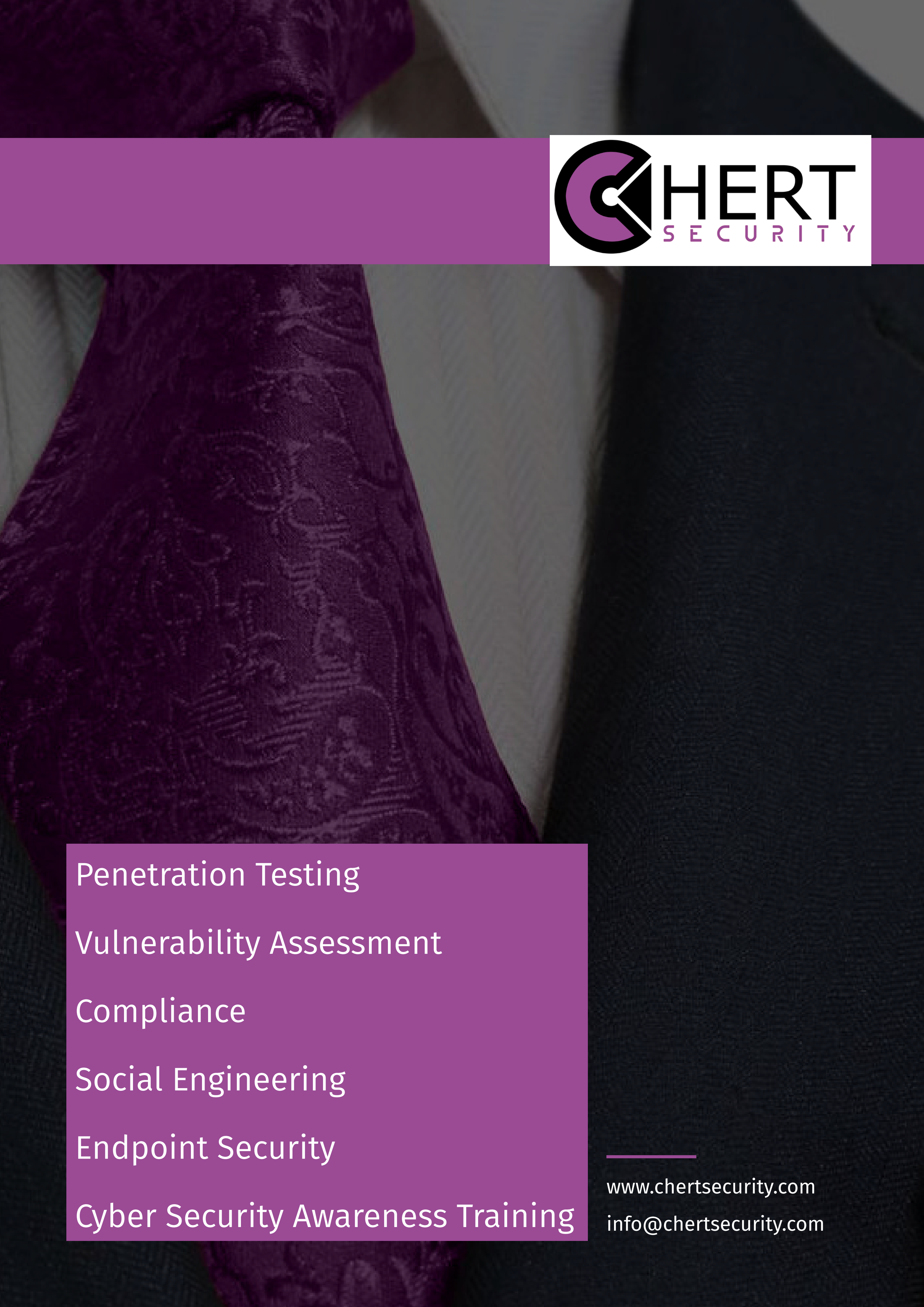


CHERT SECURITY

Penetration Testing

Vulnerability Assessment

Compliance

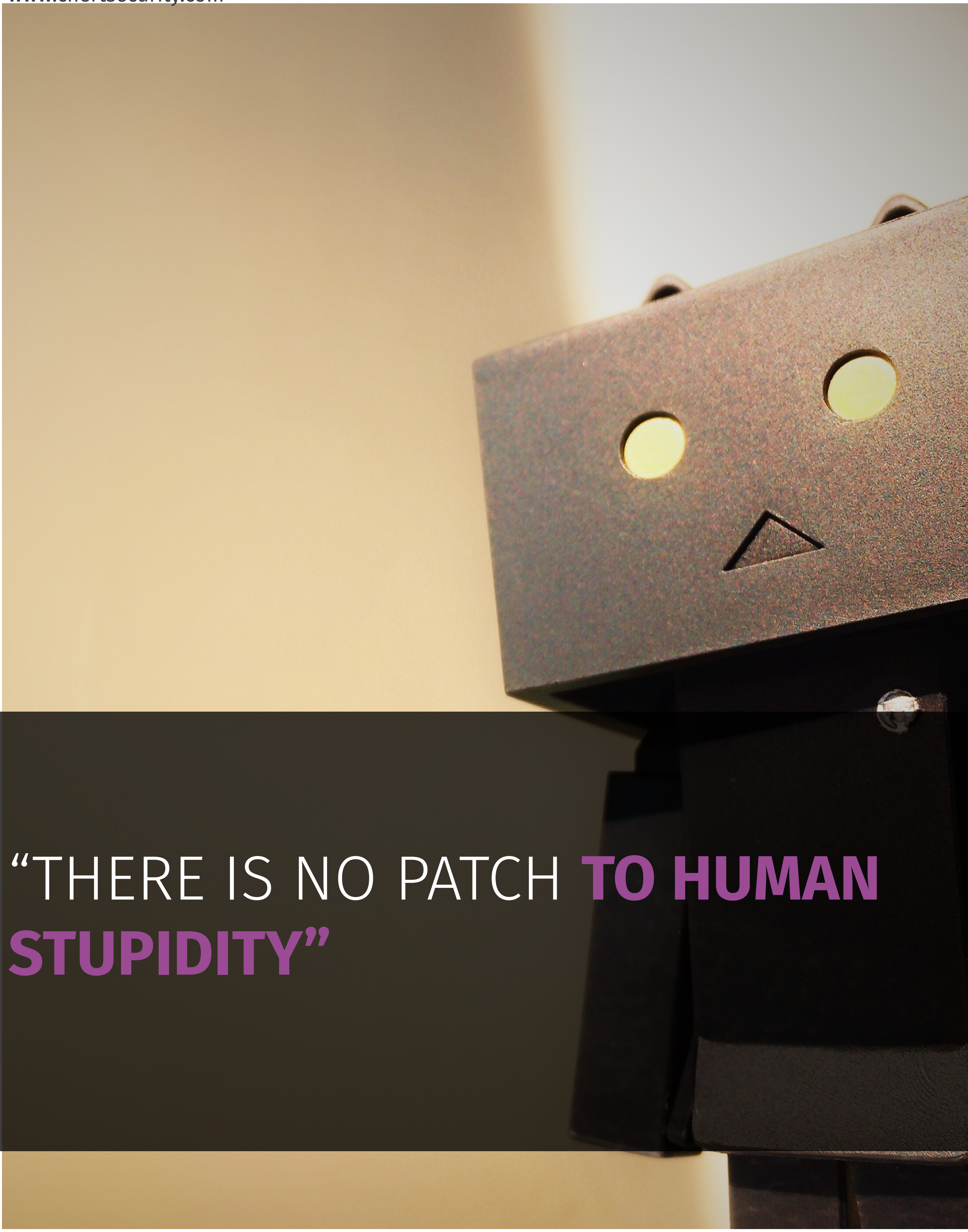
Social Engineering

Endpoint Security

Cyber Security Awareness Training

www.chertsecurity.com

info@chertsecurity.com



“THERE IS NO PATCH **TO HUMAN STUPIDITY”**

PENETRATION TESTING

YOUR CHALLENGES

As we grow ever more reliant on digital data, network security is becoming increasingly important in preventing unauthorized access to personal and corporate data. The security of IT systems is therefore essential in the protection of your organization's knowledge.

WHAT IS PENETRATION TESTING?

Penetration Testing assesses whether your IT systems are secure against the potential external threats that they face. It puts IT systems to the test by using the same methods that potential hackers would employ, revealing whether you're protected against real world attacks. Based on information gathered during the test, our security experts will then draw up a detailed risk assessment report recommending any remedial action required and, if necessary, carry out further tests to assess the effectiveness of the improvements.

WHY IS PENETRATION TESTING IMPORTANT FOR YOUR BUSINESS?

Independent penetration testing not only protects your knowledge. It also safeguards your assets and reputation. It minimizes the risk of financial loss if your network is attacked, underlines your organization's commitment to IT security, and creates confidence among the individuals and organizations you do business with.

HOW CAN WE HELP YOU?

Chert Security has a wealth of experience in penetration testing. Our highly qualified staff will probe your IT infrastructure for vulnerabilities just as if they were themselves cyber criminals and then suggest ways to plug any gaps that they find in your security. By addressing your security loopholes found through penetration testing, you can then be assured of the best possible protection against attacks from criminal hackers.

OUR PENETRATION TESTING SERVICES

Chert Security's penetration testing services are a powerful tool to achieve increased safety and added economic value for your business. The precise scope of the penetration test, and the approach adopted, are customized to your requirements. It consists of four modules, which can be used individually or in combination. We can also check your firewall, routers, mail, name and web servers, e-commerce and other online applications as well as back-end database systems. Your external systems will be tested using a black-box process and specialist software, scripts and other tools. When reviewing your internal IT, we may place a test system on your network, carry out an on-site audit, and/or analyse your system documentation.

PENETRATION TESTING MODULE

The four penetration test modules listed below can be used individually or in combination

Web Aplication

- These are especially vulnerable when accessed from multiple devices and locations.
- The main risk involves unauthorized third-party access to data.
- When the test is completed, we will rate your security and propose remedial measures for any weaknesses.
- The test is carried out in accordance with OWASP (Open Web Application Security Project) guidelines.

Infrastructure

- This tests external, publicly accessible systems such as mail servers, and/or infrastructure that can be accessed from within the organization.
- We identify and evaluate existing risks, and propose measures to deal with them
- The test is carried out in accordance with OSSTMM (Open Source Security Testing Methodology.

WLANs

- Wireless networks are vulnerable to attack because access to them is difficult to control.
- The main risk is unauthorized network and data access.
- The test identifies existing risks and recommends remedial measures.

IoT

- Wireless networks are vulnerable to attack because access to them is difficult to control.
- The main risk is unauthorized network and data access.

PENETRATION TEST PROCEDURE

PREPARATION

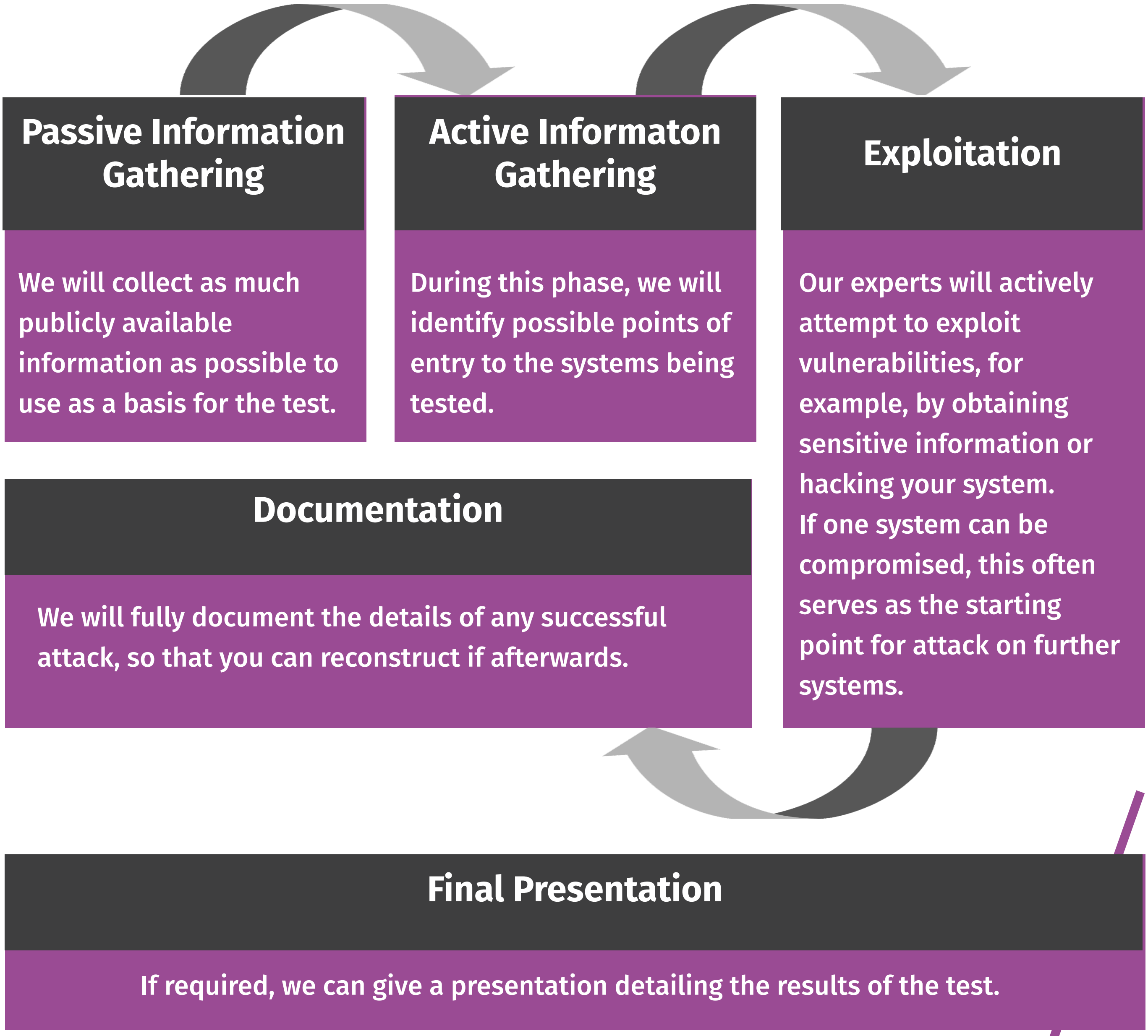
- Analyse your company's business environment.
- Define objectives and procedure.
- Identify security risks specific to your sector.

KICK-OFF MEETING

- Define scope of test.
- Determine test period and report language.
- Discuss general issues relating to the project.

IMPLEMENTATION

- How the test is implemented will depend on the areas you want to assess and the modules you select. It will normally include the following four phases:



Passive Information Gathering

We will collect as much publicly available information as possible to use as a basis for the test.

Active Informaton Gathering

During this phase, we will identify possible points of entry to the systems being tested.

Exploitation

Our experts will actively attempt to exploit vulnerabilities, for example, by obtaining sensitive information or hacking your system.
If one system can be compromised, this often serves as the starting point for attack on further systems.

Documentation

We will fully document the details of any successful attack, so that you can reconstruct if afterwards.

Final Presentation

If required, we can give a presentation detailing the results of the test.

VULNERABILITY ASSESSMENT

YOUR CHALLENGES

Increasing threats, pervasive connectivity and complexity of applications and infrastructure means it is vital to have an accurate view of your security exposure.

SUMMARY

Identify vulnerabilities to improve security, compliance and governance. Controlling security has become an increasingly demanding task. Not only has the level of threats grown due to the influence of cyber-crime, pervasive connectivity has opened up a slew of vulnerabilities. Applications have also grown in number while managing burgeoning infrastructure such operating systems, databases and servers is more complex. The critical first step in providing effective protection is to understand the extent of your exposure. That is where Chert's Vulnerability Assessment service will assist. Our comprehensive, accurate scanning will profile your risk exposure and the potential impact on business, giving you an overarching view of vulnerabilities. Detailed reporting will also assist you to meet compliance and governance requirements.

WHAT IS VULNERABILITY ASSESSMENT?

Network vulnerability assessment services helps identify vulnerabilities in external and internal networks, network services, network protocols, network convergence solutions as well as network systems and devices. This assessment may also cover VPN technologies, with testing activities that include gaining access, traffic manipulation, authentication manipulation and data analysis.
The testing will include,but will not be limited to the following types of systems:

- Router, load balancers, proxy appliances and switches
- Firewalls and/or other screening devices.
- Mail servers (SMTP, POP3 and IMAP).
- Web, name and file servers.
- Desktops and network multifunctional devices.
- Network attached storage and management appliances.
- IP cameras, DVR's and other video communication appliances.
- WAN optimization and management appliances.
- Other IP connected systems which are identified during the testing.

After both automatic and manual testing for vulnerabilities, a verification of identified vulnerabilities will be performed to remove any false positive.

YOUR BENEFITS

- Information regarding vulnerabilities and risks of your IT infrastructure.
- Existing hardware assessment and identification.
- Reducing your IT Risks.
- Increasing resilience of your IT infrastructure.
- IT Governance and Compliance to create an automatic inventory of all connected IP devices.
- Plans for patching available systems to the latest fixes and updates

WHAT WE OFFER

The following products are contained in this service package:

- Identification of active components (hardware and software inventory).
- Detailed investigation and analysis of the existing local area network security risks, vulnerabilities in operating systems and applications like Adobe Reader, Java, etc.
- Optional: Managed IT vulnerabilities minimization recommendations
- Optional: Performing an IT risk analysis.

During the testing, we will immediately report any critical and high risk vulnerabilities identified via a status update report. When the testing has been completed, you will receive a formal report that will contain:

- A detailed explanation of the testing activities that have been completed and the methods used by us to determine the results.
- A listing of all identified vulnerabilities of your Internet presence with a ranking of their level of risk based on the Common Vulnerability Scoring System (CVSS), the ease with which they can exploited, and mitigating factors.
- An explanation of how to mitigate or eliminate the vulnerabilities including enhancement of your policies, adoption of industry best practices, changes to security processes and enhancement to your Internet presence.

Within 10 days after the conclusion of testing, we will present all identified vulnerabilities to you in a final report.

info@chertsecurity.com

COMPLIANCE SERVICES

ISO 27001 SERVICES

Chert Security provides end-to-end services for all aspects of the ISO 27001 journey. This covers all of the policy and procedural aspects of the standard, as well as comprehensive information security design, implementation and support services.

ISO 27001 is an Information Security Management System (ISMS) defined by the international organization for standardization. As well as being an ISO 27001 registered company ourselves, Chert Security also provides a range of ISO 27001 services for our clients.

ISO 27001 COMPLIANCE SERVICES PROVIDED

- ISO 27001 Gap Analysis
- ISO 27001 Implementation Support
- ISO 27001 Testing and Verification Audit.

GDPR COMPLIANCE SERVICES

- GDPR Gap Analysis
- GDPR Tool-kit Documentation
- GDPR Implementation

HOW CAN CHERT HELP?

Chert recommends that the ISO 27001 roadmap starts with an initial assessment followed by a gap analysis. Afterwards, there is frequently a requirement to define policy and procedure. This is a tailored requirement, customized to every organization that pursues the adoption of the ISO 27001 ISMS.

Organizations may require additional security technology and systems assurance to mitigate against threat and risk. Although ISO 27001 does not mandate any form of security technology, the organization may benefit from security solutions so as to reduce their exposure to risk.

The final part of the ISO 27001 journey culminates in a full audit, arranged by Chert but, delivered by an independent certification body.

BENEFITS

Implementing ISO/IEC 27001 management system helps you protect valuable information and derive real benefits

- Supports compliance with relevant laws and regulations.
- Protects your reputation.
- Provides reassurance to clients that their information is secure.
- Cost savings through reduction in incidents.
- Demonstrates credibility and trust.
- Improves your ability to recover your operations and continue business as usual.
- Improved information security awareness.
- Shows commitment to information security at all levels throughout your organization.
- Reduces staff-related security breaches.

SOCIAL ENGINEERING SERVICES

Chert's Social Engineering Assessment Services test your organization's susceptibility to Social Engineering techniques with safe, approved, and authorized replication email-based attacks on targeted employees. The goal of the engagement is to help your organization understand and improve upon its present security posture.

THE SOCIAL ENGINEERING ASSESSMENT WILL:

- Assess security awareness by identifying users who click links in phishing emails
- Set phishing traps via web forms to flag data leakage risks
- Test end-user machines for exploitable vulnerabilities

Following the assessment, Chert will provide a final presentation as well as a report, outlining:

- Nature of the work performed including steps taken in exploitation
- Summary of exposures identified
- Identification of data accessed
- Remediation recommendations

Organizations struggle to ensure that safeguards are consistently applied to protect their valuable information. Inconsistencies in security measures are often attributable to variations in available security products, support tools, administration techniques and delivery mechanisms. Social Engineering attacks, in particular, can be challenging to prevent as they rely on the exploitation of humans. Social Engineering involves a set of technological, psychological, and physical techniques that trick a user into breaking security protocols.
These techniques include:

PHISHING

When an attacker masquerades as a credible source, and sends an email requesting that a user performs an action (ex: clicks a URL, or opens an attachment) and shares confidential information.

SPEAR PHISHING

Similar to phishing, but the attacker targets specific individuals and includes relevant information to appear even more convincing.

VISHING

Malicious attackers will call various individuals to gather information about a target or in order to influence an action. For example, a common scenario would involve a hacker calling a help-desk to request that a new account be created.

IMPERSONATION

Pretexting as another person or presenting a false identity can allow an attacker to gain access to information, facilities, or secure systems.
In order to minimize the likelihood and risk of a Social Engineering attack, Chert will work with your organization to test end user Security Awareness of Phishing, Spear Phishing and other Social Engineering attacks.

ENDPOINT SECURITY

YOUR CHALLENGES

For years, prevention products' primary threat protection was based on signatures. Assuming all attacks at a business had been seen before, using signatures made sense. Today, malware mutates daily, even hourly, making signature-based prevention tools obsolete. The threat landscape grows worse by the day. Increasingly sophisticated attacks are being spotted in the wild and, even as defenders apply patches, signatures and intelligence to these new attacks, the threats change again. One example is ransomware, which is not only pervasive, but has now found new ways to hide from machine learning detection

It is time to think beyond traditional antivirus.

HOW CAN CHERT HELP?

Our solution is an integrated threat prevention solution that combines the power of artificial intelligence (AI) to block malware infections with additional security controls that safeguard against script-based, fileless, memory, and external device based attacks.

Unlike traditional endpoint security products that rely on signatures and behaviour analysis to detect threats in the environment, our solution;

- Uses AI, not signatures, to identify and block known and unknown malware from running on endpoints
- Delivers prevention against common and unknown (zero-day) threats without a cloud connection
- Continuously protects the endpoint without disrupting the end-user With unmatched effectiveness, minimal system impact, and zero-day prevention,

Our solution protects endpoints and organizations from compromise.

CHERT'S ENDPOINT SECURITY FEATURES

- Stops all forms of attacks, including malware, ransomware, zero-day, non-malware, and non-file.
- Prevent attacks automatically; online and offline.
- Block emerging, never-before-seen attacks that other solutions miss

TRUE ZERO-DAY PREVENTION

Resilient AI model prevents zero-day payloads from executing.

AI DRIVEN MALWARE PREVENTION

Field-proven AI inspects any application attempting to execute on an endpoint before it executes.

SCRIPT MANAGEMENT

Maintains full control of when and where scripts are run in the environment.

DEVICE USAGE POLICY ENFORCEMENT

Controls which devices can be used in the environment, eliminating external devices as a possible attack vector.

MEMORY EXPLOITATION DETECTION AND PREVENTION

Proactively identifies malicious use of memory (fileless attacks) with immediate automated prevention responses.

APPLICATION CONTROL FOR FIXED-FUNCTION DEVICES

Ensures fixed-function devices are in a pristine state continuously, eliminating the drift that occurs with unmanaged devices.

CYBER SECURITY AWARENESS TRAINING

When it comes to Cyber Security, your employees play a pivotal role in ensuring information security. Our Cyber Security awareness training program is created to provide employers and employees with an in-depth understanding of the threats to information security. Our approach empowers your team with the tools needed to protect your data. By properly educating your employees, we reduce your chances of becoming another cyber attack statistic.

BENEFITS

- Reducing the surface area of cyber security breach.
- Instilling proper behaviours in employees when it comes to handling information and valuable assets.
- Helping the organizations maintain its stability.
- Improves the reputation of the organisation, information security integration and customer satisfaction.

ON-SITE TRAINING

We offer customizable interactive on-site training to suit every organisation, because we understand each organisation’s unique threat profile and we take that into consideration when deciding the covered subjects.

OUR CYBER SECURITY TRAINING BASELINE TOPICS:

- Antivirus and installing patches
- Phishing awareness
- Physical security
- Desktop security
- Wireless networks
- Password security
- Malware
- Passwords and Password management
- Safe internet use
- Social networking
- Mobile Device Security
- Using wireless networks
- Removable Media
- Email and Browser security
- Travel Security

CHERT
SECURITY

ADDRESS
14, Ilaka street, off
Coker road, Ilupeju,
Lagos

PHONE
0708-666-9951

WEB & EMAIL
Email: info@chertsecurity.com

Web: www.chertsecurity.com