JOB SPECIFICATION

Cyber Security Specialist

Location	**Mumbai**
Reporting To	**Helpdesk Manager (India)**
Shift Model	**40 hours per week in rotating shift pattern covering 24×7 operations (UK aligned)**
Employment Type	**Full-time (Permanent)**
Salary Bracket	**Based on experience**

Company Introduction

VirtuHost Support Private Limited, based in Ghatkopar West, Mumbai (India), delivers world-class managed IT & Infrastructure, Cloud, Telecom/VoIP, Guest Wi-Fi, CCTV and Cyber Security services to UK and global clients.

Our operations run 24×7 from India, aligned with UK business hours, providing helpdesk, NOC/SOC, voice and infrastructure management. We combine Indian technical talent with global service standards, enabling clients to focus on their business, not their infrastructure.

Job Purpose

The Cyber Security Specialist will support VirtuHost's Managed Security Services by monitoring, managing, and improving cybersecurity operations for UK and global clients. This role includes Endpoint Protection, Firewall Management, Vulnerability Scanning, Cloud Security, and Compliance Assurance. The engineer will collaborate closely with our UK teams to deliver proactive threat management and continuous protection in a 24×7 environment.

Key Responsibilities

1. Deploy, configure, and manage EDR and antivirus solutions (CrowdStrike, SentinelOne, Defender ATP).
2. Continuously monitor and triage alerts from EDR, SIEM, and firewall systems; perform event correlation and threat analysis.
3. Investigate, contain, and remediate security incidents following standard playbooks (incident lifecycle management).
4. Conduct log analysis and prepare detailed incident reports, including root cause analysis and mitigation steps.
5. Manage and optimize firewall, proxy, and VPN configurations (Meraki or similar).
6. Review and update security baselines, policies, and group policies across Microsoft 365 and Azure AD.
7. Manage email security gateways (Proofpoint, Mimecast, or Microsoft Defender for 365), anti-phishing and spam filtering rules.
8. Perform vulnerability scanning using Tenable, Qualys, or open-source tools and assist in patch management closure.
9. Execute periodic compliance and security posture checks (CIS Benchmarks, NIST, ISO 27001 readiness).
10. Conduct backup integrity checks, DR test simulations, and data recovery drills using CloudBerry/MSP360 or similar tools.
11. Develop PowerShell scripts for automation of repetitive monitoring and alert triage tasks.
12. Maintain and update cybersecurity dashboards and documentation for audits and management reviews.
13. Provide training and mentoring to junior engineers on incident handling and security awareness practices.
14. Collaborate closely with UK security and network teams to ensure seamless 24×7 operations and handovers
15. Act as the first point of contact for support via phone, email, or ticketing tool.
16. Log, diagnose and resolve incidents for desktops, laptops, printers, and business apps.
17. Provide remote support using RMM, TeamViewer, or LogMeIn123.
18. Monitor, prioritise and escalate tickets as per SLAs.

19. Work within a rotating shift roster to provide 24×7 coverage, including weekends.

Required Skills & Qualifications

1. Bachelor's or Master's degree in Information Security, Computer Science, or a related discipline.
2. 2–6 years of experience in cybersecurity operations, SOC, or managed security service provider (MSSP) environment.
3. Hands-on experience with endpoint security, firewall management, and Microsoft 365/Azure security administration.
4. EDR/XDR tools: CrowdStrike, SentinelOne, Microsoft Defender ATP.
5. SIEM platforms: Splunk, Azure Sentinel, Wazuh, or similar.
6. Network & perimeter security: Cisco Meraki, Fortinet, Palo Alto, Ubiquiti.
7. Email & DNS security: Cisco Umbrella, Mimecast, Proofpoint, or Defender for 365.
8. Cloud security: Azure Security Centre, Conditional Access, MFA, Identity Governance.
9. Vulnerability scanning and patch management tools: Tenable, Qualys, ManageEngine.
10. Knowledge of MITRE ATT&CK.
11. Familiarity with PowerShell for automation and analysis scripting.
12. Understanding of backup and disaster recovery frameworks (MSP360).
13. Strong analytical and problem-solving mindset with attention to detail.
14. Excellent communication and documentation skills for UK and international stakeholders.
15. Proactive attitude towards learning emerging security tools and frameworks.
16. Ability to work under pressure during security incidents and coordinate with multiple teams.
17. Certifications preferred: CompTIA Security+, Microsoft SC-900/SC-200, CEH, AZ-500, or equivalent.
18. Familiarity with ticketing systems processes.
19. Excellent English communication skills and customer service orientation.
20. Excellent attitude and great phone etiquette.

21. Team Player with ability to motivate and knowledge share with other team members to deliver excellent customer services.
22. Ability to demonstrate clear and confident communication skills both written and verbal.
23. Ability to deal with problems and technical issues in a friendly, calm and positive manner.
24. Passion for Technology with a drive to help customers take advantage of new solutions.
25. Ability to multi-task, prioritise and escalate accordingly
26. Tenacity and dedication to pursue an issue from beginning to end.
27. Self-motivated, with the ability to work unsupervised.
28. Desirable: Hospitality IT experience.

Working Hours & Shift Pattern

1. 40 hours per week on a rotating shift basis covering 24×7 operations (day, afternoon, night, and weekend shifts).
2. Occasional overtime or on-call support may be required.

Performance Metrics

1. Timely detection and response to incidents and alerts.
2. Reduction in security incidents through proactive measures.
3. Accuracy and completeness of incident and RCA documentation.
4. Compliance with patching, vulnerability, and reporting SLAs.
5. Training participation and certification progress.
6. Incident resolution time (First Call Resolution where possible)
7. SLA adherence (Response and Resolution time)
8. Ticket backlog and escalation volume
9. User satisfaction / client feedback
10. Knowledge base contribution
11. Attendance and shift punctuality
12. Client feedback and collaboration quality with UK teams.

What We Offer

1. Exposure to global clients and advanced cybersecurity environments.
2. Opportunities to work with cutting-edge tools like EDR, SIEM, and Azure Security Centre.
3. Career path toward security engineer or SOC analyst lead roles.
4. Ongoing training and certification support.
5. Supportive and inclusive work culture focused on innovation and excellence.
6. Friendly and inclusive work culture in a technically rich environment.

How to Apply

Email your CV to **HR@virtuhostsupport.com** with “Cyber Security Specialist” in the subject line. We will use your details only to assess your application, as described in our Privacy Policy at virtuhostsupport.com.