INITIAL CONTACT

NDA signing

Onwelo's sales and cyber security managers' representative will contact the customer with regard to Onwelo's approaches and experience in pentesting of web applications and infrastructures.

Before sharing sensitive knowledge between the customer and Onwelo we have to sign an NDA at the arrangement stage to ensure confidentiality.

ESTIMATION OF WORK

Project requirements

Scope and goals of the audit

Based on aggregated knowledge and data from the customer's side, Onwelo will estimate pentest timelines, goals and prepare scenarios based on the customer's expectations and requirements.

Arrangements allow us to identify customer's expectations, identify current pain points and elevate our service to resolve all requirements.

CONTRACT ARRANGEMENTS

Statement of work

Kick-off

After approvals for project goals, scheduling and the financial aspect – contract arrangement is the official start point for the project.

Based on the agreed scope of work and all other determinants, Onwelo can start the project. At this stage the customer will share necessary required data such as credentials, testing environment and others.

AUDIT

Procedures & policies & infrastructure review

Management and leaders interviews

On-site physical security audit*

Evidence gathering

Evidence analysis

Depending on audit scope and goals, – Onwelo's team will perform a series of activities such as analysis of current security state, gathering evidence and identifying any potential anomalies and risks.

Based on shared procedures and policies by the customer, Onwelo will contact selected teams' managers and leaders to aggregate evidence and identify anomalies. At the customer's request we will also audit the state of physical security in the selected location.

TESTING

Vulnerability scanning*

Configuration review*

Additional security scanning*

After audit, Onwelo will offer the possibility to perform a technical analysis of the selected infrastructure scope. It will include vulnerability scanning or a configuration review to identify state of hardening, security approaches and other important aspects of security maintenance.

An additional value of audit is technical scanning and analysis of the selected scope of the customer's infrastructure. It allows policies and procedures to be compared with the real state of infrastructure and business processes.

REPORTING

Risk assessment

Reporting findings

At the customer's request we will produce dedicated versions of the report: the first for C-Board which will present findings on a business level. The second is a technical report for IT and Development teams including all necessary data and recommendations to heighten security of the selected infrastructure scope.

The most important value of each audit is a deep understanding of the problem in order to minimise and avoid this kind of risk in the future. After audit, Onwelo's Security Team will deliver a complex report with a summary for selected groups of the target (C-Board, Business Owners, Technical teams, etc.). Onwelo's Security Team will present its findings, deliver Proof of Concept for them and present recommendations in the reports cited.

SUMMARY

Report presentation

Review of findings

Review of recommendations

*optional