Bhavin Amin bhavinamin.github.io

Profile

Systems admin turned Security Operations analyst proficient in using REST APIs and custom solutions to automate and streamline application and system provisioning, monitoring, and maintenance and vulnerability + malware management.

Education

University of Pittsburgh | Bachelor of Arts

Skills

Development: Powershell, c# via .NET, node + react, basic C++ for memory exploration and editing
Administration: Active Directory + IIS, SCCM, Group Policy via AGPM, basic SQL, VMWare Vcenter + ESX for managing servers / hosts, Citrix XenApp + SDK, F5 Big IP for load balancing, o365 Administration (notably Teams / OneDrive + Sharepoint / Azure AD), Dell EMC for SAN management, Okta, JAMF, ZScaler, TCP/IP + DNS management
Data and Machine Learning: Python (via Conda + jupyter Notebook), bokeh for visualisations, pandas, R + shiny dashboards
Security: Nessus, Crowdstrike, T-pot w/ Elastic SIEM, nMap, metaSploit, WireShark

Work Experience

2021- Present | Voyager Digital | **Lead Analyst - Security Operations**
Started as a technical operations lead and transitioned into our security team as a "Padawan" of our lead CISSP and GIAC security engineer.
• Security analysis: implemented Crowdstrike throughout our internal endpoints, infrastructure, and cloud services as the principal hub for the prevention and analysis of threat vectors, malware, and incident management.
• Security analysis: implemented, configured and used Tenable Nessus to perform continuous vulnerability and malware scans across our hosts
• Identity access management: implemented Okta's Single Sign On authentication platform for the company and integrated more than 50 applications for SAML and OIDC based authentication and SCIM provisioning notably among them are Atlassian Cloud, Slack, AWS, and Snowflake to provide a password-less and more secure way of accessing our sensitive applications
• Secure access: implemented ZScaler Private Access + Internet Access to provide a secure network for a fully remote workforce
• Endpoint engineering: composed and deployed application and OS security updates via JAMF Pro to over 300 MacBooks with a 90%+ compliance rate
• Endpoint engineering: wrote and deployed maintenance scripts for MacBooks to rename computers, install custom packages and backup encryption keys
• System administration and development + IAM: wrote scripts that interact with various REST APIs to provide reporting and adjustments to system access and privileges
• Identity access and management: created fully automated onboarding and offboarding provisions via Okta for new hires and terms so they receive their apps and accesses on Day 1 using Okta group rules

2012-2021 | Penn Medicine | Senior System Administrator
Due to the lengthy time I've been at Penn, entries below are in chronological order with some of my most recent efforts and accomplishments listed first. At Penn, the nature of IT work is mainly about completing projects and troubleshooting problems with the sole priority of not causing impact to our 20,000 doctors and nurses who are heavily reliant on our systems to treat patients and perform groundbreaking research. Being in healthcare, Covid-19 has had a profound impact on increasing the speed of that work, while also exceeding that same expectation of keeping our systems operational. To date, I have not caused any unscheduled downtime through my work and have earned the trust and respect of my peers in an IT department with over 800 employees.

• Architected the policies and rollout of Microsoft Teams to our emergency departments to limit Covid-19 exposure from patients and first responders to our staff. Expanded MS Teams rollout to the rest of the health system.
• Stood up additional 20 Citrix servers hosting Remote Desktop Connection to facilitate a surge of 2500

additional connections due to a shift to remote work during Covid-19. Facilitated in getting AD infrastructure ready for the premature opening of a new hospital wing in case of a surge in Covid-19 patients.
• Created real-time data dashboards in Shiny via R to help us monitor the performance of servers during an expected Covid surge. These dashboards showed user connections, memory usage, CPU usage, and the rate of logons onto our systems.
• Created a real-time data dashboard in Shiny via R to help us see our insecure LDAP connections for Microsoft's March 2020 patch that could force us into secure LDAP and break applications. Microsoft has since backed down on forcing secure connections, allowing us time to use this dashboard and convert about 100 insecure application calls into secure LDAP calls.
• Citrix Administrator (from 2017 to current) that has worked with migrating servers from XenApp 6.5 to 7.6 to 7.15. Familiar with publishing applications into StoreFront or desktop via delivery groups and machine catalogs. Familiar with Citrix SDK , opening, editing, and sealing PVS images.
• As a favor to our data team, became a de-facto Hadoop administrator in addition to my current responsibilities to help kerberize and maintain a Linux-based data cluster
• SCCM admin from 2012 to 2017 working with operating system deployment, software distribution, reporting on software/hardware inventory, and patching / deploying software updates.

• Possess deep understanding of SCCM client interactions with management points, distribution points and local WMI repository. Familiar with all client side logs (CCMExec, ExecMgr, PolicyAgent, etc) for client troubleshooting.
• Developed numerous Task Sequences (TS) for OSD and application deployment. Familiar with TS environment and developed HTAs to be presentable during Task Sequences both in PXE and OS (through ServiceUI hook). Familiar with setting up TS variables and basing step completions on them. Current OS is Windows 7.
• Developed and pushed 200+ packages via SCCM to 30,000 computers for various projects. Installation packages are primarily created via WiX, AdminStudio, and wrapper scripts using batch, VBS, and Powershell.
• Created Windows Powershell scripts to move 40,000+ workstations between OU's, add users to AD groups, join computers to the domain, query WMI for workstation information, manage SCCM clients, and remediate computers in emergency situations.
• Experience with object oriented programming for UI development and using development as a solution. Developed installation bootstrappers in C# that present countdowns, progress bars, and reboot warnings to end users. Compiled with reusable classes and dynamic application manifests.
• Deep understanding of Windows OS due to familiarity with .NET library. IE. Event handling -> Created a service that monitors when an end user logs off or locks their computer and certain maintenance actions fire off based on those events.
• Experience with web development. Front end experience includes styling HTML with CSS coupled with jQuery/making AJAX calls through angular. Backend experience includes using the Express, Tornado and Django python frameworks with database interactions (SQLite and MongoDB). Continuously learning new frameworks.

• Created and deployed GPOs at enterprise levels to manage including but not limited to: Trusted Sites, power settings, registry keys (through group policy preferences), screensaver content, and workstation lockdowns for clinical machines in urgent care areas.
• Constantly in communication with other teams and management to coordinate solutions to problems that surface through software deployment, group policy changes, patching or any other mass effect / high risk environment changes.
• Consistently weighing risk of impact against new project proposals and infrastructure changes given the complex scope and diversity of our computer environment in our inpatient and outpatient areas.

2011 | Cephalon Inc | Support Analyst
• Logged 800 tickets per month remotely troubleshooting general IT issues such as virus removal, network connectivity, unlocking AD accounts, and pushing applications through SCCM.
• Physically set up new computers, cleared printer jams and re-imaged computers via ImageX.

2010 | Select Medical Corporation| Support Specialist I
• Logged 300 tickets per week remotely troubleshooting network connectivity issues, printing halts, general OS level errors, and errors within Hospital Applications such as Therapy Source, HMS, and Rehab Toolkit.
• Led Project: Assembled 10+ pieces of documentation on how to resolve network issues and errors occurring within certain applications

2008-2010 | Transition Strategies, LLC | Bookkeeper/Administrative Assistant/IT Support
• Recorded AP/AR ledgers, itemised expenses and ran invoices for firm's checking and IOLTA accounts.
• Troubleshooted network connectivity, Amicus Attorney, PCLaw, and installed various software including MS Office.

- Performed hardware and software upgrades + deployments

Activities / About Me

Piano player, Philly sports fan (unfortunately) and new dog owner as of August 2020. Finished Kaggle's Deep Learning "Learner Track" and have dabbled in perceptron and recurrent neural networks. Recently I've gotten into exploring reverse engineering and learning about reading and writing to memory in C++.