**FARHAN MOHAMMED**

[**ffmohammed98@gmail.com**](mailto:ffmohammed98@gmail.com)

**8179180355**

**Senior Cyber Security Engineer**

**PROFESSIONAL SUMMARY:**

* Over 10+ years of experience as a seasoned Cyber Security Professional with deep expertise in threat and vulnerability management, incident response, security operations, network and application security, and risk & compliance frameworks.
* Adept at implementing comprehensive security strategies that proactively defend against evolving cyber threats while aligning with business objectives.
* Hands-on experience with Vulnerability Assessment, Security Information and Event Management (SIEM), Data Loss Prevention (DLP), Endpoint Security, and Cloud Security solutions across complex enterprise environments.
* Extensively worked with leading tools such as Tenable Nessus Cloud, Microsoft Defender for Endpoint, Azure Security Center, and Palo Alto Cortex/XDR/Xpanse for effective incident detection, remediation, and advanced threat analytics.
* Proficient in conducting penetration testing, network traffic analysis, and firewall configuration using industry-standard tools like Metasploit, Wireshark, BurpSuite, and Snort.
* Demonstrated expertise in KQL (Kusto Query Language) for querying and analyzing security telemetry in Azure Sentinel, enabling real-time threat hunting and log analysis.
* Adept in implementing and supporting security governance frameworks such as NIST Cybersecurity Framework, ISO 27001, HIPAA, and PCI DSS, including the development of internal security policies and risk controls.
* Regularly lead phishing awareness campaigns and security training initiatives to improve the organization's overall security posture.
* Proven track record in integrating SailPoint IdentityIQ, working across Compliance, Governance, and Lifecycle Management (LCM) modules to enhance identity and access management within secure architectures.
* Deep experience in InfoSec mailbox handling, incident escalation, and application risk assessments, ensuring sub-hour SLA adherence for enterprise incident response.
* Strong background in SIEM platforms including IBM QRadar, LogRhythm, and McAfee Nitro SIEM, ensuring real-time monitoring, security analytics, and actionable threat insights across on-premises and cloud-based environments.
* Skilled in designing and managing enterprise DLP strategies using tools like Symantec DLP, McAfee DLP, and FireEye HX, including email monitoring and PHI field classification in compliance with HIPAA.
* Solid understanding of security protocols (TCP/IP, SSL, SSH), authentication/authorization, OSI model, and layered defense mechanisms across cloud (AWS, Azure) and on-prem infrastructure.
* Experienced in vulnerability management and compliance platforms such as QualysGuard, Rapid7 Nexpose, and Acunetix to proactively detect and mitigate security threats.
* Contributed to projects involving log ingestion pipelines, security roadmaps, and tool evaluations (e.g., Tanium, Fusion), along with managing ServiceNow ITSM workflows for ticketing and incident lifecycle.
* Trusted team member for on-call rotations, capable of handling critical security alerts and breaches during high-risk periods.

**PROFESSIONAL EXPERIENCE:**

**Client: NBC Universal, Dallas, TX Feb 2023– Till Date**

**Role: Senior Cyber Security Engineer**

**Project Overview:** The project is centred on enhancing enterprise cybersecurity posture across hybrid environments (on-prem + Azure + AWS) by implementing advanced threat detection and response mechanisms, robust vulnerability management, endpoint protection, and cloud-native security solutions. Key goals included securing critical media IP and sensitive user data while aligning with Zero Trust principles, NIST 800-53, ISO 27001, and CIS Benchmarks.

**Responsibilities:**

* Spearheaded Microsoft Azure Security initiatives including configuration of Microsoft Defender for Endpoint and Microsoft Sentinel, focusing on incident detection, alert triaging, and automated threat response using KQL-based analytics.
* Monitored and responded to security incidents, performing real-time threat hunting and log analysis in Sentinel, Cortex XDR, and Splunk, reducing false positives and improving MTTR.
* Conducted proactive vulnerability assessments and risk prioritization using Tenable Nessus, IBM AppScan, Acunetix, and aligned remediation efforts with CVSS, OWASP Top 10, and internal risk standards.
* Managed endpoint security using Palo Alto Cortex XDR, FireEye HX, Cisco AMP, and ISE, detecting and containing malware, suspicious activity, and lateral movement.
* Regularly performed incident response for critical alerts and breaches involving phishing, malware, and anomalous user behavior; created detailed RCA reports and shared IOC for threat intelligence.
* Integrated log sources from firewalls (Palo Alto, Checkpoint), endpoints, email gateways (Mimecast), and cloud platforms (Azure, AWS) into SIEMs (QRadar, Sentinel) for unified threat correlation and alert management.
* Ran KQL queries within Sentinel for deep threat analytics, and built dashboards for visualizing security KPIs and emerging attack vectors.
* Led phishing simulations and security awareness campaigns, while managing SOC mailbox escalations with SLA-driven response times.
* Evaluated new security tools including Tanium, Tenable, and Xpanse, provided technical demos, and assessed feasibility for environment-wide adoption.
* Implemented cloud security measures in AWS and Azure, including IAM policy hardening, GuardDuty, CloudTrail, S3 encryption, and Azure Defender configuration.
* Integrated DevSecOps controls by embedding SAST/DAST tools (Fortify, SonarQube, Checkmarx) in CI/CD (Jenkins) pipelines.
* Conducted secure code reviews, threat modeling (STRIDE), and attack surface analysis to minimize security design flaws.
* Developed and maintained incident response playbooks, compliance automation scripts, and configuration drift detection routines.
* Collaborated across DevOps, Network, and GRC teams to ensure holistic alignment of infrastructure security with business objectives.

**Environment:** Azure Security, Microsoft Defender, Sentinel, KQL, Palo Alto Cortex XDR/Xpanse, Nessus, IBM AppScan, Acunetix, Fortify, SonarQube, Checkmarx, Python, .NET, JavaScript, Jenkins, QRadar, Splunk, McAfee Nitro, AWS IAM/S3/GuardDuty/CloudTrail, Mimecast, Cisco AMP, Firepower, ISE, Symantec DLP, Trend Micro, Checkpoint, VLAN, 802.1x, SNMP, Wireshark, STRIDE, IOC, RCA, GRC, SAST/DAST, DevSecOps, ISO 27001, CIS Benchmarks, NIST 800-53

**Client: HSBC, Houston TX Oct 2020 – Jan 2023**

**Role: Cyber Security/Network Security Engineer**

**Project Overview:** Led the design, implementation, and maintenance of enterprise-grade network infrastructure and security systems for HSBC. Managed end-to-end network security architecture using Cisco, Juniper, Palo Alto, and Checkpoint devices, ensuring high availability, performance optimization, and policy compliance across global LAN/WAN environments. Ensured seamless integration of routing protocols, firewall security, and VPN tunnels, contributing to reduced network downtime and increased data protection in a banking environment.

**Responsibilities:**

* Configured, installed, and maintained Cisco & Juniper routers/switches (MX480, MX960, ASR 9K, Catalyst 6500/4500/3850, Nexus 7K/5K).
* Administered advanced Layer 2/3 protocols (STP, VTP, RSTP, PVST+, HSRP, VRRP, OTV, VDC, VLANs, VPC).
* Designed and optimized LAN/WAN environments using MPLS (LDP, TDP), VLSM, CIDR, and subnetting techniques.
* Implemented dynamic routing protocols (OSPF, BGP, EIGRP, IS-IS) across edge and core layers.
* Managed route redistribution, tunnel routing policies, and multicast (PIM, IGMP) implementations.
* Deployed and maintained Palo Alto (PA-3K/5K), Cisco ASA 5500, Checkpoint (13K/12K), and Juniper SRX (1500–5800) firewalls.
* Created and managed NAT, threat prevention, URL filtering, and IPS/IDS policies via Panorama, Firemon, and Checkpoint Web UI.
* Configured Site-to-Site and Remote VPNs using IPsec, SSL, and Web VPNs across multi-vendor environments.
* Utilized tools like SolarWinds Orion, Wireshark, tcpdump, and Cacti for real-time monitoring and bottleneck resolution.
* Conducted extensive network testing and simulation using IXIA, Spirent, Netscout, and iTest to verify pre/post-production stability.
* Configured Proxy, DHCP, DNS services, and handled Cisco ISE for identity-based access control and 802.1X authentications.
* Maintained up-to-date firmware and IOS versions across Cisco and Juniper devices to prevent vulnerabilities.
* Handled security incidents by analyzing logs, traffic, and alerts from QRadar SIEM and checkpoint IPS.
* Collaborated with cross-functional teams for change requests and service improvement plans (SIPs).
* Created SOPs and network topology documentation for ongoing knowledge transfer and disaster recovery planning.

**Environment:** Cisco (ASR 9K, ISR 4K, Catalyst 6500, Nexus 2K–7K), Juniper (MX480/960, SRX Series, EX/QFX Series), BGP, OSPF, EIGRP, IS-IS, Static Routing, VRF, STP, RSTP, HSRP, VTP, VLAN, VPC, OTV, Palo Alto (PA Series, Panorama), Cisco ASA 5500, Checkpoint 13K/12K, Juniper SRX, IPsec, SSL VPN, Web VPN, DMVPN, GRE, SolarWinds, Cacti, Wireshark, tcpdump, QRadar, Cisco ISE, Firemon, IXIA, Spirent Test Center, Netscout, iTest, RADIUS, TACACS+, 802.1X, TCP/IP, DHCP, DNS, SNMP, NAT, ACL, Proxy, Subnetting, Multicast, JUNOS, Cisco IOS, Firepower OS

**Client: Discover Financial Services, Riverwoods, IL Jan 2018 – Sep 2020**

**Role: Network Security Engineer**

**Project Overview:** Worked as a key member of the infrastructure and security team, responsible for securing and maintaining a highly available enterprise network across 11+ data centers. This involved implementing advanced routing protocols, migrating firewall architectures, securing wireless environments, and using automation and monitoring tools for proactive threat detection and performance optimization.

**Responsibilities:**

* Installed and configured Cisco switches (3500, 4500, 6500) and routers (7200, 7600, ASR 9K) across multiple environments.
* Implemented and managed VxLAN overlays, VDC, and VPC on Cisco Nexus 9K for virtualization and traffic segmentation.
* Integrated Cisco Nexus 9000 NX-OS with ACI Fabric, working in tandem with Nexus 7K and ASRs for MPLS core connectivity.
* Configured and optimized MPLS, BGP, OSPF, and EIGRP for route redundancy and convergence.
* Performed configuration on ASR 9K pairs with HSRP, bundle Ethernet setups, and DHCP profiles.
* Implemented load balancing and analyzed multicast routing for enhanced availability.
* Migrated firewalls from Cisco ASA 5520 to Palo Alto, using Palo Alto conversion tools and PAN-OS via Panorama (6.3).
* Configured and maintained ASA 5505/5540/5585 with Firepower, Checkpoint R77 Gaia, Juniper, and Fortinet firewalls.
* Monitored, mitigated, and analyzed threats using Cisco Firepower IDS/IPS, Splunk SIEM, and custom correlation rules.
* Worked on Cisco ISE 802.1X (wired, wireless guest), RADIUS authentication, and policy enforcement.
* Managed Aruba Clearpass and Aruba Central, configuring Master Controllers and Access Point Groups.
* Upgraded and configured Cisco 6500-E, 3560, and 2960 switches in compliance with ISE compatibility.
* Monitored infrastructure using SolarWinds, Cisco Prime, IT Tracker, Wireshark, and Cisco Works.
* Provided 24x7 L3 support for F5 LTM/GTM, performing configuration, upgrades, and troubleshooting of traffic steering.
* Supported performance tuning with NetFlow analysis and real-time alerts.
* Administered SAN fabrics across 11 data centers using Brocade and McData Director-class switches.
* Ensured high-availability and failover across production environments.
* Designed and implemented IPSec VPNs (Site-to-Site) using various encryption standards (MD5, 3DES).
* Hardened Checkpoint firewalls pre-production, conducted OS-level security configurations (Cisco OS, Linux - Fedora/Ubuntu, Windows).
* Utilized PowerShell for administrative tasks on Linux/Unix systems and remote server management.
* Participated in configuration automation and performance troubleshooting in hybrid environments.

**Environment:** Cisco Nexus (7K/9K), ASR 9K, VxLAN, VPC, VDC, MPLS, BGP, OSPF, EIGRP, HSRP, VRRP, Cisco ASA, Checkpoint R77 Gaia, Palo Alto (PAN-OS, Panorama), Fortinet, Aruba Clearpass, Aruba Central, Cisco ISE (802.1X), SAML, Active Directory, SolarWinds, Cisco Prime, Wireshark, Splunk SIEM, NetFlow, PowerShell, Linux (Ubuntu, Fedora), Windows Server, IPSec VPN, MD5, 3DES, NAC, IDS/IPS (Cisco Firepower), ACLs, Access Controls

**Client: JP MORGAN CHASE, JERSEY CITY, NJ Dec 2015 – Nov 2017**

**Role: Cyber Security Engineer**

**Project Overview:** Served as a core member of the enterprise network infrastructure team supporting JP Morgan Chase's global operations. Provided engineering expertise in designing, configuring, and maintaining high-performance LAN/WAN networks, implementing security protocols, and ensuring compliance within a highly regulated financial environment. The role required extensive hands-on experience with Cisco routers/switches, VPNs, firewalls, and WAN optimization tools across mission-critical financial data systems.

**Responsibilities:**

* Designed and configured VLANs using 802.1Q tagging, EtherChannels, and Spanning Tree Protocol (STP) to build scalable and redundant access, distribution, and core-layer architectures.
* Performed configuration, upgrade, and troubleshooting of Cisco routers (2500, 2600, 3000, 6500, 7200, 7500, 7606, 7609) and Catalyst switches (3550, 4500, 6505).
* Configured OSPF in both single-area and multi-area environments for optimized routing and network stability; implemented RIP, EIGRP, static routes, and policy-based routing as needed.
* Participated in Internet infrastructure redesign to meet growing bandwidth and failover requirements.
* Created and tested MPLS-based VPN setups using Cisco routers and ASA firewalls, ensuring secure and stable remote access.
* Utilized OPNET for performance modeling and packet tracing to identify bottlenecks and enhance network design.
* Conducted IOS upgrades, troubleshooting routing loops, packet loss, and hardware failures to ensure maximum network uptime.
* Installed and configured VPN solutions, firewalls, and intrusion detection/prevention systems (IDS/IPS) to secure internal and external traffic flows.
* Ensured disaster recovery and remote access security by conducting assessments and deploying mitigations aligned with industry best practices and compliance mandates (e.g., SOX, GLBA).
* Secured enterprise infrastructure through firewall rule management, strict ACLs, and Cisco ASA configurations.
* Deployed cloud-based network infrastructure, reducing on-site hardware dependency and cutting storage maintenance costs by 35%.
* Configured, tested, and monitored LAN/WAN components; implemented SNMP-based monitoring tools to proactively detect and resolve latency, throughput, and connectivity issues.
* Contributed to the deployment and support of Cisco Prime Infrastructure and SNMP monitoring solutions for performance analytics and fault detection.
* Monitored and optimized WAN performance by managing TDM and Frame Relay circuits, performing both provisioning and fault management.
* Conducted ongoing capacity planning and network health diagnostics, reducing outages and improving SLA compliance.
* Configured and supported Cisco Wireless Access Points (WAPs) and integrated Cisco Prime for centralized wireless management.
* Worked with Active Directory-integrated security policies to control user access across the enterprise.
* Supported hybrid network environments with a shift to cloud infrastructure, assisting in seamless migration while maintaining compliance and performance benchmarks.
* Participated in end-to-end project delivery across LAN, WAN, VPN, and Internet services, including short/long-term planning, implementation, and post-deployment support.
* Provided technical support and root cause analysis for network issues escalated by NOC/SOC teams.
* Presented architectural improvement recommendations to leadership based on assessments of network/application performance.

**Environment:** Cisco 2500–7600, Catalyst 3550/4500/6500, VLAN, STP, Ether Channel, OSPF, EIGRP, RIP, Static Routing, Policy-Based Routing, MPLS, Cisco ASA, VPNs (IPSec), IDS/IPS, ACLs, Security Zones, OPNET, Cisco Prime Infrastructure, SNMP, Network Performance Tools, Cisco WAP, Cisco Prime, AD Integration, Cloud-based networking, Disaster Recovery, Directory Services, Cisco IOS, SNMP Tools, Wireshark, Frame Relay, TDM.

**Client: Westar Energy, Kansas, MO August 2013 – April 2015**

**Role: Jr Cyber Security Engineer**

**Project Overview:** As part of the cybersecurity operations team, I was responsible for implementing and maintaining SIEM solutions, conducting vulnerability assessments, managing IDS/IPS systems, and ensuring compliance with regulatory frameworks such as PCI-DSS and FISMA. The focus was on securing the corporate network infrastructure, monitoring for threats, and proactively improving the overall security posture.

**Responsibilities:**

* Installed, configured, and managed IBM QRadar SIEM, including local and remote log collectors.
* Monitored real-time security events, correlated logs from firewalls, servers, and endpoints to detect and respond to threats.
* Investigated and triaged offenses created by correlation rules in QRadar to identify actual security incidents.
* Deployed and maintained SourceFire IDS/IPS and Snort, analyzing alerts to detect and mitigate network intrusions.
* Developed tuning rules for false positives and worked on signature-based threat identification.
* Conducted vulnerability scans using Rapid7 Nexpose to evaluate risk exposure.
* Developed remediation plans and tracked closure of vulnerabilities in coordination with IT teams.
* Captured and analyzed network packets using Wireshark to troubleshoot traffic anomalies and potential intrusions.
* Reviewed outbound traffic logs using Splunk to identify abnormal access attempts and data exfiltration threats.
* Managed endpoint protection tools to ensure antivirus and DLP compliance across all corporate systems.
* Reviewed and managed system-level security settings across Windows and Linux systems.
* Ensured compliance with PCI-DSS, FISMA, and COSO framework controls.
* Participated in risk management reviews and security certification efforts aligned with the NIST RMF.
* Performed OS updates and security patching across servers.
* Installed and configured log forwarding from newly built Windows and Linux log servers into QRadar.
* Documented all security processes and incident response procedures for audits.
* Assisted with configuring and troubleshooting routing protocols such as BGP, OSPF, and EIGRP during MPLS VPN expansions.

**Environment:** IBM QRadar, Splunk, SourceFire, Snort, Rapid7 Nexpose, Wireshark, PCI-DSS, COSO, FISMA, NIST RMF, Windows Server, Linux (Ubuntu, CentOS), BGP, OSPF, EIGRP, MPLS, Endpoint Protection, Antivirus, DLP, Security policies, remediation plans, audit documentation

**EDUCATION DETAILS:**

Bachelors

**TECHNICAL SKILLS:**

|  |  |
| --- | --- |
| **Programming & Scripting** | C, C++, Java, Python, JavaScript, PowerShell, Linux Shell Scripting |
| **Security Tools & Platforms** | SIEM: Microsoft Sentinel, IBM QRadar, LogRhythm, McAfee Nitro SIEM  Threat Detection & Response: Microsoft Defender for Endpoint, Palo Alto Cortex XDR/Xpanse, Mimecast, Fusion  Vulnerability Management: Nessus, Tenable, Nexpose, QualysGuard, Acunetix, Retina, IBM AppScan, Rapid7  Endpoint Protection & DLP: Symantec DLP, McAfee (HIPS, MOVE AV, HDLP), FireEye HX, Cisco AMP, Carbon Black  Penetration Testing: Metasploit, BurpSuite, SQLMAP, HP WebInspect, BeEF, OWASP ZAP  IAM: SailPoint IdentityIQ (Governance, Compliance, LCM), RSA Archer |
| **Cloud & Infrastructure Security** | Azure Security: Azure AD, Defender, Sentinel, KQL, Security Center  AWS Security: IAM, EC2, S3, CloudTrail  Other Platforms: CrowdStrike, Cisco Umbrella, Tanium |
| **Networking & Protocols** | TCP/IP, DNS, DHCP, SSH, SSL/TLS, PPTP, IPSec, SNMP, HTTP/S, FTP, L2TP, NetBIOS |
| **Security Standards & Frameworks** | NIST CSF, ISO 27001, OWASP, OSSTMM, HIPAA, PCI DSS |
| **Monitoring & Logging** | Splunk, SolarWinds, Bro/Zeek, Snort, tcpdump, Wireshark, KQL, ServiceNow ITSM |
| **Operating Systems** | Windows Server, Linux (Ubuntu, CentOS, Kali), VMware ESXi |
| **Firewalls, Proxies, & Appliances** | Palo Alto, Check Point, Cisco ASA, Cisco IronPort, Blue Coat Proxy |
| **Other Tools & Platforms** | Remedy, BMC BladeLogic, Governance Risk & Compliance (GRC) Platforms, Web App Scanning, Cloud Agents |