

Security Engineer (1)

Roles and Responsibilities

The Security Engineer works on all network security issues related to OCIO, and reports to Cyber security once the security threats have been mitigated. The main duties are listed below:

ADMINISTRATIVE TASKS

- Act as the back up to the Sr. Security engineer for managing system access
- Review and revise related security standard operating procedures (SOPs) as required
- Responsible for providing input to the weekly and monthly status reports
- Provide scan results report to be briefed during the weekly CSB/NSB Knowledge Share meeting.
- Monitor all network devices using Tripwire to ensure no malicious events are occurring on network devices.
- Conduct a weekly vulnerability assessment of all CSB and NSB devices using the Internet Scanner (ISS) tool, and have weekly meeting regarding the plan of mitigation of the vulnerabilities.
- Ensure all Microsoft patches have been applied by using Patchlink. If any malicious activity or virus propagation occurs on the network I am alerted by Cyber Security and will investigate and mitigate immediately and report my finding to the appropriate officials.
- Participate in project meetings to implement all security protocols outlined in the ASSERT database and mitigate all tasks in the POA&M's (Plan of Action and Milestones). According to the FISMA, NIST and OMB requirements
- Ensure proper operation and good security practices for the firewall and IDS/IPS implementation project. Assist in wireless security measures needed for conference room project.
- Work with the VPN concentrator ensuring all security measures have been implemented and maintained.
- Generate and update ITSM tickets when required
- Act as back up for monitoring/answering the NOC service line
- Responsible for opening/updating/closing items on the WTSO bulletin board

DAILY/WEEKLY/MONTHLY TASKS

- Act as back up to the junior security engineer for reporting and managing the Tripwire application, a report is generated every week
- Conduct a weekly vulnerability assessment of all CSB and NSB devices using the Internet Scanner (ISS) tool.
- Ensure all Microsoft patches have been applied by using Patch link.
- Reporting malicious activity or virus propagation on the network
- Participate in weekly meetings regarding the plan of action to mitigate noted vulnerabilities.
- Act as primary for managing the administration of the Cisco TACACS Server application such as: adds, moves, deletes, accounts etc.
- Act as primary for managing the administration of the Cisco VPN Server application such as: adds, moves, deletes, accounts etc.
- Act as primary for providing a Patchlink patch report, on the 10th of every month.
- Management of the Network Services Branch (NSB) firewalls
- Providing remote dial- in capabilities for users

TROUBLESHOOTING/SUPPORT

- Ensure all Microsoft patches have been applied by using Patch link. If any malicious activity or virus propagation occurs on the network they will be investigated and mitigated immediately. The findings will be reported to the appropriate officials.
- Participate in project meetings to implement all security protocols outlined in the ASSERT database and mitigate all tasks in the POA&M's (Plan of Action and Milestones). According to the FISMA, NIST and OMB requirements
- Assist HQMAN with best practices and ensure availability of service, confidentiality and integrity of systems and data.
- Ensure proper operation and good security practices for the NSB firewalls.
- Assist in wireless security measures needed for conference room project.
- Work with the VPN concentrator ensuring all security measures have been implemented and maintained.
- Make recommendations on proposed projects such as wireless conference room, IDS/IPS implementation.
- Provide troubleshooting support and recommendations for security and network issues
- Investigate, report and mitigated security vulnerabilities immediately



[Click here](#) to **Submit Your Resume**