ROLE PROFILE

Position Title: Senior Manager Managed Service - Security	**Reporting to:** Assistant Director Managed Services
Business Unit: Business	
Division: Business Solutions	**Department:** Managed Services

A. ROLE AND CONTEXT

Purpose: The role is responsible for driving the adoption and governance of Ooredoo's Managed SOC platform and other managed security services, ensuring successful customer onboarding and seamless delivery of 24/7 SOC operations. This role leads the design, deployment, and management of comprehensive security solutions, including network security, threat detection, incident response, and cloud security, tailored to the needs of enterprise clients. The Senior Manager works closely with the operations team to ensure the effective monitoring and delivery of SOC services, while maintaining oversight of security governance and compliance. The primary focus of this role is to increase the adoption of Ooredoo's shared SOC platform by onboarding new customers and ensuring efficient delivery and continuous improvement of managed security services. The Senior Manager also ensures alignment between security operations and customer requirements, overseeing the governance and performance of the SOC to meet service-level agreements (SLAs) and security standards	**Functional Context:** Ooredoo's Business BU is a critical part of the company's first line customer facing activities for all Business Accounts and has a significant role to play in long term business value creation through product design, achievement of sales revenue, profit and customer satisfaction, as defined in the annual business plans. modes: responding to specific partnership requests from other departments (e.g., Product Hub, Professional Services) and proactively scouting partners based on industry trends and market opportunities. The Managed Services department is an integral revenue growth area to the newly created business solution division focused initially on providing services in the established managed connectivity and security areas and mandated with overall growth in revenue and in further new domains such as cloud. Whereas the professional services team is the overall lead in acquisition and delivery of projects, the managed services team is focused on offering and maintaining managed services as on-going customer services (recurring revenues). OQ is sending a strong signal to the enterprise market by giving focus to the managed services domain as a means to enhance customer value and engagement continuously with the OQ quality of service, and for that, the Managed services team is responsible for building and delivering that quality.

B. ROLE ACCOUNTABILITIES

- Serve as the technical lead for SOC as a managed service and other security solutions during pre-sales engagements, assessing the security posture of clients and designing tailored solutions that include SOC, SIEM (Security Information and Event Management), network security, DDoS protection, endpoint protection, and cloud security.
- Conduct security assessments to identify vulnerabilities and potential risks, then develop and propose custom solutions using technologies such as firewalls, IDS/IPS, SIEM, and encryption protocols to ensure comprehensive security for client networks.
- Work with sales teams to deliver technical presentations, demonstrations, and detailed proposals that align with the customer's business objectives and provide clear value from Ooredoo's managed security services.
- Design and deliver technical proposals that include security architecture diagrams, compliance strategies, threat detection mechanisms, and security features that are aligned with regulatory standards such as ISO 27001, PCI-DSS, and GDPR.
- Provide input on pricing strategies for SOC and managed security services, ensuring they are competitive while maintaining profitability and sustainability for Ooredoo.
- Implement advanced technologies such as machine learning-based threat detection, extended detection and response (XDR), network traffic analysis (NTA), and deception technologies within the SOC to enhance detection capabilities and reduce mean time to detect (MTTD) and mean time to respond (MTTR).
- Lead the deployment of cloud-native security services such as cloud access security brokers (CASB), multi-cloud monitoring, and cloud workload protection to protect workloads in hybrid and multi-cloud environments.
- Stay ahead of cybersecurity trends and threats, such as zero-day vulnerabilities, ransomware attacks, and supply chain threats, ensuring Ooredoo's SOC platform integrates cutting-edge solutions to mitigate new risks.

ROLE PROFILE

•	Lead efforts to increase adoption of Ooredoo's Managed SOC platform, working closely with sales and pre-sales teams to showcase the platform's capabilities and demonstrate its value in real-time threat detection, comprehensive incident response, and compliance reporting.
•	Oversee the onboarding process for new customers, managing the integration of their security infrastructure into the SOC environment, including SIEM systems, endpoint detection and response (EDR) tools, network security, and cloud security controls.
•	Ensure that all onboarding activities meet customer-specific security requirements and technical configurations such as log collection, correlation rules, alert thresholds, and incident management protocols.
•	Provide technical expertise in the integration of multi-cloud security environments (e.g., Azure, Google Cloud) into the SOC platform, ensuring seamless data flow and security event monitoring from cloud-native infrastructure.
•	Oversee the 24/7 SOC operations, ensuring that security monitoring and response activities are continuously delivered with high availability and meet Service Level Agreements (SLAs).
•	Collaborate closely with the SOC operations team to configure and maintain SIEM, SOAR (Security Orchestration, Automation, and Response) tools, and advanced threat intelligence systems to enable automated threat detection, triage, and incident response.
•	Ensure that SOC services include the use of cutting-edge technologies, such as AI/ML-based threat detection, behavioural analytics, and anomaly detection, enabling proactive identification of security breaches and suspicious activities.
•	Establish and monitor governance protocols for security event handling, ensuring adherence to best practices in incident handling, response times, and forensics.
•	Conduct regular security audits to validate the performance of the SOC against industry standards.
•	Serve as the primary security advisor for customers, from the pre-sales phase through post-deployment, ensuring that they are fully informed and satisfied with Ooredoo's managed security services.
•	Conduct regular security reviews with customers, evaluating the performance of the SOC and other security services, addressing any issues, and identifying opportunities for upgrades or additional services.
•	Provide ongoing technical support to customers, ensuring quick response to security incidents, vulnerabilities, and potential breaches, with a focus on maintaining continuous security operations.
•	Maintain knowledge of the client's security environment, business operations, competitor activities in the account, security needs, and risk appetite to proactively present solutions to OQ clients before they have identified a concern.
•	Approach the client with a consultative approach (pre-sales), and maintain a solution expert and trusted partner attitude through the RFX , contract negotiation phase and delivery, thus enhancing the value of OQ over sub-contractors and cyber security providers.
•	Provide clients with cyber security-related workshops and education to ensure high awareness and cultivate the need within client organizations to continuously improve and invest in cyber security adoption and compliance.
•	Work closely with operations and service delivery to ensure that SOC operations are delivered seamlessly.
•	Oversee the integration of various security tools, including firewalls, VPNs, IDS/IPS, and web application firewalls (WAF), within the SOC platform to enable comprehensive monitoring and protection.
•	Work with service delivery and operations to lead incident response coordination, ensuring that SOAR systems automate threat intelligence ingestion, security alerts prioritization, and incident management workflows, reducing manual intervention while maintaining operational effectiveness.
•	Maintain strong oversight of security governance for all SOC operations, ensuring that security policies, incident handling procedures, and audit trails are consistently followed and well-documented.
•	Ensure managed security services comply with international standards such as ISO 27001, PCI-DSS, GDPR, NIST, and local regulatory requirements.
•	Implement regular compliance checks and vulnerability assessments to maintain adherence to these standards.
•	Work with customers to align their security infrastructure with compliance regulations, providing tailored SOC solutions that meet data protection and privacy requirements.

C. SCOPE AND INTERACTIONS

Direct Revenue Responsibility: Yes	**Primary Interactions (Internal/External)**

ROLE PROFILE

Direct Budget Responsibility: Yes **Direct People Management Responsibility:** No	**Internal Relationships:** Cross Functional	**External Relationships:** Vendors Business Partners Customers

D. KEY PERFORMANCE INDICATORS (KPI)

• Proposal Conversion Rate: Percentage of SOC and security solution proposals converted into signed contracts.
• SOC Platform Adoption Rate: Percentage increase in the number of customers adopting Ooredoo's Managed SOC platform.
• Customer Onboarding Efficiency: Time and accuracy of customer onboarding to the SOC, ensuring seamless integration of customer security
• systems.
• Incident Detection and Response Time: Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) for incidents handled by the SOC.
• Customer Satisfaction (CSAT): Feedback on SOC services, onboarding experience, and overall security service quality.
• Compliance & Audit Success Rate: Percentage of successful compliance audits and adherence to regulatory standards across SOC operations.
• Revenue Growth: Revenue generated from SOC and other managed security services.
• Business Case Profitability: Percentage of business cases that result in improved profitability and cost savings for both the customer and Ooredoo.

E. EXPERIENCE, QUALIFICATIONS AND SKILLS

Minimum Experience, Essential Knowledge & Skills	**Minimum Entry Qualifications**
10 years' experience in a similar role. Experience in cybersecurity architecture, SOC management, or managed security services in a MSSP, telecom provider, or security vendor. Proven expertise in driving the adoption of SOC platforms and deploying SIEM technologies, including Microsoft Sentinel, Google Chronicle, SentinelOne, Palo Alto, Cisco SecureX, and Splunk. Strong understanding of AI-driven threat detection, incident response, and SOAR integration within a SOC environment. Experience managing 24/7 SOC operations and overseeing compliance with ISO 27001, PCI-DSS, GDPR, and NIST standards. Ability to work cross-functionally with sales, operations, and technical teams to ensure the successful delivery	Bachelor's Degree in Business Administration or Marketing or Engineering **Preferred Certifications / Other Qualifications** CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager), CCSP (Certified Cloud Security Professional), CEH (Certified Ethical Hacker), or other relevant certifications.

Technical Competencies	**Required Level**	**Behavioural Competencies**	**Required Level**
SECURITY OPERATIONS	Expert	Building Customer Value	Intermediate
PRODUCT DEVELOPMENT & MANAGEMENT	Advanced	Delivering Results & Fostering Collaboration	Intermediate
DATACENTRE & CLOUD	Advanced	Shaping Strategy	Intermediate
CYBERSECURITY PRESALES	Expert	Driving Change	Basic
PRICING	Advanced	Networking and Influencing Collaboratively	Basic
		Leading Teams	Basic

Competency Level (Reference Range)	**Basic**	**Intermediate**	**Advanced**	**Expert**
	Low >----------->----------->----------->High			