Alex Darras Systems Engineer (Techware)

oalexdarras@hotmail.com | 0455277283 | Melbourne, VIC
Github: https://github.com/DrosRas/tools
Linkedin: https://www.linkedin.com/in/alexandros-darras-2a790b103

CAREER GOAL

Systems Engineer with 3 years of experience in IT support, network architecture, server administration, cloud computing, and security management. Proficient in ethical hacking methodologies and frameworks, with a strong understanding of common attack vectors and exploitation techniques. Experienced with penetration testing tools such as Metasploit, Nmap, and Burp Suite. Maintains a personal lab environment for experimenting with new technologies and has honed skills on the Hack The Box platform to simulate real-world attack scenarios. Dedicated to staying current with the latest technologies and trends to provide optimal solutions for clients. Strong troubleshooting and technical issue resolution skills, combined with a commitment to outstanding customer service, enable effective support for organizations at all levels.

My career goal is to deepen my technical expertise and continue researching advanced systems engineering and cybersecurity solutions, contributing to innovative and resilient IT infrastructure for an organization.

SKILLS

- Experience with developing technical documentation
- Experience with remediating real world Ransomware attacks.
- Experience with Backup and disaster recovery planning.
- Familiar with scripting languages such as powershell,bash and python.
- Experience with planning and deploying physical and network infrastructure projects.
- Experience in maintaining security documentation and reference materials
- Experience in development of information Security policies, procedures, standards, and guidelines based on knowledge of best practices and compliance requirements.
- Extensive customer service experience
- Experience with troubleshooting digital environments
- Ability to monitor and manage vulnerability assessments, penetration tests
- Familiarity with OHS regulations
- Familiarity with various operating systems (Windows, Linux, macOS)
- Expertise with security and database information management tools
- Capable of working with various types of networks
- Stellar problem-solving and critical-thinking skills
- Strong verbal and written communication abilities
- Extensive knowledge of security vulnerabilities, solutions, and risks in IT
- Highly organized and top attention to detail
- Ability to work together with a large team
- Skills with multitasking and time management
- Awareness of security standards such as ISO 27001, NIST, Kill chain, E8
- Able to Identify gaps in service areas and contribute to development of recommendations for appropriate security controls\solutions to be implemented to resolve
- Strong technical orientation across multiple disciplines e.g., Cloud Security, Disaster Recovery, Active Directory, Network Security, Email Security, and Vulnerability Management.
- Ability to work effectively with limited supervision
- Understanding of SIEM technologies

Technical Skills:

- **Cybersecurity**
  -Tools & Frameworks: MS Defender,Kali Linux, Nmap, Metasploit, Searchsploit, Burp Suite, Wireshark, Packet

Tracer, Gophish, Owasp Zap, VirtualBox, Nikto, SQLmap, msfVenom payload creator, Fatrat payloads, Scapy, Ettercap password sniffer, Bettercap, Gobuster, Netcat, Hydra, Smbclient
-Security Frameworks: NIST security framework, ISO security frameworks, Kill chain framework
-System Security: Windows firewall, Event viewer, ACL configuration, IPS configuration, LDAP domain dump, Tails OS, Cylance, ThreatLocker, SSL certificates
-Email & Network Security: Exchange Online Protection,DMARC, Mimecast mail protection, Mailguard

- **Infrastructure & Systems Management**
  -Server Management: Microsoft Server 2012-2022, Hyper-V, VMware, Microsoft Azure, AWS
  -Systems & Operations: System Center Operation Manager, Remote Desktop Manager, Active Directory, Customer Relationship Manager, Health Checks, Data Protection Manager, Exchange Manager, AD Connect, Veeam Backups, Ubiquiti, APC UPS, StorageCraft, QNAP
  -Firewalls & Network Configuration: Fortigate, SonicWall, DNS configuration, VPN configuration
  -Cloud Computing: Microsoft Azure, AWS
  -Collaboration Tools: Microsoft 365, ConnectWise

- **Programming & Web Development**
  -Languages & Frameworks: Python 3, HTML, CSS
  -Content Management Systems: Joomla CMS

- **Data Management**
  -Tools: Splunk, MySQL Workbench

- **Software & Tools**
  -3D Design & Animation: Autodesk 3Ds Max, Blender, Zbrush
  -Game Development: Unity Engine
  -Multimedia: Flash Pro, Adobe Photoshop
  -Productivity: Microsoft Word, Microsoft Project, Microsoft PowerPoint, Microsoft Excel

WORK EXPERIENCE

Systems Engineer L2 | **Techware** **July 2023 -Now**

IT Engineer | **Maxxam Computer Systems** **Dec 2021 -July 2023**

- Management and setup of medium-large sized office environment networks along with adjustment of security measures
- Installing, configuring, and maintaining operating systems, applications, and other software.
- Installing, configuring, and maintaining physical machines and devices.
- Managing user accounts, permissions, and access control for systems and applications.
- Managed and maintained over 50 servers, both physical and virtual, across multiple sites, ensuring high availability and data protection
- Conducted a thorough analysis of backup data and implemented recovery procedures to restore affected systems to a functional state. Worked closely with external vendors and stakeholders to minimize downtime and ensure business continuity.
- Led recovery efforts from a large-scale ransomware attack, in which the organization's critical systems were encrypted and held for ransom. Coordinated with incident response and security teams to isolate affected systems, contain the attack, and mitigate further damage.
- Developed and implemented new policies and procedures to strengthen the organization's defenses against future ransomware attacks, including regular security audits, system hardening, and enhanced backup and disaster recovery capabilities.
- Conducted regular system backups and testing disaster recovery procedures.
- Monitoring system logs and analyzing system performance data to identify issues and trends.
- Developed and executed a cloud migration plans, moving critical applications and data to Microsoft 365 while minimizing

downtime and ensuring data security
- Implemented cybersecurity measures, including firewalls, intrusion detection systems, and vulnerability assessments, resulting in increased data security and compliance with industry regulations
- Provided technical support to end-users, troubleshooting and resolving hardware and software issues in a timely and efficient manner
- Developed and executed backup and disaster recovery plans, ensuring business continuity in the event of a data loss or system failure
- Collaborated with cross-functional teams, including software developers and project managers, to ensure successful delivery of projects on time and within budget
- Created and maintained technical documentation, including network diagrams, standard operating procedures, and user manuals, to facilitate knowledge transfer and ensure compliance with industry standards
- Conducted regular system monitoring and performance optimization, proactively identifying and resolving issues before they impacted end-users
- Managed vendor relationships and negotiated contracts for IT hardware and software, ensuring cost-effective procurement and timely delivery of goods and services

EDUCATION

Microsoft 365 Certified:Modern Desktop Administrator Expert (MD102) **March 2024**
Microsoft Melbourne,Vic

Microsoft 365 Certified:Modern Desktop Administrator Associate(MD100,101) **October 2022**
Microsoft Melbourne,Vic

Microsoft 365 Fundamentals **December 2021**
Microsoft Melbourne,Vic

ITIL 4 foundation Certificate **December 2021**
PeopleCert Melbourne,Vic

MCSI Remote Cybersecurity Internship **November 2021**
Mosse institute.com Melbourne,Vic

Cyber Security Certificate iv **November 2021**
Holmesglen Institute Melbourne,Vic

Splunk fundamentals 1,2 **May 2021**
Splunk.com Melbourne,Vic

Online Security courses Udemy, TCM security **October 2020**
Udemy.com, Academy.tcm-sec.com Melbourne,Vic
- Practical ethical hacking - TCM
- Zero to mastery ethical hacking - Udemy
- Complete networking fundamentals- Udemy
- Penetration testing and bug bounty hunting- Udemy
- The ultimate dark web anonymity, privacy, and security certificate- Udemy
- Complete python developer- Udemy

CYBER SECURITY EXPERIENCE

- Management and setup of a medium sized office environment network along with adjustment of security measures

through ACL's, IPS, IDS, firewalls and anti-malware software.

- Management and monitoring of an Information technology project with the creation of documents such as: Cyber hygiene for an organization, Cyber Risk assessment , Risk assessment reports and Risk implementation reports, creation, evaluation and testing of an Incident response plan using NIST and ISO frameworks, security policies, staff cyber security training programs.
- Managing a security team and assigning defensive and offensive roles for incident simulation using NIST and Kill chain frameworks (remote desktop vulnerabilities and defensive measures), coordinating team meetings and work schedules.
- Researching, launching and presenting simulated phishing campaigns with the aim to educate using software such as gophish, mailhog and powerpoint.
- Documentation and notes on every penetration testing and CTF techniques used on virtual testing and training environments such as: xvwa, brokenpc, webforpentester, metasploitable machine, as well as machines on HACKTHEBOX.com and offensive security testing labs. With the aim to take the OSCP or ENFJ penetration testing certification exams.
- Development of security tools with python such as: arp-spoofer, password sniffer, password generator, port scanner, web crawler, keylogger
- Basic training on splunk platform and management of big data as well as attending seminar on splunk phantom for automating defensive procedures against cyber threat vectors.
- Creation of a completely anonymous and untraceable working environment through tails, the portable Amnesic Incognito Live System