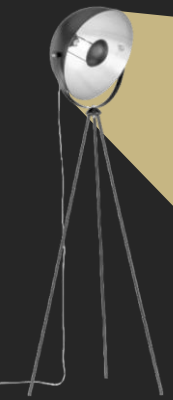
ACTIVE AUDIT AGENCY

PROVIDING CYBERSECURITY SERVICES

AAA
ACTIVE AUDIT AGENCY



ABOUT US

1

THE PHILOSOPHY OF OUR WORK

WE TAKE THIS SERIOUSLY
If there is a risk, we will find it.

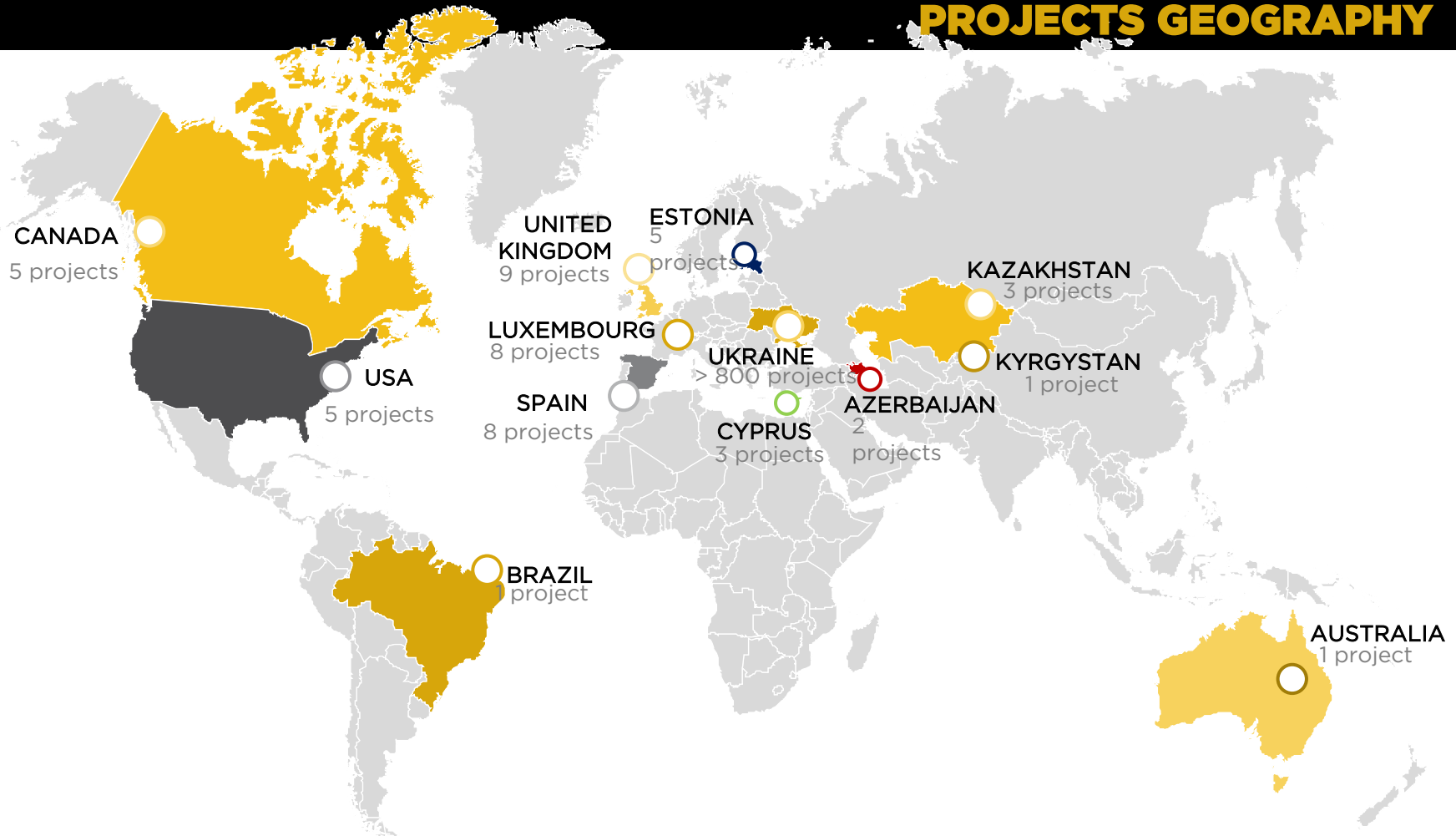
WE TAKE THIS PERSONALLY
We care about you as we care about ourselves

YOU CAN TRUST US
...like "A mother's friend's son

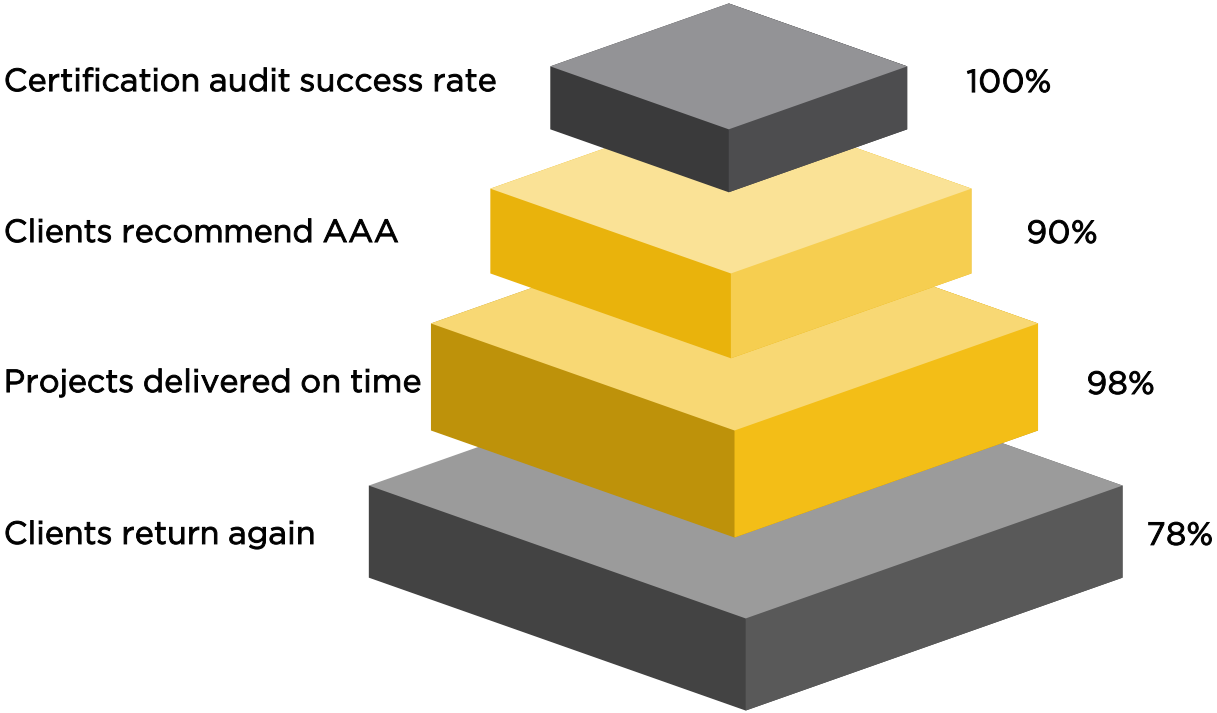
BRIEFLY ABOUT US

- Founded in 2009. 500+ projects in 15+ countries. 30+ certified experts.
- Comprehensive cybersecurity services: implementation & support of corporate information security, risk mitigation, compliance, and professional training. PECB Authorized Titanium Partner.

PROJECTS GEOGRAPHY



WHY AAA



17 years of experience — we know how an auditor thinks, so we prepare clients flawlessly

IAS accreditation (IAF MLA) — certificates without re-confirmation in 150+ countries

Specialization in IT and financial sectors — we understand your specifics

Single supplier: consulting + training + certification under one roof

COMPETENCIES BRIEF

02

WHAT WE OFFER

8 areas of cybersecurity and compliance

01

Penetration testing

Networks · Web · Mobile · API · Red Team · Cryptocurrency · TIBER-EU · PCI DSS

02

Audit and certification

ISO 27001 · 22301 · 9001 · 42001 · 37001 · EU GDPR · PCI DSS

03

Consulting and implementation

ISO · GDPR · NIST · SWIFT · PCI DSC · SOC 2 · CCSS · CIS · WLA-SCS · other frameworks&standards

04

Regulatory Compliance

NBU No143 · NBU No1 · DORA · NIS2 · CCSS ·SOC 2 · TISAX · SWIFT

05

Training and Certification

PECB Titanium · 30+ Training

06

Information Security Products and Integration

SIEM · EDR · XDR · WAF · DLP

07

AI and automation

Digital Employee
Digital Information Security Officer

08

Security Outsourcing

SOC · vCISO · Support


ING
PrivatBank
PORSCHE
Deutsche Bank
Дія
Avenga
PECB
VEON
KYIVSTAR
PROGRESS ENERGY CANADA LTD
FORTIS ALBERTA
Deloitte.
National Bank of Ukraine
MHP
AGRO & INDUSTRIAL HOLDING
otpbank
Alberta Treasury Board and Finance
ДонбасЕнерго
CIKLUM
Raiffeisen BANK AVAL
devart
НОВА ПОШТА
DTEK
AVON
ERICSSON
P2H
CONCORDBANK
Capgemini
DiPocket
ПОЛІГРАФКОМБІНАТ УКРАЇНА
CRÉDIT AGRICOLE
Volia
BIOSPHERE corporation
UMG
CRDFGLOBAL
Santander
crowdin
eleks
UIA
ЦЕНТР ГРОМАДСЬКОГО ЗДОРОВ'Я
Casino Regina
wordbee
MACROCHEM
eastone
VISEVEN
allo
ТИЦЯЙ ЩО ХОЧЕШ
OXIMIO
The SMO Group brand
ПУМБ
АТБ
uklon
Le Dogen
STUDIO
FLASH PAYMENTS
UKRSIBBANK
BNP PARIBAS GROUP
GMS
BRIEF PORTFOLIO

TEAM – OUR CERTIFICATES

Every member of our team have from 1 to 8 certifications in the field of Information Security and technical audits:

- Offensive Security Certified Professional (OSCP) by Offensive Security
- Certified Ethical Hacker by EC-council
- Penetration Tester (GPEN) by GIAC
- Certified Lead Pen Test Professional by PECB
- Certified ISO 27701 Lead Auditor by PECB
- Certified Information System Auditor (CISA) by ISACA
- Certified Information Security Manager (CISM) by ISACA
- Certified Information System Security Professional (CISSP) by ISC2
- Certified ISO/IEC 27001 Lead Auditor by PECB
- Certified ISO 27005 Risk Manager by PECB
- Certified ISO 22301 Lead Auditor/Implementer by PECB

CISA Certified Information Systems Auditor. An ISACA® Certification

CISM Certified Information Security Manager® An ISACA® Certification

CISSP® Certified Information Systems Security Professional

OFFENSIVE SECURITY OSCP

C|EH Certified Ethical Hacker

GIAC PENETRATION GPEN TESTER

PECB ISO/IEC 27001 LEAD AUDITOR

CYBERSECURITY SERVICES

03

PENETRATION TEST / RED TEAM

It is a simulation of an attack from the perspective of a potential attacker (hacker or insider) to detect and exploit found vulnerabilities in networks, software, WEB sites, physical perimeter or in the overall organization of security processes.

We have experience in security assessments of

- Network perimeter
- WEB applications and API
- Mobile applications
- Red teaming
- White-box audit (code review, architecture review, etc.)

It gives you an understanding of the real business risk from the gaps present in security processes and controls. And if your business adequately protected from hackers, insiders and other threats.

Penetration testing is needed for regulatory bodies to provide compliance with ISO 27001, GDPR, PCI DSS, HIPAA, SWIFT, NIST, etc.

Find more details on our penetration testing services at

Download pentest presentation

PENETRATION TEST THREAT MODEL

The simulated attack includes the following threat types:

A hacker from the Internet (“Black box”)

External vectors

Perimeter

Web sites

Social Engineering (Phishing)

WI-FI

oAuth (Authorization services)

API

Mobile app (both IOS & Android)

Company infrastructure

+ White Box
Network & Firewall
Security Policy Review

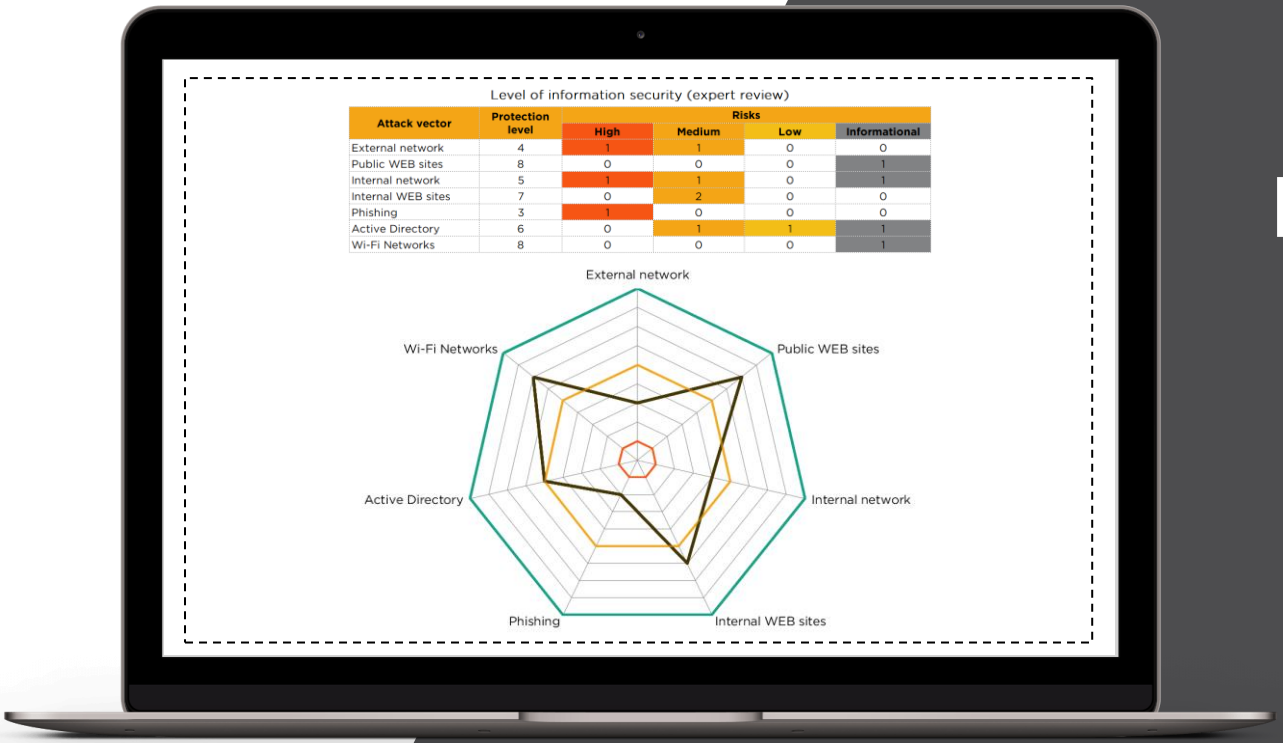
Internal vectors

Internal networks

Active Directory (simulating insider threat trying to escalate generic user privileges)

Corporate laptop hacking

An internal attacker (breach scenario)



SAMPLE HIGH-LEVEL REPORT

YOU CAN DOWNLOAD SAMPLE REPORT BY THE LINK

COMPLEX PENTEST (ENGLISH)
https://framerusercontent.com/assets/dMiMqkOq0eJMtplSB3OlomtEk.pdf

AUDITS AND CERTIFICATION

Receiving an internationally recognized certificate establishes your organization as an adaptive and flexible organization that is in pace with global best practices, which furthers customer trust in the products and/or services that you provide.

Having your organizational system/s audited by an independent third-party professional organization can be a useful tool in identifying any shortcomings of your existing systems.

On behalf of ”MSECB” certification body we provide Management Systems certification :

- **ISO 27001** – Information Security Management System
- **ISO 27701** – Privacy Information Management System
- **ISO 37001** – Anti-Bribery Management System
- **ISO 22301**– Business Continuity Management Systems
- **ISO 9001** – Quality Management Systems
- **ISO 42001** - Artificial intelligence management system

We provide compliance audits:

- **PCI DSS v.4.0.1**
- **SWIFT CSF v2024**
- **NIST**
- **COBIT 2019 (2024)**
- **WLA-SCS v.3.1**
- **MPAA CS (TPN v.6.0)**
- **CIS v8.1 Controls**
- **CCSS v 9.0**
- **Other standards**

CERTIFICATION PROCESS

Upon verifying that your organization is in compliance with the requirements of the relevant standard by means of an audit, a Management System Certification is granted. This certification is then maintained through scheduled annual surveillance audits, with the recertification audit performed on a triennial basis

**Surveillance Audit to be conducted no longer than 12 months from the previous audit*

Recertification Audit
Within two months before the triennial certificate expiration

CONSULTING AND IMPLEMENTATION

We help to implement the necessary procedures and processes based on the risk-oriented approach, as well as take all necessary measures to ensure compliance with international standards and best practices, as:

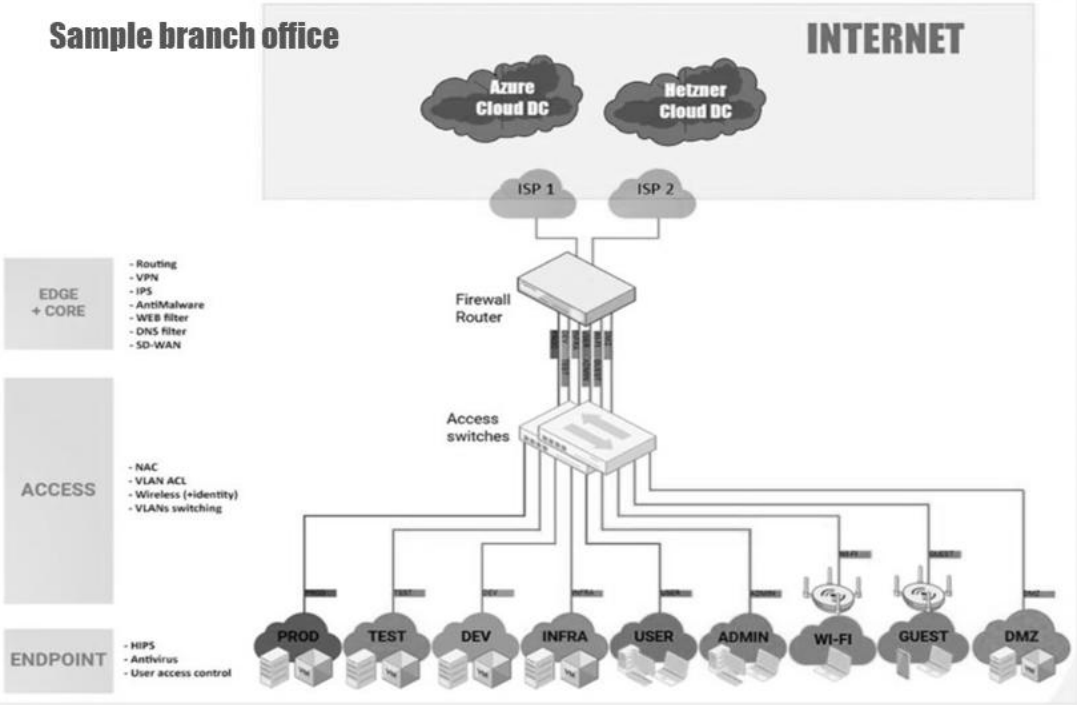
- **ISO 42001 – Artificial Intelligence Management System**
- ISO 27001 – Information Security Management System
- ISO 27701 – Personal Information Management System
- EU GDPR – Regulation in EU law on data protection and privacy
- ISO 37001 – Anti-Bribery Management System
- ISO 22301 – Business Continuity Management Systems
- ISO 9001 – Quality Management Systems
- PCI DSS – Required for Payment Card Industry
- SWIFT CSCF – Required for SWIFT users
- NIST Cybersecurity framework – Required for SWIFT users and others
- OWASP ASVS – Best practice for WEB application development
- CSA STAR – Security, Trust, Assurance & Risk Certification for clouds

As well as design security for:

- Corporate network infrastructure
- Applications
- Cloud solutions
- Producing policies and procedures to support cybersecurity Ops
- Conducting risk assessments and other cybersecurity activities as specified in the above mentioned frameworks


Information security policies
Organization of information security
Human resource security
Asset management
Access control
Cryptography
Physical and environmental security
CONSULTING AND IMPLEMENTATION
Operations security
Network security
System acquisition, development and maintenance
Supplier relationship management
Incident management
Business continuity management
Compliance management

OUR SERVICES – CONSULTING AND IMPLEMENTATION



WE HELP TO DESIGN SECURE:

- Infrastructure
- Solutions
- Applications
- Cloud

according to best practices and vendor-specific recommendations

REGULATORY COMPLIANCE

Ensuring compliance with NBU, EU, and international regulatory requirements. We help financial and non-financial institutions meet cybersecurity and data protection obligations.

We provide compliance services for

- NBU Regulation #143 — Cybersecurity for non-financial sector
- NBU Regulation #95 — Information security management system for banks
- NBU Regulation#178 – External assessments and incident reporting
- NBU Regulation#1 – Bank ID Security

- DORA — EU Digital Operational Resilience Act
- NIS2 — EU Network and Information Security Directive
- GDPR — EU General Data Protection Regulation
- AI Act – EU Artificial Intelligence Act

PCI DSS — Payment Card Industry | SWIFT CSCF — Financial Messaging Security

Our approach: Gap analysis → Controls implementation → Audit preparation → Inspection support

We provide the most up-to-date ISO trainings that are needed to succeed and assure confidence in your everyday life and globally recognized certification.

Certification provided by accredited Personnel Certification Body – PECB

SECURITY TRAININGS & PERSONNEL CERTIFICATION

- **ISO 27001** Foundation/ Lead Implementer/ Lead Auditor
- **ISO 27002** Manager/Lead Manager
- **ISO 22301 Foundation/**Lead Implementer/ Lead Auditor
- **EU GDPR** Certified Data Protection Officer
- **ISO 27701 Foundation/**Lead Implementer/ Lead Auditor
- **ISO 27017/ISO 27018** Lead Cloud Security Manager
- **ISO 37001 Foundation/**Lead Implementer/ Lead Auditor
- **ISO 27005** Risk Manager/Lead Risk Manager
- **ISO 31000** Risk Manager/Lead Risk Manager
- **ISO 9001** Foundation/ Lead Implementer/ Lead Auditor
- **ISO 22000** Foundation/ Lead Implementer/ Lead Auditor
- **Outsourcing** Lead Outsourcing Manager
- **ISO 42001 Foundation/**Lead Implementer / Lead Auditor
- **DORA** Lead Manager/NIS2 Lead Manager
- **PCI DSS** Implementation
- Certified **NIST Cybersecurity** Consultant

SECURITY TOOLS & INTEGRATION

We offer and implement top cybersecurity solutions and tools for:

- Vulnerability management
- SIEM
- Network security , NGFW
- Malware and virus detection
- User Behavior Analytics
- Application security
- Penetration testing
- Cloud security

RAPID7 nexpose
Microsoft
FORTINET
tenable network security
Bitdefender
splunk>
Acunetix by Invicti
cisco

SECURITY OUTSOURCING

WE OFFER AND IMPLEMENT TOP CYBERSECURITY SOLUTIONS AND TOOLS FOR

- SOC Operations based on Splunk
- Regular network, WebApp, mobile App vulnerability assessment
- CISO-as-a-Service
- Compliance support (SOC2, ISO27001, PCI DSS, WLA-SCS, MPAA)
- Application Code review (SAST)
- Smart Contract Audits (Blockchain, Ethereum, Solana, Polygon etc.)
- Cloud Security Assessment

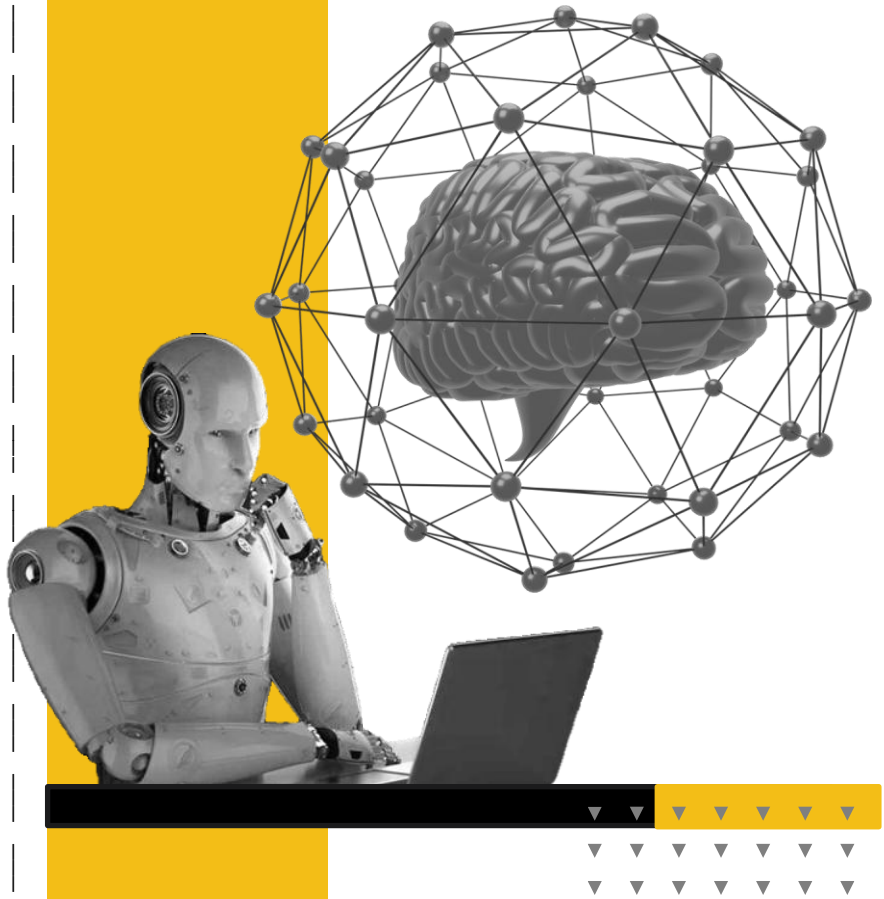
AI & PROCESS AUTOMATION

04

DIGITAL EMPLOYEE

Autonomous AI agent that runs IS processes: coordinates, reminds, prepares documents, maintains institutional memory.

- Process Orchestration — runs cases from start to close
- AI Document Generation — risk summaries, reports in minutes
- Institutional Memory — full history per asset
- Human-in-the-Loop — human approves, agent prepares
- Local Deployment — all data stays in client infrastructure
- 84% cost savings | 24/7 availability
- 2-3 FTE replacement | 11 months ROI



CONTACT US

info@audit3a.com
+38 (044) 228-15-88 | +38 (050) 464-76-06