Skop Dan Spesifikasi Pembaharuan Sokongan Penyelenggaraan Sistem E-Mail Majlis Sukan Negara Malaysia

Bil	Perkara	Memenuhi/ tidak memenuhi	Harga
	Number of Users: 814 mailbox Distribution list: 33 Groups Number of Domain: nsc.gov.my & mail.nsc.gov.my Current version: Patch 8.8.15_P45		
1	**Description Email-as-Service**		
1.1	**Professional Maintenance** a. Update and maintain mail system to the latest version. b. Update patches and Common Vulnerabilities and Exposures for Operating System. c. Maintain and update reputation block lists brute force attacks or abuse. d. Check Server Logs Regularly. e. Manage and monitor the status of the backups. f. Manage and monitor healthy check server status. g. Manage and maintain Storage Utilization. h. Review Server Resource Usage and suggestions for improvement.		
1.2	**Professional Support** a. Unlimited email support and up to 4 hours of phone support per month during our normal business hours. b. Priority response from support staff with responses within 2 hours during our normal business hours. c. Technical support for troubleshooting or any issues: - Patching - Tunning - Security Check		

1.3	**Support & Maintenance** - 2 years Warranty. - Remote support 8 hours/working days. - Provide annual report preventive maintenance.		
1.4	**Other Services** - Maintain SPF, DKIM, DMARC email domains. - Provide at least 1 (one) uptime monitoring service for Majlis Sukan Negara Malaysia.		
2.0	**Network Security Monitor (NSM)**		
2.1.0	**Provided by Majlis Sukan Negara** Standalone Deployments: Physical - 12GB RAM - 4 CPU cores - 1TB storage - Fast Ethernet		
2.1.1	**Requirement to provide:** a. Able to detect intruders: - Network visibility, - Host visibility, - Intrusion detection honeypots, - Log management, and - Case management. b. Web based Dashboard to monitor the security event c. Host to monitor: 3 hosts - 1 host Main Firewall - 1 host Main Website - 1 host Main System		

2.1.2	**Support & Maintenance:** a. Provide for 2 Year b. Half- Yearly Report		
2.2.0	**Preparation Activity:**		
2.2.1	Infrastructure Assessment: Conduct a thorough assessment of the existing infrastructure to ensure it meets the requirements for deploying NSM. This includes evaluating hardware specifications such as CPU, memory, and storage capacity, as well as network connectivity and bandwidth.		
2.2.2	Deployment Plan: Develop a comprehensive deployment plan that outlines the tasks, timelines, and responsibilities for each phase of the deployment process. Define clear objectives and milestones, and allocate resources accordingly to ensure a successful deployment.		
2.3.0	**NSM monitor:**		
2.3.1	Hardware Setup: Set up the hardware that will host the NSM deployment. Ensure that the hardware meets the minimum requirements specified by NSM, including CPU, memory, and storage capacity.		
2.3.2	Enable module: a. IDS/IPS (Intrusion Detection/Prevention System) that can analyze network traffic and detect malicious activities. b. Network analysis framework that can monitor network traffic and generate detailed logs for analysis. c. Real-time data storage and indexing, data collection and filtering, data visualization and analysis.		

	d. Intrusion detection system (HIDS) that focuses on monitoring activities on individual systems or hosts and can analyze logs and detect suspicious activities on individual systems.		
2.4.0	**Configuration:**		
2.4.1	Network Configuration: Configure network interfaces on the NSM hosts according to the network topology and requirements. Assign IP addresses, subnet masks, gateway addresses, and DNS servers as necessary. Ensure that each host can communicate with other hosts and devices on the network.		
2.4.2	Sensor Configuration: Configure NSM sensors to monitor network traffic using tools such as Suricata or Snort. Specify the network interfaces to monitor and configure detection rules and policies to detect and alert on suspicious activity.		
2.4.3	Log Collection Configuration: Set up log collection from various sources, including network devices, servers, and applications. Configure inputs to collect logs using protocols such as syslog, SNMP, or filebeat. Define filters and parsers to extract relevant information from log messages.		
2.4.4	Agent Configuration: installing an agent is to facilitate the collection, enrichment, and forwarding of data from various sources indexing and search, visualization and analytics, and additional components for data processing and storage.		

2.5.0	**Integration:**		
2.5.1	Existing System Integration: Integrate NSM with existing security systems and tools, such as SIEM platforms, threat intelligence feeds, and ticketing systems. Configure connectors or APIs to exchange data and events between NSM and other systems. Ensure that integration points are properly configured and tested to ensure seamless communication between systems.		
2.5.2	Alert Configuration: Configure alerts and notifications within NSM to notify administrators of security incidents or suspicious activity. Define alert thresholds, severity levels, and notification methods (e.g., email, SMS, SNMP). Test alerting mechanisms to ensure that alerts are triggered and delivered as expected.		
2.6	**Testing:**		
2.6.1	Functional Testing: Conduct functional testing of the NSM deployment to verify that all components are functioning correctly. Test network traffic monitoring, intrusion detection, log collection, and alerting mechanisms. Verify that sensors are capturing and analyzing network traffic, and that alerts are generated for detected security threats.		
2.6.2	Performance Testing: Perform performance testing to ensure that the deployment can handle the expected workload without degradation. Test scalability by increasing traffic volume and analyzing system performance under load. Identify any bottlenecks or performance issues and optimize the deployment accordingly.		
2.6.3	User Acceptance Testing: Involve users and stakeholders in user acceptance testing to validate that the NSM deployment meets their requirements and expectations. Gather feedback from users on usability, functionality, and performance, and incorporate any necessary changes or enhancements.		

2.7	**Knowledge sharing:**		
2.7.1	Knowledge sharing: Provide comprehensive training to users on using NSM for network monitoring and security analysis. Cover topics such as navigating the NSM interface, interpreting security alerts, and responding to security incidents. Tailor training sessions to the specific roles and responsibilities of each user group.		
2.7.2	Administrator Training: Offer specialized training to administrators on configuring and managing the NSM deployment. Cover topics such as sensor configuration, rule management, and system maintenance tasks. Provide hands-on training and exercises to reinforce learning and build practical skills.		
2.8	**Documentation:**		
2.8.1	Installation Guides: Develop detailed installation guides that provide step-by-step instructions for installing NSM on different types of hardware or virtual environments. Include screenshots, command-line examples, and troubleshooting tips to assist users during the installation process.		
2.8.2	Configuration Manuals: Create comprehensive configuration manuals that document the configuration settings and options for NSM components, including sensors, log collectors, and alerting mechanisms. Include explanations of configuration parameters, best practices, and recommended settings.		
2.8.3	Operational Procedures: Develop operational procedures that outline common tasks and workflows for operating and maintaining the NSM deployment. Document procedures for adding new sensors, updating detection rules, and responding to security incidents. Include troubleshooting guides and troubleshooting steps for common issues.		

2.9	**Handover:**		
2.9.1	Formal Handover Process: Conduct a formal handover process to transfer ownership of the NSM deployment to the users or operations team. Schedule a meeting to review the deployment documentation and training materials with the handover recipients. Clearly communicate roles, responsibilities, and expectations for ongoing support and maintenance.		
2.9.2	Knowledge Transfer: Provide hands-on training and support to the handover recipients to ensure they are comfortable with operating and maintaining the NSM deployment. Offer guidance and assistance as needed during the transition period to address any questions or concerns.		
2.9.3	Transition Support: Offer ongoing support and assistance to the handover recipients during the transition period. Address any issues or challenges that arise and provide guidance on troubleshooting and problem resolution. Monitor the deployment closely to ensure a smooth transition and address any issues proactively.		
2.1	**Post-deployment Support:**		
2.10.1	Issue Resolution: Provide post-deployment support to address any issues or questions that arise after the handover. Troubleshoot and resolve technical issues related to the NSM deployment. Document and track support requests to ensure timely resolution.		
2.10.2	Monitoring and Maintenance: Monitor the NSM deployment for performance, stability, and security incidents. Perform routine maintenance tasks, such as software updates, security patches, and system backups. Implement monitoring tools and alerts to proactively identify and address issues.		

2.10.3	Review and Audit: Conduct periodic reviews and audits of the NSM deployment to ensure that it continues to meet requirements and objectives. Evaluate performance metrics, security posture, and compliance with best practices. Identify areas for improvement and implement enhancements as needed.		
2.11	**Support:**		
2.11.1	Software Updates: Regularly update NSM components, including the base operating system, security tools, and other software packages, to ensure they are patched against known vulnerabilities and exploits.		
2.11.2	Security Rule Updates: Keep intrusion detection system (IDS) rules and signatures up to date to detect the latest threats and attack techniques. Subscribe to threat intelligence feeds and vendor updates to stay informed about emerging threats and updates.		
2.11.3	Performance Monitoring: Monitor the performance of the NSM deployment, including CPU and memory utilization, network bandwidth, and storage capacity. Identify and address any performance bottlenecks or resource constraints to ensure optimal operation.		
2.11.4	Incident Response: Develop and maintain incident response procedures to promptly respond to security incidents or alerts generated by NSM. Establish clear escalation paths and workflows for investigating and mitigating security incidents.		

2.11.5	Log Management: Regularly review and analyze log data collected by NSM to identify security events, anomalies, or indicators of compromise. Investigate suspicious activity and take appropriate action to mitigate risks and prevent further compromise.		
2.12	**Maintenance:**		
2.12.1	Regular Audits and Reviews: Conduct periodic audits and reviews of the NSM deployment to assess its effectiveness, compliance with security policies and standards, and alignment with business objectives. Identify areas for improvement and implement enhancements as needed.		
2.12.2	Vendor Support: Utilize vendor support resources and forums to troubleshoot technical issues, obtain assistance with configuration or customization, and stay informed about product updates and best practices.		
	Jumlah Keseluruhan		