CriticalSecurity
security today

UAB Critical Security

Company presentation | 2021-02-10 | v1.0

About us

SECURITY TODAY. SINCE 2007

Critical Security was established in 2007 by a group of cyber security enthusiasts. Acquired by SEC Consult in 2011

Since incorporation, our main competence and focus is delivery of high-quality security assessments and penetration tests in different sophistication forms and scope contexts

In **2021** Critical Security returns to its roots and becomes an **independent cyber security consulting company**

CriticalSecurity
security today

Service portfolio

SERVICES PROVIDED BY OUR TEAM

Penetration testing

Penetration testing allows to verify the state of security of external or internal perimeter of an organization

Web application tests

Security audits of WEB applications using manual approach

Mobile app security

Our testing methodology covers iOS and Android applications as well as back-end systems

Source code review

Source code of custom applications can be examined using SAST tools and manual review by the expert

Social engineering

Human factor can be included into penetration test or conducted as a separate activity

IoT security audits

Firmware and communications mechanisms of IoT devices are covered during such test

CriticalSecurity
security today

Penetration testing

COMES IN DIFFERENT FLAVORS

- **Black-box** penetration test is performed on a network or application without any additional knowledge of the target and organization itself
- **Grey-box** penetration test approach means that an assessment team will have partial knowledge of the networks' or applications' inner-workings
- **White-box** assessment team will have knowledge of the internal structure of a network or application in order to better uncover potential vulnerabilities. This type of test is often called a glass box test due to the full visibility that the testers will have.

CriticalSecurity
security today

WEB application tests

IN DEPTH ANALYSIS

The WEB application is subjected to a range of test patterns and payloads corresponding to multiple vulnerability classes as categorized in the OWASP testing methodology. The goal is to identify as many as possible defects in a timeframe given

OWASP v4

Detailed report

Report provides information on what security measures can be applied to further improve the quality of an application

CriticalSecurity
security today

Mobile app security

Mobile application security audit can be conducted using black-box or glass-box approaches. We recommend providing source code so that inner workings of the application are revealed to the tester

SCOPE OF AUDIT

Mobile application security audit covers:

- iOS/Android (or other platform) apps
- Back-end systems and related APIs
- Usually conducted in accordance with OWASP Mobile Security Testing Guidelines methodology and OWASP Mobile Application Security Verification standard

OWASP MSTG

OWASP MASVS

CriticalSecurity
security today

Source code review

INCREASED COVERAGE

Source code reviews allow to identify more vulnerability classes in comparison to black-box tests due to visibility of inner workings and interconnections between various software components

In addition, Static Application Security Testing (SAST) tools are used to identify low-hanging fruits and ensure maximum coverage of source code provided

CriticalSecurity
security today

Social engineering

HUMANS ARE THE WEAKEST LINK IN THE INFORMATION SECURITY CHAIN

Social engineering campaigns are a tool to increase awareness in an organization

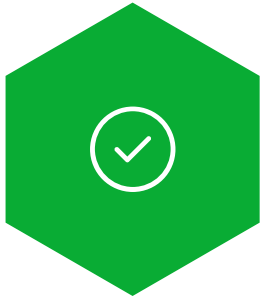
Our experts will prepare social engineering attack scenarios that fit your organization

The results are in a form of a report with all the collected user data such as login credentials

CriticalSecurity
security today

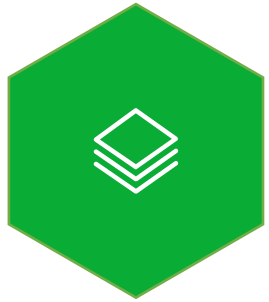
IoT and hardware security audits

CHANGING THREAT LANDSCAPE



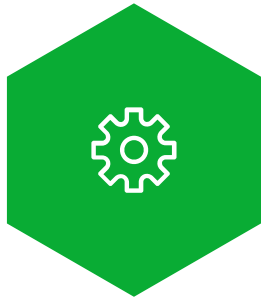
Increasing threat

Growing number of Internet of Things (IoT) devices currently means that organizations are facing additional new cybersecurity risks associated with IoT without realizing it



Firmware is key

Outdated components contain security vulnerabilities that can be exploited by attackers for their own purposes – such as running an IoT botnet



IoT security audit

Software components and communication with the cloud is audited and suggestions for improving of handling and transmission of personal data encryption are prepared.

CriticalSecurity
security today

Cloud security audits

AWS. AZURE. GCP. ORACLE

Cloud solutions have a range of in-built security features - cloud security audit ensures that security features are configured properly and best practices are followed

Cloud security audit is done in a transparent way – access to the cloud environment and architecture documentation is a must

Critical Security in media

NATIONAL CYBER SECURITY CENTRE RECOMMENDS TO CHANGE FACTORY PASSWORDS ON THE WI-FI ROUTERS

The NCSC applauds the actions of UAB Critical Security experts after discovering the bug. Responsible disclosure practices are still in the process, and this example demonstrates how the public and the private sector are able to cooperate in practice on cyber security. Submission of the information has given us the time to carry out additional investigation and inform the affected entities who then took action ahead of making the information public. We hope that making the issue of factory passwords in Wi-Fi networks public will help users to take a better care of their security," Director of the NCSC Dr. Rytis Rainys said.

SOURCE

CriticalSecurity
security today

KNOWLEDGE IS POWER

Experienced Team

Our cyber security consultants have years of experience in providing security assurance services. Most of the team members hold relevant certifications and have proven track-record in delivery of cyber security projects

Contact us

UAB Critical Security

Saulėtekio al.15, Vilnius, LT-10224, Lithuania

- **info@critical.lt**
- +370 606 75347