[Pădure Alexandru]

Cybersecurity Specialist

Chișinău, Moldova • +373 60648877 • alexandru.padure@akdev.md

PROFESSIONAL SUMMARY

Cybersecurity specialist with 5 years of hands-on experience securing IT infrastructure, cloud environments, and endpoints across multiple client engagements. Strong background in security operations, incident response, vulnerability management, system hardening, and backup/disaster recovery. Comfortable working across Windows and Linux environments, Microsoft 365 and Azure, and on-premise networks. Able to translate security findings into practical remediation plans for both technical teams and business stakeholders.

CORE COMPETENCIES

Security Operations & Monitoring: Microsoft Sentinel, Wazuh, Microsoft Defender (Endpoint / 365 / Cloud), Checkmk, log analysis, alert triage, threat hunting

Incident Response & Forensics: NIST IR lifecycle, malware triage, log correlation, root-cause analysis, post-incident reporting and lessons learned

Infrastructure & System Hardening: Windows Server, Linux, Active Directory, Group Policy, CIS Benchmarks, patch management, MFA, privileged access

Network Security: Firewalls (FortiGate, pfSense, MikroTik), VPN, network segmentation, IDS/IPS, email security (SPF, DKIM, DMARC)

Cloud Security: Microsoft 365 / Azure security, IAM and conditional access, Microsoft Defender for Cloud, secure backup architectures

Vulnerability & Risk Management: Nessus, OpenVAS, OWASP Top 10, patch prioritization, risk assessments, security audits

Backup & Disaster Recovery: Veeam Backup & Replication, immutable backups, RPO/RTO planning, restore testing

Scripting & Automation: PowerShell, Bash, Python (basics), KQL for log queries

PROFESSIONAL EXPERIENCE

Cybersecurity Specialist 2023 – Present

AKDEV — Chișinău, Moldova

- Responsible for the security of IT infrastructure across multiple client environments under managed services contracts, covering endpoints, servers, networks, and Microsoft 365 / Azure tenants.
- Hardened client Windows Server and Active Directory environments according to CIS Benchmarks: tightened Group Policy, removed legacy protocols, enforced MFA, and reduced privileged accounts where possible.
- Designed and deployed backup and disaster recovery setups using Veeam Backup & Replication, including immutable backups and tested restore procedures to defend against ransomware.

- Configured and tuned monitoring with Checkmk and security alerting in Microsoft Defender / Sentinel; triaged alerts, investigated suspicious activity, and led containment of confirmed incidents.
- Performed periodic vulnerability scans (Nessus / OpenVAS) and security reviews on client infrastructure; produced prioritized remediation plans and worked with internal engineers to close findings.
- Configured perimeter and internal network security on FortiGate, pfSense, and MikroTik devices: firewall rules, VPN access, network segmentation, and IDS where applicable.
- Hardened Microsoft 365 environments: conditional access policies, anti-phishing and anti-malware rules, SPF/DKIM/DMARC, mailbox auditing, and user awareness training material.
- Acted as the security point of contact during client incidents and audits; documented procedures, wrote response runbooks, and presented findings to non-technical client stakeholders.

IT / Security Support Engineer 2021 – 2022
Clik IT — Chișinău, Moldova

- Provided day-to-day IT and security support for internal users and small business clients: workstation setup, user accounts, email, and access management.
- Assisted with basic system administration on Windows and Linux, patching, antivirus deployment, and routine security checks.
- Helped configure firewalls, VPN access, and basic network setups; learned hands-on the fundamentals of secure infrastructure operations.

TRAINING & CONTINUOUS LEARNING

- CompTIA Security+ — exam preparation course covering network security, threats and vulnerabilities, identity and access management, cryptography, risk management and incident response.
- AWS Cloud Practitioner Essentials — Amazon Web Services introductory course on cloud concepts, core AWS services, security and pricing models.
- Active Directory Security — complete course covering AD architecture, common attacks (Kerberoasting, Pass-the-Hash, Golden Ticket), GPO hardening and defensive monitoring.
- Ethical Hacking — complete course on penetration testing methodology: reconnaissance, scanning, exploitation, post-exploitation and reporting.
- Ethical Hacking with Kali Linux — hands-on training with the Kali toolset (Nmap, Metasploit, Burp Suite, Hydra, John the Ripper).
- OSINT (Open Source Intelligence) — complete course on information gathering, footprinting, public data sources and investigative techniques.
- Cisco Networking Academy — completed Introduction to Cybersecurity and Networking Essentials modules.
- TryHackMe — practical hands-on labs on SOC operations, Active Directory attacks, threat hunting and incident response.

- HackTheBox — active practitioner on offensive security labs (Windows, Linux, web).

EDUCATION

B.Sc. in Information Security (Securitate Informațională)
Technical University of Moldova (UTM) — Faculty of Computers, Informatics and Microelectronics (FCIM), Chișinău

LANGUAGES

Romanian (Native / Fluent) • **Russian** (Fluent) • **English** (Intermediate, B1 — technical reading and written communication)

Digitally signed by Colosov Alexei
Date: 2026.06.24 17:07:53 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ