Interview

Monday, July 22, 2019 4:15 PM

Skillset:-

6+ years' experience in a hands-on technical role in Cyber Security Engineering for Security Operations, or Security Monitoring solutions Engineering.

- Excellent knowledge of SIEM, Security Monitoring, Machine Learning, Behaviour Analytics, Advanced Persistent Threats, attack tools, techniques, and methods used by adversaries.
- Excellent knowledge on design, installation, configuration and management of SIEM
- Excellent written and verbal communication skills and ability to escalate timely to management.
- Experienced in multicultural virtual team management and coordination.
- Strong decision making capability on remediation actions to respond to security engineering incidents.
- Ability to define, prioritize and execute process in a structured manner.
- Experience with networking and TCP/IP traffic, along with **firewall**, SIEM, **Orchestration**, IPS, **NGAV, EDR, APT, DLP, proxy and antivirus solutions**.
- Desirable: Experience with a programming/scripting language.
- Desirable: CISSP, IBM Certified Associate Administrator - Security QRadar SIEM Certification, HP ArcSight Security Administrator Certification, Splunk Architect Certification

Cybersecurity terms:

1. IPS:
   An **Intrusion Prevention System** (IPS) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. Vulnerability exploits usually come in the form of malicious inputs to a target application or service that attackers use to interrupt and gain control of an application or machine. Following a successful exploit, the attacker can disable the target application (resulting in a denial-of-service state), or can potentially access to all the rights and permissions available to the compromised application.

   From <https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips>
   Detections:
   a. Signature-based detection
      i. Exploit-facing signatures
      ii. Vulnerability-facing signatures
   b. Statistical anomaly detection

2. SIEM: Log data analysis to detect threat and penetrations
3. TCP/IP Security architecture:
   a. Application layer
   b. Transport layer
   c. Network layer
   d. Data link layer

Technical

Monday, July 22, 2019 4:17 PM

Tableau Dashboard Designing -

1. Refer documents

KNIME -

1. Refer link and find documents

IT Security -

1. Refer links and learn