dionach

Service Overview

1.0 INTRODUCTION

Dionach are an **ISO 27001**, **PCI QSA**, **NCSC CHECK**, and **CREST** certified independent information security consultancy. Dionach consists of specialist consultant teams in the following security disciplines: Penetration Testing, Auditing and Consultancy, and Incident Response. The specific services that Dionach provides in each of these disciplines are listed below.

Service Name	Service Elements
Penetration Testing	Cloud Security Assessment CHECK and CREST IT Health Checks Network Penetration Testing Application Penetration Testing AI Application Penetration Testing Internal Penetration Testing – Including VoIP and Wireless Mobile Application Penetration Testing
Social Engineering	Email & Telephone Phishing Physical Social Engineering Testing Security Awareness Training
Red Team Engagement	Bespoke Red and Purple Team Engagements
PCI DSS	PCI DSS Scope Review PCI DSS Gap Audit PCI DSS Consultancy PCI DSS Checklist Audit Report on Compliance
ISO27001 Services	ISO27001 Gap Assessment ISO27001 Audit
Incident Response and Forensics	Incident Response Planning and Remediation Support Post Intrusion and Forensic Investigation and Analysis
Technical Information Security Auditing	Network and Systems Security Audit Cloud Security Review Application Security Audit Application Code Review Firewall Rule Audit Network Infrastructure Review Build Review Audit against specific government and industry standards

Cyber Security and Information Assurance Consultancy	Information Assurance (IA) consultancy ISO 27001 Consultancy

The main differentiators between Dionach and most other companies providing information security services in the market place are:

- Dionach are Independent: We have no connections or reseller agreements with any product providers/third party companies.
- Dionach provide a manual based testing service, using tools where necessary, but relying on the skills and experience of a team of specialist testers.

New information security threats and vulnerabilities appear at an astonishing rate and Dionach keep abreast of these through the work done by our Research and Development team. As well as monitoring the appearance of all new threats, Dionach actively research new and known vulnerabilities, liaising with both the major security vendors and our clients with any major new discoveries.

2.0 PENETRATION TESTING

The management of information is of critical concern to all organisations. The importance of understanding the risks associated with various types of information, assists businesses in protecting both itself and its' clients. The loss or disruption of services can cause devastating consequences to any organisation and can lead to reputational damage, loss of revenue and increased fines. Penetration testing is an accepted way of determining technical vulnerabilities in both applications and infrastructures and reducing the likelihood of a security breach.

Penetration testing is a key requirement in determining whether security policies are effective, and is also essential for compliance to financial regulations such as PCI DSS, SWIFT, Sarbanes-Oxley, and for certification to standards such as ISO 27001.

Dionach offer a range of penetration testing services including:

- **Cloud Security Assessment**
  Identify and remediate vulnerabilities within your cloud environments, protect against attacks and ensure compliance with data privacy and security regulations.

- **External Network Infrastructure Penetration Test**
  Identify vulnerabilities exposed through your internet gateways to external attacks on your systems.

- **Web Application Penetration Test**
  Ensure that your websites, web shops, intranets, extranets and web-based applications are secure.

- **AI Application Penetration Test**
  Protect AI systems that use Machine Learning (AL) or Large Language Models (LLM's) from the unique vulnerabilities and attack vectors they are exposed to.

- **Internal Infrastructure Penetration Test**
  Assess risks posed by hackers or malicious employees with access to your internal systems.

- **Mobile App Penetration Test**
  Check your mobile apps and related web services for mobile app specific vulnerabilities.

Dionach approach each pen testing as any potential hacker would. Our highly skilled CREST and CHECK qualified consultants use a combination of manual methods and tools to carry out a full security vulnerability assessment.

3.0 SOCIAL ENGINEERING

Social engineering involves the manipulation or deception of individuals when trying to gain unauthorised access to the office premises or computer systems. In social engineering situations attackers need to achieve access to avoid the various preventative security measures such as intruder detection systems, intruder prevention systems and firewalls.

A determined attacker will go to any extent to obtain unauthorised access to confidential information. A social engineering assessment will see how susceptible employees within your organisation are to various social engineering methods such as phishing attacks, Trojan viruses, over the phone manipulation or physical access to the premises. An individual with direct and undetected access to this information could result in extremely costly consequences for the business.

When performing a social engineering assessment, Dionach will attempt to deceptively achieve privileges and gain access to systems or physical areas of the business which are agreed prior to testing. Through the exposure of weakness in security, Dionach can report on the vulnerabilities in a fully comprehensive report delivered face to face to enable discussion and full understanding of the risks identified.

Our consultants can be made available for further meetings and discussions with those who are tasked with fixing any issues. Dionach can provide training and follow up social engineering testing to ensure that your organisation is as resistant to social engineering attacks as it can be.

We offer a range of services within the field including the following:

- **Untargeted Email Phishing Campaigns**
  The purpose of this type of campaign is to test the susceptibility of the internal staff into clicking blatant phishing emails.
- **Targeted Email Phishing Campaigns**
  The purpose of this type of campaign is to utilise the information which we can find on individuals to develop a more sophisticated phishing email which is design to target key users.
- **Telephone Campaigns**
- **Security Awareness Training**
  Dionach can provide security awareness training to employees on how best to identify and prevent social engineering attacks at a standard user level. Dionach can incorporate statistics from previous engagements and live hacking demonstrations within this.
- **Physical Social Engineering Testing**
  Dionach can test the physical security of your offices or property assets to determine how easily an attacker may compromise it.

4.0 RED TEAM ENGAGEMENT

Dionach's Red Team service is designed to offer organisations the highest level of assurance that their most critical assets are secure.

Unlike a traditional penetration test, our Red Team engagements are tailored to rigorously test your security posture across multiple domains. Our team of specialists will simulate how a real-world threat actor would target your company, deploying a range of electronic, social and physical strategies to circumvent your existing security controls.

Whatever asset you are looking to protect, our dedicated and experienced team of experts can assist you in identifying and rectifying the weaknesses in your current security practices.

Benefits of a Red Team Engagement:

- Designed to emulate real world attacks through advanced adversary modelling
- Thoroughly tests your security posture across multiple domains
- Identifies weaknesses in your existing security technologies, controls, policies and practices
- Detailed client report provides comprehensive remediation strategies
- Good performance in engagements provides assurance that company assets are secure

There are a number of options that the Dionach red team can follow during the engagement. The ultimate goal of the engagement is to gain access to a predefined trophy, such as the domain administrator passwords or client information.

5.0 PCI DSS

As a PCI QSA provider company, Dionach can assist organisations of all sizes in achieving PCI DSS compliance. Ensuring that the transmission, storage and processing of cardholder data is done so in the most secure and practical way, will not only achieve the required level of compliance but more importantly will minimize the potential of being subjected to a data breach . Dionach offer a variety of services to help with your compliance.

- **PCI DSS Scope**

Dionach can assist in scoping out areas where cardholder data is stored, processed or transmitted to understand how and if scope can be reduced, and therefore how to attain PCI DSS compliance more quickly.

- **PCI QSA Consultancy**

Dionach's consultants can provide experienced comprehensive guidance on the best methods and practice for your business. We will provide clear and practical advice for any non-compliant areas to help your business attain PCI DSS compliance.

- **PCI SAQ Consultancy**

As an annual requirement for PCI DSS most businesses taking card payments are required to complete an annual self-assessment questionnaire (SAQ). Dionach can provide accurate advice and assistance to help ease the stress to make sure that your SAQ is well documented, accurate and dependable.

- **PCI ASV Scanning**

A vulnerability assessment simply identifies and reports areas of weakness by means of scanning all resources. The scan will need to be carried out through a PCI approved scanning vendor.

- **PCI Penetration Test**

Dionach have years of experience in manual penetration testing and can ensure that a fully comprehensive penetration test will be carried out for your security. PCI DSS requires that annual network and application penetration tests are completed by qualified penetration testers.

- **PCI PA-QSA Services**

Dionach is a Payment Application Qualified Security Assessor (PA-QSA) and are qualified by the PCI Security Standards Council to perform PA-DSS Assessments for PA-DSS Program purposes.

6.0 ISO 27001

ISO 27001 is the best practice international standard for an Information Security Management System (ISMS), that allows an organisation to comprehensively secure information and provide independent assurance that this has been implemented correctly. An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management.

Dionach offer a range of ISO 27001 auditing services, including:

- **ISO 27001 Consultancy**

Dionach can provide experienced ISO 27001 consultants to assist your internal teams and provide additional short term resource for certification to the information security standard

- **ISO 27001 Gap Audit**

Identify the things that your organisation needs to do to obtain certification to information security standard ISO 27001.

- **ISO 27001 Internal Audits**

Perform regular independent internal audits of your ISMS as required as part of adhering to the ISO 27001 information security standard.

- **Gambling Commission**

An annual requirement for companies regulated by the gambling commission to comply with certain aspects of the standard.

7.0 INCIDENT RESPONSE

A vital aspect of Information Security is the ability to effectively respond to any breach or suspected breach. Having worked with a number of organisations to help determine the root cause of a breach or attack, Dionach has a formal approach to responding to breaches and forensic analysis, through being a CREST registered Cyber Security Incident Response (CSIR) provider.

Understanding what procedures should be followed in the event of a breach or suspected breach is vital to any organisation. With this in mind, Dionach has developed a preparedness calculator. This questionnaire allows all organisations regardless of size, to understand how prepared they are should they be breached. By understanding an organisations approach to security and the policies and procedures that are in place, will allow any business to implement an effective CSIR plan.

- **Initial Incident Response**

  Dionach's clients rely on Dionach to be able to respond quickly to any potential breach, compromise or general cyber security incident. Dionach are often called upon at short notice to investigate a suspected breach or security incident and to provide guidance and support throughout the process of containing, eradicating, and recovering from the incident.

- **Forensic Investigation & and Data Analysis**

  Dionach can provide detailed analysis of evidence relevant to the incident, in order to ensure that responses are appropriate, recovery efforts are effective, and strategic processes implemented to prevent recurrence. Dionach will provide detailed reports offering a clear timeline of events leading to the incident, including executive summary recommendations on how to address any vulnerabilities in systems or processes which lead to the incident occurring.

- **Recovery and Remediation**

  Dionach consultants can work alongside your staff, where required, to remediate and recover from the incident. This can sometimes be a simple as isolating and rebuilding a single workstation. Other times this can be a complex strategy affecting many systems, and requiring extensive changes to system architecture or information security management processes. Dionach will assemble a team, specifically qualified to handle your requirements.

- **Post incident Consultancy**

  Dionach can offer ongoing consultancy based upon further review of the client's systems in light of any security incident to ensure that lessons are learnt and any similar weaknesses are highlighted and addressed. This could take the form of auditing, penetration testing or other supporting services as appropriate.

Examples of the types of work Dionach have been involved with include:

- Analysis of malware or suspicious network traffic discovered within a network.
- Analysis of a compromised web application or network.
- Forensic collection of evidence, post breach.
- Establishing the extent of the compromise, with recommendations for remediation.

8.0 TECHNICAL INFORMATION SECURITY AUDITING

Information Security Audits are an essential tool to ensure that you have the necessary security policies and infrastructure in place to protect your computer systems and the information that they contain, and that security policies and procedures are being adhered to.

- **Cloud Security Review**

A Cloud Security Review is a comprehensive service designed to evaluate the security posture of your cloud environment. Our experienced consultants will assesses the configuration, management, and operation of cloud services, including public, private, and hybrid cloud deployments. The review covers critical aspects such as identity and access management, data protection, network configuration, and compliance with cloud security best practices. By identifying vulnerabilities and recommending enhancements, this service ensures that cloud infrastructures are robust, resilient, and aligned with industry security standards.

- **Application Security Audit**

An Application Security Audit is a thorough assessment aimed at identifying security vulnerabilities within an application. This audit encompasses the evaluation of both the application's design and its runtime environment to detect issues like insecure coding practices, susceptibility to common attack vectors such as SQL injection and cross-site scripting, and flaws in authentication and authorization mechanisms. The goal is to provide actionable insights that help fortify the application against attacks and ensure compliance with relevant security standards.

- **Application Code Review**

Application Code Review is a detailed inspection of the source code of an application to identify security vulnerabilities, coding errors, and compliance issues. The service aims is to uncover potential security weaknesses in the applications code base such as buffer overflows, race conditions, and improper error handling. The review not only enhances the security of the application but also improves code quality and adherence to coding standards.

- **Firewall Ruleset Review**

Dionach will systematically examine the rules and policies configured in your organisations firewalls to ensure they are both effective and optimised for security. This review checks for any misconfigurations, redundant rules, overly permissive settings, and compliance with the organization's security policy. The aim is to tighten security by closing unnecessary openings in the network while maintaining the necessary access for business operations.

- **Network Infrastructure Review**

Network Infrastructure Review is a critical service that evaluates the security and integrity of an organisation's networking setup. This review includes an analysis of the physical and logical architecture, the performance and configuration of network devices, and the adherence to network security best practices. By identifying vulnerabilities and inefficiencies, the service helps to ensure that the network supports secure and stable connectivity critical for your operations.

- **Build Reviews**

Our auditing team carries out build reviews of standard operating system builds, either servers or endpoint, such as Windows 10, Windows Server, Linux servers or Mac OSX.
Build reviews are based on the appropriate standards such as the specific CIS Benchmark or the specific NCSC End-User Device Security Guidance. We carry out a full range of checks on a server VM or endpoint build that you provide.

- **Audit against Specific Government and Industry Standards**

This service involves conducting a detailed audit to assess an organisation's compliance with specific government and industry regulations and standards, such as GDPR, CAF and PCI DSS. The audit includes a comprehensive review of the policies, procedures, controls, and technologies to ensure all regulatory requirements are met. This not only helps you avoid legal and financial penalties but also builds trust with your customers and partners by demonstrating a commitment to compliance and security.

9.0 CYBER SECURITY AND INFORMATION ASSURANCE CONSULTANCY

Dionach's consultants can provide support and advice around information security and assurance related issues, for the public sector and their supporting organisations. Common services delivered by Dionach as part of this scheme are listed below. Please note that this list is not exhaustive, and so please contact Dionach to discuss your individual needs in more detail.

- **Production and Review of RMADS**

RMADS – Risk Management and Accreditation Document Sets provide an overall appraisal of the risk level and profile of a given environment or infrastructure. The production of RMADS depends upon the Impact Level (IL) of a given environment or infrastructure; for low IL systems, an audit against the international standard ISO 27001:2013 may be more appropriate, and Dionach can assist with this, whilst for high IL systems, RMADS are mandatory.

- **Security Architecture Consultancy**

As experienced information security consultants, cyber security incident responders, auditors and IT service professionals, Dionach are able to advise on proposed security architecture designs for a wide range of projects. This advice can take the form of a trusted-advisory support provision, review of existing or planned infrastructure, or proposed architecture designs.

- **Risk Assessment and Management Consultancy**

Dionach have many years of experience in both risk assessment and risk management processes. Dionach can perform risk assessment activities for your organisation, support or review existing internal processes, review or recommend risk treatment, management or mitigation plans, or advise on other supporting technical services.

- **Advice and Support for HMG and NCSC Policies and Standards Compliance**

This includes consultancy in areas related to the Security Policy Framework, NCSC Guidance and Code of Connection requirements. This could take the form of risk assessments, security architecture reviews, or planning for new information processing systems.

- **Penetration Testing and Vulnerability Analysis Review and Support**

Our CHECK accredited team hold a minimum security clearance level of SC, and can assist you in determining the appropriate engagement scope for penetration testing. They can also support you in interpreting the results of any other testing previously undertaken.

dionach

10.0QUALIFICATIONS AND ACCREDITATIONS