CONTACT

Phone

(+94) 778757584

Email

Sachirademein15@gmail.com

Address

Panadura, Colombo, Sri Lanka

LinkedIn

Sachira Demein

TECHNICAL SKILLS

- Linux
- Firewall & IPS/IDS
- On-premises AD
- Routing & Switching
- Azure Cloud & o365
- Security Auditing
- Penetration Testing
- Microsoft Intune (EDR)

SOFT SKILLS

- Attention to Detail
- Teamwork
- Communication
- Problem-solving
- Adaptability

LANGUAGES

- English
- Sinhala

SACHIRA DEMEIN

SECURITY ENGINEER

Security Engineer with hands-on experience in managing firewalls, configuring network infrastructure, & administering both cloud-based & on-premises identity solutions. Proficient in ASA firewall policies, Cisco routing & switching, Azure Active Directory, & on-prem Active Directory. Experienced in Linux server management & certified in Sophos Endpoint Management. Currently pursuing Frortinet Network Security Engineer & MD-102 certification, with a strong focus on securing modern IT environment through robust access controls & infrastructure hardening.

WORK EXPERIENCE

SECURITY ENGINEER

Converzed Network Solutions — Dec 2024 - Present

- Configured and managed Cisco ASA firewalls, including **Access Control Lists (ACL)**, **Network Address Translation (NAT)**, and **firewall policies**.
- Set up and maintained Cisco routers and switches; configured IP addresses, implemented **OSPF routing**, and created **VLANs** to segment LAN networks.
- Worked with Azure Cloud, focusing on **Azure Active Directory (AD)** as Identity as a Service (IDaaS); created **policies, groups, users,** managed Role-Based Access Control (RBAC), and enabled **Multi-Factor Authentication (MFA)**.
- Configured and administered Linux servers, including **web services**, **VSFTP (FTP)**, and **SSH** services and other.

EDUCATION

BSC IN CYBER SECURITY — Jan 2024 – Present

University of Staffordshire (APIIT)

(Undergraduate)

CERTIFICATIONS

SOPHOS DETECTION & RESPONSE CERTIFIED ENGINEER V5.5

RED HAT CERTIFIED SYSTEM ADMINISTRATOR V9

FORTINET FORTIGATE 7.6 OPERATOR

FORTINET CERTIFIED ASSOCIATE CYBERSECURITY

UBUNTU LINUX PROFESSIONAL CERTIFICATE BY CANONICAL

FUNCTIONAL SKILLS	
Auditing & Hardening	• Hardening Linux servers to align CIS benchmark • Harden Cisco routers & switches • Audit & Hardent On-prem active directory with **CIS-CAT Pro** • Harden o365 according to CIS foundation benchmark v4.0.0 • Security assessment of Azure AD • Configuration audit of Cisco firewalls according to CIS benchmark • Create a customized benchmark for services/platforms where there is no CIS benchmark
Linux	• Linux system installation, configuration, and management • User and group administration, permissions, and access control • Filesystem management (**partitions**, **LVM**, **mount** points) • Software package management with **YUM/DNF** and **RPM** • Service management using **systemd** (start, stop, enable, disable services) • Network configuration and troubleshooting (IP addressing, hostname, DNS, routing) • Firewall configuration with **firewalld** and **SELinux** management • Bash scripting and automation of routine tasks • Scheduled task automation using **cron** and **at** • Storage management (**NFS**, **SMB**) • Process monitoring and resource management (**top**, **ps**, **systemctl**) • Basic troubleshooting and log analysis • Managing containers with **Podman** • Configure Services: **Apache**, **vsFTP**, **OpenVAS**, **Snort**, **MariaDB**, **PostgreSQL**, **Qmail**. • Container management using **PODMAN** and **DOCKER**
Routing & Switching	• Network design and troubleshooting (LAN/WAN, two-tier & three-tier architectures) • IPv4/IPv6 addressing, **subnetting**, and routing (static, **OSPF**, **RIP**) • **VLAN** configuration, **trunking** (802.1Q), and **inter-VLAN routing** • Switch and router configuration (Cisco IOS) • Spanning Tree Protocol (**STP**), **EtherChannel**, and **port security** • Access Control Lists (**ACLs**) and network security fundamentals • **NAT**, **DHCP**, **DNS**, and **NTP** configuration • Wireless LAN setup and security • Device management with **SSH**, **Telnet**, **Syslog**
On-prem AD	• Active Directory Domain Services (AD DS) deployment and management • User and group account administration, including provisioning, disabling, and permission assignments

	• Group Policy Object (**GPO**) creation and management for security and configuration enforcement • Organizational Unit (**OU**) structure design and delegation
Azure Cloud & o365	• Azure identity and access management (**Microsoft Entra ID**/Azure AD, **RBAC**, **users**, **groups**, **SSPR**) • Azure governance (**policies**, resource locks, **tags**, management groups, cost management) • Azure compute resource deployment and management (VMs, scale sets, App Services) • Azure storage management (blob, file, disk, backup, recovery vaults, Azure Site Recovery) • Virtual networking (**VNets**, subnets, **peering**, **NSG**, VPN, private endpoints, Azure DNS, **load balancers**) • Monitoring and troubleshooting with **Azure Monitor**, **Network Watcher**, and **log analytics** • Automation and resource management using Azure CLI, PowerShell, and **ARM templates** • Microsoft 365 productivity apps (Word, Excel, PowerPoint, Outlook, OneDrive, Teams, SharePoint) • Collaboration and communication solutions (Teams, Yammer, Viva, Stream) • Endpoint management and deployment (**Intune**, Endpoint Manager, Windows Autopilot) • Identity and access management (Azure AD, **MFA**, SSPR, **conditional access**) • Security, compliance, privacy, and trust (**Microsoft Defender**, **Purview**, **Zero Trust**, **Secure Score**) • Microsoft 365 **licensing**, **pricing**, and **support options**
Microsoft Intune	• **deploying**, **configuring**, **securing**, and **monitoring** devices and client applications across various operating systems (**Windows**, **iOS**, **Android**, **macOS**) • modern deployment techniques including **Windows Autopilot** and **Microsoft Deployment Toolkit (MDT)** • Configuring and managing device enrollment into **Microsoft Intune (automatic, bulk enrollment, enrollment profiles)** • Managing device lifecycle within Intune **(sync**, **restart**, **retire**, **wipe)** • Implementing and monitoring **compliance policies** for all supported device platforms using Intune • Configuring **Conditional Access policies** that require **compliance status** • **Managing local group membership** on Windows devices using Intune • Planning and implementing **app protection** (MAM) and **app configuration policies** for managed apps and devices • Configuring **antivirus**, **disk encryption (BitLocker)**, and **firewall policies** • Configuring Attack Surface Reduction **(ASR)** policies • Integrating Intune with **Microsoft Defender for Endpoint** and onboarding devices • Managing device updates using Intune **(Update rings)**

	• Implementing **Endpoint Privilege Management (EPM)** • Monitoring devices using Intune and **Azure Monitor** • Analyzing and responding to issues identified in **Endpoint Analytics** • Basic troubleshooting and log analysis related to endpoint management **(Log Analytics workspace)**
Firewalls & IPS/IDS	• Cisco ASA firewall configuration and management (**stateful inspection**, **access control policies**, **NAT**) • Snort IDS/IPS deployment and management (**real-time traffic analysis**, **packet logging**, protocol and content inspection) • **Signature-based** threat detection and alerting • Custom rule creation for tailored network protection • Operation in IDS (detection) and IPS (prevention) modes
Penetration Testing	• **Kali Linux**: Specialized Linux distro preloaded with hundreds of penetration tools • **Metasploit**: Exploit development, payload delivery, and post-exploitation tasks. • **Burp Suite**: Web app vulnerability scanning (SQLi, XSS), intercepting proxy, and manual testing. • **Nmap**: Network discovery, port scanning, OS fingerprinting, and scripting (NSE). • **Wireshark**: Deep packet analysis for protocol inspection and anomaly detection. • **Nessus/OpenVAS**: Automated vulnerability scanning with CVSS scoring and compliance checks • **John the Ripper**: Password cracking for various hash types
Fortinet Firewall and Threat Intelligence	• Configuration and management of **FortiGate NGFW**s • Implementing comprehensive network security features: ➢ **intrusion prevention (IPS)** ➢ **application control** ➢ **web filtering** ➢ **antivirus** • **Deep packet inspection (DPI)** for granular traffic analysis • VPN support and secure remote access. • **SSL VPN** • **IPsec VPN**