Chris Abney Cyber Security Engineer and IT Professional

mail@chrisabney.com chrisabney.com linkedin.com/in/chrisabney

Lexington, Kentucky (Remote)

SUMMARY

Throughout my career, I have held various technical roles, leveraging my natural problem-solving skills to see projects through to completion. I have a passion for continuous learning and exploring new technologies, with a particular interest in Cloud, Cybersecurity, DevOps, and creating time-saving automations.

SKILLS

Languages
Python, PowerShell, Bash, Ansible, Terraform

Cloud Platforms
Microsoft Azure, Google Cloud Platform (GCP)

DevOps & Automation
GitHub, Azure DevOps, Docker, Azure Logic Apps, Ansible, Infrastructure as Code (IaC)

Security Tools
CrowdStrike Falcon, Wiz, Microsoft Defender, Microsoft Sentinel (SIEM), SentinelOne, DataTheorem, Snyk, Rapid7

Networking
Imperva Cloud Web Application Firewall, Azure Firewall

Ticketing
ServiceNow, ServiceNow VR, JIRA, ConnectWise Manage

Data Visualization
Microsoft Power BI

EDUCATION

Florida State University 08/2007 – 05/2011 | Tallahassee, Florida
BS, Information Technology

EXPERIENCE

Vice President, Mobile Application Security Engineer 09/2024 – Present | Lexington, KY
SMBC MANUBANK (Jenius Bank)

- Served as the Owner and Subject Matter Expert (SME) for our Mobile Application Security Testing (MAST) tool, maturing the platform by implementing Single Sign-On (SSO) and automated Identity and Access Management (IAM) access packages to standardize secure access for security teams and developers.
- Acted as the primary technical bridge between Android/iOS teams and 3rd-party vendors to troubleshoot and resolve critical SDK bugs that caused production app crashes.
- Partnered with mobile engineering to triage findings from detection to production fix, managing the remediation of vulnerabilities within custom code and 3rd-party SDKs.
- Facilitated mobile penetration tests and bug bounty missions by coordinating security-specific builds for Android and iOS while triaging researcher findings into actionable remediation tickets for development teams.
- Assisted with a massive, year-long transition of the bank's vulnerability management ecosystem from a custom Python/PowerBI stack to ServiceNow Vulnerability Response (SNOW VR), ensuring zero loss of data or functionality for reporting.
- Collaborated with the SNOW VR team to enhance platform integrations and refine the data model for the bank's vulnerability posture.

- Provided critical evidence and technical walkthroughs for high-stakes regulatory audits, including the Federal Deposit Insurance Corporation (FDIC), the Federal Reserve Board (FRB), and System and Organization Controls (SOC2).
- Evaluated emerging Artificial Intelligence (AI) and Application Programming Interface (API) security solutions to stay ahead of the evolving threat landscape for cloud-native and mobile applications.

Associate, Application Security Engineer 06/2023 – 08/2024 | Lexington, KY

SMBC MANUBANK (Jenius Bank)

- Orchestrated the transition of the bank's vulnerability management program from manual data collection to a more automated, risk-based Power BI dashboard.
- Developed custom Python automation scripts to ingest and normalize vulnerability data and findings via APIs from a diverse security stack, including CrowdStrike Falcon, CrowdStrike Spotlight, Wiz, Rapid7, Snyk, Microsoft Defender, DataTheorem, SonarQube, and more.
- Engineered a centralized PowerBI dashboard that serves as the "single source of truth" for the bank's security posture, integrating Exploit Prediction Scoring System (EPSS) scores and Mandiant Threat Intelligence for risk-based prioritization.
- Programmed complex business logic into the data pipeline to automate Service Level Agreement (SLA) tracking, exception management, de-duplication, and false-positive filtering, reducing administrative overhead for engineering teams.
- Served as a primary technical Subject Matter Expert (SME) for the Imperva Cloud Web Application Firewall (WAF), overseeing security configurations for critical bank product launches.
- Implemented and maintained advanced edge features, including Distributed Denial of Service (DDoS) mitigation, API Security, and Advanced Bot Protection, ensuring high availability and a hardened security posture.
- Partnered with Engineering and Product teams to securely onboard new sites for critical product launches.
- Helped lead technical triage and Root Cause Analysis (RCA) for WAF-related security incidents and Priority 1 (P1) issues, collaborating with development teams to analyze logs, traffic patterns, and errors.
- Orchestrated major production deployments through the Change Advisory Board (CAB) and approval processes, ensuring 100% alignment between technical execution and the bank's launch timelines.

Cyber Security Engineer 11/2021 – 06/2023 | Lexington, KY

Dataprise

- Played a key role in designing, building, deploying, and maintaining our Microsoft Sentinel solution in Azure.
- Leveraged PowerShell, ARM Templates, Bicep, and Ansible to automate the setup and configuration of infrastructure in Azure for our Microsoft Sentinel solution, reducing the time and effort required for onboarding new clients and minimizing the risk of errors or inconsistencies.
- Designed and created custom Ansible playbooks and roles to automate the configuration of infrastructure components such as virtual machines in Azure.
- Leveraged PowerShell scripting to automate a range of tasks within Microsoft Sentinel, including the deployment of new analytic rules for threat detection and incident response.
- Utilized Azure Logic Apps to develop new custom automations that leveraged APIs from tools like CrowdStrike, enabling SOAR (Security Orchestration, Automation, and Response) capabilities such as automated device isolation, AD account lockouts, and automated alert notifications to third-party partner ticketing systems via APIs. This improved incident response efficiency and effectiveness, reducing response time and minimizing the impact of security breaches.
- Managed PowerShell scripts, Ansible playbooks, ARM templates, and more using GitHub and Azure DevOps as content repositories for Microsoft Sentinel rules and workbooks, ensuring version control, collaboration, and consistency for effective infrastructure and security content management and deployment.

Network Operations Center Administrator 10/2019 – 11/2021 | Lexington, KY

The AME Group

- Responsible for the design, setup, maintenance, and continual improvement of all Network Operations Center tools. These tools include RMM platforms, network monitoring software, AV and EDR security products, documentation platforms, reporting, data analytics, and more. These tools assist engineers and technicians in supporting tens of thousands of endpoints across hundreds of clients.

- Responsible for the planning, preparation, and implementation of all internal and client-facing toolset migration following Integrity IT's acquisition.
- Assisted and led multiple company-wide toolset migrations following new acquisitions. This included the planning and execution of migrating thousands of agents from various tools across acquired clients and rolling them into our Network Operations Center software stack.

System Administrator 01/2016 – 10/2019 | Lexington, KY

The AME Group (formerly Integrity IT)

- Responsible for the design, setup, monitoring, and maintenance of the company's network systems and centralized managed service systems, including customer-facing hosted and cloud environments.
- Created and managed proactive measures and automation that increased the company's profitability and value to the customer.
- Worked on multiple large projects to switch internal toolsets from one vendor to another.

Network Control Technician 01/2015 – 01/2016 | Lexington, KY

The AME Group (formerly Integrity IT)

- Maintained, supported, and continually improved all internal tools (Remote Monitoring & Management Software, Security Software, Documentation Platforms, etc.) used by over 20 employees to support thousands of endpoints across more than 50 clients.
- Created and deployed automated scripts and monitors to save engineers and technicians vast amounts of manual labor and increase company profitability.

Service Desk Technician 09/2011 – 01/2015 | Lexington, KY

The AME Group (formerly Integrity IT)

- Responsible for server, network, workstation, and application support for thousands of endpoints across 50+ customers.
- Worked remotely and on-site to resolve a wide range of customers' technical issues.
- Worked on-site at customers' locations to deploy workstations, servers, and networking equipment.
- Initial triage and troubleshooting for customers' urgent issues.

CERTIFICATIONS

CompTIA Security+
Issued Jul 2020

Certified Ethical Hacker (CEH)
Issued Apr 2016

Sophos Certified Architect
Issued Dec 2018

Sophos Certified Engineer
Issued Nov 2018