Chris Abney

Lexington, Kentucky, United States

✉ mail@chrisabney.com

in linkedin.com/in/chrisabney   🔗 https://chrisabney.com

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.

Experience

Cyber Security Engineer
Dataprise
Nov 2021 - Present (1 year 7 months)

• 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
The AME Group
Oct 2019 - Nov 2021 (2 years 2 months)

• Responsible for the design, setup, maintenance, and continual improvement of all Network Operation 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 support 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 Operation Center software stack.

System Administrator
The AME Group, formerly Integrity IT
Jan 2016 - Oct 2019 (3 years 10 months)
• 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
The AME Group, formerly Integrity IT
Jan 2015 - Jan 2016 (1 year 1 month)
• 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 increased company profitability.

Service Desk Technician
The AME Group, formerly Integrity IT
Sep 2011 - Jan 2015 (3 years 5 months)
• 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.

Education

Florida State University
BS, Information Technology
Aug 2007 - May 2011

Licenses & Certifications

CompTIA Security+ - CompTIA
Issued Jul 2020 - Expires Jul 2023

Certified Ethical Hacker (CEH) - EC-Council
Issued Apr 2016 - Expires Apr 2019

ECC43228308225

Sophos Certified Architect - Sophos

LogicMonitor Certified Professional (LMCP) - LogicMonitor

Sophos Certified Engineer - Sophos

Skills

GitHub • Docker Products • Azure Logic Apps • Microsoft Azure • Microsoft Sentinel • Ansible • Infrastructure as code (IaC) • Windows • Managed Services • Building Automation