



Pentest E-Guide

Everything you need
to know



Provided by
IthacaLabs™

Table of Contents

What a Penetration Test is	3
Penetration Test vs. Vulnerability Assessment	5
Why your organization needs penetration testing	7
Types of Pentest	9
External Penetration Testing	9
Internal Penetration Testing	9
Web Application Penetration Testing	9
Mobile Application Penetration Testing	10
Wireless Penetration Testing	10
Remote Access (VPN) Penetration Testing	10
Social Engineering	11
Penetration Test Methodology	12
What to look for in a Penetration Test provider	14
Why IthacaLabs™ by Odyssey	16
About Odyssey	17

What a Penetration Test is

A simulation of real-world hacking

Penetration Testing (pentest) is an ethical hacking exercise, during which authorized specialists emulate threat actors' techniques in near-real scenarios, with the aim of identifying vulnerabilities and configuration weaknesses in your organization's systems, applications, networks, processes and people.

Once such vulnerabilities and weaknesses are identified, pentesters attempt, in a controlled manner, to verify them. This is done in order to understand the potential impact of those vulnerabilities and weaknesses on your organization's viability, if they are to be exploited by threat-actors.

This is accomplished first by finding your organization's security gaps. Secondly, they are prioritized and quantified by assessing their likelihood and their impact when exploited. Lastly, individualized recommendations are provided to effectively address each and every vulnerability and weakness identified.

Such flaws may provide threat-actors with unauthorized access to your systems, allowing them to steal/delete data, affect your networks' availability, or take control of system resources for malicious purposes.

Depending on the classification of exposed data, such loss may seriously impact your operational continuity, financial stability, brand value, and reputation. Depending on your industry and the severity of the loss, it may also give rise to legal proceedings brought against your organization, by affected business partners, employees, legal/regulatory bodies and customers.



Penetration Testing helps organizations identify vulnerabilities and configuration weaknesses before threat-actors do.

Not all pentests are created equal.

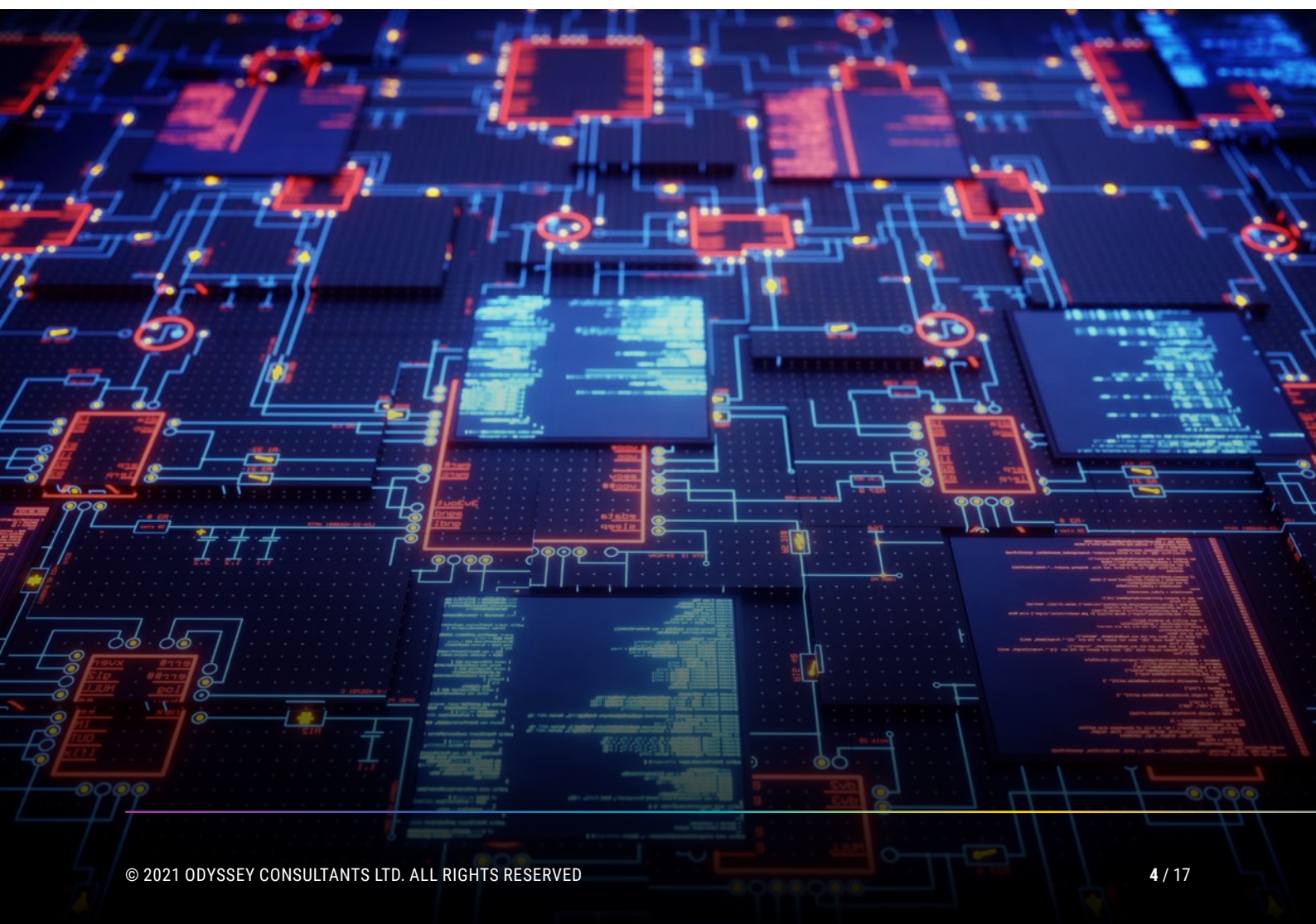
The real value of a comprehensive penetration testing exercise is that it adds context via the intelligence and accumulated know-how of dedicated experienced specialists, since they are in a unique position to identify and test the extent to which elusive weaknesses can be exploited by real-world motivated threat-actors.

This provides immense added value to the pentest service which, unfortunately, is perceived by many to be nothing more than a simple compliance requirement.

Proactive and regular penetration testing is not only a compliance requirement. Its true value lies in the fact that it helps you mitigate the continually evolving and transforming risks posed by the expanding information-threat landscape.



Top-of-the-range providers offer expert, up-to-date and relevant recommendations, not only for the flaws identified during the penetration testing process, but also on how to reform your Risk Management strategy to avoid them in the future.





A **vulnerability assessment**

is simply an automated scan and detection of security gaps and vulnerabilities found in your cyber defenses and security controls at the specific time of assessment.

A **Pentest**, on the other hand, goes well beyond simple identification of such vulnerabilities by proceeding to exploit them and verify them.

Penetration Test vs. Vulnerability Assessment

Understanding the Differences

Many IT professionals still confuse vulnerability assessments with penetration tests (pentests) with regards to their scope, as well as their practical application. Even though both services help provide situational awareness over the security posture of your organization, as well as achieve compliance with relevant regulatory frameworks, there are fundamental differences to their approach, methodology, scope of work and deliverables. In essence, their usefulness and practical application of results differ.

Main differences between vulnerability assessments and penetration tests:

Vulnerability assessment	Areas of Differences	Penetration testing
Discovery of weaknesses and vulnerabilities	Depth	Exploration of their depth and exploitation
Automated methods	Automation	Combined methods
Some security knowledge needed	Expertise	Requires specialization, expertise and know-how

Depth: While vulnerability assessments aim to discover as many weaknesses and vulnerabilities as possible, penetration tests explore their depth in exploiting them using real-world attack scenarios.

Automation: Vulnerability assessments are usually mostly automated methods of scanning for vulnerabilities. Penetration tests combine automated methods with manual ones for more comprehensive results.

Expertise: Because of the automated nature of vulnerability assessments, non-specialized IT professionals with minimal security knowledge may be the ones providing them. Penetration tests are mostly implemented by highly specialized security experts with the accumulated know-how to identify even the most elusive vulnerabilities, to exploit them as much as possible, and to provide recommendations to address them using industry best practices.



Cybercrime costs are expected to increase by 15% each year by 2025, up to \$10.5 trillion yearly, and \$3 trillion higher than 2015.

Cybersecurity Ventures

Why your organization needs penetration testing

More than just compliance

The world is changing. Cloud adoption, Hybrid Working and Digital Transformation are exponentially increasing the complexity and dependency on the IT Ecosystem. Digital Boundaries blur, formulating a “Complex Digital Ecosystem” where Internal, Cloud and External parties are practically indistinguishable. The perimeter as we know it is gone, resulting in new threats and vulnerabilities emerging faster than organizations can adapt.

As a result, security policies and best practices are also in a constant state of change and transformation. Therefore, penetration testing is the most realistic way for an organization to know whether security controls in place are still relevant, effective, or even configured in an up-to-date or appropriate manner.

In essence, when engaging in regular penetration testing, your organization benefits from up-to-date situational awareness of your cyber defense status.

The adoption of a penetration testing strategy is necessary for safeguarding your valuable business assets and long-term viability.



Penetration Tests help organizations optimize their return on investment by mitigating the risk of security-related operation disruption, legal liability, reputation damage and intellectual property theft.

Alexander
Kaniklides,
Manager,
IthacaLabs™

Penetration testing empowers your organization to:

- ✓ **Identify your actual security posture.** Test how well your organization's security infrastructure, applications, controls and staff measure up against exploitation attempts, this way maintaining clear situational awareness of how effective your cyber defenses are, when put to the test with ethical hacking.
- ✓ **Identify Weaknesses.** Emerging threats, exploitation paths, vulnerabilities, configuration weaknesses and forgotten sensitive information in the wrong places may be exploited by threat-actors, or they can be accidentally exposed.
- ✓ **Align with industry security standards** (such as those found under relevant regulatory frameworks, e.g. PCI-DSS). Ensure adherence to mandatory, as well as recommended, industry standards while maintaining your compliance status with regulatory frameworks relevant to your industry. Maintain confidentiality, integrity and availability of your business-critical information, and as a result, brand goodwill and trust.
- ✓ **Test new technologies.** Remain up to date with information security and risk management best practices from leading experts and specialists by putting your configurations to the test as part of your ongoing digital transformation strategy.
- ✓ **Improve policies and procedures.** Gain knowledge regarding the "root cause" of identified issues rising from certain security areas such as Patching, configuration management, Access control, Identification & Authentication, Cryptography etc.
- ✓ **Mitigate your overall cyber risk.** Gain peace of mind knowing that your brand and operations are safe from cyber disasters. Divert your resources and attention to your core business competencies.
- ✓ **Raise security awareness.** Train and continuously educate security staff. Expose your staff to best-in-class knowledge and tap into the tacit experience of world-class security experts to foster security awareness within your organization, with regards to security best practices, as well as social engineering tactics employed by malicious actors.

Types of Pentest



External Penetration Testing

Ethical Hacking is purposely designed to assess how effective your existing security controls are against an active, human, skilled, cybercriminal in the real world. Ethical Hacking exercises focus on the external perimeter of the organization. They aim to proactively identify critical exposures in operating systems, services and applications across your enterprise and determine the extent at which they can be exploited.



Internal Penetration Testing

Internal penetration tests are designed to determine how effective your internal security controls are against an active, human, skilled, cybercriminal in the real world, with access to the internal network. Such Ethical Hacking exercises focus on the internal network of the organization and proactively identify critical exposures in networks (VoIP, Data-Centre, Users-LAN etc.) operating systems, services and applications across your enterprise.



Web Application Penetration Testing

Web Application penetration testing exercises are designed to answer how robust, reliable and secure your web applications are against an active, human, skilled, cybercriminal in the real world. Web Application penetration testing exercises focus on the internet accessible and internal web applications of the organization and proactively identify critical exposures in the web applications, underlying infrastructure, and the communication between the web application clients and servers.



Mobile Application Penetration Testing

Mobile Application penetration testing proactively detects critical exposures in mobile application platforms (iOS & Android), across your mobile infrastructure (including associated APIs), in order to identify how protective measures might be misused, mismanaged, attacked, or incorrectly configured. It is noted that to safeguard your Mobile Applications and data, a comprehensive approach to risk management is required.



Wireless Penetration Testing

Wireless Network Penetration Testing is designed to answer what is the real-world effectiveness of existing security controls on your Wireless network, against an active, human, skilled, cybercriminal. This test focuses on the wireless network infrastructure of the organization and proactively identifies critical exposures in devices and hosts connected to your network. Wireless penetration testing also determines the level and effectiveness of the segmentation which exists between your wireless network and your internal networks, by examining aspects like SSID isolation, client isolation and many more.



Remote Access (VPN) Penetration Testing

Remote Access (VPN) Penetration Testing is designed to determine the effectiveness of your existing security controls against a skilled cybercriminal targeting your Remote Access services (VPN). Sophisticated cyberattacks are in a constant state of evolution, the latest trend being the targeting of organizational remote access services (VPN) and attempting to hide their malicious activity and exploiting seemingly insignificant vulnerabilities. Simulating such an attack under controlled conditions, is probably the best way to realize how intruders would actually approach your remote access (VPN) network and reveal the actual risk posed to your organization by a potential compromise.

Social Engineering

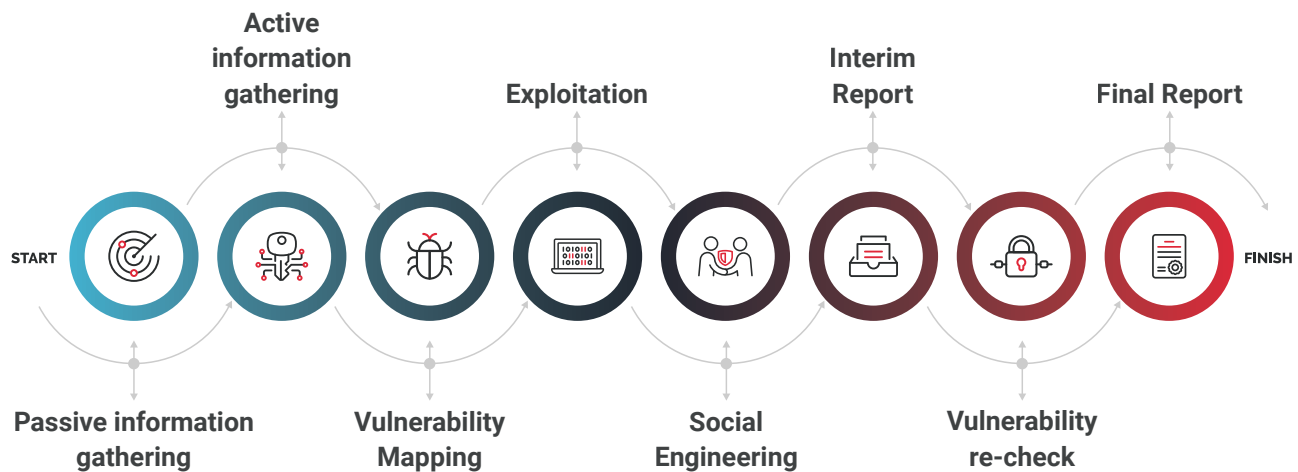
Social Engineering describes a non-technical type of intrusion that relies heavily on human interaction, either via remote communication (Phishing/Spear Phishing or Vishing) or physical presence. During a Social Engineering attack, perpetrators will mislead and trick a person, usually an authorized employee or partner whose real identity was acquired, into performing malicious actions and/or persuade them to disclose sensitive information.

When motivated threat-actors target your organization, they are willing to go to any length and depth to achieve their objective, and their attack methods will not be limited to digital. Physical social engineering (on-premises accessibility level), aims to uncover weaknesses in your physical security defences and attempts to bypass normal security procedures or physical access controls in an effort to identify staff- and process-related security gaps, before threat actors do.

By identifying weaknesses in your staff security awareness, physical perimeter as well as security processes and controls, you are in a better position of improving your existing physical security controls and policies against unauthorized access.



Penetration Test Methodology



A comprehensive penetration test adheres to a strict methodology that is ultimately the key to its successful implementation. A proven pentest methodology is comprised of the following steps:

- ✓ **Passive information gathering (Reconnaissance/Web Intelligence)** consists of a series of passive probes for gathering as much information as possible pertaining to the targeted organization, in-scope systems and network components, without probing the organization's infrastructure. This involves scouting the Internet (harvesters, social media, leaked documents, leaked email addresses and passwords through leaked databases etc.) and DarkWeb to obtain relevant information about the targeted organization. This exercise helps organizations understand their exposure and how such information could be leveraged for more targeted and sophisticated attacks, such as Social Engineering (Phishing and Spear Phishing).
- ✓ **Active information gathering (Reconnaissance)** consists of a series of active probes against the targeted networks, hosts and applications, for gathering as much information as possible pertaining to the in-scope systems and network components. Relevant information is collected with the use of automated (Commercial and non-commercial tools) as well as manual methods.
- ✓ **Vulnerability Mapping** involves the collation, classification and mapping of the information obtained during the passive and active information gathering phases. At this point, it is possible to draw a "map" of the security behavior of the in-scope systems, applications and networks components, which allows experienced penetration testers to determine their course of action.

- ✓ **Exploitation** of the vulnerabilities and configuration weaknesses identified and mapped during the previous phases of the Ethical Hacking process. Exploitation is not limited to isolated attacks aiming to exploit a single vulnerability. The “attacks” are formulated so that they take advantage of a number (or combination) of identified vulnerabilities and configuration weaknesses.
- ✓ **Social Engineering** refers to the malicious/fraudulent usage of information obtained during the Passive Information gathering/Web Intelligence phase regarding the organization’s employees (email addresses, roles) and published resources (such as information portals, Web Email etc.). The aim is to deceive members of staff into revealing passwords or other information that compromises account security or business internal processes.
- ✓ **Interim Report** involves the summarization of the observations and findings from the Ethical Hacking exercise. The Report is designed to provide you with focused in-depth technical explanation of each identified vulnerability, as well as instructions for remediation and related recommendations. It addresses individual weaknesses but also provides a more holistic view of the risks inherent in your operations, based on the penetration testing work, findings and conclusions.
- ✓ **Vulnerability re-check** is essentially the re-check of the vulnerabilities and configuration weaknesses identified to ensure that the identified issues have been fixed and relevant risks mitigated. Tests are specific to the assets, services and applications assessed during the original test. In essence, it is a re-test to determine whether the findings communicated through the Interim Report document have been effectively addressed. This step is usually performed within 90 days of service commencement, in order to avoid significant changes in the infrastructure, in which case, it would deem the re-test results inaccurate.
- ✓ **Final Report** is the final phase of the project, which includes a summarization of the observations and findings from the Ethical Hacking exercise, but most importantly, the status of the targeted environment, following the mitigation of the identified vulnerabilities.

What to look for in a Penetration Test provider

Not all Penetration Test providers are the same. Each provider offers a unique blend of specialties, expertise and talent in the actual conducting of their pentests, as well as in their deliverables. When you embark on your quest to find a Penetration Test provider that is right for you and your organization's unique characteristics and needs, you must take into consideration that it is a long-term partnership with a security partner who is in charge of something extremely important for the information security and risk management strategy of your organization.

✓ Extensive and combined Experience

Look into their experience in conducting Penetration Tests, and the scope that those cover. It is recommended that penetration tests are conducted by professional security consultants whose knowledge extends far beyond traditional penetrating testing. Such teams can provide unique expertise, guidance and support towards the effective mitigation of the risks identified during the exercise.

✓ Expertise and know-how

Look into their staff's know-how, reputation, awards, and whether the provider has a dedicated professional team with diverse talent and expertise so as to deliver high-quality results. Look for a holistic approach to information security and risk management, with a complete range of related services, products and solutions, indicating a cross-departmental sharing of knowledge and expertise.

✓ 360° approach

To be relevant and effective, a pentest provider should adopt a 360° approach to the penetration testing process. A careful combination of automated solutions (commercial and open-source) for Network/Infrastructure/Application assessments and manual checks performed by multiple specialized engineers should be deployed, so that vulnerabilities, architecture/design flaws and configuration weaknesses can be accurately identified. Subsequently, based on the information obtained, an orchestrated exploitation plan should be crafted and executed to both validate the findings but also to determine the level of exposure of the organization.

✓ **Following the strictest industry standards**

Adherence to internationally accepted industry standards is an indication of commitment to high-quality service and deliverables. Check whether a pentest provider maintains relevant certifications and accreditations. If, for example, the Payment Card Industry Data Security Standard is relevant to your organization, then a provider suited for you must also apply the strictest framework requirements of PCI DSS while performing their penetration testing exercises.

✓ **Comprehensive reporting**

Find out whether they provide comprehensive reporting and actionable deliverables beyond traditional penetration testing reports, including an Executive Summary, findings/observations, key recommendations, security control areas of weaknesses associated with technical details, and supporting evidence.

✓ **Always up-to-date with the latest threats**

The more up-to-date a pentest provider is with the latest emerging threats and vulnerabilities, the more value you can get out of your Penetration Tests. Look for a provider that conducts Threat Research leveraging Threat Intelligence feeds, that is involved in incident response and digital forensics cases, and who provides actionable step-by-step recommendations for you to effectively mitigate risk identified through findings.

Why IthacaLabs™

by Odyssey



IthacaLabs™ is Odyssey's Threat Research & Assessment team specialized in delivering Penetration Tests to top organizations around the world.

Combined Experience

Over 20 years of combined experience in diverse security areas, and with more than 1000 tailor-made assessments under their belt.

Threat Research & Assessment team

IthacaLabs™ has been a fully dedicated Threat Research & Assessment team for the last 10 years, supported by 140 consultants and engineers from other departments within Odyssey.

World-class security experts

The team includes industry experts with the highest of standards, who constantly stay one step ahead of the information-threat curve, delivering high-quality up-to-date results.

Holistic Methodology

The IthacaLabs™ methodology takes a 360° approach to the penetration testing process, addressing the needs of the Digital Era.

Following the strictest requirements

Delivering high-quality service and results by following the strictest framework requirements of PCI DSS.

Beyond traditional penetration testing report

What sets IthacaLabs™ apart is the over-and-above value of their Penetration Test deliverables, which include usable recommendations on how to address each security gap and vulnerability spotted during each pentest. This is due to the fact that IthacaLabs™ involves Threat Research leveraging Threat Intelligence feeds that help provide actionable step-by-step relevant recommendations for your organization to effectively mitigate risk identified through findings.

Recent achievements

- ✓ Identified 0-days in several products
- ✓ Obtained Domain Admin privileges in more than 100 assessments
- ✓ Bypassed Microsoft ATP In Office 365 to deliver malware via email
- ✓ Executed Data Exfiltration techniques in robust environments during red teaming exercises
- ✓ Developed custom payloads and Social Engineering framework (custom Trojans communicating via HTTP and DNS protocols)
- ✓ Prepared Hacking video for a Big organization presented to Board of Directors exploiting a serious vulnerability
- ✓ Mentoring for several years the National Hacking Team of Cyprus in the European competition

About Odyssey

Odyssey is a leader in Cloud & Information Security, supporting organizations around the globe into their cyber resilience journey.

For more than two decades, we continuously evolve our Cloud & Information Security solutions, services and products to support our clients in effectively managing their digital risks and adhering to compliance requirements.

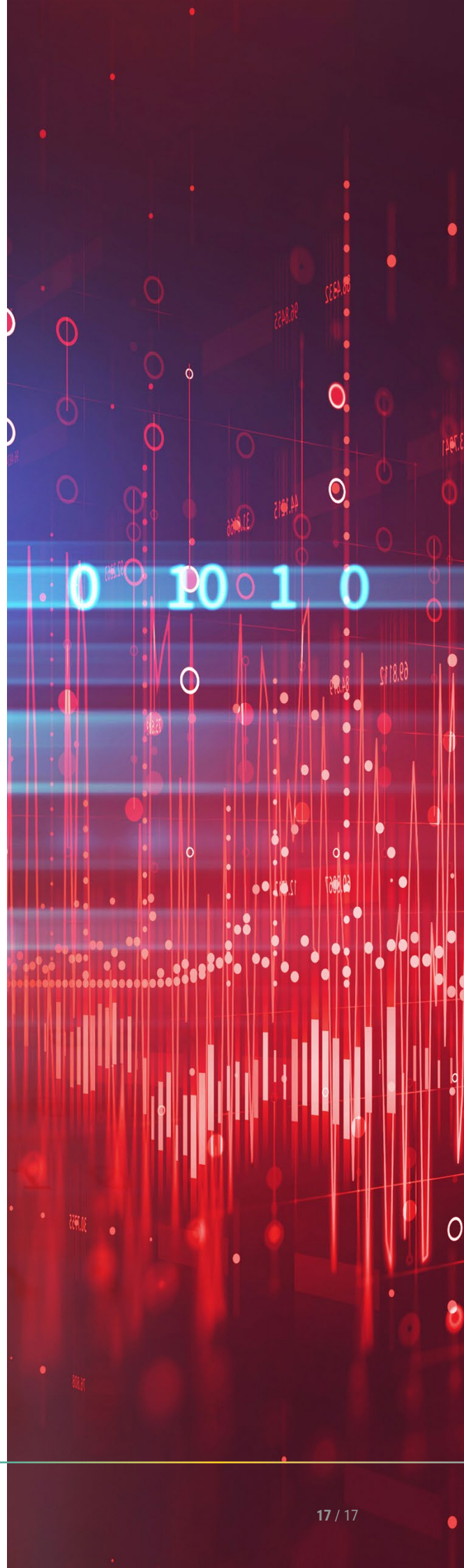
Odyssey's Advisory Services empowers you to build a cyber resilient organization to effectively anticipate, respond, swiftly recover, and adapt to the emerging threats and vulnerabilities of a dynamically expanding and unpredictable threat landscape.

Our holistic approach combines the ClearSkies™ Threat & Vulnerability Management Platform, Managed Security Services (MSS), Governance, Risk & Compliance, Threat Risk Assessment services, Cloud Security and Integrated Solutions, to support your cyber resilience efforts.

Odyssey's award-winning ClearSkies™ Threat & Vulnerability Management Platform is a unique tool that empowers organizations to unlock the intelligence of their log & event data, delivering real-time visibility into their security posture, and enhancing their detection and response capabilities.

Odyssey is among the top 20 global SIEM vendors with ClearSkies™ Cloud SIEM, based on Gartner's 2021 Magic Quadrant for Security Information and Event Management.

Odyssey is ISO 27001, ISO 9001 and ISO 22301 certified, and accredited by the Payment Card Industry Security Standards Council (PCI SSC) as a Qualified Security Assessor (QSA). We are also honoured with the globally recognised Great Place to Work® certification, the assessment methodology used by "The Fortune 100 Best Companies to Work in America".





Your **ONE** Strategic Partner in
Information Security &
Risk Management.

www.odysseycs.com



OFFICES GREECE | KSA | CYPRUS | UK | USA

© 2021 Odyssey Consultants LTD.

All rights reserved. This product and related documentation are protected by copyright law and are distributed under licensing restricting the copy, distribution, and reverse-engineering. No part of this product or related documentation may be reproduced in any form or by any means without prior written permission from Odyssey Consultants LTD.

Trademarks © 2021 Odyssey Cybersecurity™ and IthacaLabs™ are all registered trademarks of Odyssey Consultants LTD. All other marks mentioned herein are trademarks of their respective companies.