FORTINET NSE 1 ASSOCIATE
FORTINET NSE 2 ASSOCIATE
FORTINET NSE 3 ASSOCIATE
CISCO CERTIFIED CCIE SECURITY
ISC2 CC SM
aws certified Cloud Practitioner FOUNDATIONAL
aws certified Solutions Architect ASSOCIATE
aws certified Security SPECIALTY
Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE
Microsoft CERTIFIED CYBERSECURITY ARCHITECT EXPERT

# MOHAMMED HABEEB UDDIN

KL Sentral, Jalan Tun Sambanthan, Kuala Lumpur, Malaysia 50470 | +60 197897239 | habeebccie@gmail.com

## Professional Summary

Dynamic and accomplished cybersecurity professional with over 9 years of extensive experience in designing, implementing, and managing comprehensive security solutions to safeguard organizations from emerging cyber threats. Proven expertise in leading Cloud Security, Security Operations Center (SOC) management, advanced incident response, and threat hunting across cloud, network, and on-premises environments. Skilled in mitigating advanced persistent threats (APTs), addressing zero-day vulnerabilities, and optimizing security posture through innovative strategies and robust security architectures.

Recognized for successfully handling high-severity ransomware attacks, deploying advanced NDR/EDR/XDR/SIEM solutions, and ensuring compliance with global regulatory standards such as GDPR, PCI-DSS, HIPAA and NIST. Adept at conducting in-depth security assessments, developing strategic security initiatives, and aligning cybersecurity objectives with business goals to drive operational efficiency and minimize risks.

Strong technical proficiency with a proven track record of fostering cross-functional collaboration and achieving measurable improvements in security posture. Seeking to leverage my leadership, technical expertise, and strategic vision to enhance an organization’s cybersecurity resilience and innovation.

## Key Skills & Expertise

- **Cloud Security and Security Operations Center (SOC) Management**
- **Advanced Incident Response & Threat Mitigation**
- **Threat Intelligence & Cyber Forensics**
- **Security Architecture & Governance**
- **Zero Trust, and Network Security**
- **Risk Assessment & Vulnerability Management**
- **Data Loss Prevention (DLP) & Email Security**
- **SIEM Integration & Optimization (Splunk, Elastic Stack, QRadar)**
- **Network Security (Firewalls, SD-WAN, VPNs)**
- **DevSecOps & Automation (SIEM, SOAR, Infrastructure as Code, CI/CD Security, Container Security, Kubernetes Security)**
- **Security Frameworks & Regulatory Compliance**
- **Cloud Workload Protection & Cloud Security Posture Management (CWPP, CSPM)**
- **Endpoint Detection & Response (EDR/XDR) and Threat Hunting**
- **Cloud-native Security Solutions & Security Automation**
- **Security Logging, Monitoring & Incident Investigation**
- **Infrastructure Security & Microsegmentation**
- **Automation & Scripting (Python, PowerShell)**

# Experience

**Cyber Security Threat Defence L3 Engineer**
**Tenaga Nasional Berhad (TNB) Malaysia (Minfy Technologies SDN BHD Payroll) 07/2024 to Present**

**Core Responsibilities and Technical Expertise:**

- Specialized in advanced incident analysis using industry-standard tools such as Splunk and AWS-native services (e.g., GuardDuty, CloudTrail, CloudWatch) to identify and analyze security incidents in cloud and on-prem environments.
- Led incident qualification by triaging events, categorizing incidents by severity, and assessing potential impact, leveraging MITRE ATT&CK frameworks to identify attack patterns TTP's.
- Conducted detailed root cause analysis (RCA) to determine the origin and nature of cyber-attacks, implementing actionable findings to enhance detection capabilities and mitigate reoccurrence of similar incidents.
- Monitored AWS Cloud Security Console and SIEM platforms for security alerts from integrated log sources, such as AWS CloudTrail, VPC Flow Logs, and GuardDuty, providing Level 3 insights for detecting advanced persistent threats (APTs), insider threats, and external attacks.
- Utilized AWS Security Hub and CloudWatch to aggregate and correlate security events across AWS accounts and regions, ensuring real-time visibility and quick action on potential threats.
- Conducted deep-dive investigations into suspicious network activity and abnormal API calls, analyzing logs to uncover tactics, techniques, and procedures (TTPs) used by attackers.
- Led incident response efforts for AWS-based security incidents, coordinating with cross-functional teams to contain and mitigate threats in real-time.
- Developed and executed containment strategies for security incidents such as data breaches or ransomware attacks, utilizing AWS Lambda functions, AWS WAF, Security Groups, and NACLs to isolate affected resources and limit the scope of damage.
- Ensured proper forensic preservation of compromised AWS resources, using tools like AWS CloudTrail and Amazon Macie for data classification and protecting PII (Personally Identifiable Information).
- Led efforts to continuously improve AWS security posture through Security Hub, ensuring adherence to best practices, such as CIS AWS Foundations Benchmark
- Utilized tools like AWS Config, Inspector, and Trusted Advisor to perform regular security assessments and implement automated remediation actions to enforce strong security configurations and patching cycles.
- Deployed AWS IAM best practices to enforce least privilege access policies and performed regular audits of IAM roles, policies, and permissions to minimize attack surfaces.
- Led triage and remediation of complex attack vectors such as botnets, APTs, and webshells, leveraging endpoint detection (e.g., CrowdStrike, SentinelOne) and network Detection and response tools to gather forensic evidence and mitigate threats.
- Worked with Multiple SOC tools to review network and system logs, DNS records, and payloads, helping identify and block malicious IP addresses and domains related to active threats.
- Collaborated directly with data asset owners (e.g., application owners, and database administrators) to develop tailored response plans during high-severity incidents, ensuring minimal business disruption and rapid recovery.
- Provided Level 3 expertise and technical guidance during security incident escalation, ensuring proper action is taken across affected systems while maintaining continuous communication with executive and business stakeholders.
- Developed incident playbooks for common threat scenarios, working closely with business units to ensure quick recovery and compliance with business continuity plans.
- Integrated threat intelligence feeds (e.g., MISP) with AWS tools to enhance detection and response capabilities, improving visibility into emerging threats.
- Worked with the security operations team to continuously update use cases for SIEM tools (e.g., Splunk, AWS Security Hub, AWS OpenSearch) based on evolving attack patterns and threat intelligence, reducing false positives while ensuring timely detection of critical incidents.
- Utilized AWS GuardDuty to create custom detection rules for detecting specific suspicious behaviours, such as port scanning, privilege escalation, and reconnaissance activities, improving incident detection and response time.

**Cloud Security Lead**
**Minfy Technologies Pvt. Ltd. 11/2023 to 06/2024**

**Core Responsibilities and Technical Expertise:**

- Served as the subject matter expert for cloud security solutions, ensuring **architecture designs** adhered to industry standards and compliance requirements.
- Developed and implemented security architectures for **AWS and Azure environments**, incorporating advanced controls such as encryption, firewalls, and identity management systems.

- Led the implementation of information security frameworks (ISO 27001, NIST, GDPR) to protect sensitive data, manage risks, and ensure confidentiality, integrity, and availability across systems.
- Monitored global cloud environments for security incidents, integrating threat intelligence feeds with detection tools like **AWS Security Hub, Azure Sentinel, and SIEM** platforms to enhance threat visibility.
- Conducted forensic investigations of cloud-related cyber incidents, leveraging tools like AWS CloudTrail, **Azure Security Center, and GuardDuty** to analyze root causes and prevent future occurrences.
- Designed and maintained cloud security policies, standards, and procedures, ensuring alignment with organizational goals and regulations, including GDPR and CIS Benchmarks.
- Provided advanced response strategies during security breaches, leading cross-functional efforts to mitigate threats with minimal business disruption.
- Developed risk mitigation strategies and automated security configurations using tools such as **AWS Config** and Azure Policy to ensure compliance and enhance security posture.
- Regularly collaborated with business stakeholders to ensure alignment between **cloud security** measures and operational goals.

**SOC Specialist** **09/2021 to 11/2023**
**Garrett Advancing Motion**

**Core Responsibilities and Technical Expertise:**

- Conducting in-depth analysis and investigation of critical and high-score detections across various security tools including EDR, NDR, IDS/IPS, Proxy, Zscaler-VPN, Windows, AWS, CyberArk, AD, CyberX, ESET, DLP, MSO365, Firewall, SDWAN, and MDN events.
- Proactively performing threat hunting, identifying threat vectors, and developing use cases on security tools such as EDR, SIEM, NDR, and Agari.
- Managing prevention policies, exceptions, custom IOA, and correlation rules across all security tools to enhance protection measures.
- Deploying NDR sensors organization-wide to monitor network traffic detections and authentications effectively.
- Delivering daily security investigation reports to the Chief Information Security Officer (CISO) for comprehensive insights.
- Ensuring the stability of email infrastructure by deploying policies and conducting deep investigations on imposter, malicious, spoofed, and spam emails.
- Strengthening security tools utilized in security operations to fortify the organization's defense mechanisms.
- Generating Monthly KPI Risk Dashboards and presenting insights to the leadership team to drive informed decision-making.
- Identifying security environment gaps and providing actionable insights to the CISO for strategic improvements.
- Developing correlation rules, reports, and alerts on the SIEM Splunk tool to enhance threat detection capabilities.
- Integrating logs from diverse technologies into Splunk for centralized monitoring and analysis.
- Regularly reviewing existing use cases on the SIEM Splunk Tool and optimizing detection logic to minimize false positives.
- Performing root cause analysis and responding promptly to critical/non-critical incidents.
- Reporting potential security breaches, incidents, and policy violations, ensuring timely resolution and mitigation.
- Contributing to the Cyber Incident Response Team (CIRT) by executing end-to-end incident response activities including incident communication, host triage and recovery, remote system analysis, and remediation efforts using various tools.
- Addressing red flags highlighted in Technical Account Manager (TAM) meetings to mitigate risks effectively.
- Monitoring and ensuring staff analysts and engineers adhere to ticket management within SLAs.
- Continuously revising and developing processes to enhance security monitoring and response capabilities.
- Keeping abreast of emerging security threats and industry best practices to stay proactive in threat mitigation strategies.

**Senior Technical Engineer** **09/2021 to 06/2022**
**Hitachi India Pvt. Ltd.**

**Core Responsibilities and Technical Expertise:**

- Monitoring and Investigating of Cyber security incidents and detections, addressing all security incidents and ensuring timely escalation
- Performing all Security event monitoring, management, and response operations
- Fine-tuning IPS/IDS signatures on Perimeter firewalls in the organization
- Working on Security Tools like EDR(Crowdstrike), SIEM(Splunk), Email security (Agari)
- Investigating deeper on the detected behavioral anomalies Adding context to the incident to understand the behavior
- Supporting on Integration of logs in Splunk from Onprem and Cloud devices within the organization
- Monthly auditing policies on Firewall and Proxy for security hygiene
- Working with cross-functional teams to resolve security incidents
- Co-ordinating with stakeholders, building and maintaining positive working relationships with them
- Analyzing data from multiple tools and data sources
- Interacting with different IT stakeholders to remediate the incidents on a defined time
- Ensuring compliance with SLA, process adherence, and process improvisation to achieve operational objectives
- Working as part of a team to ensure that corporate data and technology platform components to safeguarded from known threats

**Security and Network Engineer** **01/2020 to 09/2021**
**Adecco India Pvt Ltd**

**Core Responsibilities and Technical Expertise:**

- Monitored and analyzed security events using SIEM platforms, investigating incidents across endpoints, applications, and network logs.
- Conducted vulnerability assessments and threat analysis, proactively mitigating risks based on real-time threat intelligence.
- Investigated endpoint anomalies and implemented whitelisting strategies for business-critical applications.
- Supported escalation processes during security incidents, providing detailed forensic insights to improve response times.
- Collaborated on projects to enhance network security architecture, including firewall rule optimizations and traffic segmentation.
- Delivered regular security audits and policy reviews to maintain compliance with organizational and regulatory standards.

**Security Engineer** **11/2015 to 12/2019**
**Gleam Telesolutions Pvt. Ltd.**

**Core Responsibilities and Technical Expertise:**

- Managed and supported IPsec tunnels for secure intranet communication with partners and customers.
- Designed and implemented network segmentation strategies including DMZ, and shop floor network using firewalls (Checkpoint, Cisco ASA, Juniper) to enhance security.
- Configured and monitored SD-WAN solutions, aligning with security best practices to optimize performance and protection.
- Conducted regular firewall backups, audits, and policy reviews to maintain robust network defenses.
- Provided technical expertise for POCs, including Fortinet and Palo Alto implementations, to evaluate new security solutions.
- Supported VPN deployments, including IPsec SSL and AnyConnect, ensuring secure remote access for users.

## Core Technology Proficiencies

- **SOC Management & Cybersecurity Incident Response**
- **EDR Solutions**: CrowdStrike Cortex XDR, SentinelOne
- **NDR Tools**: Vectra
- **SIEM Platforms**: Splunk, QRadar, OpenSearch, Elastic Cloud
- **Email Security**: Agari Phishing Defense & Response
- **DLP Solutions**: AWS Macie, Forcepoint, Symantec DLP
- **Vulnerability Management**: AWS Inspector, Rapid7, Nessus, Security score card
- **Threat Intelligence**: MISP, Mandiant, Bluesify
- **Cloud Platforms & Security**: AWS (Amazon Web Services), Microsoft Azure, Google Cloud Platform GCP

- **Cloud Security**: AWS GuardDuty, AWS Detective, AWS Config, Cloudtrail, Cloud Watch, Trusted Advisor, AWS Identity and Access Management (IAM) Azure Security Center
- **Application Security**: Paloalto ADEM, SentinelOne, WAF
- **VAPT**: Burp Suite, Metasploit, Nmap, Owasp ZAP
- **Security Frameworks**: MITRE ATT&CK, GDPR, PCI-DSS, NIST, SOC 2, ISO 27001, CISA, HIPAA
- **Network Security**: Firewalls (Checkpoint, Cisco ASA, Fortinet), VPN (Site-to-Site, Remote Access), SD-WAN (Opensystem, Aryaka, VMware)
- **Proxy**: WSS Symmantec Cloud, Zscaler
- **SDWAN:** Opensystem, Aryaka, Vmware
- **Wireless:** Cisco Wireless controller, Aruba access-points
- **Authentication & Access Control**: Cisco Identity Services Engine (ISE), RADIUS
- **Networking Hardware**: Cisco Routers (3000, 4000, 7000), Catalyst Switches (2000x, 3000x)
- **Endpoint Security**: Seqrite EPS, Trend Micro, Cisco AMP, McAfee
- **Monitoring & Diagnostics**: SolarWinds, Wireshark

## Education, Training and Certifications

| | | |
|---|---|---|
| **Certified Information System Security Professional CISSP (In progress)** | **ISC2** | **2025** |
| **Microsoft Certified Cybersecurity Architect (SC-100)** | **Azure** | **2025** |
| **Microsoft Certified Azure Security Engineer Associate (AZ-500)** | **Azure** | **2025** |
| **AWS Certified Security Specialty (SCS-C02)** | **AWS** | **2024** |
| **Certified in Cyber security by ISC2 (CC)** | **ISC2** | **2024** |
| **AWS certified solutions architect associate (SAA-C03)** | **AWS** | **2024** |
| **AWS Cloud Practitioner (CLF-C02)** | **AWS** | **2023** |
| **Fortinet NSE 3 certified Fortinet** | **Fortinet** | **2023** |
| **Fortinet NSE 2 Certified Fortinet** | **Fortinet** | **2022** |
| **Fortinet NSE 1 Certified Fortinet** | **Fortinet** | **2022** |
| **Digital Forensics and Incident Response (self-paced) DFIR** | **DFIR** | **2021** |
| **Certified Ethical Hacker (CEH) Training CEH** | **EC-council** | **2021** |
| **Attempted CCIE - Security LAB** | **Cisco** | **2019** |
| **Cisco Certified Internetwork Expert - Security (written) Cisco** | **Cisco** | **2019** |
| **CCIE-Security Training** | **Netmetric** | **2019** |
| **Seqrite - End Point Security & DLP Training** | **Seqrite** | **2018** |
| **Palo Alto Certified Network Security Engineer (PCNSE)** | **Space Media** | **2016** |
| **CCNA, MCSE & Linux** | **Space Media** | **2015** |
| **Bachelors: Electronic & Communication Engineering** | **JNTU Hyderabad** | **2015** |