Alexey Laktionov

Senior Security Engineer

Princeton, NJ

267-331-0012

linkedin.com/in/alaktionov

alexey@laktionov.com

laktionov.com

@yourDomainAdmin

A senior security engineer with over 10 years of experience in IT security consulting and software development, specializing in penetration testing and web application assessment, working on Bloomberg's product security assessment team.

CERTIFICATIONS

OSWE (Offensive Security Web Expert)
License # OS-AWAE-10185

OSCP (Offensive Security Certified Professional)
105% score, License # OS-101-026327

CPSA (CREST Practitioner Security Analyst)

GXPN (Exploit Researcher and Advanced Pentester)
95% score, License # 164681

CRT (CREST Registered Penetration Tester)

OSCE (Offensive Security Certified Expert)
in-progress

PROFESSIONAL EXPERIENCE

Bloomberg, *Senior Security Engineer*
Oct 2020 – present
Princeton, NJ

Advancing security at Bloomberg by:

- Performing blackbox and whitebox penetration testing on new applications, products, and features before they are released
- Conducting security architecture and design reviews of applications and application stacks
- Reviewing source code for potential security issues
- Providing specific risk assessment and remediation guidance to developers and technical managers
- Triaging, reviewing and validating vulnerabilities identified by SAST and DAST tools
- Manually testing mobile applications and APIs
- Researching the latest security best practices, trends, threats and vulnerabilities, and technology frameworks
- Improving security review processes

Optiv, *Senior Security Consultant, Attack & Penetration Testing*
Dec 2018 – Oct 2020

Helping Fortune 100 clients perform:

- Perimeter & internal penetration testing leveraging comprehensive, targeted, evasive, non-evasive approaches
- PCI assessments and segmentation testing with the goal of accessing CDE enclave and credit card data

- Specialized targeted assessments with the goal of accessing sensitive business data stored within the company's ERP solution or a mainframe
- Web application assessments using manual testing with Burp Suite Pro and automated testing with dynamic application security testing tools like NetSparker and Fortify WebInspect
- Manual API testing using platforms such as Postman
- Attack surface management (aka continuous penetration testing) to provide visibility into the new vulnerabilities introduced by news systems and services or configuration changes made over time
- Product security assessments for new products (single devices like ATMs, kiosks, etc. or entire systems of devices) to identify weaknesses and potential attack vectors
- Social engineering assessments (phishing) to identify the “human element” risk introduced by company's employees
- Wireless assessments to uncover weaknesses that could lead to a security incident
- Vulnerability assessments to identify weaknesses and provide detailed recommendations for mitigation

World Auto Sales, *Co-Founder & Vice President* Feb 2013 – Oct 2019
Philadelphia

- Managed dealership relationship with automotive auctions and banking institutions.
- Managed auction and trade-in asset acquisitions.
- Maintained asset inventory and project management systems.
- Managed inventory exports from invent. management system to 3rd party classifieds websites.
- Maintained dealership’s compliance with PA DoT and PA DoB regulations.

Protiviti, *Senior Red Team Penetration Tester* Oct 2017 – Dec 2018
Philadelphia

- Performed PCI/external/internal penetration testing.
- Performed red teaming exercises.
- Performed web application penetration testing.
- Created and executed social engineering campaigns.
- Implemented and maintained reporting automation system (collaborative findings DB, templating, team access).

Grant Thornton, *Senior Penetration Tester* Jun 2015 – Oct 2017
Philadelphia

- Performed external/internal penetration testing and red team assessments.
- Performed web application vulnerability assessments.
- Created and executed social engineering campaigns (phishing/vishing/physical).
- Performed IT audits: network security, DB, IT general controls, IT governance.
- Developed and maintained GT’s Cyber Lab in Microsoft Azure: pentest collaboration, C2 server, password hash recovery, phishing platform, vulnerability scanning (Nessus, Nmap).

Retailproof Company, *Co-Founder / Developer* Jan 2011 – Feb 2013
Langhorne

- Developed and maintained Retailproof.com website based on Magento e-commerce platform.
- Developed custom dynamic and universal eBay template (HTML, CSS, Javascript) that could be used for a wide variety of company’s products.
- Setup and maintained product export to Amazon.com and other platforms.

Novik Design, *Web Developer* May 2009 – Jan 2011
Philadelphia

- Created website layouts from provided design concepts according to HTML/CSS standards.
- Created dynamic websites on Magento e-commerce, Joomla, and WordPress platforms.
- Created Search Engine Optimization (SEO) and SEM campaigns for client websites.

EDUCATION

Temple University, *Management Information Systems, BBA* May 2016
Philadelphia

- Summa cum laude
- Cumulative GPA: 3.88 (3.91 major)
- Dean's List: Spring 2014 – May 2016

Kuban State University of Technology, May 2006
Bachelor of Computer Science, Bachelor of Economics
Majors: Software Engineering, Management

TRAININGS

Dark Side Ops: Malware Development, *Silent Break Security*
Deep dive into the source code to gain a strong understanding of execution vectors, payload generation, automation, staging, command and control, and exfiltration. Intensive, hands-on labs provide a structured and challenging approach to write custom code and bypass the very latest in offensive countermeasures.

Dark Side Ops 2: Adversary Simulation, *Silent Break Security*
Understand, research, build, and integrate advanced new techniques into existing toolkits. Challenge yourself to move beyond blog posts, how-to's, and simple payloads. Start simulating real world threats with real world methodology.

ACHIEVEMENTS

GIAC Advisory Board Member, *GIAC / SANS*

1st Place (out of 8) in SANS SEC660/GXPN CTF Challenge, *SANS*

6th Place (out of 25) in 2017 SANS NetWars Challenge, *SANS*

LANGUAGES

English ● ● ● ● ● Russian ● ● ● ● ●

SKILLS

Network / Infrastructure Penetration Testing
Internal / External, Comprehensive / Targeted, Evasive / Non-Evasive

API Testing
REST API, GraphQL

Security Architecture, Design Review
Applications, Application Stacks, Products

Vulnerability Assessments
Triage, Review, Validation of SAST/DAST Vulnerabilities

Attack Surface Management
Continuous Penetration Testing

Social Engineering
Payload Execution, Credential Harvesting, MFA Bypass

Wireless Assessments
WPA/WPA2/802.11x, Rogue Access Hunting, Wardriving

Web Application Assessments
Blackbox / Whitebox, Static / Dynamic

Source Code Review
Python, Javascript, C++

PCI Assessments
Accessing CC data, Segmentation Testing, Accessing CDE Enclave, etc.

Red Teaming
Recon, Compromise, Foothold, Privesc, Int. Recon, Goal

Product Security Assessments
ATMs, Kiosks, Slot Machines, etc.

Mobile Application Assessments