PRODUCT PRESENTATION

QTRUST® Check4Hack®

Are you safe?

The Check4Hack® provides you:

- Holistic overview of the status quo of IT security
- Optimal basis for further budget planning and follow-up action
- Detection of unknown potential dangers and intruders
- Support in the implementation of the GDPR (General Data Protection Regulation)

In our experience, pure prevention is no longer sufficient. Too often, we notice that the attack against which a company wants to protect itself, has already taken place in the past - companies often don‘t even notice significant attacks. For this reason, we have developed a comprehensive security assessment program, the Check4Hack. Various procedures and approaches are used in combination with highly specialized hardware and software as well as expert knowledge.

In contrast to penetration testing, we not only examine a selection of possible attack vectors, but also get a comprehensive picture of the current compromise, the most critical attack vectors and their elimination options.

Attack Vector Analysis

Together with the customer, we develop an overview of the existing IT infrastructure. Based on our experience in the military IT security area, we identify attack vectors, which we use in the subsequent tests if necessary.

Network Forensics

This module detects advanced persistent threats (APTs), complex malware, exploits and remote command & control. By using the high-end Fidelis Scout active attackers can be detected in real time and analyzed forensically. This makes it transparent which data infiltrates a network or which leave it. Attacks from the past can be detected due to the behavior of compromised devices.

Vulnerability Analysis

Based on the results of the attack vector analysis, different vulnerability scans are started on the systems to be tested. The final report gives a critical assessment of the vulnerabilities and misconfigurations found. In addition, possibilities for eliminating these vulnerabilities are shown. The focus here is on establishing the relationship between the investigation results and the financial and business risks in both, a pragmatic and analytical manner and in collaboration with our customers. The result is a clear picture of how much an attacker would have to invest to compromise the company‘s information security.

Password Audit

Password security is essential. Company passwords are checked using methods such as brute force, dictionary attack, known initial passwords, and combinations of these methods. The resulting findings provide information as to which of the passwords used are easy to break. In this way, measures can be taken to ensure and control the quality of the passwords.

Active Directory Security Audit

The Active Directory (AD) can become a threat to an organisation through vulnerabilities such as insecure processes introduced by mitigations or outdated processes. Compromising the AD can lead to full access to all computers in the corresponding domain. The AD security audit uncovers these critical gaps and assists in remediating the vulnerabilities.

QGROUP
GMBH

QGroup GmbH
Am Joseph 15
61273 Wehrheim
Germany

www.qgroup.de
+49 69 17 53 63 - 00
info@qgroup.de

WE SECURE IT.

PRODUCT PRESENTATION

QTRUST® Check4Hack®

Optional Modules

The necessity of these modules results from the implementation of the core modules.

IoT Analysis

One of the most common entry points for hackers today are IoT devices such as surveillance cameras, access points, etc. These devices firmware is rarely patched or not patched at all and are currently often not in the security focus. The QGroup supports you in closing this gap.

Penetration Testing

The penetration test usually takes place after the introduction of new (sub) systems in order to check them for their vulnerability or after a Check4Hack in order to manually track the found vulnerabilities and generally to investigate how deep one could penetrate the system. It is repeated regularly to ensure system compliance.

Social Hack

What used to be true for top companies and public authorities has now become the norm in the entire economy: espionage and targeted, destructive attacks. The attackers go beyond technical measures - social engineering means are increasingly used, i.e. social attacks on people, to improve the chances of a successful attack. Therefore, in many cases an assessment of an organization‘s technical defensive capabilities is not enough. For this reason, we offer the QGroup Social Hack, a security check that supplements technical attack vectors with the technology of social engineering. After a social hack has been carried out, holistic improvements for the security of the organisation can be derived and appropriate awareness can be created among the employees.

Optional Follow-Up Actions

- Prioritization of measures
- Determination of protection requirements
- Creating a Security Policy
- 24/7 Incident Response
- Password Audit als Managed Service

Do the

CHECK4HACK®

Then you are safe!