**Sriparna Ghosh**

Sriparnaghosh93@gmail.com

+1 469-496-8203

**Cybersecurity Engineer**

**Professional Summary:**

* Experienced Professional with over 10 years of experience as an IT Security Professional in IT Infrastructure, Cybersecurity and Risk Management.
* 6 Years of experience as Network Security Analyst for creating incident reports on alerts by SIEM.
* 7 Years of experience working on incident reports, risk management and risk analysis.
* 5 years in customer-facing Support, Professional Services, Implementation or Client Service role.
* Proactively research and monitor security-related information sources to aid in the identification of threats to networks, systems, and intellectual property.
* Worked on QRadar SIEM on a variety of logs sources (Firewall logs, Network Logs, host logs and IDS logs) to identify potential threats.
* Good Understanding of IAM and Multifactor authentication.
* Skilled in configuring and optimizing DLP tools like Symantec, Forcepoint to prevent data breaches and ensure regulatory compliance. Expertise in threat analysis, data classification, and policy creation to mitigate risks and enhance security posture.
* Monitor and respond to alerts generated from the DLP systems and other technologies.
* Administration of the DLP tools which includes configuring policies and reporting.
* Expert in designing, implementing, and overseeing control frameworks that mitigate risks, enhance operational efficiency, and ensure regulatory compliance.
* Proficient in threat analysis, network security, and incident response.
* Adept at leveraging tools and frameworks like Splunk, SIEM, and NIST to minimize risks and safeguard data integrity.
* Capable of directing incident response teams and ensuring the timely and effective mitigation of security incidents. My experience includes conducting tabletop exercises and post-event analyses to continuously improve incident response capabilities.
* I have a thorough understanding of security architecture concepts, which allows me to design and deploy robust security solutions. I have effectively secured networks, systems, and applications against a wide spectrum of attacks.
* Use IBM QRadar Security Manager to identify threats and assigned categories.
* Passionate about solving complex security challenges in dynamic environments.
* Broad knowledge of Incident Handling and other SOC operations.
* Adept at conducting risk assessments, designing compliance programs, and collaborating with cross-functional teams to address security, operational, and financial risks.
* Expertise in implementing, configuring, and managing Data Loss Prevention solutions, as well as responding to and remediating data leakage incidents.
* Proven ability to identify and investigate DLP alerts, conduct root cause analysis, and recommend data protection strategies to enhance data security posture.
* Experienced Third Party Risk Assessment in identifying, assessing and mitigating risks associated with third party vendors.
* Proven ability to enhance supply chain security and minimize risks while fostering collaborative relationships with vendors and stakeholders.
* Strong understanding of ISO 27001, NIST CSF Framework and GDPR to enhance the organization’s risk posture.

**Technical Skills:**

|  |  |
| --- | --- |
| **DLP** | Symantec, McAfee |
| **Endpoint Security** | Symantec SEP, O365 security, McAfee |
| **IPS/IDS** | McAfee IPS, Secure Works IDS/IPS, SNORT |
| **SIEM** | IBM QRadar, Splunk |
| **Firewalls** | Palo Alto, Cisco ASA, SolarWinds, Check Point. |
| **Security Knowledge** | Security Standards, OWASP, Cryptography, Hashing, Encryption, Virtualization, Identity Management, Incident Response, PulseSecure VPN, Firewalls, Log Analysis, Malware Analysis, LDAP, SSL, IDS, IPS, HTTPS, TCP, DNS, DHCP, HIPAA, PCI, SOX, ISO. |
| **Compliance & Frameworks** | GDPR, PCI-DSS, ISO 27001, NIST CSF |
| **Threat Analysis & Response** | Incident response, malware analysis, threat intelligence |
| **Administration** | Information Security tools, Active Directory |
| **Reporting & Documentation** | Expertise in preparing audit reports, risk assessments, and compliance documentation |
| **Operating System** | Windows, Linux |

**Professional Experience:**

**CVS, Woonsocket, RI May 2024 –Till Date**

**Cybersecurity Engineer**

**Responsibilities:**

* Gathered requirements through interactions with business and development teams, preparing Proactively monitor the SIEM for security events; analyze them to detect potential threats.
* Identifying and working with cross functional organizations towards resolving security issues
* Assist with the development, revision, and maintenance of Standard Operating Procedures and Working Instructions related to IT Security
* Strong knowledge of technology and security topics including network and application security, infrastructure hardening, security baselines, web server, and database security
* Analyze threat and vulnerability alerts, determine current impacts, and coordinate remediation actions as necessary
* Perform routine checks and triage, escalation of any critical alerts
* Work extensively on SIEM to secure clients from cyber threats.
* Work on QRadar SIEM for logs sources.
* On a daily basis observed and responded to Phishing attack, Exploit kit, Large outbound file transfers and AD group user changes on SIEM and raised the incident reports.
* Work on suspicious emails submitted by different agencies which were suspected to be Phishing.
* Triage and investigate cybersecurity alerts.
* Follow established incident response processes to triage security events.
* Analyze the email for Suspicious links and attachments.
* Monitored and analyzed security incidents monthly using SIEM tools like Splunk and QRadar to prepare business reports to share with higher management.
* Monitored SIEM dashboards to detect and respond to real-time security threats.
* Define the policies and checklist to maintain and implement Antivirus; Endpoint protection; Collecting logs; vulnerability scans; and create it as mandatory in the checklist before clearing ATO(Authorize to Operate).
* Involved in planning, discussions and assessing for business continuity plans and disaster recovery by categorizing the systems and applications in Tier levels.
* Provided security training to employees, increasing awareness of phishing tactics.
* Lead the project for availability of business applications and talk to various business owners to understand what components involved in application unavailability which impacted the business and remediated accordingly.
* Conducted regular security assessments, identifying and mitigating vulnerabilities across network infrastructure.
* Designed and deployed DLP solutions for safeguarding sensitive data across endpoints and email systems.
* Developed and maintained DLP policies to prevent unauthorized data access and exfiltration and reduce false positives.
* Monitored and analyzed DLP alerts, responding to incidents monthly, and ensuring timely resolution of high-priority cases.
* Developed automated scripts to monitor and respond to potential threats, reducing incident response time.
* Document and manage investigations and incidents in our Incident Management System.
* Improve our detection capabilities by building and enhancing alert rules and actively hunting for evidence of malicious activity.
* Operate and maintain security tools and platforms.
* Develop and continuously improve incident response runbooks to ensure we efficiently and effectively analyze and respond to security alerts.
* Monitor fault and performance of network infrastructure and networked applications.
* Investigate and research improvements on existing workflows to improve efficiency.
* Worked on monthly reports to calculate total outage, outage during business hours, non-business hours and any impact on business.
* Responsible for assisting security tools administrators with improving rules and alerts on incident monitoring tools.
* Monitor Security Information and Event Management (SIEM); Intrusion Detection System (IDS); Network Monitoring and Response Services.
* Good understanding of chain of custody, evidence handling and confidentiality of investigating information.
* Conduct regular risk assessments of internal controls, identifying potential compliance risks and formulating mitigation strategies that reduce organizational exposure.
* Conducted comprehensive risk assessments across organization, identifying and mitigating key risks.
* Generated risk dashboards and reports for senior leadership, facilitating informed decision-making.
* Collaborated with compliance teams to ensure adherence to regulatory requirements.

**EXL Services, Gurgaon, India Aug 2019- Jan 2024 LAM, Information Security and Risk Management**

**Responsibilities:**

* Develop and implement comprehensive third-party risk management programs to identify, assess, and mitigate risks associated with vendor relationships, improving risk awareness across the organization.
* Create and maintain risk assessment documentation and reports, providing management with actionable insights and recommendations for risk mitigation.
* Collaborate with compliance, legal, and IT departments to ensure all vendors meet internal compliance and regulatory requirements, reducing potential liabilities.
* Managed the end-to-end vendor assessment process, including initial due diligence, risk scoring, and ongoing monitoring, ensuring a robust vendor risk management lifecycle.
* Monitor and review vendor performance and risk status regularly, facilitating ongoing risk assessments and updates to risk profiles as necessary.
* Ensured vendor adherence to regulatory standards, including GDPR and PCI DSS.
* Monitored vendor performance and compliance through routine audits and periodic reviews.
* Developed and utilized vendor risk scoring models to prioritize high-risk vendors for remediation or
* reassessment.
* Reviewed vendor questionnaires and evidence (SOC 2 reports, ISO certifications, etc.) to validate control and effectiveness.
* Lead and manage a team of 5 professionals in executing internal controls across the organization, ensuring adherence to company policies, regulations, and industry best practices.
* Supported risk management efforts by conducting comprehensive risk assessments, identifying emerging risks, and providing recommendations for risk mitigation strategies.
* Assisted in the creation of risk management policies and procedures aligned with industry standards.
* Monitored risk exposure and performance across multiple business units, producing monthly risk reports that identified potential vulnerabilities and recommended actions.
* Developed risk reporting tools and dashboards for senior leadership to provide insights into key risk indicators (KRIs), trends, and emerging threats.
* Conduct internal and external audits, track findings, and ensure timely remediation of identified issues.
* Develop and conduct risk and compliance training programs for employees and stakeholders to raise awareness of policies and regulations.
* Assisted with audit preparation, including gathering evidence, reviewing processes, and responding to auditor inquiries.
* Worked on disaster recovery and back up plan in case of disaster.
* Design, implement, and monitor robust risk control frameworks to identify, assess, and manage operational and compliance risks.
* Investigate and Monitor compliance risks and share risk reports with senior management identifying the areas of process improvement and operational efficiency.
* Develop and implement exception management policies and procedures, improving the efficiency of the review process.
* Collaborate with internal departments to design and implement effective internal controls and compliance policies, ensuring full organizational adherence.
* Assisted in identifying risks and weaknesses in internal controls and drafted reports with recommendations for remediation.
* Prepare and present risk reports to senior management, offering insights and actionable recommendations.
* Develop and conduct risk and compliance training programs for employees and stakeholders to raise awareness of policies and regulations.
* Collaborate with the audit teams to assess operational risks and recommended mitigating actions.
* Provide support for internal and external audits by gathering evidence, coordinating with auditors, and implementing corrective actions based on audit findings.
* Worked closely with legal and internal teams in preparing for regulatory audits, ensuring all documentation, reports, and systems were in place and accurate.
* Assist with preparing audit documentation and conducting follow-up activities on remediation of audit findings.

**Wipro Technologies, Gurgaon, India July 2017 – Aug 2019**

**CyberSecurity Incident Response Analyst**

**Responsibilities:**

* Perform log analysis and investigate the threat landscape.
* Develop incident response workflow for DLP incidents as raised through the DLP tool.
* Work with vendors to support the DLP technology (troubleshooting, upgrades, etc.).
* Opened incident tickets and tracked them from start to completion following closely on its lifecycle stages, identify, contain, eradicate, recover and lessons learned.
* Collected evidence for future use on similar cases, lessons learned, training and awareness.
* Develop and continually improve incident response runbooks to ensure we efficiently and effectively analyze and respond to security alerts.
* Advanced experience in network (TCP/IP) protocols, computer security, and System Administration.
* Built and patches on IBM QRADAR Data Nodes and Event Collector
* Modified rules in SIEM and Server for alerts related to individual customers.
* Monitored and analyzed DLP alerts, responding to incidents monthly, and ensuring timely resolution of high-priority cases.
* Manage and respond to data loss prevention incidents, ensuring timely containment, investigation, and resolution of all DLP-related alerts.
* Conduct root cause analysis on DLP incidents, identifying potential data leakage vectors, and coordinating with IT and Security teams to implement mitigation strategies.
* Configure and fine-tune DLP policies, rules, and thresholds in Symantec DLP and Forcepoint to minimize false positives and ensure effective detection of sensitive data breaches.
* Lead cross-functional incident response teams, ensuring a coordinated approach to contain and remediate DLP incidents involving email, cloud storage, USB devices, and endpoints.
* Work with legal, compliance, and risk management teams to ensure that all data loss incidents comply with regulatory requirements (GDPR, PCI-DSS).
* Provide incident reports, post-mortem analyses, and recommendations for data security improvements to senior leadership.
* Collaborate with stakeholders to develop and deliver training on data protection policies, DLP tools, and best practices to mitigate data loss risks.
* Drive Security Trainings for all the employees, check the security content and 100% completion status by following up with business leaders, and conduct information security awareness sessions for clients.
* Assisted senior risk managers in conducting risk assessments, identifying internal and external risks, and preparing risk mitigation strategies.
* Performed research on industry trends, emerging risks, and regulations to provide insights into improving risk management practices for clients.
* Assisted in creating risk management presentations for client meetings, highlighting key findings, and presenting recommendations for mitigating potential risks.

**Genpact, Gurgaon, India Jun 2014 - Jul 2017**

**CyberSecurity Analyst**

**Responsibilities:**

* Monitor and respond to alerts generated by QRadar SIEM.
* Raised incident report on IRT if some suspicious traffic was monitored on SIEM.
* Triaged and investigated cybersecurity alerts.
* Followed established incident response processes to triage security events.
* Developed and tuned alerts in SIEM.
* Improved our detection capabilities by building and enhancing alert rules and actively hunting for evidence of malicious activity
* Analyze threat and vulnerability alerts, determine current impacts, and coordinate remediation actions as necessary.
* Proactively researched and monitored security-related information sources to aid in the identification of threats to networks, systems, and intellectual property.
* Worked on QRadar SIEM for logs sources from different clients.
* Co-ordinated with clients to make the server up ASAP if it is down due to any reason.
* Patched up the system to the latest version as per the recommendations.
* Monitored the health of the servers, Operating system, database and the network.
* Conducted vulnerability assessments and penetration testing, identifying and remediating critical security risks.
* Deployed and managed firewalls, IDS/IPS, and endpoint protection tools to safeguard enterprise assets.
* Performed threat hunting and forensic analysis to identify and mitigate advanced persistent threats.
* Integrated DLP tools with SIEM platforms, enhancing real-time threat visibility and response capabilities.
* Assisted in deploying and fine-tuning DLP solutions, improving detection accuracy.
* Analyzed security logs and alerts from SIEM tools, correlating events with DLP incidents to detect patterns of malicious activity.

**Education:**

* Masters Of Computer Science
* Bachelor Of Computer Application

The Heritage Academy, Kolkata, India