Angel Ramirez

89 Hawick Cres, Caledonia ON, N3W-0G6 (905) - 906 -3031 |
aar_security@protonmail.com | www.aar-security.com

EDUCATION

Hack The Box Academy – HTB Certified Defensive Security Analyst (HTB CDSA)

CompTIA – CySA+

Harvard University – Computer Science for Cybersecurity

TECHNICAL & LANGUAGE SKILLS

Splunk | ELK Stack | Security Onion | MS Sentinel | MS Endpoint | Webroot DNS & Endpoint | Azure AD (Entra ID)
Azure Security (Defender) | NIST Framework | Python | PowerShell | CLI | IDS/IPS | Network Protocols
Network Architecture | VMware | Vulnerability Assessment | IAM | Docker | Windows & Linux Servers
SonicWall | Sage50 | Hyper-V | Proxmox | Nessus | Wazuh | pfsense | kali

PROJECTS

CITADEL: Virtual SOC environment   August 2024 - Present

Personal Home Server

- Developed a virtual SOC lab environment simulating real-world scenarios.
- Utilized the lab environment to perform malware analysis, and red team operations
- Conducted hands-on experiments with vulnerable applications like DVWA to explore and mitigate vulnerabilities listed in the OWASP Top 10, providing experience in identifying and addressing common application security risks
- Implemented network segmentation using pfSense firewall with multiple VLANs.
- Integrated a suite of cybersecurity tools including Kali Linux, Nessus, and Wazuh.
- Utilized Docker for container management, showcasing understanding in modern application deployment.
- Managed virtualization with Proxmox, optimizing server hardware for cybersecurity tasks.

WORK EXPERIENCE

Network & Security Administrator   September 2023 – Present

Verduyn Tarps Inc. | Hamilton, Ontario

• Implemented and managed security infrastructures to protect organizations assets.
• Participated in security audits and assisted in remediation efforts.
• Deployed and maintained SIEM (MS sentinel & defender for Endpoint) systems for enhanced threat detection and response.
• Oversaw email and endpoint security measures to mitigate phishing and malware risks.
• Managed identity and access controls, including multi-factor authentication and conditional access policies.
• Developed and implemented data protection strategies, disaster recovery and conducted vulnerability assessments.
• Transitioned legacy security tools to integrated solutions, improving efficiency and reducing costs.
• Developed and delivered security awareness training programs, boosting employee security competency.
• Continuously monitored emerging threats and security trends, proposing and implementing improvements
• Monitored and maintained IT systems health, including servers, workstations, and network devices.
• Provided prompt technical support to end-users, addressing hardware and software-related inquiries.
• Implemented and managed patch management processes to keep systems secure and up to date.
• Assisted in managing network infrastructure, including AP's, switches, firewalls, and VPN's.
• Established and maintained data backup and recovery procedures, conducting regular disaster recovery testing.
• Enforced security policies, access controls, and compliance standards.
• Assisted in the procurement and deployment of hardware and software assets.
• Evaluated and recommended technological solutions aligned with company needs and budget.
• Maintained accurate documentation of IT assets, configurations, and procedures.
• Audit existing infrastructure to provide recommendations for security hardware/software.

IT Support Technician   April 2019 – August 2023

Best Buy Canada - Geeksquad | Hamilton, Ontario

• Trained team members on advanced techniques, company procedures, & safety requirements.
• Managed technical operations across multiple stations, ensuring optimal coverage & meeting production goals.
• Demonstrated expertise in MacOS, Windows & Linux devices as well as the latest hardware/software technology.
• Provided technical support troubleshooting hardware and software issues for customers personal devices.
• Maintained a high level of customer satisfaction by providing friendly, efficient and effective service