Vadim Ovcearenco
str. Milescu Spataru 23 ap 248
MD- 2075, Chisinau, Republic of Moldova
Phone:+37369143294

Citizenship: Romania

vadov75@gmail.com

Information Technology Security Expert

IT&N Security specialist whose qualifications include about 15 years of experience in the creation and deployment of IT&N security solutions for protecting networks, systems, information assets and a deep understanding of information technologies. I have a big passion and interest for the field of computer security and for information technology.
I have capacity to solve complex problems involving a wide variety of information systems, to work independently and in the team on large-scale projects.
Adept at communicating with other engineers and clients in a clear and understandable manner. Able to maintain the highest standards of confidentiality in handling and protecting sensitive information.

Areas of Expertise

- Network and Systems Security
- Multi Tier Network Architectures
- Log management, monitoring and analysis
- Risk Management/Risk Assessment / Impact Analysis
- Business Continuity Management
- Vulnerability Assessments
- Public Key Infrastructure
- Cryptography
- Operation system and services security
- Web Application Security
- Active directory security
- Database Security
- Strong Authentication
- Regulatory Compliance
- Policy Planning / Implementation
- Technical Specifications Development
- Team and Project Leadership

Digitally signed by Alexeev Dmitri
Date: 2022.03.01 01:30:26 EET
Reason: MoldSign Signature
Location: Moldova

Technology summary

Security Technologies:	IBM Qradar SIEM, Fortigate IPS/Application Control/Web Filter/DNS Filter, FortiManager, FortiAnalyzer, Cisco ASA, Cisco Firepower, F5 ASM Web Application Firewall, Anti DDOS WanGuard tools, Flowmon tools (Flowmon Probe, Flowmon Collector, Flowmon Anomaly Detection System, Flowmon Application Performance module, Flowmon Traffic Recorder), RSA Netwitness SIEM, Algosec Firewall Rule Management, PAM Wallix (access manager, session manager and password manager) Cyber Ark Privileged Management tool, Qualys Vulnerability Scanner, Nessus Vulnerability Scanner, Acunetix Web Vulnerability Scanner, OWASP ZAP, BurpSuite, Fiddler, Penetration testing Parrot Security, Kali Linux, Metasploit, etc, Checkmarx, Sonarqube, PKI technologies implementation Microsoft CA/EJBCA, Cryptography and Digital signature tools implementation, Zone Central encryption tool, Microsoft Active Directory, AD Right management system, Evidian Single Sign On, Anti-Virus Tools (Symantec, McAfee, BitDefender), McAfee ePO, McAfee Endpoint Security ENS, McAfee Host DLP, McAfee Endpoint encryption for PC, McAfee TIE DXL, McAfee Advanced Threat Protection, SEP Manager, Network Security (Firewalling, NAT, IDS & IPS), VPN technologies (IPSec, SSL).
International standard compliancy	ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, PCI DSS, OWASP, CIS Benchmarks
Risk Management ISO 27005	Risk Management process, building of the process – Asset inventory, Risk assessment report and Risk treatment plan
Networking:	ISO/OSI model, LAN/WAN, VPN technologies, TCP/IP, Cisco Routers and Switches, Switch Security, Wireless Security, 802.1 X Network authentication, IP protocols and ports, network protocol and services.
Operation Systems:	Windows 7/10, Windows Server 2012, 2016, 2020, UNIX, Solaris, Linux (Red Hat, CentOS), VMware.
Software:	Microsoft Office, MS Project, Office365

Professional Experience

Mobiasbanca OTP Group SA, Chisinau, Moldova 06/2020 - Present

IT&N Security Coordinator

Responsible for implementation of information-security systems, policies and controls. Identification and evaluation of risks on all critical systems. Design and implementation of security tools, processes and procedures.

Key Achievements:

- Design, implementation and management of F5 web application firewall - ASM. Creation, maintenance and monitoring of policies for internet facing servers.
- Design, implementation and management of Wallix Access Manager and Session Manager for supplier remote access.
- Design, implementation and management of Proxy - Symantec Web Gateway, Antispam filter - Symantec Messaging Gateway.
- Implementation of DLP Network Prevent and connection to Symantec Web Gateway and Symantec Messaging Gateway.
- Starting of the project for implementation of Content Analysis System (Sandbox) and Endpoint Detection and Response.
- Identity Access Management, Creation of Application Access Matrix, performing of user inventory and access rights certification.
- Elaboration of security requirements for the new project implemented in bank.
- Audit of all Banc Firewalls, management of Access lists in network.
- Audit of DC infrastructure and elaboration of security baseline for Domain controllers, member servers and workstation
- Management of SIEM RSA Netwitness platform, log sources connection to SIEM.
- Development of company policies and procedures governing IT security.

IM Orange Moldova SA, Chisinau, Moldova 05/2011 - 06/2020

IT&N Security Coordinator

Responsible for implementation of information-security systems, policies and controls. Identification and evaluation of risks on all critical systems. Design and implementation of security tools, processes and procedures.

Key Achievements:

- Design, implementation and management of SIEM IBM QRADAR, connection to Qradar more than 1000 log sources, parsing of non-standard log sources, and creation of custom rules.
- Design, implementation and management of Fortigate intrusion prevention system, application control. Creation, maintenance and monitoring of security policies for internet facing servers. Creation and maintenance of the security policies for internal network.
- Design, implementation and management of F5 web application firewall. Creation, maintenance and monitoring of policies for internet facing servers.
- Implementation of Fortigate Web Proxy with application of security sensors (web filter, app control, antivirus) for user local network.
- Implementation of vulnerability assessment for operation system, services and web applications
- Implementation of PKI with smartcard authentication on user workstation
- Implementation of cryptographic tools Zone Central and McAfee Drive Encryption.
- Implementation and management of Evidian Single Sign On
- Design and implementation of AntiDDOS protection for company internet facing services.
- Development and implementation of information security policy and risk management procedure.

- Risk analysis of all new projects.
- ISO 27001 internal audit, elaboration of Risk assessment report and Risk treatment plan, participation in ISO 27001 company certification
- Design and implementation of threat identification for customers of fix network broadband services based on net flows from routers. Maintenance of own reputation feed.
- Implementation and managing of Mobile ID – digital signature on mobile phones.
- Implementation of McAfee Endpoint Security, Threat Prevention, Web Control, Firewall, Adaptive Threat Protection, McAfee Threat Intelligence Exchange, DXL.
- Development of company policies and procedures governing IT security (IT&N security Policy, SIEM procedure, Web Application Firewall procedure, IPS procedure, Vulnerability assessment procedure, Antivirus Procedure etc).

Service of Information and Security, Chisinau, Moldova 10/2000 - 05/2011

Head of IT security team

Responsible for implementation of information-security systems, policies and controls. Identification and evaluation of risks on all critical systems. Design and implement security systems, processes and procedures.

Key Achievements:

- Design and Implementation of national PKI system – qualified electronic signature. Building and managing of National Root Certification Authority. Development of all technical standards and documents for functioning of national certification
- Design and implementation of multilayered secured local network: DMZ, VLANs for production servers, LAN.
- Design and implementation of central log management tool.
- Design and implementation of network intrusion protection system based on CISCO ASA.
- Implementation of Active Directory, elaboration and implementation of security policies for servers and workstations.
- Implementation of centralized antimalware tool based on ESET NOD 32.
- Implementation and management of vulnerability assessment for operation system and services
- Implementation and management of cryptographic tools and smartcards for encryption.
- Performing of security system updates on a regular basis using WSUS.
- Conducted evaluation of threats to the DMZ, servers and hosts.
- Resolving of all fraud and virus infections.
- Development of company policies and procedures governing corporate security (IT&N security Policy)

Technical University of Moldova, Chisinau, Moldova 01/2000 - 10/2000

System engineer

Responsible for maintenance of local network, access to internet, development of client server application.

Key Achievements:

- Maintenance of local network, switches.
- Solving of the problem in the network.
- Development of client server application.

High Education

- **Bachelor degree in Information Technologies-** State University of Moldova. 09.1997-07.1999
- **Master degree in Networks and Information systems -**Free University of Moldova. 09.2004-03.2006

Professional Trainings

- CPENT - Certified Penetration Testing professional, Online Curs, June 2021
- CEH - Certified Ethical Hacker - Online Curs, January 2021
- CND – Certified Network Defender – Online Curs, December 2020
- Configuring F5 Advanced Web Application Firewall – Germany 2020
- Fortigate Network Security Analyst NSE 5 – Romania 2019
- Fortigate Infrastructure and Security NSE4 – Romania 2018
- Certified Information System Security Professional - Romania 2017
- Flowmon System Administrator, Online training and certification 2018
- IBM Security QRadar SIEM 7.2 Administration and Configuration, Milan 2016
- Algosec Firewall Analyzer Technical training, Online training 2016
- ISO 27001 – Introduction, Implementation and Internal Auditor, Moscow 2011
- Combating of Cyber Criminality, Chisinau 2008
- Ensuring of Network Security, Moscow 2007
- Ensuring of Cryptographic protection of information, Moscow 2004

Professional Certifications

- CEH Master
- CEH Practical
- CEH - Certified Ethical Hacker
- CND - Certified Network Defender
- CISSP – Certified Information System Security Professional
- NSE4 – Network Security Professional
- NSE5 – Network Security Analyst
- Fortimanager Specialist
- Fortianalyzer Specialist

- Flowmon System Specialist
- IBM Qradar Associate Administrator
- Algosec Administrator

Languages

- English – fluent
- French – medium
- German - medium
- Romanian – native
- Russian – native