MUKHADDAR

CYBER SECURITY

Information Security Professional

Phone: +91-7780178243
E-Mail: mukhaddar.mk@gmail.com

Professional Summary:

Working as a Security Analyst, having around 3.8 years of experience in IT security operations with a broad exposure on infrastructure/network/IT security tools, Security incident response and operations.

Core Skills:

- SIEM –Splunk
- Endpoint security tools – Trend Micro Apex One, Deep security
- Phishing Email Analysis - Cloud App Security
- Email Security – Office 365 Suite
- Intrusion Analysis – Cisco Firepower IPS
- Network analysis - Palo Alto Firewalls
- Incident Management & Response- (ServiceNow)
- Web security gateway – ZScalar

Work Experience:

- Working as a Cyber Security Analyst in **Wipro** from January 2018 to till date.

Responsibilities:

- Responsible for security incidents as L1 analyst Monitoring the Splunk Dashboard and initiating the incidence response workflow
- Experience in handling and investigating offences in Splunk
- Analysing threats on EDR –Apex One and providing in-depth analysis and reporting.
- Identify malicious or anomalous activity based on event data from Firewalls, WAF, IPS, HIPS, Anti-Virus, and other sources
- Experience in triaging viruses, malware, Ransomware and other security events on endpoints, including Windows, Linux, and OSX.
- Performed investigation of network and hosts/endpoints for malicious activity, to include analysis of packet captures

- Experienced in examining suspicious emails for malicious content and provide recommendations on remediation actions using PhishMe triage.
- Experienced in preparing detailed analysis for external cyber threats for new vulnerabilities, exploits, and Intrusion patterns, malware behaviours, based on the information proactively checking with the vendor to deploy the signatures for collected IOCs.
- Responsible for managing of SPLUNK SIEM and experienced with creating new alerts for Security use cases. Log sources integration to SIEM solution.
- Installation, Configuration and management of Palo Alto firewalls.
- Strong knowledge of infrastructure security services and security monitoring process.
- Managed Security policies and Security features like Threat Prevention, Antivirus, URL filtering and Anti Spyware in Palo Alto Firewalls.
- Performed security event monitoring of heterogeneous networks such as firewalls, IDS/IPS, Cisco ASA, DLP devices using Splunk.
- Performed root cause analysis for the incidents reported at security operations center.
- Manage security incident investigation and diagnosis and incident follow up.

Environment:

Splunk, Sophos AV, Cisco AMP, Cisco SourceFire IPS.ServiceNow.Qradar

Education:

- B.Tech in Electrical & Electronics Engineering from JNTUA in 2016.

Certifications & Training:

Splunk Certified User
Comptia Security +