PRASHANTH PATHURI

SENIOR CYBER SECURITY OPERATIONS ANALYST

CONTACT

Location: Siddipet, Telangana.
Mobile: 8332057841
Email:
prashanthpathuri5798@gmail.com
LinkedIn: Prashanth P

EDUCATION

BTech- Electronics and communication Engineering.
Aurora's Technological and Research institute, Hyderabad.

TECHNICAL SKILLS

Incident response, Cloud Security, Network security, Data security, Identity access management, Privilege access management, SIEM, EDR, XDR, MDR, Email Security, Vulnerability, Brand protection, Infrastructure provisioning, Phishing Detection and Mitigation, Behavioral Analytics, Threat Mitigation, Post-Incident Analysis.

TECHNOLOGIES

- SIEM: Microsoft Sentinel, Qradar, ArcSight.
- EDR: Microsoft Defender (XDR), Countercept (MDR)
- Email Gateway: Microsoft O365, Proof-Point
- Anti-virus: Sophos
- IAM: Okta, MFA
- Forcepoint DLP and Proxy
- Brand protection: Net craft
- Ticketing tool: Service Now, Jira

CERTIFICATIONS

- Certified Ethical Hacking Essentials (EHE) by EC COUNCIL
- Google Chronicle fundamentals.

PROFESSIONAL SUMMARY:

A zealous cyber security professional with nearly 5+ years of working experience in the security operations field, I'm an accomplished professional currently seeking a position as a Cyber Security Analyst. My expertise lies in offering cybersecurity solutions and proactively maintaining security against various cyber threats, including cyber-attacks, hackers, malware, and other potential risks. Skilled in Email Security, EDR & SIEM with proven history of delivering exceptional support.

PROFESSIONAL EXPERIENCE:

WPP IT (March 2022-Present) Cyber Security Operation Analyst-L2

- Managed 24/7 SOC monitoring for software, hardware logs, web servers, and endpoints, ensuring real-time incident detection and resolution.
- Built and led the SOC team, defining workflows, playbooks, and operational processes for global incident response.
- Developed custom detection rules in Microsoft Defender to identify and isolate malware, preventing lateral movement.
- Managed security incidents, coordinating response efforts, and ensuring business continuity through clear communication with clients and vendors.
- Guided tier-1 analysts on triage, incident analysis, and updated playbooks to create knowledge-based resources.
- Monitored email security threats, initiated IOC blocks in Microsoft Defender, and responded to user-reported incidents.
- Led the design and implementation of Qualys modules for vulnerability management, streamlining workflows with cross-functional teams.
- Enhanced vulnerability remediation efficiency through optimized workflows, integrated with Change Management and supported by SOPs and runbooks.
- Leveraged Wiz, Microsoft MDE, and AWS Trusted Advisor to bolster cloud security posture and visibility.
- Managed and escalated high-risk security incidents, ensuring thorough investigation and response within SLA.
- Conducted log analysis to detect and escalate security incidents, improving threat detection and overall network security.
- Developed and administered SOPs, runbooks, and risk categorization documentation, while providing training to the SOC team on security best practices.

Skyylives infotech Pvt Ltd (June 2019-March 2022) Security Analyst.

- Monitored and analyzed security alerts using SIEM tools for real-time threat detection and response.
- Conducted root cause analysis of security incidents and provided timely remediation strategies. Managed incident response activities, including triage, escalation, containment, and recovery, with detailed documentation.
- Monitored and analyzed infrastructure threats, vulnerabilities, and security alerts 24/7 using SIEM tools and technologies like Watermark, Referrer, and Abuse mailbox.
- Collected and analyzed network device logs to detect suspicious activities, investigating security incidents and preparing incident reports.
- Implemented and optimized threat detection rules, reducing false positives and improving identification workflows.
- Experience of performing security monitoring and incident response activities in an advanced. Security operation centers (SOC) environment (log analysis, event analysis, incident
- Performed regular vulnerability scans with Nessus and provided actionable risk mitigation recommendations.