CYBER ATTACK SIMULATION AND MODELING WHITEPAPER

CIPHER SECURITY

www.cipher-security.com

1

WHAT IS A CYBER ATTACK SIMULATION AND MODELING SERVICE?

The Cyber Attack Simulation and Modeling (CASM) service is a security breach readiness assessment that demonstrates the cyber threats an organization is facing by an external attacker, as a part of the organizational risk management process.

During this test, a security expert will try to infiltrate in the internal organization infrastructure from the publicly-accessed Internet - while being remote, unauthenticated, unauthorized (IT-wise) and remaining undetected. The security expert has no prior knowledge or setup related to the target organization, acting from what is known as Black Box approach.

The test is performed from "outside" the organization - in a similar manner an actual attacker would perform the attack. Having limited knowledge of the network infrastructure, the security expert will gather information from accessible resources, attempting to safely gain access to the IT infrastructure.
This test offers true insights about the external exposure of the organization's confidential information and internal data via IT infrastructure, exposed systems and data files while demonstrating that a security breach could eventually be realized by a malicious source.

Leveraging the Cyber Attack Simulation and Modeling promotes and boosts your co-operation with your clients one step ahead your competitors. This unique service offers the most cost-effective win-win situation and it constitutes a decisive channel for growing your business.

THE STAGES OF A CYBER ATTACK SIMULATION AND MODELING TEST

The security expert performs the assessment in three different stages.

First, the security expert discovers the target by gathering information from the publicly-facing organization interfaces. This stage consist mainly in the setting the goals, the reconnaissance and the discovery steps. After setting the objectives of the assessment, the security expert starts the search in the attempt of finding out as much as possible about the company and the System Under Test, in the quest for potential weaknesses.

Although we have performed hundreds of tests in all business areas, we have a perfect track-record of providing safe, secure and successful test. We consider our client's service availability and data integrity as our most important objectives.

In the second phase, the security expert gains access to the system, with the aim to precisely determine which data could eventually be exposed if a real attack would occur. Using proprietary tools and work methods, the security expert will gather evidence of the exposed data, while actively removing any potential risk might associate to such an act.

The third phase of the test is the reporting phase, in which the conclusions of the Cyber Attack Simulation and Modeling test constitute the basis of a written report. The successful and unsuccessful penetration vectors and the security failures that allowed to the external factor to infiltrate the internal infrastructure are described in detail. The report contains detailed references concerning the level of associated risk of the discovered security failures. This report will also include actionable elements, whose immediate application will help the organization to improve its security robustness. The findings are presented in explicit and coherent way, allowing the client's team to effortlessly and clearly understand the identified issues and the remediation suggestions. However, if a direct communication situation would eventually be required, Cipher Security will happily assist your company in the discussion with your client.

For the evidence gathering phase Cipher Security is using secure and encrypted channels of communication, using DLP best-practices and perimeter security best-practices.

During the assessment time, that generally takes about one week, our security experts will keep an open communication channel with client point of contact and will keep him update on a constant basis.

2

BUSINESS BENEFITS FOR YOUR CLIENT

Avoiding a data exposure may save substantial amount of money (estimated 6-7 figures numbers) that otherwise should be used for remediation and notification costs.

Providing comprehensive and elaborate evidence of an organization ability to detect and mitigate risks will lower the cost of security audits, thereby contributing to business growth.

Audit teams may use the Cyber Attack Simulation and Modeling test data for internal regulatory compliance inspections.

The Cyber Attack Simulation and Modeling test report magnifies the awareness of information security's importance at the highest management level, hence providing a substantial basis for approval of larger security budgets.

The Cyber Attack Simulation and Modeling also supports the validation of the effectiveness of other security products that the organization is using or evaluating to implement.

The service may lay the foundations for greater co-operation with your client.

3

IT / TECHNICAL BENEFITS FOR YOUR CLIENT

Supports the IT staff in their attempt to precisely identify the real and potential data exposures and allow them to adapt their security strategies to proactively eliminate identified security issues.

The Cyber Attack Simulation and Modeling test is the best prioritizing method for the IT team.

4

THE BENEFITS OF PERFORMING A CYBER ATTACK SIMULATION AND MODELING SERVICE FOR YOU

Being aware of Cyber Attack Simulation and Modeling service' high economic potential, Cipher Security uses the opportunity offered by this information security necessity and is ready to offer to its business partners an amazing new business growth channel.

We are ready to provide under your umbrella an outstanding Cyber Attack Simulation and Modeling service, being fast, flexible, light footprint and with zero effort on your side.

5

BUSINESS BENEFITS FOR YOUR COMPANY

Cyber Attack Simulation and Modeling service may represent an amazing business growth channel in the near future. Cyber Attack Simulation and Modeling service may secure the business relationships with your actual clients and enables you to establish new business relationships.

Exercising the Cyber Attack Simulation and Modeling has proven to be an outstanding business enabler, with sequential projects as a common practice.

Offering to the market an **"out-of-the-box"** service might just place you few steps ahead your competitors.

IS THIS SERVICE AN EXTERNAL PENETRATION TEST ?

No. The Cyber Attack Simulation and Modeling is not an External Penetration Test. While a penetration test will show the current cyber risks an organization is facing, the Cyber Attack Simulation and Modeling will demonstrate a safe and controlled cyber infiltration incident. As the Penetration Tester will examine the logical aspect of current security status of an organization, the security expert will use all available attack vectors to accomplish an infiltration. In addition to logical and technical attacks, the consultant will use Social Engineering, Spear Phishing and proprietary practices to attain successful demonstration. The focus of the Cyber expert is to imitate real-world scenarios and attack flows, rather than using automated scanners and filling a pre-written report template.

ABOUT US

Based in Tel-Aviv, Israel, Cipher Security is a unique Information Security provider that operates in respect with its main values - integrity, accountability, reliability, and partnership.

A trusted partner, we are ready to fulfill requirements and surpass expectations, delivering outstanding value in any given challenge. The Cipher Security specialized services portfolio includes cutting-edge Distributed Denial of Service Tests (DDoS) Consulting, Cyber Workshops, Infrastructure and SCADA Penetration Tests, and tailor-made Exploit Development.

We address our innovative services to a vast scope of industries; from Banking and Investments sector, through the Industrial domain and Critical Infrastructure, to vendors and service providers from around the world.

CIPHER SECURITY