L3 SOC ANALYST

Requirement: SOC SIEM Analyst
Job Location : Mumbai / Pune
Experience Range: 5 to 10 Years

Job Description:

We're looking for a dynamic and experienced Security Analyst to be part of an our leading client's SOC. Working with the Security Team the SOC will deliver strong Incident response capabilities, oversight of technical controls and assist with continual service improvement.

Primary Roles and Responsibilities:

Roles :

- Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities.
- Isolate and remove malware.
- Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warnings).
- Provide daily summary reports of network events and activity relevant to cyber defense practices.
- Receive and analyze network alerts from various sources and determine possible causes of such alerts.
- Notify designated managers, cyber incident responders and articulate the event's history, status, and potential impact for further action in accordance with the organization's incident response plan.
- Analyze and report system security posture trends.
- Assess adequate access controls based on principles of least privilege and need-to-know.
  Work with stakeholders to resolve computer security incidents and vulnerability compliance.

Required Knowledge :

- Computer networking concepts and protocols, and network security methodologies.
- Cyber threats and vulnerabilities.
- Authentication, authorization, and access control methods.
- Cryptography and cryptographic key management concepts
- Incident response and handling methodologies.
- Network traffic analysis methods.
- Key concepts in security management (e.g., Release Management, Patch Management).

- Network tools (e.g., ping, traceroute, nslookup)
- Network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.
- Encryption methodologies.
- Windows/Unix ports and services.
- Systems security testing and evaluation methods.
- Network mapping and recreating network topologies.
- Packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).
- Operating system command-line tools.

Required Skills and Experience:

- Skill in using incident handling methodologies.
- Skill in collecting data from a variety of cyber defence resources.
- Skill in recognizing and categorizing types of vulnerabilities and associated attacks.
- Skill in performing packet-level analysis.
- Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).
- Experience in conducting trend analysis.
- Experience analyzing malware.
- Experience conducting vulnerability scans and recognize vulnerabilities in security systems.
- Experience detecting host and network-based intrusions using intrusion detection technologies.
- Experience to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).
- Experience with SIEM (e.g. RSA Netwitness, IBM QRadar, Splunk, Arcsight)

- **Security Certifications Preferred (Including but not limited to the following certifications):**

- Certified Incident Handler(GCIH)
- Certified Intrusion Analyst (GIAC)
- Certified Ethical hacker (CEH)
- CISSP

Candidate profile

Experience/ Qualifications:

- Bachelor's degree in Computer Science, Information Technology, Systems Engineering, or a related field.
- Good oral and written communication skills to collaborate with the team.
- Minimum 7+ years of Security engineering or Security IT experience required
- 2+ years experience working with cloud based infrastructure such as AWS, Azure and GCP
- Understanding of how operating systems work and how exploitation works for different Operation Systems and applications.
- Understanding of network traffic and be able to analyse network traffic introduced by the malware.
- Thorough understanding of Windows and Linux Internals .
- Knowledge of common hacking tools and techniques
- Experience in understanding and analysing various log formats from various sources.
- Experience in analysing reports generated of SIM/SEM tools.

Employment Type:Full Time, Permanent

Salary: As per Industry Standards

Role:Team Lead / Technical Lead

Industry:IT-Software / Software Services

Functional Area:IT Software - Network Administration, Security