Periculo

Full Stack Security

Service Definitions

G-Cloud 14

Version: 1.0

Date: 02/05/2024

Penetration Testing & Vulnerability Scanning

We adhere to the Open Web Application Security Project (OWASP) standards Testing Guide v4.2, focusing on the 'Top 10' list for web & mobile applications.

For non web applications, backend services or infrastructure, we follow a version of the PTES (Penetration Testing Execution Standard), whilst also following our CREST accredited penetration testing framework.

For both the Web application and the Infrastructure penetration process, we follow the same path:

- Pre-engagement Interaction (Scoping)
- Intel Gathering
- Vulnerability Analysis
- Exploitation (Testing)
- Reporting

Scoping

As an organisation we follow repeated and measured processes, including standardised web application, infrastructure and mobile device scoping. To ensure that we have identified the correct scope, a scoping form must be completed at the first instance.

Following this process ensures that your organisation is provided with a full, comprehensive view of your security posture at all points identified in the scope.

Intelligence Gathering

Once the scope and the testing time frame has been agreed, the discovery phase will start in the allowed scope and time frame. The discovery phase consists of scanning the allowed scope assets as well as open/public source information sources, for information on assets in the scope, technology used and any useful information on the allowed scope.

Vulnerability analysis

During the Vulnerability analysis phase we are actively looking for any vulnerabilities that might be in the allowed scope of assets, this is done both by manually testing and by using automated tools. During this phase new information might be uncovered that will be joined with information collected during the Intelligence Gathering phase

Testing

Once we have completed the information gathering and vulnerability analysis phase we will use that information to attempt to exploit any possible vulnerabilities or weaknesses that were uncovered.

For Web Application testing stage we focus on the following areas;

- leakage checks
- Authentication controls
- Authorisation controls
- Session Management
- Data validation and injection
- encryption
- Transport security
- Business logic
- Client-side vulnerabilities

For Infrastructure testing stage we focus on the following areas;

- Exploitation of know vulnerabilities
- Access controls
- Whitelist Bypass
- Authentication controls
- Bruteforce authentication
- Code injection
- Access to internal network
- Man in the middle type weakness
- Domain takeover type weakness

Testing/Exploitation will only be done on the allowed scope. If during this phase, or any other, a major weakness or vulnerability is discovered this will be communicated to the lead contact but wont be included in the final report and will not be tested/exploited. Unless we receive explicit authorization to include that area into the scope, at which point it will be tested and added to the report.

Reporting

We finish the process with a reporting cycle which will summarise the results of the security test including a detailed description, steps to reproduce the issue, remediation and recommendations when applicable.

Our vulnerability scoring uses the Common Vulnerability Scoring System version 3 (CVSS) to ensure a uniform approach.

Cloud Infrastructure Security Testing

Our Cloud Infrastructure Security Testing service encompasses a rigorous three-phase process tailored to your specific environment of either Azure, Google Cloud, or AWS.

Scoping

We begin with an in-depth scoping phase where we collaborate with your team to define the testing perimeter, aligning our objectives with your security goals. This includes identifying critical assets, selecting relevant security benchmarks (CIS, NIST, ISO27001, etc.), and establishing the scope of the testing environment.

Testing

Following the scoping phase, our experts conduct comprehensive security assessments using the latest tools and methodologies to identify vulnerabilities across your cloud infrastructure. We test for compliance with the agreed-upon security benchmarks and seek out any potential security gaps that could be exploited.

Reporting

The final phase involves the preparation of a detailed technical report that documents our findings. This report includes an enumeration of identified vulnerabilities, categorised by severity, and provides prioritised remediation recommendations. Our aim is to equip your team with all the necessary information to enhance your infrastructure against emerging threats.

IASME Cyber Essentials & Cyber Essentials Plus

Cyber Essentials

Cyber Essentials is an independent self-assessment certification developed by IASME in partnership with the National Cyber Security Centre. The basic Cyber Essentials certification requires organisations to assess themselves against five basic security controls. A qualified assessor then verifies the information provided and, if the answers meet the requirements of the standard, a certification is issued.

The five security controls covered by Cyber Essentials are:

1. Firewalls
2. Secure configuration
3. User access control
4. Malware protection
5. Patch management

Cyber Essentials represents the Government's minimum baseline standard for Cyber Security in the UK.

Cyber Essentials Plus

Cyber Essentials Plus is an expansion upon the Cyber Essentials self assessment. Cyber Essentials Plus still has the Cyber Essentials trademark simplicity of approach, and the

protections organisations need to put in place are the same, but for Cyber Essentials Plus a technical verification is carried out. It consists of a one day external audit including a vulnerability assessment, an internal scan and a technical assessment.

The technical verification will cover the same five security controls as the Cyber Essentials self assessment.

Managed ISO27001

Our Managed ISO27001 compliance service streamlines the compliance process using our advanced compliance management system.

Delivered by a dedicated security manager, this service ensures adherence to all ISO27001 controls, simplifying the path to certification and maintaining ongoing compliance for your organisation.

Assign vCISO

An integral part of this engagement, we will assign a dedicated virtual Chief Information Security Officer (vCISO). The vCISO will serve as an advisor and strategic partner, working closely with your organisation to provide expert guidance on all information security matters.

The vCISO will assist your organisation in developing and maintaining a comprehensive information security strategy aligned with ISO27001.

This dedicated resource will ensure that your organisation benefits from proactive risk management, robust security controls, and ongoing support to maintain ISO27001 compliance and strengthen your cyber resilience.

Onboard to Harpe

Throughout this process, our compliance management tool, Harpe, will serve as a central hub for the development of the ISMS. This tool streamlines the process, fostering efficient

collaboration and providing a structured framework for the ongoing management and enhancement of your security systems.

Develop ISMS

The vCISO will conduct a thorough review to assess the current state of the ISMS at your organisation.

Following the review, we collaboratively develop a maintenance and enhancement plan for the ISMS. This plan is crafted to align with industry standards, ensuring the highest levels of security and operational excellence.

Schedule Security Testing

By systematically scheduling and executing quarterly vulnerability scanning and annual penetration testing (where applicable), we proactively identify and address security risks within your website, application or platform, contributing to the continuous improvement of your information security measures.

Monthly progress updates and review meetings

We will hold monthly progress updates and review meetings to ensure that the project is on track and identify areas for improvement.

These meetings will provide an opportunity to review progress, discuss any issues that arise, and ensure that the project is aligned with your business goals.

The benefit of these meetings is improved communication, better project management, and increased likelihood of success.

NHS DSPT Audit

Our Independent Audit of the NHS Data Security and Protection Toolkit (DSPT) is designed to ensure healthcare organisations meet the stringent data security and protection requirements set forth by NHS England.

This service focuses on the 13 mandatory assertions required for compliance, providing a thorough evaluation and validation of your organisation's adherence to these standards.

Pre-Assessment Review

Prior to the assessment, we conduct a review of your organisation's DSP Toolkit self-assessment to understand your current compliance status and prepare for the detailed evaluation.

Preliminary Consultation

A preliminary call is held with your organisation to discuss the purpose of the assessment, clarify the in-scope mandatory assertions, and agree on access to necessary artefacts that support evidence texts to be examined.

Document Review

We review the artefacts provided in relation to our evidence text request. This review primarily focuses on those documents that are in scope of the mandatory assertions, and includes additional documentation to enhance our understanding of your organisation and better meet the assessment objectives.

Stakeholder Meetings Arrangement

Before the audit, meetings are scheduled with key stakeholders needed for the successful completion of the assessment.

Stakeholder Interviews

During the audit, interviews are conducted with relevant stakeholders who are responsible for each of the assertions, evidence texts, self-assessment responses, or the people, processes, and technology involved in the in-scope control environment.

Operational Review

We carry out a review of a subset of evidence texts relating to each in-scope assertion and key technical controls using the DSP Toolkit Independent Assessment Framework.

Discussion on Additional Frameworks

During the audit we will advise on other security frameworks and standards, such as Cyber Essentials, ISO 27001, and CIS, to identify any weaknesses and facilitate potential remediation efforts.

Phishing Campaign

Our phishing campaign service offers tailored simulations designed to enhance cybersecurity awareness within your organisation.

By customising scenarios to your specific environment, we identify vulnerabilities in staff email practices, providing detailed insights and actionable recommendations.

This personalised approach increases vigilance and strengthens defences against real phishing threats.

Campaign Generation

We work closely with you to understand goals, objectives, and specific requirements for the campaign.

We will identify potential attack vectors and develop a tailored strategy by creating customised and realistic email templates or SMS messages that mimic legitimate communication.

These are designed to entice recipients into taking specific actions, such as clicking on a malicious link or providing sensitive information.

Targeted Campaign

Using Harpe, our security management tool, we automate the targeted phishing campaign. The tool allows us to precisely select the intended recipients based on job roles, departments, or other specified criteria.

Each recipient receives a carefully crafted email or SMS designed to test their resilience against social engineering techniques.

Monitoring and Data Collection

Throughout the campaign, we closely monitor the delivery, opening, and interaction rates of the phishing messages. This data provides valuable insights into employee behaviour, susceptibility to phishing attacks, and overall security awareness within the organisation.

Reporting

After the campaign concludes, we analyse the collected data, including the number of clicks, responses, or other metrics.

We provide a detailed report outlining the objectives, methodologies, findings, and recommendations for improving employee awareness and security measures.

Training and Awareness

Following the campaign, we can conduct training sessions to educate employees about social engineering threats and enhance awareness.

This includes guidance on identifying phishing emails, safe practices for handling suspicious emails, and best practices for maintaining a strong security posture.

Secure Application Code Review

Our secure application code review service merges manual analysis with industry leading code review tools to assess source code for vulnerabilities.

Our skilled security engineers highlight flaws in applications often overlooked by automated tools, ensuring comprehensive security analysis.

We provide a detailed technical report of findings with recommended remediation measures.

Discovery

We begin by understanding your application architecture, technology stack, and security concerns. This initial discovery helps tailor the code review process to your specific needs and security requirements.

Scope Definition

Define the scope of the code review, focusing on critical components of the application that handle sensitive data, authentication, authorisation, and other security-critical functionalities.

Codebase Access

Arrange for secure access to your codebase. We work with your IT and development teams to establish a secure and compliant method of accessing the source code, ensuring that confidentiality and integrity are maintained throughout the review process.

Automated Scanning:

Use state-of-the-art static application security testing tools to perform an automated scan of the codebase. This helps in quickly identifying common security flaws and vulnerabilities.

Manual Inspection:

Our experienced security analysts perform a thorough manual review of the code to uncover more complex security issues that automated tools might miss. This includes reviewing code for business logic errors, insecure coding practices, and compliance with secure coding standards.

Detailed Reporting

We provide a comprehensive report detailing all discovered vulnerabilities, their potential impact, and actionable remediation guidance. The report also includes an executive summary that provides a high-level overview of the code's security posture.

Issue Prioritisation

All identified vulnerabilities are categorised and prioritised based on their severity and potential impact on the application. This prioritisation helps in focusing remediation efforts where they are most needed.

Remediation Support:

We offer guidance and support in the remediation process. Our team can assist with developing patches, suggesting code improvements, and retesting the code to ensure vulnerabilities are properly addressed.

Follow-Up Review:

Once remediation efforts are complete, perform a follow-up review to ensure all fixes are implemented correctly and that no new issues have been introduced.