12.1. Regular Maintenance Tasks

Regular maintenance is essential for the optimal performance and security of the Spectra360 Security Operations Center (SOC) platform. Implementing a structured maintenance schedule ensures that systems remain up-to-date, vulnerabilities are addressed promptly, and the SOC operates efficiently.

Key Maintenance Tasks:

1. **System Updates and Patch Management:**
    - Regularly apply software patches and updates to operating systems, security tools, and applications to address vulnerabilities and enhance functionality.
2. **Security Policy Review and Updates:**
    - Periodically review and update security policies, firewall rules, and access controls to align with evolving threats and organizational changes.
3. **Backup Verification:**
    - Ensure that data backups are performed regularly and verify their integrity to guarantee data recovery in case of incidents.
4. **Vulnerability Assessments:**
    - Conduct regular vulnerability scans and assessments to identify and remediate security weaknesses within the infrastructure.
5. **Log Management:**
    - Maintain and review logs of all network communications and activities to detect anomalies and support forensic investigations.
6. **Performance Monitoring:**
    - Continuously monitor system performance metrics to identify and address potential issues before they impact operations.
7. **Incident Response Plan Testing:**
    - Regularly test and update the incident response plan through tabletop exercises and simulations to ensure preparedness.

      learn.microsoft.com
8. **Asset Inventory Management:**
    - Keep an up-to-date inventory of all hardware and software assets to manage configurations and assess security posture effectively.
9. **User Access Reviews:**
    - Periodically review user accounts and permissions to ensure appropriate access levels and remove any unnecessary privileges.
10. **Documentation Updates:**

    - Maintain and update documentation for processes, configurations, and procedures to reflect current practices and support training efforts.

Recommended Maintenance Schedule:

- **Daily:**
    - Monitor security alerts and system performance.
    - Review critical logs for unusual activities.
- **Weekly:**
    - Apply routine system updates and patches.
    - Verify the success of data backups.
- **Monthly:**
    - Conduct vulnerability assessments and remediate findings.
    - Review and update security policies as needed.
- **Quarterly:**
    - Test the incident response plan with simulations.
    - Perform comprehensive user access reviews.
- **Annually:**
    - Audit the asset inventory for accuracy.
    - Review and update all documentation.

Revision #3
Created 9 February 2025 21:06:51 by Admin
Updated 10 February 2025 10:52:47 by Admin