BRIAN OLLIFF

RESUME@BRIANOLLIFF.COM

SUMMARY OF QUALIFICATIONS – NETWORK/SECURITY ADMIN & INSTRUCTOR

A network, server and security administrator with 15 years of network infrastructure and senior security analyst work experience, specializing in the coordination, maintenance, and support of servers and network infrastructure, while ensuring the highest level of security based on current standards and regulations.

WORK EXPERIENCE

Defensive Security Engineering Instructor   October 2021 – Present
INE (Internetwork Expert)   **Cary, NC (remote position)**
Course/Learning Path Creation:
- Developed a complete learning path for novice learners interested in entering the cybersecurity field, geared around cybersecurity engineering (Enterprise Defense Administrator).
- Planned and created numerous instructional courses covering topics such as "Secure Architecture Design", "PKI Design", and "Authentication, Authorization, & Identity Engineering".
- Built multiple lab environments to correspond with topics in individual courses to facilitate a hands-on learning approach for students.
- Along with the courses, created individual assessment questions that correspond with individual videos in each course, to continuously evaluate students' retention of information.
- With the assistance of an instructional designer, created a new industry certification with hands-on lab examination coupled with multiple choice questions (Enterprise Defense Administrator – eEDA)
- Created learning paths for Security+ and Cisco CyperOps Associate certifications, in addition to introductory courses for AI use in cybersecurity.

Audio/Video Production:
- Responsible for independent audio/video production quality control to ensure highest level of product for customers.
- Recorded videos up to 30 minutes in length, ensuring proper camera framing and audio levels, while maintaining eye contact with camera (and indirectly, viewer) throughout each video.
- Created all visuals for use in videos, ensuring they would be visually appealing and informative for viewers/students.

Network Administrator/Cyber Security Manager   June 2014 – October 2021
Lexington Medical Center   **West Columbia, SC**
Management:
- Led team of Information Security Analysts and coordinated day-to-day tasks while ensuring each member was responsible for technologies that highlighted their strengths.
- Created and maintained documentation for all responsible systems and provided support as needed.
- Acting as project lead, developed and successfully executed a migration plan to transition from Websense email and web security products to Cisco Ironport products with zero downtime or negative impact to user population.
- Continued the expansion and modernization of LMC's email security posture while migrating to Proofpoint email security products, to include Security Awareness Training, Targeted Attack Prevention, and Email URL Isolation.
- Created and maintained policies relating to mobile device management for both corporate owned devices and personally owned devices.
- Managed the onboarding of a new vendor to provide critical threat intelligence information to help ensure the security and integrity of the organization's data.
- Collaborated with other team managers to develop and maintain security polices for cloud-based environments, such as Microsoft 365.
- As lead analyst, deployed and continued to manage the organization's Security Information and Event Management system, Splunk, which is used to consolidate and analyze security logs from various systems using machine learning and various automatic analytics.

- In my capacity as senior analyst, assisted Director of Information Security with routine audits and risk assessments.

Administration:
- Administered a mostly Microsoft server environment of over 1,700 servers for a multi-location healthcare system, including assisting with management of VMWare environment.
- Managed email infrastructure including multiple Exchange servers, email security appliances such as Websense, Cisco ESA, and Proofpoint Email Security, while ensuring proper mailflow and delivery, and maintaining security and usability for over 7,000 users.
- Handled escalation of help desk tickets to resolve more advanced issues, while guiding and training first-line support personnel.
- Developed numerous Powershell scripts to automate several processes, including writing a custom GUI-based application to assist departments with Active Directory management.
- Designed and deployed an AirWatch MDM environment to support organization's needs for mobile devices, including assisting with policy requirements, while ensuring security of devices and sensitive information. Later, migrated that AirWatch deployment to Microsoft Intune while continuing to manage policies and device configurations.

Security:
- Managed web filtering and email filtering systems for all users, including migration from Websense to Cisco IronPort ESA/WSA systems, and then Proofpoint.
- Designed and implemented RSA SecurID multi-factor authentication system, utilizing tokencode access in addition to risk-based authentication.
- Transitioned that RSA deployment into a new, more modern solution using Duo. Instead of tokencodes, moved to a push notification verification system for additional security and ease of use for end-users.
- Participated in daily incident response as needed, in addition to on-call rotation for security incidents and support of managed security systems.
- Analyzed malware and other threats to assess risk to organization and adjust or implement controls as necessary for appropriate protection and remediation.
- Designed and deployed Splunk implementation, including custom dashboards, searches, and reports to assist in monitoring security posture of organization.

Network Administrator   **August 2010 – June 2014**
Rogers Townsend & Thomas, PC   **Columbia, SC**
Administration:
- Administered a Microsoft centric multi-office law firm of workstations, servers, switches, firewalls and Toshiba/Cisco phone systems for 350 users, 75 managers, and 60 attorneys.
- Troubleshot and repaired 32bit and 64 bit server hardware and Microsoft Windows software issues while working with hardware and software vendors such as Dell, SonicWALL, Symantec, Toshiba, HP, Microsoft, and Cisco.
- Created Active Directory group polices to automate updated software package rollouts and other patches.
- Created custom Powershell scripts to assist in Active Directory and Exchange management tasks.

Management:
- Created purchase orders and requests for virtualization projects such as software packages and associated costs.
- Performed IT audits from an information gathering role.
- Provided support of disaster recovery and business continuity plans as issues unfolded.
- Created Microsoft Visio diagrams for center floor plan, network, and organizational layouts.
- Acted in a Senior Network Administrator capacity during IT Director transitions, and assisted new Directors during transition periods.

Deployment:
- Managed desktop PC processes such as PC imaging and software deployment.

BRIAN OLLIFF

RESUME@BRIANOLLIFF.COM

- Gathered information such as baseline compliance, software packages installed, and application usage data.
- Built new Active Directory group policies that automated common tasks to decrease daily maintenance.
- Deployed Symantec Endpoint Protection to replace McAfee AV which reduced licensing costs.
- Deployed Nagios for software and hardware monitoring and alerting.
- Deployed Spiceworks for software and hardware inventory and helpdesk systems.
- Created, tested and deployed workstation and server images using Windows Deployment Server and Windows Automated Installation Kit.
- Installed custom security camera system using off the shelf hardware and software to reduce costs by thousands when compared to a commercial CCTV system.
- Designed and deployed Microsoft System Center environment across multiple sites to aid in inventory management, monitoring, software deployment and testing, and patch/update management.

Network Administrator   December 2007 – May 2010
STM   **Charlotte, NC**
Administration:
- Oversaw an infrastructure that included technologies such as: HP Servers, VMware, SAN, NAS, Terminal Server, IPSec/VPN, Linux, Backup Exec, and extensive Microsoft environment centered on Exchange and Terminal Services.
- Designed, installed and supported multiple HP Servers and end-user Dell and HP PCs.
- Performed primary server administration tasks, including setup, installation, OS patching, data backup, user management and access control using Microsoft Active Directory and Microsoft Server 2003.
- Provided offsite backup management and administration of multiple tape libraries using Veritas Backup Exec software.
- Deployed software, anti-virus, and operating system updates to MS Windows 2003/2008 servers and XP/Vista/7 desktops.
- Ensured all end-users from multiple sites maintained connectivity to Datacenter using SonicWALL VPN clients and IPSec VPN tunnels

Management:
- Coordinated Help Desk support staff to ensure efficient workflow routing and prompt service requests.
- Provided telephone and email support for helpdesk issues, such as desktop, laptop, printers, software including Microsoft Office, telephones and networking.
- Performed software, hardware, and network troubleshooting to clients on-site, over the phone, and though remote connections.

INDUSTRY CERTIFICATIONS

CompTIA Security+
Splunk Core Certified User
Recorded Future Certified Analyst
eLearnSecurity eJPT
Cisco CyberOps Associate