H-X

TANGIBLE CYBER SECURITY

Security Analysis of Source Code

Commercial Proposal

Version 1.4

www.h-x.technology

About us

H-X

H-X Technologies is an international MSSP (Managed Security Service Provider).

Our consulting services include the **assessment** and **implementation** of information security, as well as **training** and workshops.

We perform:

- ✓ Security analysis of software source code
- ✓ Vulnerability scanning
- ✓ Penetration testing
- ✓ Audits of smart contracts
- ✓ Security audit of organizations
- ✓ Implementation of security standards
- ✓ Development and implementation of IT systems
- ✓ Industrial IT audits and implementations
- ✓ Other types of audits and implementations

We cover **all stages** of the system life cycle – from planning and engineering to security management, security monitoring and incident investigations.

Our certificates

- **(ISC)2:** Certified Information Systems Security Professional (CISSP)
- **Offensive Security:** Offensive Security Certified Professional (OSCP), Offensive Security Experienced Penetration Tester (OSEP), Certified Red Teaming Expert (CRTE)
- **EC Council:** Certified Ethical Hacker (CEH)
- **ISACA:** Certified Information Security Auditor (CISA), Certified Information Security Manager (CISM)
- **BSI:** ISO 27001 Lead Auditor and ISO 27001 Implementation
- **PECB:** Certified Lead Pen Test Professional (Certified LPTP, CLPTP)
- **ISA:** ISA/IEC 62443 Cybersecurity Fundamentals Specialist (ISA/CFS)

Top ratings and testimonials

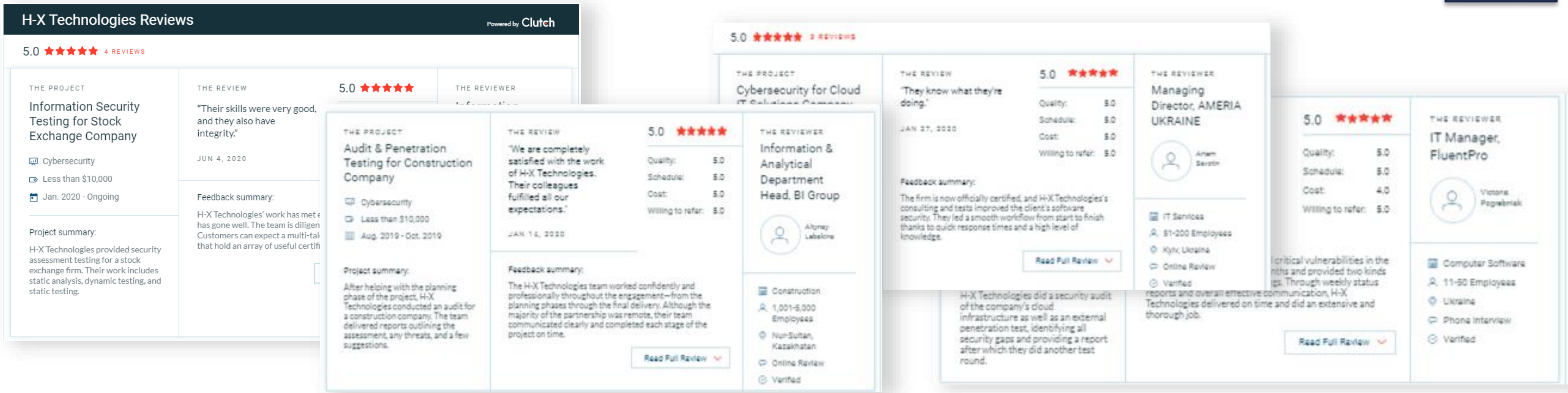
H-X

TOP
IT SERVICES
Clutch
UKRAINE
2020

BI GROUP
fluentpro
AMERIA
PIONEERING TOMORROW
favro.
HealthJoy
INTECRACY GROUP
CANTEMO
astarios

Clutch FIRMS THAT DELIVER recommendations

Check



Security Analysis of Source Code – Objectives

H-X

The objective of this analysis is security assessment of the source code of your systems or applications: checking integrity and consistency of your code, secure coding principles, finding unsafe or deprecated functions, hidden logical bombs and traps, backdoors, undocumented features, non-optimal coding practices, and OWASP top 10 vulnerabilities:

- A1:2017-Injection
- A2:2017-Broken Authentication
- A3:2017-Sensitive Data Exposure
- A4:2017-XML External Entities (XXE)
- A5:2017-Broken Access Control
- A6:2017-Security Misconfiguration
- A7:2017-Cross-Site Scripting (XSS)
- A8:2017-Insecure Deserialization
- A9:2017-Using Components with Known Vulnerabilities
- A10:2017-Insufficient Logging&Monitoring

tm

Platforms and Languages

H-X

We support the following languages and technologies:

- **.Net/ASP.Net**
- **Java EE (JBoss, Tomcat, etc.)**
- **Java Android**
- **Objective-C/Swift iOS/MacOS**
- **PHP**
- **Javascript**
- **Python**
- **C/C++/Assembler**
- **Solidity**
- **Golang**
- **Lua**
- **your language or platform**

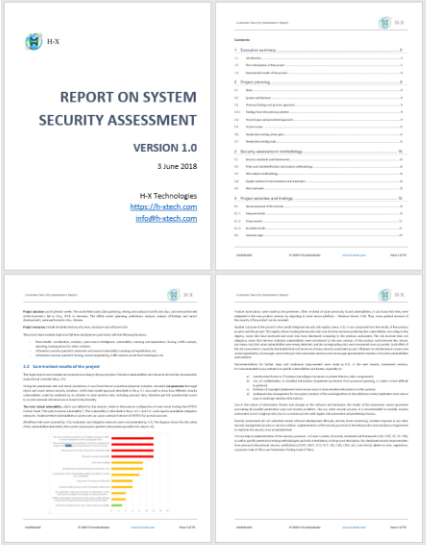
- Containers: Docker stack (Compose, Swarm, Machine, Registry), GCE Kubernetes, AWS ECS, Terraform, Vault
- Frameworks and technologies: NodeJS, Socket.IO, WebRTC, PhantomJS, YF framework, Yii, Laravel, Symfony components
- Frontend: Angular 2, AngularJS, ReactJS, JQuery, Less/Sass, Grunt/Gulp/Webpack, Bootstrap 3/4, etc.
- Mobile development (hybrid): Cordova, Ionic framework 1-4, NativeScript, ReactNative
- Desktop development (hybrid): Electron, NWJS, ReactNative
- RDBMS: MySQL / MariaDB / Percona, PostgreSQL, Oracle
- NoSQL: Redis, CouchBase, MongoDB, Cassandra, GCloud Datastorage
- Queues: RabbitMQ, Kafka, Redis, Beanstackd, AWS SQS
- Automation / CI / CD: Jenkins, GitlabCI, TravisCI, CircleCI, Ansible, Bash scripting
- Different virtualization technologies, OSes, SCM, web / proxy / mail servers, cloud and dedicated hosting services, monitoring and backup technologies, blockchain technologies, payment gateways, etc.

Methods and Results

H-X

To achieve the objectives, the auditors use two methods:

- SAST (Static Application Security Testing), which allows analyzing source code for known vulnerabilities using automated tools.
- Manual source code review and analysis, in order to reveal unsafe and non-optimal coding practices, hidden logical bombs and traps, backdoors and undocumented features.



Report on Security Analysis of Source Code includes:

- Executive summary
- Identified technical and functional vulnerabilities
- Modeling of attack vectors, proof of concept and exploitation of vulnerabilities
- Risk assessment
- Prioritized list of recommendations to mitigate identified weaknesses

Project price depends on lines of code (see next slide).

Pricing and duration

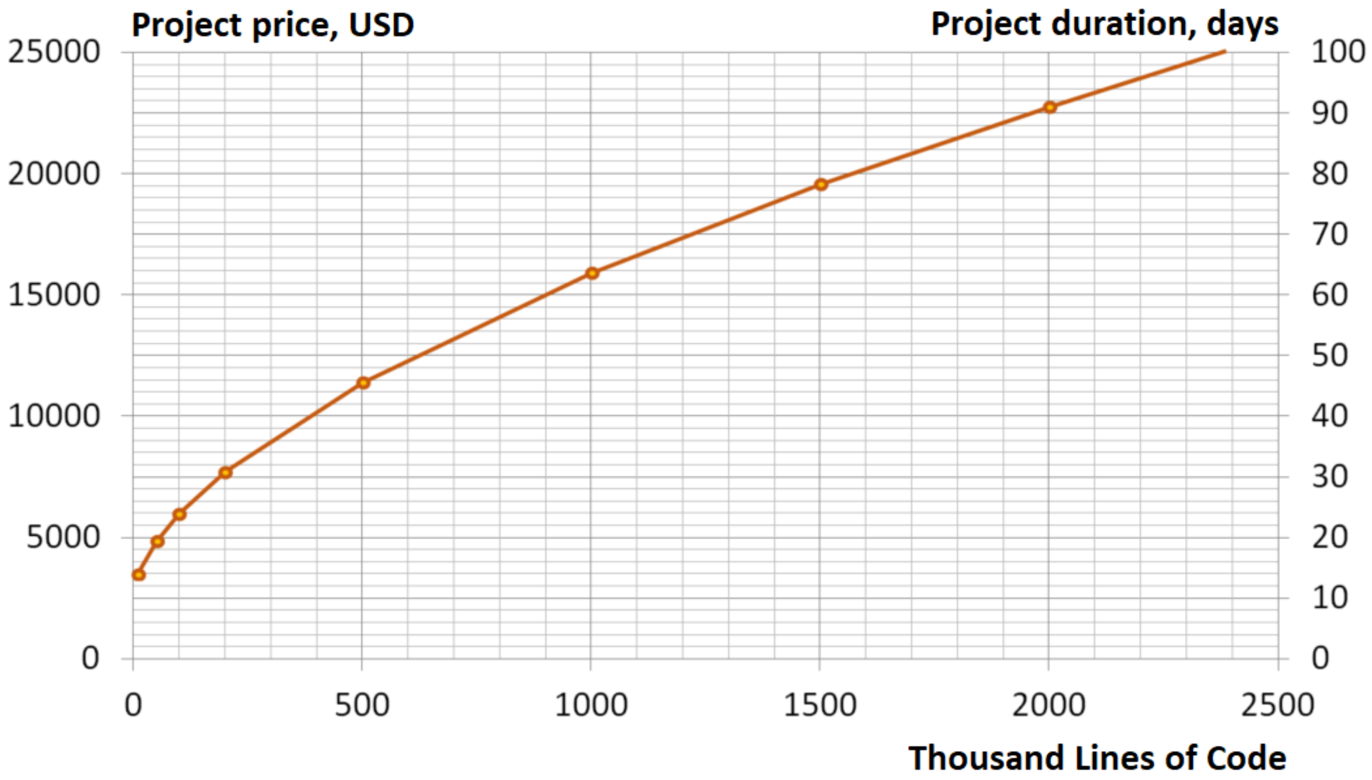
H-X

Project price and duration can be defined using the formula, the table or the diagram:

Project price = (lines of code / 1000) $^{0.6}$ *× 210 + 2650 USD*

Project duration = (lines of code / 1000) $^{0.6}$ *× 0.84 + 11 days*

Thousand lines	Days	Price, USD
10	14	3486
50	20	4846
100	24	5978
200	31	7695
500	46	11392
1000	64	15900
1500	79	19550
2000	91	22733



Security Assessment Services – How we work

H-X

Project Workflow of a typical security assessment is the following:

1. **Confidentiality.** We sign a *Non-Disclosure Agreement* and commit to confidentiality.
2. **Clarification.** You answer our questions about the conditions and environment to help us define your requirements and expectations.
3. **Engagement.** We analyze your source data and develop the *Rules of Engagement (RoE)* and the *Project plan*.
4. **Approval.** We send you a draft *Service Agreement*, and *Statement of Works* including *Specification (Rules of Engagement)* and *Project plan*. Those documents define all the specific conditions and parameters of the audit or penetration test. After you accept our offer and approve the documents, we proceed with the *Service Agreement*.
5. **Field works.** Passive audit phase begins with Open-Source Intelligence (OSINT). Active audit phase can include interviews with your personnel, vulnerability identification, verification, exploitation and evidence collection. Then we assess risks of each found vulnerability and develop recommendations on vulnerability mitigation and continuous improvement.
6. **Reporting.** The *Security Assessment Report* describes the findings and what should be done to improve your security. We consult on vulnerability mitigation and perform a retest on demand. The project is completed.

Case Study: Audit of source code for an international payment system

H-X

A brief description of the system. Our customer's electronic wallets system allows their clients to replenish the balance using bank payment cards, PerfectMoney, WebMoney, LiqPay, SWIFT and other methods. Payment card information is not transmitted or stored. In the same way, money withdrawal is possible. The wallets are multi-currency, and it is possible to exchange one currency to another inside the system at internal rates. The system has an API for integration with merchants. The main target category of users consists of Forex brokers' clients. Additionally, mobile operators and electronic stores selling mobile phones and accessories are connected to the payment system.

Technologies: modular client-server distributed architecture, cloud hosting, DBMS: PostgreSQL, MySQL, GT.M, programming languages: C++, PHP, Go, Hack, Python, M, Java, JavaScript, Perl.

Total number of lines of source code: 1.8 million.

Objective. In white-box mode, find the flaws in the architecture, insecure use of code, system vulnerabilities, and penetration methods.

Solution. During the audit, first automated, then manual code analysis was used. We identified a large number of uninitialized variables, obsolete and insecure functions that work with memory, and insufficient input validation. In some places of the code, user input was used in SQL queries without validation. This allowed us to perform SQL injection attacks and compromise the personal data of clients. We revealed an insecure data transfer, through a proxy, between the frontend and backend of some modules. This could have led to a successful implementation of a MitM attack. Weaknesses in the protection of the administrative panel were uncovered. They allowed privilege escalation of the users with Verifier and Financier roles. We identified logical errors, which could lead to bankruptcy if the perpetrator manipulated the internal currency exchange processes. Transaction logging errors were detected. We revealed logical errors in system integrity monitoring, namely, in the control calculations of transaction chains. Detailed reports were compiled for the top management, IT director and technical specialists. The reports contained descriptions of all the problems that were found and recommendations on how to solve them.

Duration of work: 3 months.

Conclusions. We provided indispensable help to the payment gateway by supplying a complete line-by-line analysis of the source code. It took much less time to analyze the code than to develop it.. With our help, the company was able to pass the PCI DSS audit successfully, obtain the official certificate, publish the gateway application and successfully begin their financial activities.

Please find more our case studies at https://www.h-x.technology/case-group/software-source-code-audit

Full-cycle Cybersecurity Services

H-X

Penetration Testing and Risk Assessment

Manual and automated vulnerability analysis and exploitation. OWASP tests, DoS/DDoS, social engineering tests, Red Team, reverse engineering, 0-day research, security review of source code of applications. Risk assessment, remediation recommendations, and reporting. Vulnerability mitigation assistance and retest after mitigation.

Security Protection and Monitoring

DDoS attack protection, Web Application Firewall management, availability protection, transaction checks, RUM (Real-User Monitoring) checks, log collection, global CDN management, optimization and acceleration of traffic for mobile devices. Hotline support in English, Ukrainian or Russian 24x7 by email or IM. Cybersecurity incident response.

Virtual Chief Information Security Officer

Outsourcing of Chief Information Security Officer (CISO) functions: security monitoring, threat hunting, security incident response, forensic investigations, application security, security compliance, personnel training, regular security assessments, internal and external reporting.

Website Security Protection and Monitoring

H-X

- Ultimate protection against DDoS attacks
- Enhanced security using Web Application Firewall (WAF)
- Protection from OWASP TOP-10 vulnerabilities
- Availability checks every 1 minute
- Transaction checks – run from the user's browser and test the important functions of the website, for example, login/registration, moving to the basket, etc.
- RUM (Real-User Monitoring) checks – test the download time of the website from the real user perspective
- Collecting and storing event logs for up to 12 months
- Global CDN for static content optimization
- Optimization and acceleration of traffic for mobile devices
- Support for IPv6, HTTP/2, SPDY, WebSockets
- Hotline support in English, Ukrainian or Russian 24x7 by email or IM
- Cybersecurity incident response (see next slide)

Subscription price: **650 USD/month**
10% off for annual subscription

Website Security Incident Response and Investigation

H-X

The Incident Response and Investigation are included in the Website Security Protection and Monitoring service:

- **Security incident response** including damage containment
- **Security incident analysis** and investigation
- Security vulnerability and risk mitigation
- Depending on the extent of the breach, the investigation can take 1 to 3 days or more
- **Forensic investigation** is needed in case you believe that your cybersecurity incident is a cybercrime and want to manage it according to local and international legal regulations, including:
  - Collecting the cybercrime evidence admissible in court.
  - Cyber forensic professional services, the rate is **650 USD/day** (without travel expenses).
  - Business trips of the cyber forensic professionals on demand.

Virtual CISO service

If you do not have a Chief Information Security Officer (CISO) role yet, you can outsource it. You can subscribe to our Virtual CISO service and get **more security functions**, in particular:

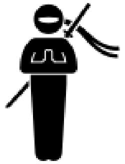
Monitor security processes, systems and events, do threat hunting

Train your software developers, testers and other personnel

Respond to all types of security incidents, including internal ones, and perform forensic investigations

Perform regular security assessments including social engineering and Red Team

Participate in your workflows, ensure application security, monitor compliance with the security requirements



Develop regular internal and external reports

Expert Rate: **60 USD/hour**

Delivery Team Management

H-X

Dennis Kudin
ISA/CFS, CISO

Andrew Buldyzhov
CIO

Glib Pakharenko
CISSP, OSCP, CISA, CTO

Vladimir Buldyzhov
CISSP, CEH, CEO

Compliance & Investigation Dept.
- Compliance Team
- Investigation Team

IT & IIOT Dept.
- Industrial Team
- Doc Team

Security Assessment & DevOps Dept.
- Assessment Team
- DevSecOps Team

Training & Consulting Dept.
- Training Team
- Consulting Team

Why our clients choose us…

…and stay with us

Best rating

We have been given the Top IT Services award by Clutch.co, a recognized authority who publishes honest testimonials.

Reliability

We value our reputation, so we strictly adhere to laws and ethics. Our specialists sign your commitment forms personally, just like your employees.

Customization

Customer’s needs are our main standard. We study and consider in detail all the nuances of your specific IT infrastructure and processes.

Expert team

We are certified professionals with decades of experience. We will bring vast and comprehensive knowledge and experience to your projects.

Quality

We not only provide one-time services, but also support the life cycle of our customers' systems using our Security Operations Center services.

Thank you for your attention!

H-X

- Feel free to ask any questions about this offer
- This offer is valid within 14 days
- Learn more about our services, projects and customers at www.h-x.technology

03035 Ukraine,
Kyiv, Provulok Khomova,
14a

+380958860891

info@h-xtech.com