Alabama Supercomputer Authority

ASA

Position: SOC Analyst
Reports to: SOC Lead
Location: Alabama Supercomputer Center- Huntsville
Send resumes to personnel@asc.edu

General Description

SOC Analysts are responsible for the daily investigations and resolutions of security events and issues experienced by ASA and ASA members. SOC Analysts assist the SOC lead and other technical staff in the development of playbooks used to systematically address security alerts. SOC Analysts will work closely with firewall, systems, and network specialists to audit configurations and recommend enhancements. They interface extensively with ASA's SIEM and network management platforms to gather information needed to counter security threats.

Responsibilities

- Gather information and address current security events and incidents on ASA and ASA member networks through use of the ASA SIEM and systems and network management platforms including Cortex XSIAM, Strata Cloud Manager, Zabbix, XDR, Sophos, Nessus, etc.
- Where possible, follow and execute established incident response playbooks to systematically address events and issues while fully documenting issues, challenges, and resolutions.
- Work with the SOC lead and other technical staff in networking, security, and systems administration to assist in the development of additional procedures and playbooks as needed.
- Work with firewall specialists to audit configurations and recommend needed changes or enhancements.
- Schedule, execute, and validate recurring and ad-hoc Tenable Nessus vulnerability scans, review findings to filter false positives, and deliver simplified and focused reports to member technical staff to address issus.
- Create detailed documentation for review with ASA and member staff on all incidents.
- Assist ASA members as needed with local incident response (travel may be required)

Minimum Requirements

- Must work on site in Huntsville, Alabama. Remote work arrangements are not available.
- Bachelor's degree or equivalent experience in Cybersecurity, Computer Science, Information Technology, or a related field from an accredited college, university.
- One year of experience in at least one related field: Cybersecurity, Networking, Systems Administration, etc.
- Solid understanding of the basics of cybersecurity, systems administration and computer networking.
- Solid understanding of cyber security terms, processes, and event types.
- Basic understanding of Palo Alto Next Generation Firewalls and Juniper SRX firewalls architectures and capabilities.
- Strong work ethic, communication skills, and customer service expertise

Preferred Qualifications

- Practical, direct experience with SIEM/SOAR tools, ticketing systems, and vulnerability scanners.
- Certifications: CompTIA CySA+, CompTIA Security+, Palo Alto Security Operations Professional, Palo Alto XSIAM Analyst, or related.