Mikhail Aleksandrov

Public Trust ⁂ Baltimore, MD ⁂ 410 - 598 - 7426 ⁂ maleks01@gmail.com

Education

- University of Maryland, Baltimore County (UMBC). B.S. in Computer Science **08/2012 – 12/2015**

Skills

- **Programming:** PowerShell, Perl, Python, JavaScript, HTML/CSS, SAS, R, Java, JSON, XML
- **IDE/Version Control/Disassemblers:** Eclipse, NetBeans, Android Studio, WebMatrix, GitHub, TFS, IDA Pro, OllyDbg, PEview/PEstudio
- **Cloud/Virtual:** VMware (vSphere), AWS (EC2, DynamoDB, S3, Redshift, RDS/Aurora, Data Pipeline, SQS, SNS), VirtualBox, Heroku, Azure
- **Database:** MySQL, PostgreSQL, MongoDB, CouchDB
- **Network:** Sysinternals, HP SiteScope/OMi, Putty, WinSCP, Wireshark, Nmap, Cain & Abel, Nessus, Acunetix, Burp Suite
- **Operating Systems:** Windows (NT 5.0 – NT 10.0), Linux (Ubuntu, Debian, Fedora), Android (5.0 Lollipop – 8.1 Oreo)
- **Natural Languages:** English (fluent), Russian (fluent)

Employment

Money Map Press - Business Intelligence Developer **02/2019 – Present (40 Hours Per Week)**

- Provided daily oversight of data quality and created / maintained all technical business intelligence documentation.
- Created automated quality assurance routines where possible and monitored ongoing ETL processes and incoming data feeds.
- Assisted in building, maintaining, and scaling a web-ready, operational database to support in-house applications.
- Wrote a Python script to pull data from the NICE inContact REST API as part of an ongoing effort towards building out a data extraction framework.

Prometric Inc. - Technology Operations Business Systems Analyst II **11/2016 – 02/2019 (40 Hours Per Week)**

- By monitoring the activity of a network comprised of 8,000 locations operating in 160 countries, contributed towards addressing over 99% of system outages and data retrieval discrepancies.
- Used PowerShell to automate a daily reconciliation task to update exam result statuses in a SQL database, then integrate with the SalesForce API to create missing tickets in the production readiness queue.
- Created an ad-hoc PowerShell script during a severe network outage to decrypt and display remote stored passwords which allowed for a 50% quicker turn around for the global command center business continuity.
- Laid the foundation for the security of a CouchDB R&D project now serving as the backend for a companywide application beginning to expand to every testing center.
- Wrote an action plan to optimize incident response in HP OMi/SiteScope, analyzed candidate exam logs and interpreted the data to make difficult decisions, and improved upon the knowledge base documentation and SQL queries used by the global teams to troubleshoot and sustain 24/7 system availability.

Savli Group Inc. - IT Delivery Consultant **04/2016 – 06/2016 (40 Hours Per Week)**

- Used Java and the FreeMarker template engine to integrate a Global Service Event Management adapter with HPE's Propel service broker and established end-to-end communications with the Service Anywhere help center.
- Decompiled JAR files to understand application functionality and error checked paths and events for a ServiceNow adapter.
- Translated business requirements into solution features with customer representatives and key stakeholders using Agile principles.

Selected Personal / Academic Projects

Android Software Security Consultation

- Analyzed custom software as part of Purdue University's INSuRE project to test a geographically distributed research coalition.
- Implemented various dynamic analysis techniques to enumerate system vulnerabilities in the UMBC mobile application.
- Carried out a complete static source code evaluation and prioritized vulnerabilities based on corresponding threat levels.
- Developed an adversarial model to identify intrusive activity and recommended improvements in architecture and policy.

Research Study on malware, SCADA/ICS, and politics of cyber warfare

- Studied methods of steganography/obfuscation/encryption and the complexity of oligomorphic, polymorphic, and metamorphic malware. Created presentations on Computer Command Control (CCC) about various rootkits, network penetration, and exploitation.
- Wrote blog posts about international cyber news and translated multilingual websites to extract information and form relationships between different types of global attacks.

Tweet Data Scanner

- Created an aggregation tool using Node.js and the Twitter API to scan for incoming tweets. Features include finding the location of a Tweet by status ID, retrieving the most recent Tweets since a given date within a range of a specific place, streaming geofenced Tweets around a given keyword, and streaming Tweets live in the vicinity of given coordinates.

Large Scale Security Incident Prediction

- Currently working on a solution to predict how likely it is for an entity to be hit by a cyber-attack in present time by using sentiment analysis on a mass scale, combined with system vulnerability/open port assessment, the financial anxiety index, and the correlation of various cyber-attacks to the history of event time proximity to determine a pattern for predicting preemptive strikes based on techniques used to predict stock market crashes and corrections.