**ETHICAL HACKING / PENETRATION TESTING PROFILE**

Datawarrior offers intense and customised services in this category which are provided by our highly qualified and experienced team, managed by our Team Leader whose personal qualifications and experience are provided below.

**WHAT IS IT?**

This service is a personalized offering based on hours of system scoping during which interviews with operational management includes examination of a client’s exclusive infrastructure, customised systems, and areas of operation. This process of personalized attention to detail is of paramount importance.

**WHAT IS IT NOT?**

This is most definitely not an off the shelf software application which runs an unchartered and unmanned system scan to spit out a penetration test result. We offer an in-depth personalised service, customised to your requirement. DIY solutions inevitably leads to later consultation costs and damage control of greater proportions than any professional approach from the outset.

**WE TRY TO PROVIDE ALL COSTS UP FRONT!**

**Just remember, a criminal hacker has all the time in the world to attack you, we have only days or weeks to find the real vulnerabilities and the weaknesses exploited by criminals.**

**Ongoing services in this regard are therefore essential in the battle against cybercrime.**

**THE SERVICES PORTFOLIO**

The services are provided in two phases, allowing the business Executive to decide on ongoing costs based on real risk factor reporting:

**Phase 1** In this phase, we include the face-to-face discovery and scoping of the customer’s systems and infrastructure, as well as 3 weeks of intense testing as described in our Services section. Ongoing cost implications thereafter become a choice for the customer as Phase 2.

**Phase 2** This phase is based on Phase 1 results-driven application of ongoing vulnerability studies whilst remedial action is being undertaken. This phase is an annual time-based contract for ensuring continued reporting and further adjustment to remedies.

***Flexible payment plans allow for easier decision making by IT Executives.***

**The summarized specifics** of the first phase of the portfolio include:

•      All pre-engagement Interactions & interviewing

•      System and Infrastructure overviews

* Intelligence Gathering

•      Threat modelling

•      Vulnerability Analyses

•      Exploitation potential assessment

•      Post Exploitation discussions

* Remedial consultations

•      Report provision

* Time limited to 5 weeks including expanded hours option

**Specific areas of concentration**:

* Passive Information Collection: Using specialized internet portals, search engines and social networks in order to collect information that may be useful on portals, services, technologies, collaborators and/or users. *Using various tools and experiences to obtain passive information not read by automatic tools*;
* Active Information Collection: in this phase there will be direct, non-offensive access to the various portals and online services, in order to better identify and confirm the technologies used. According to the specificities of the portals, *manual tests will also be carried out in order to obtain information that escapes automatic tools*;
* Identification of vulnerabilities in the security perimeter (DMZ), servers and web applications: after performing the survey of all information passively and actively, customized tests will be carried out on the technologies identified in the servers and web portals. The test points will depend on what is identified in the information collection phases, as well as on the results that arise in this same phase, but in a generic way will be tested, where applicable by Cross Site Scripting (XSS) vulnerabilities, Blind Structured Query Language Injection (Blind Sqli), Sqli, vulnerabilities in Procedural Language/Structured Query Language (PL/SQL), Remote File Inclusion (RFI), Cookies, Javascript, Applets, Flash Code, Digital Certificates, Fuzzing (IP, TCP, UDP.
* Identification of vulnerabilities in other services such as SNMP/POP3/IMAP, NTP, VPN SSL/IPSEC, DNS, FTP, HTTP/HTTPS, among others: Post the survey of all information passively and actively, customized tests will be performed on the technologies identified on the servers;
* Exploitation Zero-day/Zero-hour: if vulnerabilities are discovered and in order to eliminate false positives, it will be simulated in the laboratory under approximate conditions, in order to validate whether the identified failures are confirmed, and if so, at what level of severity. The malware vs exploitation lab (Hardsecure public exploits and/or exploits) exists on Hardsecure premises and proprietary tools will be used.
* In addition, code development demonstrating the usability of detected vulnerabilities will be carried out if none are publicly available either in Internet databases or through open source and/or commercial tools;
* Intrusion testing: Whenever a critical vulnerability is confirmed, the entity will be promptly informed in order to minimize the time of exposure to the security failure (categorized as Severe or Very Severe vulnerability). The tools to be used are available in portals and exploits developed by Hardsecure, if necessary. Intrusion testing shall be carried out as vulnerabilities are identified to enable it to be carried out.
* Land Attacks (Denial of Service attacks): attacks on availability using generic Denial of Service (Denial of Service - Dos) tools. Specific tools may be used or developed according to possible vulnerabilities that may be detected.

**RESOURCES QUALIFICATIONS**

Datawarrior’s Managing Consultant of DPSaaS, (Data Protection & Security as a Service) personally supervises and manages each case of ethical hacking and penetration testing. The relevant qualifications and experiences are provided hereunder.

General

* Manager in Technology Consulting Services - Cybersecurity since 2013
* Domains: Audit Managing ISMS implementation Projects ISO 27001 (Information Security) ISO 22301 (Business Continuity) - Risk Management & Security Governance Security Systems Architecture - PCI-DSS
* University Lecturer on data systems and security

Skillsets

* ISO/IEC 27001:2013 Lead Implementer
* ISO 22301:2012 Lead Implementer
* Risk Manager (ISO 31000)
* Risk Manager ISO 27005:2018
* ISO/IEC 27017:2015 - Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
* CEH - EC-Council Certified Ethical Hacker
* GRC

Professional experience

* Many and varied Business Continuity Management Projects based on ISO 22301, including Business Impact Analysis, Risk Assessment, Business Continuity Strategy, Test Coordination and Exercises;
* IT strategic planning aligned with strategic business objectives, which covered the definition of a Reference Functional Architecture, Gap Assessment based on functional and technical perspectives, study of multiple scenarios for IT Architecture and its Organization
* Roadmap of projects and corresponding Business Cases in finance banking sector;
* Varied Information Security Management Projects based on ISO 27001, CIS Critical Security Controls, including the definition of security policies, procedures and plans;
* Operational risk assessment based on ISO 27005 & ISO 31000 in several well-known financial organizations;
* Definition and implementation of the privacy program in various organizations to comply with GDPR
* Definition and design of information security controls, based on ISO 27K and NIST CSF focused on access control, change management in the financial and automotive sectors;
* Experience in implementing PKI infrastructures and digital certificates in the banking sector;
* Development of strategic information security plans and internal controls;
* Experience in Banking and Capital Markets;
* Experience in Automotive Industry; and
* Experience in implementing Identity and Access Management solutions.

**Relevant History**

**DATAWARRIOR LDA: INTERNATIONAL CYBERSECURITY EXPERT & IT NOMAD**

**O C TO B E R 2 0 2 0 — P R E S E N T**

* Head of Data Security and Protection, and Advisor on Board of Directors
* General Cybersecurity consulting
* Penetration testing and vulnerability studies
* Audit of Information Systems;
* Information Security Consulting;
* Cyber Forensic Investigation;
* Security Systems Architecture;
* Project and team management;
* Internal Audits;
* Managing ISMS implementation projects;
* Drafting the ISMS context based on the needs of an organization;
* Participating and mentoring on information security training and awareness sessions;
* Drafting information security policies;

**HARDSECURE: INFORMATION SYSTEMS PROTECTION MANAGER**

**A P R I L 2 0 1 8 — O C TO B E R 2 0 2 0**

* Audit of Information Systems;
* Pentesting Team Management
* Information Security Consulting;
* Cyber Forensic Investigation;
* Security Systems Architecture;
* Project and team management;
* Internal Audit;
* Managing ISMS implementation projects;
* Drafting the ISMS context based on the needs of an organization;
* Participating and mentoring on information security training and awareness sessions;
* Drafting information security policies;
* Participating on internal audit programme development as part of ISMS implementation; Elaboration of policies and procedures within the scope of ISO27001;
* SOC Manager;

**VISIONWARE: Information Security Auditor and Consultant**

**S E P T E M B E R 2 0 1 3 — M A R C H 2 0 1 8**

* Audit of Information Systems;
* Information Security Consulting;
* Compliance;
* Security Systems Architecture;
* Project and team management;
* Internal Audit;
* Managing ISMS implementation projects;
* Drafting the ISMS context based on the needs of an organization;
* Participating and mentoring on information security training and awareness sessions;

**CONTACT US BEFORE ITS TOO LATE**

**Sales@datawarrrior.pt**