Nirmal Unagar

📱+44 7752713231 | 📧 nirmalunagar.uk@gmail.com | 📍 United Kingdom | 🌐 LinkedIn

---

SUMMARY :

Cybersecurity professional with expertise in **Elasticsearch SIEM**, **Logpoint SIEM**, and **Fortigate Firewall**. Successfully reduced cyber threats, optimised security infrastructure, and led migration initiatives, holding an MSC in Computer Forensics Cybersecurity.

TECHNICAL SKILLS :

- **SECURITY** : Elasticsearch(SIEM), LogPoint(SIEM), Defender, EDR, Wireshark, PCAP Analysis, Network Monitoring & Analysis, WAF,Vulnerability Assessment and Penetration Testing(VAPT), BloodHound(AD), KQL Basic.
- **SCRIPTING** : Python basic, Bash
- **NETWORK** : TCP/IP, OSI, HTTP, SSH, DHCP, FTP, DNS, Switching/Routing, Fortigate Firewall, IDS/IPS, Cisco
- **CLOUD** : AWS, Azure, Entra ID, Microsoft 365
- **SYSTEM ADMINISTRATION** : Windows IIS, SQLServer, Exchange Server, Ubuntu, Active Directory(AD), VMWare
- **Compliance :** ISO 27001, NIST, Cyber Essentials, PCI DSS

EXPERIENCE :

Security Engineer - SIEM/SOAR | University Of Winchester | UK | April 2024 - Present

- Investigate and triage **100+ monthly alerts** in **Logpoint SIEM** and **Microsoft Defender XDR**, improving threat detection and response accuracy.
- Reduced **false positives by 30%** and improved **response time by 40%** by fine-tuning SIEM rules and developing **15+ SOAR playbooks.**
- Handled weekly phishing incidents, performing **root cause analysis** and correlating data across email, SIEM, and endpoint logs.
- Uploaded and **enriched 200+ IOCs in OpenCTI**, identifying and tracking malicious IPs, domains, and file hashes.
- Conducted monthly **BloodHound AD** reviews, helping remediate **10+ privilege escalation paths** and reduce **attack surface**.
- Ran bi-weekly **Nessus scans** and coordinated patching to close **50+ vulnerabilities,** enhancing internal and external security.
- Collaborated with **IT/network teams** to block threats, update firewall policies, and enforce mitigation steps during active incidents.
- Created use cases mapped to the **MITRE ATT&CK framework** and automated agent deployment across **100+ systems** using **Ansible.**
- Authored detailed documentation and **monthly reports** to track improvements in threat coverage and reduce organizational risk.

SOC Analyst | CyberTalos | India| March 2022 - August 2023

- Proactively monitored and analysed security logs for clients, leveraging **Microsoft Defender, ELK** (SIEM), Grafana, and Zabbix to identify and mitigate potential threats. Achieved a **25% reduction** in attacks on clients and **20% improvement** in overall network infrastructure.
- Collaborated on incident response efforts, demonstrating a keen understanding of the business and efficiently containing security incidents within the Virtual Private Cloud (VPC) environment.
- Led successful migration initiatives, transitioning clients from on-premises infrastructure to CyberTalos' cloud services. Resulted in a significant **50% cost reduction** for infrastructure and security maintenance.
- Provided valuable insights into tuning and optimising Security Information and Event Management (**SIEM**) rules tailored to VPC environments. Contributed to a **15% improvement** in the efficiency of client's security operations.

System Admin| ECS Corporation | India | October 2021 - March 2022

- Offering **1st and 2nd** level IT support to a substantial customer base of **200+ clients**, troubleshooting and resolving a wide range of technical problems, including Desktop PC, Server, Network, hardware, software, and application issues.
- Demonstrated expertise **Fortinet FortiGate** and **SonicWALL** firewalls to ensure secure network operations, crafting comprehensive security policies, **DOS** policies, and managed access policies to safeguard against cyber threats and maintain network integrity.
- Managed **Citrix** Xen and **VMware ESXi** virtualization environments, utilising **PRTG, Nagios**, and **Cacti** to gain comprehensive network visibility and maintain optimal performance, resulting in **50% cost reduction** of client security expenses.

PROJECTS/HOMELAB :

BUILDING A IT SECURITY OPERATION (**SOC**) — USING OPEN-SOURCE TOOLS (ELK STACK, GNS3)

- Designed a small enterprise network to monitor **24x7 IT infrastructure** and practice **threat detection**. Utilised GNS3 tool, ELK Stack, **Ubuntu server** to simulate small enterprise network.
- Simulated 3 use cases: DOS attack prevented with Fortigate firewall, malware detected with ELK SIEM and **endpoint protection**, directory traversal attack detected on Apache using ELK SIEM.
- Strengthened network security and **incident response** capabilities, enhancing overall cybersecurity posture.

ACTIVE DIRECTORY WITH POWERSHELL (WINDOWS SERVER, VIRTUALBOX, WINDOWS 10)

- Configured **Windows Server 2019** as Domain Controller(**DC**) for **nmunagar.com**, implemented **NAT** services and **DHCP** for seamless communication in a VirtualBox Environment.

- Created user accounts, groups, and organisational units for streamlined access control. Established an admin-privileged user and automated the creation of **1000 users** using **PowerShell** scripting and Successfully **integrated** Windows client machines with the **AD domain.**

CERTIFICATES :

- **CompTIA Security+** | 2023 – 2026 | by CompTIA
- eLearn Junior Penetration Tester(**eJPTv2**) | 2023 - 2026 | by INE
- **AZ-900**: Azure Fundamentals | August 2021 | by Microsoft
- **AWS** Cloud Foundations | August 2019 | by AWS Academy
- **SC-200**: Microsoft Security Operations Analyst | Running | by Microsoft

EDUCATION :

MSC. COMPUTER FORENSICS & CYBERSECURITY | University of Greenwich, London, UK, 2022 - 23

Cybersecurity • Audit and Security • System administration & Security • Network Technology Design • Penetration Testing

B.TECH COMPUTER SCIENCE | Ganpat University, Ahmedabad, India, 2017 - 21