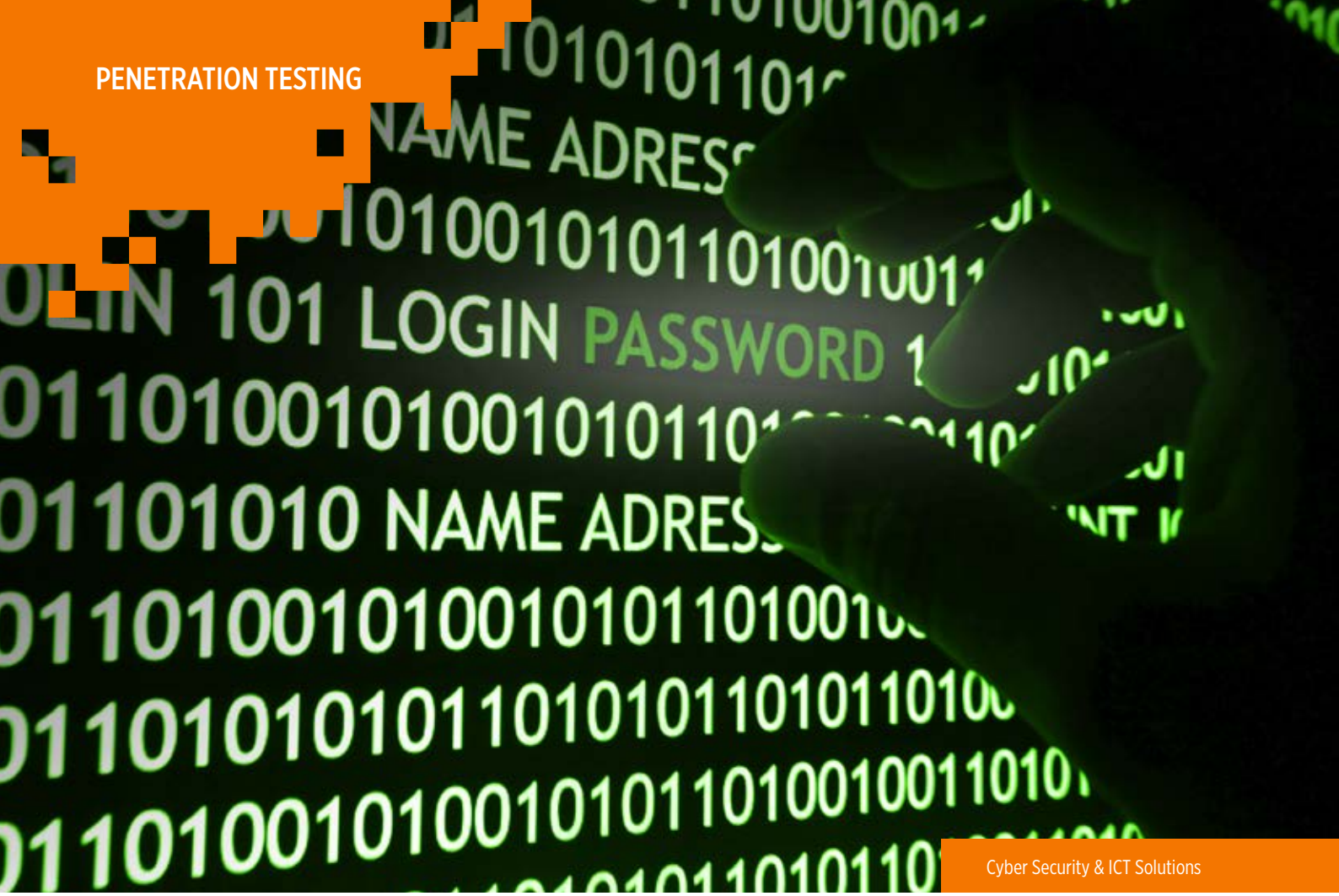


PENETRATION TESTING

There is now a relentless bombardment of unwanted malicious attempts to penetrate organisations connected to the internet. Generally they are easily repelled by the systems you have installed. However, occasionally the attack may succeed, exposing business critical assets and information, jeopardising the reputation you may have built up over many years.

A penetration test is a focussed and comprehensive test of your network and web infrastructure. With your authorisation, we will use highly skilled analysts to probe your network and web technologies, exposing weaknesses and threats. The reason for any vulnerabilities is also explored. After testing, which can be configured to suit your needs and budget, we will produce a set of results and recommendations which paint a detailed picture of your digital landscape, its strengths and weaknesses.

PENETRATION TESTING TEAM

All company penetration consultants are extremely experienced in network, web and application engineering, and have undergone detailed and exacting training under various schemes, the most notable being CEH and, for UK,the CHECK training scheme, ratified by the UK CESG.

With this pedigree of personnel performing testing, the likelihood of successful attacks reduces significantly. All consultants are security cleared and can therefore work in the most restricted of environments.

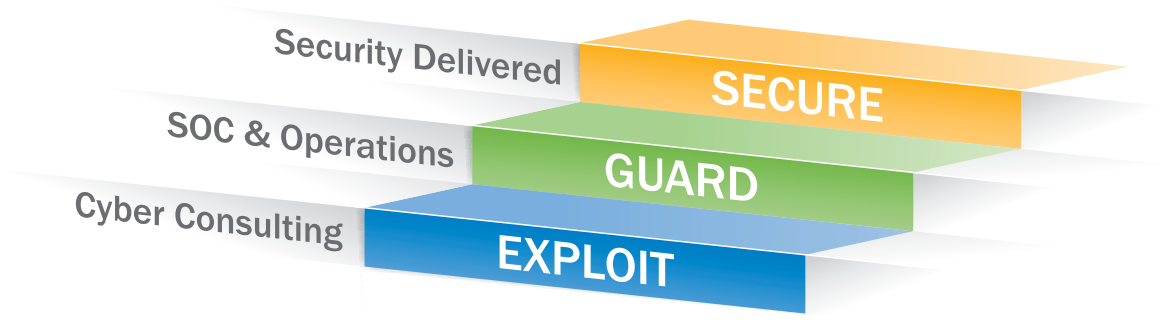
HOW IT WORKS

The penetration team will agree with you what part of the network or web needs to be tested. The team then performs a series of crafted tests to discover the state of your network. They do not change anything, but produce a detailed report detailing:

- A profile of attacks
- Highlights of unusual or threatening attacks
- An analysis of vulnerabilities in your estate
- A risk profile of these parameters
- A list of recommendations to harden the network.

Cyber And Consulting Operations
The company can be retained to engineer solutions to mitigate this risk if required, and the penetration specialists can contribute specific knowledge to help you in this.

PENETRATION TESTING



SECURITY OPERATIONS CENTRES AND OPERATIONS

Our Security Operations Centres (SOCs) provide a flexible and comprehensive set of management and monitoring services that can be quickly tailored around an organisations' specific needs. Security services offer efficient, around-the-clock perimeter and internal security with real-time monitoring, device maintenance, event correlation, and analysis of the customer's infrastructure and critical applications to ensure the cyber threat is pro-actively managed and attacks are mitigated.

Protective monitoring
Multiple SIEMs families, deep analysis and company designed probes and one way diodes. These can monitors different levels of restricted data for commercial and defence customers.

Penetration testing
Test and advises on vulnerabilities and exposures. Digital, physical and human resources and capabilities tested. Accredited CHECK team available.

Incident response
24/7/365 response to incidents. Highly diverse and knowledgeable people / systems. Can provide forensics, reverse engineering, lab skills.

Estate management
Design, Build, Operate and Manage security functions and devices in organisations.platesc illibeaquost labo. Unte consequaesto ommolor minus.

CYBER CONSULTING

The company delivers professional services developed specifically for organisations that want to have full assurance of effective information protection measures and to improve them in line with business needs.
We have a qualified team who have developed a full set of skills including deep technical, regulatory and organisational experience.

Health checks
Experienced consultants deep inspect policy, procedure and devices in the organisation and make it safer, less vulnerable and better protected. Accredited CLAS team available.

Policy management
Consultants test and follow policy impact across the organisation, report and recommend change.

Policy design
Create security policy and posture and assist in engaging staff across the organisation to implement them.

Business risk and impact assessment
Undertake risk and impact analysis on business and quantify data, IPR and staff to align security to the business. Reduce vulnerabilities, increase protection.

Security awareness and training
Assists organisations to educate and inform technical and non-technical staff information security.

LOCATIONS
Italy
Via Laurentina 760, 00143 Rome
UK
430 Bristol Business Park, Coldharbour Lane, Bristol BS16 1EJ

CERTIFICATIONS
UNI EN ISO 9001:2008
Information security - ISO/IEC 27001:2005
Business continuity - ISO 22301
Safety – OHSAS 18001
LSR18.6E certified datacentre infrastructure (Lampertz room - Resilient infrastructure with disaster recovery datacentre and UPS)
UK CLAS
UK CHECK

LEONARDO
SECURITY & INFORMATION SYSTEMS

For more information please email infomarketing@leonardocompany.com
Leonardo – Finmeccanica – Società per azioni
Via Laurentina, 760 - 00143 Rome - Italy - Tel: +39 06 50271 - Fax: +39 06 5051140