RAJNISH KUMAR SRIVASTAVA

• +491623493932 • rajkumsriv@outlook.com

Professional Summary

I am an Information Security Lead with over 11 years of experience specializing in 24/7 Security Operations Centers (SOC – Dedicated and MSSP) responding to incidents using cyber kill chain. My incident management expertise includes SIEM tools such as QRadar, Google Chronicle, and Splunk. I have successfully secured networks and managed vulnerabilities for large organizations. Skilled in conducting security gap assessments and root cause analysis, I provide actionable recommendations to mitigate operational risks. I focus on client relationship management to ensure cybersecurity services align with business needs while maintaining compliance with industry standards, including ISO 27001, NIST and OWASP Top 10.

Skills

- Incident Response
- SIEM Solutions
- Email Security
- Risk Management
- Data Security and DLP
- Cloud Security
- Network Security
- Vulnerability Management
- Project Management
- Firewall and WAF
- IT Service management
- Antivirus and EDR
- Threat Intelligence
- Process Improvement
- Security Awareness Training

Work History

Information Security lead, 05/2019 to Current
Tata Consultancy Services

- Led a 20-member team responsible for Security Operations Center (SOC), Vulnerability Management, Endpoint Security, and Public Key Infrastructure (PKI).
- Deployed and managed SIEM tools such as QRadar, Splunk, and Google Chronicle, ensuring effective real-time monitoring and threat detection across client environments.
- Utilized Crowdstrike, Microsoft Defender, and McAfee ePO to implement robust endpointsecurity, focusing on proactive threat detection and incident response.
- Managed Proofpoint and KnowBe4 to strengthen email security and improve phishingawareness through targeted user training programs.
- Directed risk management activities, identifying, assessing, and mitigating security risks acrossIT infrastructure in alignment with business requirements.
- Managed Netskope cloud security solutions to ensure secure cloud usage and data protection, complying with GDPR and other relevant regulations.
- Acted as the primary client liaison for cybersecurity services, ensuring service delivery aligned with client business objectives and regulatory requirements.
- Developed comprehensive security reports and dashboards for executive leadership, providing insight into security risks, compliance, and incident response performance.

Senior Security Analyst, 09/2011 to 04/2019
Wipro Technologies

- Monitored and managed SIEM tools like QRadar and Splunk for real-time threat detection, security monitoring, and incident response across various IT environments.
- Investigated phishing attempts, malicious domains, and IP addresses using open-source tools, recommending blocking actions to enhance cybersecurity.
- Collaborated with cross-functional teams to identify, assess, and remediate vulnerabilities in networks and applications, ensuring compliance with ISO 27001 and NIST standards.
- Conducted root cause analysis and forensic investigations of complex security incidents, implementing preventative measures to avoid recurrence.
- Optimized security tools and processes, improving incident response times, increasingefficiency, and reducing operational costs.
- Developed and maintained Standard Operating Procedures (SOPs), Playbooks, and Known Error Databases (KEDB) to ensure consistency in security operations and incident management.
- Managed risk registers to proactively identify and mitigate security risks, aligning with organizational goals and regulatory requirements.
- Engaged with stakeholders to ensure that security initiatives were aligned with both operational needs and regulatory compliance, particularly GDPR.

Education

Bachelor's in science: Physics, Mathematics & Statistics
Calcutta University

Key Achievements

- Deployed the on-premise QRadar SIEM tool for enhanced security monitoring.
- Migrated from McAfee Drive Encryption to BitLocker for improved data protection.
- Completed proof of concept for Google Chronicle, Demisto (SOAR), and Cymulate.
- Conducted a comparison proof of concept for OSQuery, EDR, and Sysmon.
- Fully deployed Google Chronicle SIEM, streamlining log management.
- Developed a cloud log shipper to forward Netskope proxy logs to Google Chronicle.
- Integrated multiple log sources, including Checkpoint, Cisco ASA, and Crowdstrike, into Google Chronicle.
- Established a Linux server for installing the Chronicle forwarder.

Certification

- Microsoft Certified Security Analyst Associate SC-200, 10/01/22
- Microsoft Certified Azure Fundamentales SC-900, 09/01/22
- Splunk Certified Power User, 01/01/17
- CEH - EC-Council, 07/01/17
- IBM QRadar Certified Analyst, 01/01/18
- EC-Council Certified Security Analyst V10, 03/01/18

Training

- Certified Information Systems Security Professional (CISSP), **12/31/24**