INFORMATION SECURITY ANALYST

Bhargav Suresh Pathikayala

dbsureshpathikayala@gmail.com

+91 8977082654

SUMMARY:

- SOC Analyst having **3+** years experience in handling Information security incidents. Expertise in Cyber security & Information Assurance with deep Knowledge of Identity and Access Management security, Cyber Threat Intelligence, AWS Cloud, malware detection techniques, information security policies and standards.
- Experience in Vulnerability Assessment using Nessus to evaluate attack vectors, identify system vulnerabilities and guide through the remediation plans and security procedures.
- Experience in Threat hunting on EDR and SIEM tools using latest threat feeds & IOC's.
- Excellent verbal and written communication skills, able to effectively communicate complex technical information to both technical and non-technical stakeholders.
- Strong experience in network and endpoint security, cloud security, and identity and access management.
- Assisted in development and implementation of information security policies, standards, and procedures, adhering to industry best practices for clients.
- Assisted in ensuring that the corporate IT environment is secure and complies with all external audit requirements.
- Experience in Gathering and analyzing metrics, key risk indicators and maintaining scorecards defined within the area of information security to ensure our information security program is performing effectively and efficiently.
- Experience in managing Network infrastructure security using Arcsight for monitoring and classifying and responding to incidents and threats.
- Supported the information security audit and third-party assessment initiatives during planning, execution, and remediation phases.
- Familiar with threats and vulnerabilities, latest trends and risks and be able to understand the technical remediation action steps or plans and communicate them effectively to teams within the organization.
- Responsible for monitoring and providing analysis in a 24x7x365 Security Operation Center (SOC) using SIEM, IDS/IPS tools.
- Experience with industry recognized SIEM (Security Information and Event Management) solutions such as IBM QRadar and ArcSight.
- Excellent understanding of computing environments Linux: RHEL-8/Ubuntu/DEB-KALI, Windows 8/10/11, Server 2016/2019 and Unix Operating systems.
- Good understanding of enterprise, network, system/endpoint, and application-level security issues and risks.
- Oversee Vulnerability assessment / penetration testing of scoped systems and applications to identify system vulnerabilities.
- Good knowledge of PCI-DSS, HIPAA and NIST Compliance usage, rules and regulations
- Processed daily security operations and log analysis.

TECHNICAL SKILLS:

SIEM	IBM Qradar, ArcSight, Splunk
Endpoint Security	SentinelOne, MacAfee DLP, MacAfee ePO, MacAfee web-proxy
WAF	Imperva
OSINT	MX Tooolbox, AbusedIPdb, VirusTotal, Urlscan, IBM X-force and etc.

EDUCATION:

Bcom(Computers),Pacific Institute of Engineering and Management
(2018)

WORK EXPERIENCE:

WIPRO (Mumbai) **June** 2021 to Till-Date

Responsibilities:

- Responsible for detection and response to security events and incidents within SentinelOne, Imperva WAF, MacAfee DLP, MacAfee ePO & web-proxy, QRADAR SIEM, security tools, etc. to gather, analyze, and present forensic evidence of cyber malware and intrusions.
- Oversee Vulnerability assessment of scoped systems and applications to identify system vulnerabilities.
- Assisted in day-to-day EPO Security Alert threats by response using SIEM & SentinelOne to track down security threaten workstations, virtual servers and devices on the Confidential Network.
- Responsible for web filtering (blocking/unblocking the websites) according to the client needs in MacAfee web-proxy.
- Analyzing vulnerability using scanning tools (Nessus) provided to us by our client to remove false positives before creating and delivering a final report.
- Working with SentinelOne EDR & McAfee ePO for managing client's workstations and providing end point security.
- Performed user access management (review, enable, disable, access request approvals) on SailPoint.
- Worked on Joe Security sandbox to perform malware analysis on the email attachments.
- Recognize, adopt, utilize and teach best practices in Information security.
- Internal Network Vulnerability Assessments to enhance the Information Security culture of an organization through identifying, analyzing and reporting the gaps which may be used to threaten the CIA of information.
- Monitored and researched Cyber Threats with a direct & indirect impact to the organization internally.
- Ability to create, update and maintain technical documentation. Ability to work independently.
- Experience with ServiceNow. Experienced with Mimecast Email Gateway Security.
- Used Splunk SIEM to manage and analyze security-based events, risks & reporting.

- Simplified knowledge sharing by creating and maintaining detailed and comprehensive documentation and necessary diagrams.
- Assisted internal users of SIEM in designing & maintaining security dashboards, assisted team to understand the use case of business and provided technical services to projects, user requests & data queries.
- Responsible for monitoring and investigation of Website/API traffic using Imperva, SIEM.
- Using Tenable and Patch Manager Pro to control vulnerabilities and mitigate them by severity.
- Audit Support: Facilitated the AWS Cloud audit for the client, took charge of end-to-end co- ordination and support during the onsite assessment.
- Conduct daily IDS analysis/monitoring for potential compromise, intrusion, deficiency, significant event or threat to the security posture and security baseline and numerous activities against spam.
- Review System and firewall logs based on individual preset client policies, rules, and standards; also review all host activity for specified timeframe.
- Work directly with SIEM engineers and Information Security Officers to adjust alert criteria
- Coordinated escalations to Forensic Analyst Team with recommendations for remediation
- Evaluated and fulfilled requests from the Information Security Risk & Compliance Officers for each client and aligned with the appropriate runbook procedures to attain Client Service Level Objectives and Agreements.
- Utilizing SentinelOne Endpoint Security to create reports to resolve various information security issues.
- Adjusted SIEM alerts temporarily to suppress excessive alerts prior to engineers making permanent threshold changes.
- Facilitated and operated direct telephone communication in order to perform the immediate required escalation requests or engagements of required teams to support clients.

DECLARATION:

I hereby declared that all information furnished above is correct to the best of my knowledge.

Bhargav Suresh Pathikayala