SOC Analyst (WarU E-ITSS)

Concept Plus is a mission-focused technology solutions provider that transforms IT concepts into impactful solutions for federal agencies. Headquartered in Fairfax, VA, we bring the agility, responsiveness, and customer intimacy of a small business combined with the quality and infrastructure of a larger firm.

Recognized as an award-winning Oracle partner, we have delivered innovative solutions across Defense, Intelligence, Civilian, Health IT, and Tribal sectors. Our highly certified experts build systems that drive efficiency, accelerate modernization, and ensure mission outcomes with certainty.

We offer competitive pay, comprehensive health, dental, and vision insurance, paid life insurance, paid time off, 11 paid holidays, performance bonuses, tuition reimbursement, unlimited training, and the opportunity to thrive in a collaborative, flexible, and innovative environment.

For more information, visit www.conceptplus.com.

About the role

Concept Plus is seeking a SOC Analyst to support the Enterprise Cybersecurity Operations Support Team by performing foundational monitoring, analysis, and incident reporting activities. This role assists in identifying potential security events, learns to operate approved cybersecurity tools, and helps maintain the security posture of mission critical information systems in accordance with FISMA/NIST and DoW standards.

What you'll do

- Monitor network, host, and security systems for basic indicators of suspicious activity and escalate findings according to SOC procedures.
- Use approved cybersecurity tools (e.g., Splunk/Sentinel, ACAS) to conduct initial event triage and support vulnerability identification.
- Assist with reviewing alerts, IDS/IPS notifications, antivirus logs, and host based security findings.
- Support incident response activities by gathering data, documenting observations, and preparing reports for senior analysts.
- Assist in evaluating system updates or deployments for potential cybersecurity impacts.
- Participate in threat research, correlation activities, and SOC process improvement efforts under the guidance of senior staff.
- Maintain awareness of emerging threats, cybersecurity best practices, and DoD security requirements

Required Qualifications

- US Citizen with active Secret clearance
- Bachelor’s degree in Computer Science, Information Technology, Cybersecurity, or a related field (or equivalent experience)
- Exposure to Microsoft Defender

- Understanding of TCP/IP, basic networking concepts, OSI model, and common security terminology
- Exposure to SIEM platforms (Splunk or Sentinel) or vulnerability scanning tools such as ACAS
- Ability to write or interpret simple SPL or KQL queries (or willingness to learn quickly)
- Understanding of common cyber threats, malware behavior basics, and alert triage concepts
- Strong analytical skills and willingness to learn in a fast paced SOC environment
- DoD 8140 Certification Requirements
    - Must meet IAT Level II baseline (Security+ CE, CySA+, CASP+, GSEC, SSCP, CND, CCNA Security, CCNP Security, CCSP, CISA, CISSP or Associate)
    - Compliant for CSSP Analyst within 6 months of hire (CEH, CySA+, GCIA, GCIH, GICSP, PenTest+, Cloud+, CFR, CCNA Cyber Ops, SCYBER)

Concept Plus is an Equal Opportunity Employer. As such, we will give your application full consideration without regard to your race, color, religion, sex, age, national origin, disability, veteran status, sexual orientation, gender identity, or any other classification protected by federal, state, or local law.