Bowman Williams

Driven IT professional with 4+ years of experience in desktop support, system administration, and IT infrastructure management. Skilled in Windows and MacOS environments, cloud technologies (Azure), and mobile device management (MDM). Experienced in troubleshooting hardware/software issues, deploying enterprise applications, and maintaining system stability, security, and performance. Adept at leveraging ITSM tools (Jira/ServiceNow), collaborating with security teams to remediate risks, and aligning processes with NIST and CIS frameworks. Committed to delivering efficient, customer-focused support while optimizing IT operations.

EDUCATION

Bachelor of Science – Computer Science and Cybersecurity – *Kennesaw State University*

TryHackMe - Active participation in hacking challenges such as CTF's and hands-on learning of various penetration testing methods and techniques.

WORK EXPERIENCE

Mid-Sized (MSP), Kennesaw — August 2021 - Present

Desktop Support Administrator — June 2023 – Present

- Provide onsite and remote end-user support in Windows 10/11 and macOS environments, troubleshooting hardware/software issues, configuring network printers, and maintaining desktops, scanners, and peripheral devices.
- Deliver system administration support including Active Directory account management, Intune/Azure-based device configuration, and Office 365 application support, ensuring smooth onboarding and offboarding of employees.
- Manage ticketing workflows (Jira/ServiceNow), documenting resolutions, tracking incidents, and contributing to the knowledge base to streamline future troubleshooting.
- Support vulnerability remediation by partnering with Information Security to patch endpoints and secure desktop environments in compliance with organizational standards.
- Deploy and test software updates across physical desktops and virtual desktop environments, ensuring consistent performance and security.
- Document server configurations, standard operating procedures, and network diagrams for knowledge sharing and troubleshooting.

Computer Technician — August 2021- April 2023

- Manage pre-production tasks, including content plan development and message creation for 5 projects.
- Lead a team in preparing PCs and Chromebooks for local school districts by ensuring correct update.
- Utilize experience with Disk Imaging and automated software distribution tools.
- Conduct hardware and software troubleshooting to maximize customer computer performance.

Software Engineer — May 2021 - August 2021

Financial Services Firm, Atlanta, GA

- Dedicated and detail-oriented Software Engineer with hands-on experience.
- Collaborate with cross-functional teams to develop and maintain financial software solutions, contributing to the enhancement of trading.
- Assist in designing, coding, testing, and debugging complex applications using Python and Java.
- Conduct research on emerging trends in finance and technology to propose innovative solutions.

Technical Skills

- Operating Systems: Windows, Windows Server, Mac OS, Kali Linux (Ubuntu) | Scripting and Programming Languages: Python, Java, Hyper-V
- Networking: TCP/IP, NIST Framework, OWASP Top 10, MITRE ATT&CK Framework
- Security Tools: Wireshark, Snort, Nessus, Burp Suite

Soft Skills

- Time Management | Teamwork and Collaboration | Communication | Problem Solving | Technical Proficiency

Projects

Cybersecurity SOC Lab Project

- **SIEM Implementation**: Set up and configured the Elastic Stack (Elasticsearch, Logstash, Kibana) to serve as a Security Information and Event Management (SIEM) platform for real-time log monitoring, threat detection, and analysis.
- **Active Directory Integration**: Deployed and integrated Active Directory to simulate an enterprise-grade network environment, implementing user roles, group policies, and access controls to manage identity and authorization.
- **Incident Response**: Conducted simulated incident response scenarios, including detecting brute force attacks, privilege escalation attempts, and malicious logins.
- **Log Ingestion & Parsing**: Automated the ingestion of logs from multiple sources (Windows, Linux, network devices) using Logstash pipelines; parsed and enriched logs for actionable insights.
- **Data Visualization & Reporting**: Created interactive dashboards in Kibana for threat intelligence, identifying trends, and providing comprehensive security metrics.
- **Alerting**: Configured alerts for critical events, such as failed login attempts and unauthorized access, to ensure rapid response to potential security incidents.
- **Custom Scripts**: Developed Python and PowerShell scripts to automate repetitive tasks, such as log rotation, data backup, and event correlation.
- **Threat Hunting**: Utilized SIEM tools to identify and analyze Indicators of Compromise (IoCs) and conducted root cause analysis for simulated attacks.
- **Documentation**: Produced detailed documentation for SOC workflows, lab setup, and step-by-step incident response processes.
- Key Skills Gained: Log management, network monitoring, system hardening, threat detection, security reporting, and familiarity with industry frameworks like MITRE ATT&CK.

SIEM | Azure Sentinel

- Used custom PowerShell script to extract metadata from Windows Event Viewer to be forwarded to third party API in order to drive geolocation data.
- Configured Log Analytic Workspace in Azure to ingest custom logs containing geographic information (latitude, longitude, state/providence, and country)
- Configured custom fields in Log Analytics Workspace with the intent of mapping geo data in Azure Sentinel
- Configured Azure Sentinel (Microsoft's cloud SIEM) workbook to display global attack data (RDP brute force) on world map according to physical location and magnitude of attacks.

SQL | Microsoft SQL Server Management Studio

- Designed and implemented complex database schemas to meet specified requirements, ensuring data integrity and normalization.
- Developed and optimized SQL queries for various use cases, including data retrieval, aggregation, and reporting.
- Performed data analysis and generated insightful reports using advanced SQL techniques.

Cybersecurity SOC Lab Project

- Designed and implemented a SOC lab with a SIEM setup using the Elastic Stack (Elasticsearch, Logstash, Kibana) to monitor and analyze security events.
- Configured Active Directory for enhanced security practice, simulating real-world enterprise environments.
- Conducted threat detection and incident response exercises, including log analysis and correlation.
- Automated log ingestion and parsing using custom pipelines in Logstash for efficient data handling.
- Gained hands-on experience in monitoring network activity, identifying anomalies, and generating security reports.
- Demonstrated skills in managing and securing IT systems while utilizing industry-standard tools and techniques.

Certifications

- Cisco Networking Academy- Intro to Cybersecurity
- CompTIA Security Plus
- TryHackMe- Jr Penetration Tester
- Cisco Networking Academy- Junior Cybersecurity Analyst