Serious About Security & Compliance

Service Definition

Version: 1.0

Date: 14/07/2020

Tel: +44 (0) 1302 639470 Email: info@digitalxraid.com Web: https://www.digitalxraid.com

SUITE 9a: CAVENDISH COURT, DONCASTER, SOUTH YORKSHIRE, DN1 2DJ

DOCUMENT CONTROL

Change Control Table

Date:	Version Number:	Changed by:	Summary of Changes:
10/01/2020	0.1	SG	Internal Review
19/01/2020	1.0	RJ	Final Issue

Table of Contents

1 INTRODUCTION

1.1 Company Brief

DigitalXRAID was formed in 2015, the two founders identified a significant GAP in the market for a risk based approach to the implementation of information security services. Add to this the shortage of reliable services, they knew the GAP could be bridged with improved services which in turn would secure more organisations. There is no quick fix when it comes to securing your organisation. Implementing Information Security correctly is a journey, one that takes time and careful management. Building a team of highly certified industry experts has been the heart of DigitalXRAID, leading them to be an award winning, leading Cyber Security partner. DigitalXRAID is fully certified to ISO, CHECK and CREST Standards, proudly being the **6th fully certified CREST Security Operations Centre in the world.**

We pride ourselves on our agility and ability to service our clients to the highest standards.

DigitalXRAID is not a traditional bolt on service, we become your security team. We care about your organisation like it was our own and we know backed by our skilled professionals we can develop a robust security framework.

Our partnership approach will provide the support and protection for our customers enabling them concentrate on delivering service and key projects with the assurance their cyber roadmap is clearly defined with a partner who can support them through their journey of security maturity.

1.2 Our Vision

To be recognised as the UK's leading cyber security company, giving our global clients complete peace of mind. Our cutting-edge innovation, expertise and unrivalled service mean we will take care of your security whilst you take care of business!

1.3 Our Mission

To stay ahead of the curve by continually learning and improving our skills and knowledge, enabling us to provide the best possible protection for our clients.

We break boundaries and explore the dark evolving world of cyber by identifying emerging threats that could carry devastating consequences for our customers.

Providing 24/7 all year round, robust state-of-the-art cyber security solutions. We never sleep, so our customers can. We pride ourselves on delivering the best possible customer service, arming our clients with the support and knowledge they need to fight back against the cyber criminals.

1.4 Our Values (The basis on which we provide all our services.)

- **One team.**
  We Share The Load; We Support Each Other, Together We Are Stronger.
- **Customer First.**
  They Are The Heart of The Business; We Love Them.
- **Have Fun.**
  We Find The Fun In Everything We Do; We Smile, We are never Mood Hoovers.
- **Be The Best Version of Yourself.**
  We show that we Care, We Make Things Better, We Are Great Role Models For Others.
- **It's Good Enough is NOT Good Enough.**
  We Challenge Ourselves & Others & Strive For Excellence.
- **See it Through.**
  We are Accountable; We Take Ownership, No Excuses.

1.5 Our Services & Accreditations

We offer a comprehensive range of services and packages to suit your organisational needs, ranging from fully managed security services to individual bespoke packages. All our solutions are created with your organisation's security as the key deliverable. Our flexible approach allows customers to pick and choose the solutions that best suit their organisational needs. Additional elements can be bolted on at any time as your organisational requirements evolve.

Additional Services Include;

- 24/7/365 CREST Accredited Advanced Threat Detection SOC
- All Penetration Testing Services
- Red Team Exercises
- HarpoonX Managed Phishing and Training
- ISO-27001 Implementation & Management
- Cyber Essentials Certification
- Incident Response and Forensics
- Vulnerability Assessment and Management
- PCI-DSS Consultancy
- IT Health Check (ITHC) PSN Compliance
- Cyber Security Consultancy
- Cloud Security Reviews
- Managed SIEM and Endpoint detection.

Don't just take our word for it, our status is backed up by our extensive certifications.

- CHECK approved (National Cyber Security Centre/GCHQ Endorsed)
- Cyber Essentials Certification Body for both CREST and IASME
- CREST Certified Security Operations Centre
- IASME Gold Certified Company
- ISO-9001 Certified
- ISO-27001 Certified
- ISO 2000 Certified
- Cyber Essentials Plus Certified

Our staff hold the following certifications;

- CHECK Team Leader (CTL)
- Crest Registered Testers (CRT)
- Offensive Security Certified Professional (OSCP)
- Cyber Scheme Team Members
- Cisco Certified Internetworking Expert (CCIE Security)
- Certified Information Systems Security Professional (CISSP)
- TOGAF certified architects
- ISO 27001 Lead Implementer
- IASME Auditor including GDPR
- Along with holding relevant degrees in information security or forensics.

1.6 Current customers

DigitalXRAID has approximately 1500 active customers ranging from government bodies including councils and NHS trusts, international football clubs, large well known retailers and manufacturing based organisations. These companies use a whole range of our services and we pride ourselves on our customer retention rates.

1.7 Our Social Values

DigitalXRAID Ltd is committed to the promotion of equal opportunities in employment. DigitalXRAID believe all employees and potential candidates should be treated fairly in all day-to-day activities and work-related decisions, embracing people's differences and facilitating a more diverse workforce. We employ the most suitable candidate for each role, regardless of:

- Age;
- Disability;
- Gender reassignment;

- Marital or civil partnership status;
- Pregnancy or maternity;
- Race;
- Colour;
- Nationality
- Ethnic;
- National origin;
- Religion or belief;
- Gender;
- Sexual Preference.

Recruitment, promotion, and other selection exercises such as redundancy selection will be conducted on the basis of merit, against objective criteria that avoids discrimination. Shortlisting should be done by more than one person and with the involvement of the Human Resources Department, where possible. Our recruitment procedures should be reviewed regularly to ensure that individuals are treated on the basis of their relevant merits and abilities. Vacancies should generally be advertised to a diverse section of the labour market and during interviews, candidates should not be asked questions which might suggest an intention to discriminate on grounds the above.

We promote equality and diversity across the organisation, appointing senior diversity champions. Employees passionate about certain social groups have the opportunity to champion and spread awareness of upcoming events in regard to this. Examples of this include; participating in gay pride, black history month and entering diversity awards. We also take the time to promote these issues with our clients and suppliers.

To ensure that our equality / diversity policy is operating effectively, and to identify groups that may be underrepresented or disadvantaged in our organisation, we monitor applicants' ethnic group, gender, disability, sexual orientation, religion and age as part of the recruitment procedure. Provision of this information is voluntary, and it will not adversely affect an individual's chances of recruitment or any other decision related to their employment. The information is removed from applications before shortlisting and kept in an anonymised format solely for the purposes stated in this policy. Analysing this data helps us take appropriate steps to avoid discrimination and improve equality and diversity.

We monitor all equality data within our organisation and annually audit our policy to ensure our compliance with government legislation and regulation.

1.8 Case Studies

At DigitalXRAID we share in our customers success and take pride in demonstrating how our values have help our customers achieve their cyber security goals.

Read what some of our customers say about how our services help them deliver their cyber security objectives.

Click the link on the customer logo's to load the case studies.

CLOUD GATEWAY	Cognism	GridDuck
"We chose DigitalXRAID for their reputation of being skilled with penetration testing and providing advice. This was our flagship product that carries sensitive data for public sector organisations and we needed someone that we felt that could help us secure this environment, point us in the right direction with any remediation activities, and DigitalXRAID delivered in a clear comprehensive manner. So much so, we engaged DigitalXRAID to help us with various other areas of our cyber posture and accreditations". Neil Briscoe – CTO	"DigitalXRAID have made our lives considerably easier with this managed ISO27001 service. Although we are always conscious about our information security, implementing ISO27001 was a big task that was going to be difficult not only to implement but maintain. DigitalXRAID have taken this pain point and resolved it." James Isilay – CEO	"DigitalXRAID had the perfect level of technical expertise and account management to make our experience with them even better than expected. The devices are now very secure, but we know that we need to continue to ensure the devices are secure. Since our initial penetration testing we have approached DigitalXRAID again for further cyber security work and they have proved to be a key security partner for our business." Richard Tolley - CTO

To read more about how we have helped our customer please follow the link below to read more case studies.

https://www.digitalxraid.com/case-studies/

2 SERVICE DESCRIPTION

Description

This type of testing assesses security through the eyes of an attacker attempting to identify weaknesses in the web application(s). Web application penetration tests can be conducted remotely from DigitalXRAID's network or from an internal perspective. The tests will observe whether vulnerabilities within the web application(s) could result in a foothold being obtained by an attacker, which could lead to the compromise of the application and the data held within. Testers will assess the web application from an unauthenticated and authenticated perspective, where applicable, and determine whether the web application(s) can be compromised or do not adhere to security best practices.

Technical Benefits

- Hidden Vulnerabilities Exposure – Penetration testing identifies unknown vulnerabilities that may not be evident through automated scanning tools, addressing potential weaknesses in the organisation's security.
- Attack Simulation – Testers simulate realistic attack scenarios, employing techniques real attackers use to evaluate the effectiveness of security and response mechanisms from the environment.
- Custom Exploitation Techniques – Skilled testers employ custom exploitation techniques beyond known vulnerabilities, ensuring a thorough evaluation of the environment's resilience.
- Compliance Assurance – Penetration testing helps organisations meet regulatory requirements (e.g., PCI DSS, HIPAA) by identifying security gaps that could lead to violations.
- Strategic Insight – The results guide strategic security decisions, allowing organisations to allocate resources more effectively for future security improvements.

Methodology

DigitalXRAID uses various tools and techniques to complete the agreed-upon penetration testing methodology. Testing is performed using an advanced testing methodology that is comprised of years of experience and aligned closely with the Open Web Application Security Project (OWASP), the Open Source Security Testing Methodology Manual (OSSTMM), and other industry standards. The high-level overview is outlined below with a brief description of, but not limited to, what is assessed during each section.

- Information Leakage - Reviewing the application configuration to ensure that information is not being leaked. This is assessed by reviewing configurations, fingerprinting the underlying server technology of the application framework and examining how the application communicates content to discover information disclosure that could cause a security risk.

- Secure Configurations - Analysing the deployed configuration of the server hosting the web application and verifying that the application server has gone through an appropriate hardening process by implementing appropriate security controls, for example, HTTP security headers and ensuring that administrative interfaces are not publicly available.

- Identity Management - Testing for account enumeration, weak registration processes, role definition and verifying that accounts can not be easily determined based on application responses.

- Input Validation - Checking that the application appropriately validates and sanitises all input from the user or the environment before using it, checking for common input validation vulnerabilities such as cross-site scripting, SQL injection, code injection, server-side attacks, and host header injection.

- Error Handling - Ensuring that the application handles errors gracefully and implements custom error pages that do not disclose sensitive information.

- Encryption - Assessing the encryption security around the transmission of communication. This includes checking for common weaknesses in SSL/TLS configurations and verifying that all sensitive data is securely transferred.

- Business Logic - Understanding how the application uses, stores and maintains data and checking whether the application processes and workflows can be bypassed. Tests are conducted to ensure that application workflows cannot be bypassed by either tampering with the parameters or forcefully browsing. Ensuring, where applicable, that file upload cannot be manipulated or allow malicious files.

- Client-side Validation - Checking that the application does not solely rely on client-side validation and appropriately validates and sanitises all input from the user or the environment before using it server-side. Checking for common client-side attacks such as HTML injection, client-side bypasses, and cross-origin resource sharing.

Authenticated Testing Only

- Authentication - Ensuring appropriate mechanisms are in place to confirm a user's identity, understanding the authentication process and using that information to circumvent the authentication mechanism, ensuring that users are required to set strong passwords and that password reset and change functionality is secure.

- Authorisation - After understanding a well-defined set of roles and privileges, attempts will be made to bypass the authorisation schema, find path-traversal vulnerabilities and Insecure Direct Object References (IDOR), and find ways to escalate the privileges assigned to the user roles provided.

- Session Management - Ensuring effective session management configurations are implemented. This broadly covers anything from how user authentication is performed to what happens when logging out. The penetration test includes testing how the session is managed and maintained, checking that the session is terminated once a user has logged out, and confirming that the session cannot be hijacked.

3 COMMERCIALS & PRICING

2.1 Expenses

When an onsite visit is required expenses are charged at cost, with a maximum of £150 per person, per day for subsistence, travel, and accommodation only and will be invoiced separately.

2.2 Payment Terms

Invoice due in full upon signed acceptance in accordance with our standard 30 day credit payment terms. Payment will be paid in full within 30 days of invoice whether the projects has started or is part way complete.
Invoice due in 50% instalments. The fist payment of 50% invoice value is due 7 days from when the invoice is issued and is required before any works are carried out. The remainder is due 7 days after completion of the engagement.

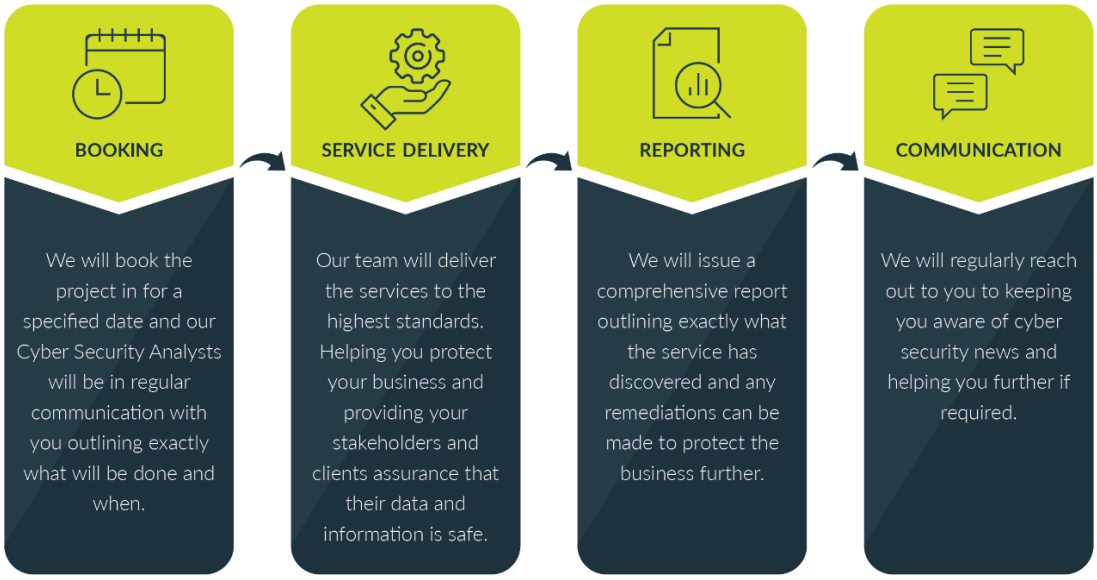
2.3 Re-testing of discovered High and Critical Vulnerabilities

Any external re-testing will be completed free of charge to the limit of one days effort to confirm mitigation steps have been successful. In the event of a larger number of issues being identified during the initial test, additional test days at a discounted rate will need to be purchased to complete a thorough retest.

4 SERVICE DELIVERY DISPUTE RESOLUTION

Once this scope and proposal document has been signed we can commence your cyber security services. We are committed to providing every client with a service second to none. We are looking forward to joining you in your cyber security journey.

We will be in regular communication with you throughout the process to ensure you are happy with the progress.



Disputes will be resolved using our complaints process in accordance to our membership to CREST, CHECK and ISO9001 standards. As an extension of your team any issues will be handled with the upmost importance and escalated to senior management immediately.