hardsecure
WE MAKE SECURITY

H-CYBER INTRUSION

(CYBER SECURITY PENTEST SERVICE)

CYBER EFFECT - LEVEL 2 - PROACTIVE

h·cyber INTRUSION

SERVICE DESCRIPTION

The Cyber Security Vulnerability Assessment & Pentest Service seeks to assess compliance to standards and identify vulnerabilities, through the online or onsite analysis of CIS, infrastructure, web, mobile, wireless, to allow remediation to occur.

VALUE PROPOSITION

Support to Cyber Security – Prevent This service enables the customer to have a better understanding of their vulnerabilities and so be able to remediate them before being exploited. Being able to understand any vulnerabilities and strengths also supports being able to build a picture of overall security, creating a baseline for measure progress to security improvements.

SERVICE FEATURES

Online Vulnerability Assessment and Remediation Support: Provision of Online Vulnerability Assessment resources to carry out continuous and dynamic evaluations/audits of CIS infrastructures /systems to identify any vulnerabilities in software or configurations and to provide detailed reports. Includes the conduct of the following checks:

- Inventory of all connected devices.
- Inventory of authorized and unauthorized software.
- Inventory of patch and update status of all installed software and operating systems.
- Secure configurations for hardware and software on workstations and servers.
- Malware defenses and endpoint security mechanisms.
- Secure configurations for locally managed network devices.

Rua Acácio de Paiva 16
1ºD - 1700-006 Lisbon
https://en.hardsecure.com
(+351) 218 278 126
geral@hardsecure.com

H-CYBER INTRUSION

(CYBER SECURITY PENTEST SERVICE)

CYBER EFFECT - LEVEL 2 - PROACTIVE

Remediation Support: OVA reports containing cyber security hygiene indicators status, findings and prioritized remediation measures. Advising on mitigation techniques, escalating issues, with the objective of closing vulnerabilities at sites.

On-Site Vulnerability Assessment and Remediation Support: Provision of resources to carry out Security Assets checks on customer CIS, including Industrial Control Systems and Building Management Systems, to ensure compliance with Cyber Security Standards & CIS security policies, directives and guidance documents including Security Guidance that the customers have approved. Includes the conduct of the following checks:

- Inventory of all connected devices.
- Inventory of authorized and unauthorized software.
- Inventory of patch and update status of all installed software and operating systems.
- Secure configurations for hardware and software on workstations and servers.
- Malware defenses and endpoint security mechanisms.
- Secure configurations for locally managed network devices.
- Controlled use of administrative privileges.
- Controlled access based on the “need to know” principle.
- Data loss prevention.
- Locally managed boundary defense.

Remediation Support: Processing follow up sheet report. Advising on mitigation techniques and escalating issues, with the objective of closing vulnerabilities at sites.

Penetration Testing: Provision of resources to evaluate the security of computer systems or networks by simulating an attack from malicious outsiders or insiders and to provide detailed reports about the findings.

Red Teaming: Provision of resources to evaluate the security of computer systems or networks by simulating an attack from malicious outsiders or insiders with no notification to personnel other than IT Director and security officer and to provide detailed reports.

Rua Acácio de Paiva 16
1ºD - 1700-006 Lisbon
https://en.hardsecure.com
(+351) 218 278 126
geral@hardsecure.com

H-CYBER INTRUSION

(CYBER SECURITY PENTEST SERVICE)

CYBER EFFECT - LEVEL 2 - PROACTIVE

Web Application / Database Security Audit: Provision of resources to assess internet facing web applications for security mis-configuration, vulnerabilities and coding bad practices, as well as identifying security weaknesses in databases to help prevent data breaches. The findings and remediation recommendations are provided with the assessment report.

External Attack Surface Monitoring: Provision of resources to continually assess the exposure of Customer CIS to the Internet. The findings and remediation recommendations are provided with the assessment report.

Phishing / Social Engineering Simulation Campaigns: Provision of resources to configuring phishing simulation campaigns and run them. The findings and remediation recommendations are provided with the campaign reports.

Mobile Vulnerability Assessment: Provision of real time monitoring of an organisation's mobile assets, with the purpose of presenting realistic and effective countermeasures to limit the disclosure of intelligence information to unauthorised personnel, for security mis-configuration, vulnerabilities and coding bad practices. The findings and remediation recommendations are provided with the assessment report.

Network Scanning: Provision of resources to perform scanning on wired or wireless networks to identify and remedy potential security flaws. The findings and remediation recommendations are provided with the assessment report.

Wireless network penetration test: support identifying Wi-Fi networks, including wireless fingerprinting, information leakage, and signal leakage, determining encryption weaknesses, such as encryption cracking, wireless sniffing and session hijacking, identifying opportunities to penetrate a network by using wireless or evading WLAN access control measures and identifying legitimate users' identities and credentials to access otherwise private networks and services.

ADDED VALUE OF OUR SERVICE

The main differences in the way a Pentest is performed by us:

» Exploitation development, new exploits & CVEs are published by us, in accordance with the environment of each customer.

Rua Acácio de Paiva 16
1ºD - 1700-006 Lisbon
https://en.hardsecure.com
(+351) 218 278 126
geral@hardsecure.com

H-CYBER INTRUSION

(CYBER SECURITY PENTEST SERVICE)

CYBER EFFECT - LEVEL 2 - PROACTIVE

- All systems & networks (infrastructure, mobile, web applications, databases, wireless, perimeter)

- In accordance with the IT environment of our customer, we validate (manually) new exploits/CVEs that can directly affect the customer in a real time bases way.

- We show technically to our cybersecurity customers how to do it, to promote the exchange of experiences and knowledge.

- We can identify high-risk weaknesses that result from a combination of smaller vulnerabilities.

- The Service is available in the following options:
  - One Shot.
  - As a Service (weekly, monthly or quarterly).
  - Ad Hoc.

SERVICE QUOTE REQUEST

For further information, please contact us using one of the following means:

"Hardsecure – Cyber Security Pentest Service" form (available on the service page on the website)

Contact Hardsecure Account Management:
(+351) 218 278 126 (PT)
(+44) 204 538 6686 (UK)
(+1) 202 2318 9859 (USA)
geral@hardsecure.com

Website:
https://en.hardsecure.com (**"Request Proposal"** form).