|  |
| --- |
| Nick Brown |

Seattle, WA | nick@altonimb.us | [linkedin.com/in/nicholaspbrown](http://www.linkedin.com/in/nicholaspbrown) | [github.com/nonik0](http://www.github.com/nonik0)

# Work Experience

## Software Development Engineer | Microsoft Defender For Cloud DevOps | September 2023 – April 2024

* Developed and maintained Security DevOps CLI used to automate a variety of static analysis security tools (e.g. Terrascan, Template Analyzer, etc.), enhancing the security evaluation pipeline for all Azure releases and customers.
* Owned and maintained the open-source [Template Analyzer static analysis tool](https://github.com/Azure/template-analyzer), which scans ARM and Bicep templates for security issues. Designed and implemented many key features for tool, primary bicep language support, which also required designing and implementing source code mapping for [Azure's bicep language](https://github.com/Azure/bicep) for improved integration with Template Analyzer.
* Redesigned release pipeline and automated repackaging dependencies to eliminate single points of failure (SPOF) from the static analysis tool pipeline, enhancing release pipeline reliability for all customers.

## Security Software Engineer | Microsoft C+AI SecUrity Green Team | April 2016 – SEPTEMBER 2023

* Founding member of a new security team paradigm focused on addressing systemic security issues, leading to the development of innovative solutions.
* Primary owner and maintainer of the popular [open-source AppAuthentication library](https://github.com/Azure/azure-sdk-for-net/tree/53e2f0b1f95ea712c407bdc616f3506d1477f914/sdk/mgmtcommon/AppAuthentication) that simplified development by managing identity and credentials automatically, with [250M+ total downloads](https://www.nuget.org/packages/Microsoft.Azure.Services.AppAuthentication) over its lifetime. Designed and implemented many integral features that simplified identity/key management for new and existing applications, often with no code changes needed. Sole driver to successfully migrate/transition all scenarios to new Azure.Identity library with dedicated team. Primary contact and communicator with customers over lifetime. Successfully deprecated with minimal developer impact.
* Created a scalable workflow using Azure Durable Functions and Azure Data Explorer to monitor activity of and apply the principle of least privilege to RBAC role assignments in Azure Resource Manager, mitigating attack potential for lateral movement. Received a patent for the least privilege selection algorithm. Also developed workflow in Azure Databricks, Spark, and Scala.
* Designed and implemented efficient data workflow using Azure Cosmos DB to process AAD security principal sign-in trace data, tracking every individual credential’s usage and mitigating unused credentials. Pulled data from multiple external sources, including AAD Graph API and Neo4J databases with Red Team data. Developed custom client libraries to speed data ingestion and able to scale effectively to cover all traces.
* Spearheaded PoC project to mitigate the presence of credentials in source code across org, reducing the count from approximately 200k to under 1k within a year. Developed rapidly with PowerShell. Successfully utilized various sources and metrics (commit history, Git blame, Active Directory/LDAP, TFS) to identify code owners and assign issues directly when attribution metadata not present. Project continued to provide value well beyond target lifetime, rapidly providing ad-hoc scanning solutions for partner teams when needed and covering security tool gaps until its deprecation.
* Designed and implemented core features to the popular internal Windows Form application "Subscription Cleanup Tool," improving the bulk management of Azure permissions across org and directly leading to reduced attack surface across org. Drove the process to update and deploy tool for use in national/government/air-gapped cloud environments (e.g. JEDI) where it was deemed required for effective security posture managements.

## Security Software Engineer | Microsoft C+AI SecUrity Assurance Team | March 2014 – Aprl 2016

* Primary security driver for authn/authz services. Authored threat models, conducted security reviews, wrote security-specific tests, and found, filed, and triaged security issues.
* Designed and implemented E2E test framework with TAEF and wrote security-domain specific regression tests for fixed issues. Framework was able to be used/reused by multiple other teams for their own tests.
* Scheduled, managed, and tracked issues found in external pen test reviews for org, bolstering services’ security with 3rd party reviews.
* Designed and implemented scanner agent and baseline security policies for Azure OS (IaaS) and web applications (PaaS) in collaboration with Azure Security Monitoring team

## SoftWare Development Engineer In Test | Microsoft Azure Active Directory Team | October 2010 – march 2014

* Tested authentication protocols and standards (OAuth WRAP/2.0, SAML 1.1/2.0, WS-\*, Open ID, etc.) for security token services, ensuring robust and secure authentication across systems, including Office 365.
* Tested end-to-end live data migration from previous STS service to new version/database schema, with no issues discovered or customer impact during the migration.
* Known on team for taking initiative to build creative solutions to expediate and bolster reliability of manual and automated testing. Developed service that improved the speed and reliability of test infrastructure for whole team by outsourcing slow and error-prone cloud tenant provisioning to a resilient "checkout" service. Developed local tooling used by whole team for ad-hoc testing and validation of arbitrary OAuth auth profiles/flows ad-hoc.

## SoftWare Development Engineer In Test | Microsoft Forefront Protection Manager Team | October 2009 – april 2010

* Tested client agent and software on variety of environments, including localization/globalization testing.

# Blockchain/Crypto Experience

* **Fundamentals**: strong foundation and understanding of broad spectrum of math and cryptographic technologies used in general cryptography and extending to blockchains and cryptocurrency. Hash and encryption algorithms, PKI, commitment schemes, consensus algorithms/BFT, hands-on experience working with newer advancements such as zk-SNARKS and zk-STARKS.
* **Ethereum Technology:** familiarity with Ethereum technology and development, EVM, Solidity, smart contracts, smart contract verification. Hands-on experience with using many L2s/sidechains such as Polygon, Arbitrum, Optimism. Experimented with Uniswap V3.0 liquidity pools and automated liquidity management.
* **Ethereum Staking (2022-Present):** Built and manage own at-home Proxmox cluster with redundant distributed, containerized Ethereum nodes (no majority clients), achieving >99.9% uptime. Built battery backup system to manage occasional power outages.
* **Ethereum Mining (2018):** Recognized “arbitrage” opportunity and developed a solution to efficiently manage AWS spot instances with GPU acceleration for Ethereum mining, automating spot instance creation with miner configured to a pool. Optimizing mining costs based on spot pricing.
* **Early Enthusiast/Investor:** Followed crypto/blockchain development since 2011, more seriously since 2017. Most interest in Ethereum but Bitcoin and Solana as well. Full-self custody of own crypto, using Shamir secret sharing, secret wallets, etc. for self-custody security.

# Education

## Bachelor of Science in Computer Science and Engineering | 2009 | University of California, LoS ANgeles

**Graduated Magna cum Laude, 3.85 GPA**

# Technologies Used

|  |  |
| --- | --- |
| **Scripting/Programming Languages:** .NET/C#/PowerShell, C/C++, Python, Bash, Rust, Go, Javascript/Typescript  **Virtualization/Containers:** Docker, LXC/LXD, Kubernetes, Proxmox, Hyper-V  **Cloud Providers:** Azure, AWS | **Operating Systems:** Windows, Linux (primarily Debian family, but also Red Hat) |

# Activities and Interests

I enjoy getting hands-on and lower level with electronics, hardware, microcontrollers, etc. Familiar with all the common architectures/platforms like Atmel, ESP, nRF, Raspberry Pi as well as RISC-V. Enjoy writing/modifying embedded firmware which I primarily use to make clocks/devices to give life to old Nixie tubes or improve my home automation with Home Assistant. Familiar with circuit design/PCB layout with KiCad as well as 3D modelling with Fusion 360.