Here is the revised table following your exact instructions, with each requirement presented verbatim from the tender documents and responsibility assigned according to the specified logic:

| **Requirement (exact from tender)** | **Responsible Party** | **Explanation** |
| --- | --- | --- |
| "Submit large-scale SOC/NOC operations reference projects" | MSP Partner | MSP manages continuous operations and maintains reference project documentation. |
| "Demonstrate case studies of incident response strategies" | Cytomate via MSP escalation | MSP provides initial response documentation; Cytomate supplies specialized IR case studies for escalation scenarios. |
| "Handling advanced persistent threats" | Cytomate via MSP escalation | APT detection initiated by MSP; specialized APT response handled by Cytomate through escalation. |
| "Application of SIEM tools" | MSP Partner | Core SIEM operation is fundamental to MSP's continuous monitoring service. |
| "SOAR implementation experience" | MSP Partner | Automation implementation falls under MSP's managed security operations. |
| "Personnel must hold certifications such as GIAC, CISSP" | MSP Partner | Staffing certification requirements fulfilled by MSP's HR and team management. |
| "24-hour SOC team structure and resource qualifications" | MSP Partner | Continuous SOC operations are core MSP responsibility. |
| "SOC Manager must have a computer-related degree and CISSP/CISM certification" | MSP Partner | Management role staffing handled by MSP. |
| "Provide a role skills table" | MSP Partner | Operational documentation maintained by MSP. |
| "GIAC Security Operations Manager (GSOM) role: 10+ years of cybersecurity experience" | MSP Partner | Management personnel qualifications provided by MSP. |
| "GIAC Security Operations Manager (GSOM) role: 3-5 years of SOC management experience" | MSP Partner | Operational management expertise delivered by MSP. |
| "GIAC Security Operations Manager (GSOM) role: Responsible for 24x7 SOC operations" | MSP Partner | Continuous SOC management is core MSP function. |
| "GIAC Security Operations Manager (GSOM) role: Team management" | MSP Partner | Personnel management is MSP responsibility. |
| "GIAC Security Operations Manager (GSOM) role: Establishing incident response procedures" | MSP Partner | Procedure development is part of MSP's service framework. |
| "GIAC Security Operations Manager (GSOM) role: Compliance and SLA management" | MSP Partner | Operational compliance managed by MSP. |
| "L1 SOC Analyst (6 people): Bachelor's degree and relevant certifications" | MSP Partner | Entry-level staffing requirements handled by MSP. |
| "L1 SOC Analyst (6 people): 2-3 years of SOC environment experience" | MSP Partner | Tier-1 operational expertise provided by MSP. |
| "L1 SOC Analyst (6 people): 24/7 monitoring and initial triage" | MSP Partner | Continuous monitoring is core SOC function. |
| "L2 SOC Analyst (3 people): Higher education and certifications" | MSP Partner | Mid-level staffing requirements fulfilled by MSP. |
| "L2 SOC Analyst (3 people): 4-6 years of SOC or network security response experience" | MSP Partner | Tier-2 operational expertise provided by MSP. |
| "L2 SOC Analyst (3 people): Incident analysis and investigation" | MSP Partner | Mid-level incident handling is MSP responsibility. |
| "L2 SOC Analyst (3 people): Detection use case development" | MSP Partner | SIEM optimization is part of MSP's monitoring service. |
| "L2 SOC Analyst (3 people): Cross-departmental collaboration" | MSP Partner | Operational coordination handled by MSP team. |
| "L2 SOC Analyst (3 people): Strategic reporting" | MSP Partner | Reporting deliverables are part of MSP's service. |
| "L3 SOC Analyst: Handling complex security events" | Cytomate via MSP escalation | Complex incidents escalated to Cytomate's specialized IR team. |
| "L3 SOC Analyst: Threat hunting" | Cytomate | Proactive threat hunting is Cytomate's core capability. |
| "L3 SOC Analyst: Digital forensics" | Cytomate | Forensic analysis is Cytomate's specialized service. |
| "L3 SOC Analyst: Education: computer-related major" | Cytomate | Cytomate provides certified experts for advanced roles. |
| "L3 SOC Analyst: Experience: multiple years in information security" | Cytomate | Specialized expertise provided by Cytomate. |
| "L3 SOC Analyst: Skills: knowledge of SIEM and other tools" | Cytomate | Tool expertise for advanced analysis provided by Cytomate. |
| "Vulnerability Assessment (VA) Analyst: Conduct vulnerability scanning" | MSP Partner | Vulnerability management is part of MSP's continuous monitoring. |
| "Vulnerability Assessment (VA) Analyst: Analyze and prioritize by risk and business impact" | MSP Partner | Risk analysis is core to MSP's VA service. |
| "Vulnerability Assessment (VA) Analyst: Report remediation recommendations" | MSP Partner | Reporting deliverables provided by MSP. |
| "Vulnerability Assessment (VA) Analyst: Education: computer science or related degree" | MSP Partner | Staffing requirements handled by MSP. |
| "Vulnerability Assessment (VA) Analyst: Experience: 3-5 years in vulnerability management/IT security" | MSP Partner | Operational expertise provided by MSP. |
| "Threat Hunter: Develop hypotheses based on threat intelligence" | Cytomate | Threat intelligence analysis is Cytomate's specialization. |
| "Threat Hunter: Execute threat hunting using SIEM and other tools" | Cytomate | Proactive threat hunting is Cytomate's core service. |
| "Threat Hunter: Education: computer science or related degree" | Cytomate | Cytomate provides certified threat hunting experts. |
| "Threat Hunter: Experience: 5+ years in threat hunting/response" | Cytomate | Specialized expertise provided by Cytomate. |
| "Threat Intelligence Analyst: 3-5 years of experience in cybersecurity" | MSP Partner | Intelligence analysis is part of MSP's SOC operations. |
| "Threat Intelligence Analyst: Monitor threat intelligence" | MSP Partner | Continuous monitoring is core MSP function. |
| "Threat Intelligence Analyst: Analyze incident data" | MSP Partner | Data analysis is part of MSP's intelligence service. |
| "Threat Intelligence Analyst: Education and certifications as required" | MSP Partner | Staffing requirements handled by MSP. |
| "NOC Manager: 10+ years of network operations experience (including management)" | MSP Partner | Network operations management is core MSP responsibility. |
| "NOC Manager: Manage 24-hour NOC operations" | MSP Partner | Continuous NOC management provided by MSP. |
| "NOC Manager: Team compliance" | MSP Partner | Operational compliance managed by MSP. |
| "L1 NOC Analyst (6 people): Network event monitoring" | MSP Partner | Tier-1 network monitoring is core NOC function. |
| "L1 NOC Analyst (6 people): Basic fault diagnosis" | MSP Partner | Initial troubleshooting handled by MSP. |
| "L1 NOC Analyst (6 people): Education, certification, experience as specified" | MSP Partner | Staffing requirements fulfilled by MSP. |
| "L2 NOC Analyst (3 people): Handle escalated issues" | MSP Partner | Tier-2 network support provided by MSP. |
| "L2 NOC Analyst (3 people): In-depth diagnosis" | MSP Partner | Advanced troubleshooting handled by MSP. |
| "Senior Network Specialist (L3): Resolve routing, switching and other network issues" | MSP Partner | Advanced network support is part of MSP's NOC service. |
| "Senior Network Specialist (L3): Collaborate with team for configuration backups" | MSP Partner | Network management tasks handled by MSP. |
| "Senior Network Specialist (L3): Education, experience as specified" | MSP Partner | Staffing requirements fulfilled by MSP. |
| "Senior Network Specialist (L3): Lead resolution of major incidents" | Cytomate via MSP escalation | Major security incidents escalated to Cytomate's IR team. |
| "Senior Network Specialist (L3): Optimize network architecture" | MSP Partner | Network optimization is part of MSP's service delivery. |