Security Operations Center

Summary

The AEC SOC located in AEC Headquarters in Riyadh is capable of monitoring, detecting, and isolating security related incidents and the security management of the organization's security products, network devices, servers, security systems and IT Data Center. The SOC services offered are in compliance with Saudi National Cybersecurity Authorities regulation. AEC Offers multiple service delivery models tailored to customer needs. Offsite models utilize a secure channel between the SOC and Client Premises. SIEM administration can be onsite/offsite as needed.

AEC SOC Team are 100% Saudi Nationals who are highly experienced in handling security incidents and have expert skills working with leading SIEM Solutions such as LogRhythm, QRadar, RSA, Splunk and ArcSight. Our SOC analysts are trained to work with advanced Security Solutions and in executing below offerings

Benefits

- No Need to Hire, Manage and Train Resources
- SLA Commitment to keep the customers satisfied
- Flexible and Adaptive
- Utilize Back-office Resources when required
- Letting Organizations Focus on their Core Strength
- Cost Optimization (Shared Resources; Offshore)
- Simplified Accountability
- AEC Strong Partnership means strong support from vendors

Security Operations Center

Offering

Governance

- Create/Review SOC Playbook (policies, procedures)
- Assessment & Remediation

Log Analysis and Monitoring

- 24x7x365 monitoring for malicious activities, network traffic, endpoints, logs and security events
- Advanced Log and Vulnerability Management
- Incident Ticketing and Workflow Management

SIEM Management

- Managing and Administering SIEM Solutions
- Periodic and Continuous Fine tuning of Use Cases

Metrics and Reporting

- Well defined and meaningful KPIs, KRAs
- Easy to setup and use search and alert features
- Highly configurable reports and dashboards

Digital Forensics and Incident response

- RCA for incidents
- Data Recovery and Analysis
- Malware Analysis to understand the behavior and purpose of a suspicious file or URL.

Threat Intelligence

- Scoring and prioritization to ensure your threat intelligence is relevant
- Aggregate, correlate, and analyze threat data from multiple sources in real time to support defensive actions.
- Continuous Threat Hunting and Analysis

Training and Certifications

- Certified SOC Analyst Training (CSA)
- Cyber Security Certifications
- SIEM Training (Vendor specific)
- OTJ Trainings