Samuel Prashker

Email: samuel@prashker.net
Phone: +1 613 513 9684
Web: http://prashker.net

This whitespace has been
left intentionally blank.

Work Experience

Senior Security Engineer

Securonix

May 2017 to
Present

- Senior technical lead for many Canadian organizations, delivering a high quality end-to-end implementation of the Securonix SNYPR SIEM platform deployed both on-premise and on Cloud Platforms (AWS). My customer engagements are multi-million dollar renewing accounts.

SIEM, UEBA
Hadoop, Kafka, Spark, Solr,
Python, Java, Bash
Linux, Syslog
SSL, Kerberos

- Ingested, parsed, and enriched up to 100K EPS and high volumes of event data on distributed Hadoop platforms with a Kafka and Spark backbone, providing organizations with the tools to quickly and effectively respond to cybersecurity events with real-time urgency.

Log Parsing, IAM, PAM,
Security Operations, Network
Monitoring, Threat Analytics,
Adversary Tracking,
MITRE ATT&CK,
Network Security

- Worked closely as an additional limb to customer teams in transitioning from old services (Splunk, ArcSight, QRadar) to SNYPR and providing new-value and organization-applicable techniques to combat threats with effective incident response solutions. Big data analytics used to tackle security challenges.
- Produced custom and highly resilient scripts and operational processes catering to organizational requirements (and specific network topologies) exceeding the functionality of the core product to improve stability, performance and user experience - all while maintaining a deep and thorough understanding of each individual customers specific requirements and infrastructure.

Backup, DR, HA, Archival
API Producer and Consumers
Reporting and Metrics
System Monitoring

- Developed a Chrome Extension for power users to supplement existing UI with advanced insight into ingestion metrics, advanced debugging and diagnostics as well as supplementing threat hunting with quality of life changes.

Chrome Extension
JavaScript

- Deep and thorough training provided to internal junior resources, as well as directed training sessions with customers and stakeholders.

Customer Training

- Maintained a thorough and routine professional relationship with all customers and have received stellar reviews across the board for my work in delivering solid customer solutions consistently year over year.

Software Development Engineer (Contract)

Canadian Radio-television and Telecommunications Commission

February 2017 to
April 2017

- Built a public-facing API for the CRTC that can facilitate the submission of reports of SMS text message spam and other spam and phishing reports from third party applications (e.g., smartphones, email service providers, WhatsApp, and other proprietary messaging systems).

Python, Flask, SQLite,
MySQL, Redis, REST API,
Rate Limiting, API
Development, Unit Tests

Software Development Engineer (Working Holiday)
Microsoft Tokyo

September 2016 to
December 2016

- Developed and released to Apple App Store a new and improved version of Office Lens iOS with new features and bug fixes - Top 100 rank in iOS App Store in Productivity. Facilitated a unified codebase for iPad support.
- Designed and implemented ‘Immersive Reader’ including a new and improved language detection algorithm as well as many UI improvements and functionality to navigate through voice-read text - in collaboration with Apple.

Objective-C, iOS, Telemetry and Reports, Image Recognition, OCR, Accessibility (VoiceOver), JavaScript, ScopeScript

Software Development Engineer (Contract)
Rock-Hopper

April 2016 to
September 2016

- Retrofit an existing CakePHP 1.3 project with a comprehensive system-wide auditing system to record user actions with a tiered administrative permission model for filtering, querying and interacting with audit data.

PHP, Bash, Debian, MySQL, SQL Optimization, Security Audit, Cron

Intelligence Systems Developer
Cyber Security Intelligence Analyst (Co-op)
Canadian Radio-television and Telecommunications Commission

April 2014 to
August 2016

- Implemented analytical algorithms to decode, interpret and categorize spam messages, malware, robo-calls and other unsolicited telecommunications.
- Developed the Spam Reporting Centre, a web portal facilitating multiple collaborating Canadian Government organizations to pursue cases, enforcing the Canadian Anti-Spam Legislation, resulting in millions of dollars collected through fines assessed from violations captured using the Spam Reporting Centre platform.
- Created custom Lucene QueryParser and Lucene Analyzers allowing for efficient and tailored full-text searching.

PostgreSQL, MySQL, Python, Django, Perl, Java, Bash, TCP/IP, SSL, HTML, CSS, JavaScript, Bootstrap, JSON, Git, Lucene, Big Data, Eclipse, PyCharm, Regex, Celery, RabbitMQ, Natural Language Processing, ESXi

Computer Science Teaching Assistant – Mobile Applications Development
Carleton University

September 2013 to
April 2014

Quality Assurance Tester
Transport Canada – Rail Safety Directorate

May 2013 to
December 2013

Freelance Developer

July 2006 to
April 2013

Education

Bachelor of Computer Science – Computer and Internet Security *with Distinction*
Minor in Business – Information Systems
Carleton University, 2016

Fluent in English
Fluent in French
JLPT N5 Japanese