ANDREI CHOULGA

Email: nyc9293@gmail.com / **LinkedIn:** linkedin.com/in/ac317 / **cell:** 646-714-2422 / **US Citizen for DoD**

EDUCATION:

NYU Grad M.S. in Cybersecurity: GPA 3.9/4 / Started **QRCP Q**uantum **R**esistant **C**ryptocurrency **P**roject
Brooklyn College: B.S. in Computer Information Science (2006)
Certifications: Sun Microsystems (Oracle) - SCJD, SCWCD, SCDJWS, SCEA see LinkedIn for details

PROFESSIONAL SUMMARY:

Experienced professional with 20+ years of experience in Software Development with 8+ years of experience in the Cybersecurity field, is eager to contribute to company and team success. I bring research, test-driven development, detailed planning, documentation, and dedication to my team. I thrive in both team and individual settings, and welcome challenging projects that will take my skills to the next level.

WORK EXPERIENCE:

Company: **Ameritas (ameritas.com) [financial/insurance company]** New York, NY
Position: **Sr Information Security Architect** 10.2022-present

- Evaluated and improved security for all company services and infrastructure, worked with six different dev teams,
- Created **Security Baseline Requirements** based on **NIST 800-53** controls, introduced **threat modeling**.
- Trained a security team to properly assess and triage new features for risk & work w. dev teams to remediate.
- Performed extensive **DAST** and **SAST** with API, Web and Apps, **OWASP** and **MITRE ATT&CK** based.
- via **Tenable.io** Interfaced with teams for whom vulnerability tests were done, explained what needed to be fixed.
- Managed public and hybrid cloud architectures in **AWS, Azure**
- Writing, scheduling, maintaining automated tests to check web, desktop and mobile apps (Android/iPhone) functionality in Dev, QA and Production environment.
- Performed vulnerability testing, risk analyses, security assessments on product lines for every release phase (**BurpSuite, Mimikatz, Cobalt Strike, PowerSploit**) Managed services from **CrowdStrike and Rapid7**.

Company: **Cisco - Webex team (webex.com) [mission critical video platform]** New York, NY
Position: **Cybersecurity specialist** 01.2022-08.2022

- Aligned security baseline to reflect **NIST 800-53** by breaking it down into 15 security domains for **CSDL** - Cisco Secure Development Lifecycle. Consulted Engineering teams to ensure secure development is implemented in all of our products, helped select the best solution & outcomes our security posture.
- Performed **DAST** (Invicti, Burp, ZAP) and **SAST** (Veracode). Ensuring compliance w. **FedRAMP, SOC 2, FISMA.**
- Managed and improved **Vulnerability Management lifecycle (Helped migrate from Qualys to Tenable.io)**
- Worked with developers on application security relevant to: **OWASP, SANS 25, Threat Modeling, API security, Validating Encryption and Key Mgmt, Validating Identity and Access Mgmt, Validating Client security, Security hygiene - TPSD (Third-Party Software Digitization), Static/Dynamic analysis, X.509, OAuth.**

Company: **NetworkShark (networkshark.net) [security for various FX Forex/crypto clients]** New York, NY
Position: **Cybersecurity specialist** 04.2014 - 12.2021

- Setting up **DevSecOps CICD** process automating **Qualis, Jenkins** following **NIST 800-53** controls baseline.
- Performed pen testing/**DAST** using **Burp Suite, Acunetix, Kali Linux, Metasploit, Nessus; SAST** (Checkmarx)
- Improved **Docker+Kubernetes** by setting up **Terraform** and **HashiCorp Vault**.
- designed/improved and deployed **DMZ**, Network Access Control (**NAC**), Software Defined Perimeter (**SDP**), Endpoint Detection & Response (**EDR**), Data Loss Prevention (**DLP**), configured **firewall rules**, **automated security test scripts**, troubleshooted issues by analyzing packet captures (**WireShark**).

Company: **SAXO Bank - Software Engineer** (2009-2014) **/** Company: **FXCM - Software Engineer** (2004-2009)

SKILLS/TOOLS:

Languages: C/C++, Java/J2EE, C#, Python, JavaScript (React.js/Node.JS/EmberJS/jQuery), Bash, PowerShell
Cloud: AWS - EC2, EKS, S3, IAM, RDS, KMS, CloudFormation, CloudWatch, CloudTrail // SailPoint
DB: Oracle, MongoDB, SQL, SQLite, MySQL, Cassandra, Redis **DB Tools**: IDERA, RazorSQL, Toad SQL
Static Application Security Testing (SAST): Checkmarx, GitLab, Veracode, SourceGuard, Fortify SCA
Dynamic Application Security Testing (DAST): Fortify, Web Inspect, Arachni, Coverity, Checkmarx, AppScan, Invicti, Snyk, Semgrep, Burp Suite Pro, Zap, Acunetix, Kali Linux, Metasploit, Nessus, Wireshark.
Network Security / Monitoring: Splunk, Nagios, Argus, P0f. **Proxy**: Zed Attack Proxy (ZAP), Charles, Fiddler.
SIEM platforms: Splunk, Datadog, QRadar (limited: AlienVault and LogRhythm) + Zscaler Zero Trust Exchange
Build Technologies & CD/CI: Jenkins, Teamcity, Apache Ant, Apache Maven, Docker, Kubernetes, Terraform