Richard Rostum

richard@richardrostum.com
richardrostum.com

Skills

- **Applications**: Microsoft Office 365, G Suite, Adobe Suite
- **Operating Systems**: VMware ESXi, Microsoft Hyper-V, Windows, Windows Server, Linux, MacOS, Android, iOS
- **Technologies**: VPN (OpenVPN/WireGuard), Docker/Kubernetes, Nmap, Wireshark, DNS, Veracrypt, FTK Imager
- **Services**: AWS, Azure, Google Compute/GCP, Cloudflare
- **Languages**: Python, Bash, Powershell, HTML, CSS, LaTeX

Experience

- **Booz Allen Hamilton** — Washington, D.C.
  Incident Response — *2023 – Present*
  - Traveled to multiple clients across the country to restore systems infected with viruses/malware/ransomware/etc.
  - Coordinated with the local I.T. team and Digital Forensics and Incident Response to get the business back online.
  - Restored servers and end-user machines to working backups/re-imaged machines that could not be recovered.
  - Rebuilt domain controllers, hypervisors, and workstations if restoration was not possible.
  - Assisted clients with satellite offices in reestablishing inter-office network communication and recovery.
  - Used decryption tools to restore critical systems and workstations.
  - Helped clients with building an inventory tracker to confirm each machine on-site was investigated.
  - Installed and configured endpoint security software on all user machines and servers for monitoring.
  - Created forensic images of infected machines to run analysis on.
  - Assisted end users with getting back to day-to-day business.
- **Computer Resources of America** — New York, NY
  Network Administrator — *2018 – 2022*
  - Maintained networking infrastructures for 20+ clients, 100+ servers, 1000+ workstations.
  - Advised and provided input on network restructuring following the NIST framework/ISO 27001 for clients.
  - Configured MFA policies for all clients.
  - Wrote and continuously updated infrastructure documentation for clients.
  - Implemented remote deployment of antivirus software, backup software, and system updates.
  - Setup a critical alert system for remote server status (offline alerts, hard drive status, etc.).
  - Created and maintained weekly ticket reports to provide management and clients insight into issues.
  - Created and implemented several training programs for clients to improve cybersecurity/threat awareness.
  - Supported user and server-side applications.
  - Performed on-call support for all clients.

Education

- **New York Institute of Technology** — Old Westbury, NY
  Master of Science in Computer Science — *2019 – 2021*
  - Focus on courses centered on information security, cryptography, and physical security.
  - Worked on projects involving NIST Framework, ISO 27001, SOC 2, and MITRE ATT&CK.
  - Designed an Android application that extended the Google Maps API and Spotify API to generate music playlists based on location (i.e. Gym, Library, Shopping Center, etc.).
  - Utilized SDLC to build an A.I. TensorFlow application to recognize human handwriting.
  - Conducted network and packet analysis using tools such as Wireshark.
  - Compiled several Linux kernels from scratch and built out operating systems.
  - Built out several small-scale networks to attack utilizing OWASP.
- **New York Institute of Technology** — Old Westbury, NY
  Bachelor of Science in Computer Science — *2015 – 2019*
  - President of the Game Club (2017 – 2019)
    - Ran multiple events such as fundraisers and tournaments for the club.
    - Participated in Extra Life (Charity Event) 2016 – 2018.
    - Created a TESPA chapter for NYIT in 2017 and established an Esports team.
  - Treasurer of the Game Club (2015 – 2017)