of their journey through various stages of each threat scenario. This report supports you to close possible security gaps.

2.3 Improvement plan

We will create a Security Improvement Plan, that answers how you can increase your security and how you can mitigate the risks those were revealed during ILPT. Answering both questions supports determining whether your existing security resources are allocated appropriately and where further investments are most valuable.

About SAMA PARTNERS

- Corporate Headquarter: Mannheim, Germany
- Offices: Munich, Germany / Tunis, Tunisia
- Year Established: 2010
- Employees : 70
- Certified according to ISO/IEC 27001: (TÜV-SÜD)
- High qualifications and many years of practical experience in various industries sectors
- Operates its own Cyber Security Academy offering several security courses and certifications
- Operates its own „SOC-as-a-Service“: SOCurity®
- Official Information Security Lecturer at Hochschule Mannheim (University of Applied Sciences), Faculty Digital Business Technology
- Selected best midsized company of the year 2018 in Germany (“UnternehmerStar” 2018 Prize)
- Member of the European Cyber Security Organisation (ECSO)
- Official regional representative of Teletrust in Baden-Württemberg
- Labeled IT Security made in Germany and IT Security made in Europe
- Member of the cluster Electric Mobility South-West Germany, emobil-BW
- Initiator and organizer of the yearly Cybersecurity Conference, Mannheim (Germany) since 2015

To learn more about SAMA PARTNERS' Cyber Intelligence Led Penetration Testing (ILPT), talk to our experts: info@samapartners.com

Headquarter

SAMA PARTNERS Business Solutions GmbH
Hermsheimer Straße 3
68163 Mannheim
Deutschland
Phone: +49 621 10759977
E-mail: info@samapartners.com

Tunisian Office

SAMA PARTNERS Business Solutions SARL
Immeuble Le Coral, B11-3
Centre Urbain Nord
1082 Tunis – TUNISIA
Phone : +216 71 947 457
E-mail: info@samapartners.com