RAJNISH KUMAR SRIVASTAVA, CISSP, CEH

(+49)1623493932 rajkumsriv@outlook.com https://www.cyberdharaa.com

Professional Summary

I am an Information Security Lead with over 13 years of experience, specializing in 24/7 Security Operations Centers (SOC – both dedicated and MSSP models), while ensuring compliance with industry standards such as ISO 27001, NIST, and the OWASP Top 10. I have successfully secured enterprise networks, led vulnerability management efforts, and played a key role in building, transforming, and optimizing SOC capabilities for large organizations across multiple geographies. My expertise includes designing SOC operating models, defining processes and KPIs, implementing SIEM, Endpoint Security and other platforms, and leading end-to-end SOC transformations. I am also skilled in conducting security gap assessments and root cause analyses, providing actionable recommendations to mitigate operational and strategic risks.

My current role has involved frequent interaction with C-level stakeholders as well, where I've developed the ability to tailor my communication—clearly translating technical risks into business impact for executives, while engaging in deep technical discussions with engineering/security teams.

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 the Security Operations Center (SOC), Vulnerability Management, Endpoint Security, Proxy, and Public Key Infrastructure (PKI).
- Deployed, managed, and transformed SIEM platforms including QRadar, Splunk, and Google SecOps, ensuring effective real-time monitoring and threat detection across client environments.
- Implemented and managed endpoint security solutions such as CrowdStrike, Microsoft Defender for Endpoint, and McAfee ePO, with a strong focus on proactive threat detection and rapid incident response.
- Oversaw the administration of Proofpoint, Office 365 security controls, and KnowBe4 to enhance email security posture and drive phishing awareness through targeted user training programs.
- Directed comprehensive risk management activities, including risk identification, assessment, prioritization, and mitigation strategies to reduce exposure across IT infrastructure and ensure alignment with business goals.
- Promoted a security-conscious culture by guiding and mentoring both leadership and teams on matters of security, compliance, and governance, ensuring strong alignment with industry standards and internal policies.
- Served as the primary client liaison for cybersecurity services, ensuring service delivery met client objectives, industry best practices, and compliance requirements.
- Developed and presented executive-level security reports and dashboards, offering insights into threat trends, compliance status, and incident response effectiveness.

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 withorganizational 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

- **Leadership in Security Operations** : Led a 20-member SOC team, enhancing incident response efficiency by 30% through streamlined processes.
- **Implementation of Security Policies** : Developed a NIST-based Security Incident Response Plan and Policy, reducing incident resolution time by 25%.
- **Optimization of Security Tools** : Enhanced threat detection and operational efficiency by 20% through optimization of tools like QRadar and Splunk, while reducing costs.
- **SIEM Migration (QRadar to Google SecOps) :** Successfully led the enterprise-wide migration from IBM QRadar to Google SecOps SIEM for a U.S.-Canada financial services firm, eliminating on-prem infra-dependencies and achieving cost savings through high-speed, cloud-native analytics.
- **Endpoint Encryption Migration (McAfee to BitLocker) -** Directed the migration of full disk encryption from McAfee Drive Encryption to Microsoft BitLocker across the EMEA region, completing the project within one year and delivering annual cost savings of ~$50K, while aligning with the global security modernization strategy.
- **SIEM Deployment (IBM QRadar) -** Spearheaded the deployment of IBM QRadar SIEM in on-premise infrastructure, transitioning from manual log monitoring to automated threat detection, and enhancing incident response and regulatory compliance across operations.

Certification

- **Certified Information Systems Security Professional (CISSP), 30/04/2025**
- 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