Karumujji Rajesh Kumar

SECURITY ENGINEER

rajeshkarumujji96@gmail.com 9036952752 Indian Male

31/05/1996

OBJECTIVE

Dynamic and skilled Security Engineer with 3.4 years of experience in monitoring, analyzing, and responding to security incidents. Seeking to leverage expertise in threat detection, incident response, and security tool management to contribute to a forward-thinking organization's cybersecurity efforts.

PROFESSIONAL EXPERIENCE

- Understanding the client requirement and responsible for providing solution proposal (SIEM) to the client.
- Responsible for providing walk through about the SIEM solution on all functionalities based on the licenses procured.
- Understanding the client infrastructure and providing the designs with the flow of traffic.
- Prepared High Level Design Documents (HLDD)
- Prepared Low Level Design Document (LLDD)
- Prepared service documents, Work Level Agreement (WLA) and got signed off.
- Implemented Securonix SIEM in client Multi Cloud environment (AWS & Azure).
- Connecting with clients and performing data gathering exercises for implementation.
- Worked with multiple teams to fulfill the Securonix SIEM implementation project needs such as Account creation in AWS with the dedicated VPC for SIEM, Transit gateway attachment spin up of servers & Load Balancer etc.
- Installed Remote Ingestion Node (RIN) in the servers as per the design.
- Installed Nxlog manager in the server as per the design.
- Integrated various cloud (AWS & Azure) data sources to the Securonix SIEM such as AWS Guardduty, AWS VPC, AWS WAF, AWS ALB, Azure AD, Azure Firewall, O365 / Office 365, Defender for cloud apps etc.
- Integrated various other data sources such as Checkpoint NGFW, SentinelOne EDR, Mimecast etc.
- Performed Securonix integration with Service now ITSM tool.
- Providing the requirements to the respective teams for implementations.
- Connecting weekly with the clients for providing updates and working on improvising the process.
- Monitored security events and alerts using SIEM (Security Information and Event Management) tools to detect potential threats and vulnerabilities.
- Conducted thorough analysis of security incidents to determine the scope, impact, and root cause, andinitiated appropriate response actions.
- Developed and maintained security policies, procedures, and guidelines to ensure compliance with industry standards and regulatory requirements.

- Collaborated with cross-functional teams to implement security controls and remediation measures to mitigate identified risks.
- Provided timely and accurate reports on security incidents, trends, and performance metrics to management and stakeholders.
- Performed vulnerability assessments and penetration testing to identify weaknesses in network infrastructure, applications, and systems.
- Conducted security assessments and audits of IT environments to identify gaps in security controls and recommend remediation measures.
- Assisted in the development and implementation of incident response plans and procedures to ensure effective handling of security breaches and incidents.
- Conducted security awareness training sessions for employees to educate them about cybersecurity best practices and raise awareness about emerging threats.
- Participated in incident response exercises and simulations to test the effectiveness of security controls and response procedures.
- Assisted Team in monitoring and analyzing security events and alerts from various sources, including IDS/IPS, firewalls, and endpoint protection tools.
- Investigated and triaged security incidents to determine their severity and impact on the organization's infrastructure and data.
- Documented incident findings, actions taken, and lessons learned for post-incident analysis and improvement of security processes.
- Contributed to the development of SOC documentation, including standard operating procedures (SOPs).
- CCNA-certified Network Engineer with expertise in Network Operations, configuration and monitoring.
- Expertise in troubleshooting network connectivity issues.
- Expertise in analyzing and documenting the root cause of network connectivity issues.
- Expert-level knowledge of TCP/IP and OSI models.
- Experience working on Cisco ASA 5500 series.
- Experience working on Cisco Firepower 1000, 2100,4100 series.
- Hands-on experience with Upgrading IOS, ACLs, NAT, Failover, and Syslog on Cisco ASA.
- Hands-on experience with Upgrading paths, Reimaging, Backup, Backup & Restore, Migration, HA pair, and Policy deployment on FMC.
- Hands-on experience with ASA Platform SFR.
- Hands-on experience on creating the policy and deploying in the FMC.
- Experience on monitoring the Malware, URL, and security intelligence.

CERTIFICATES

Cisco Certified Network Associate (CCNA)
(CISCO ID: CSCO14048930)

Google Cloud Platform Associate
(Certification ID: jL5vvL)

TECHNOLOGY & SKILLS

SIEM
Securonix, Qradar, Splunk

EDR
Falcon Crowdstrike & Trendmicro

Vulnerability
Nessus & Qualys

Ticketing Tool
ServiceNow & Snow

IDS & IPS

Phishing &Email Analysis

Antivirus(Trendmicro)

ISO27001(GDPR & NIST)

Security Incident Management

Cisco & Palo Alto Firewall

Network Analysis
Wireshark

ROLES & RESPONSIBILITIES

VIRTUSA CONSULTING SERVICES PVT LTD

06/2022 – 10/2024 | Hyderabad, India

Security Engineer

- Understanding the client requirement and responsible for providing solution proposal (SIEM) to the client.
- Responsible for providing walk through about the SIEM solution on all functionalities based on the licenses procured.
- Understanding the client infrastructure and providing the designs with the flow of traffic.
- Prepared Multi Level Design Documents (HLDD& LLDD)
- Prepared service documents, Work Level Agreement (WLA) and got signed off.
- Implemented Securonix SIEM in client Multi Cloud environment (AWS & Azure).
- Connecting with clients and performing data gathering exercises for implementation.
- Worked with multiple teams to fulfill the Securonix SIEM implementation project needs such as Account creation in AWS with the dedicated VPC for SIEM, Transit gateway attachment spin up of servers & Load Balancer etc.
- Installed Remote Ingestion Node (RIN) in the servers as per the design.
- Installed Nxlog manager in the server as per the design.
- Integrated various cloud (AWS & Azure) data sources to the Securonix SIEM such as AWS Guardduty, AWS VPC, AWS WAF, AWS ALB, Azure AD, Azure Firewall, O365 / Office 365, Defender for cloud apps etc.
- Integrated various other data sources such as Checkpoint NGFW, SentinelOne EDR, Mimecast.
- Performed Securonix integration with Service now ITSM tool.
- Providing the requirements to the respective teams for implementations.
- Connecting weekly with the clients for providing updates and working on improvising the process.
- Defined SOC operations, Usecases creation workflow and the process.
- Enabling the Usecases as per the data sources integrated to Securonix SIEM. Created a few custom use cases in Securonix SIEM.
- Monitor, manage, and respond to group email and distribution lists, ensuring timely communication andcoordination across relevant teams and stakeholders.
- Security Incident Response and closure of Incidents within SLA using Service Now.
- Performing Health check of network security devices.
- Analyzing Phishing and Spam related activities and notifying to the users.
- Preparing daily and weekly dashboard on the security threats and trends on the network.

- Working on Real time network traffic by analyzing the logs from IDS and Firewalls through SIEM Tool. Handling the complete incident management framework cycle right from incident identification, incident containment, performing root cause analysis, suggestion and implementation of preventive and corrective controls and perform network analysis as needed on a case to case basis.
- Reviewing and maintaining internal documentation for policies and procedures
- Sampling evidence from the ISMS as part of a field review, demonstrating that the policies and procedures are followed consistently
- Analyzing findings from document review and field review to ensure they meet ISO 27001 requirements
- Implementing improvements, as needed, based on audit findings.

Capgemini(Cisco TAC)

05/2021 – 05/2022 |Hyderabad, India

Technical Consulting Engineer

- Understanding the client requirement and responsible for providing solution proposal (SIEM) to the client.
- Responsible for providing walk through about the SIEM solution on all functionalities based on the licenses procured.
- Understanding the client infrastructure and providing the designs with the flow of traffic.
- Prepared Multi Level Design Documents (HLDD& LLDD)
- Prepared service documents, Work Level Agreement (WLA) and got signed off.
- Implemented Securonix SIEM in client Multi Cloud environment (AWS & Azure).
- Connecting with clients and performing data gathering exercises for implementation.
- Worked with multiple teams to fulfill the Securonix SIEM implementation project needs such as Account creation in AWS with the dedicated VPC for SIEM, Transit gateway attachment spin up of servers & Load Balancer etc.
- Installed Remote Ingestion Node (RIN) in the servers as per the design.
- Installed Nxlog manager in the server as per the design.
- Integrated various cloud (AWS & Azure) data sources to the Securonix SIEM such as AWS Guardduty, AWS VPC, AWS WAF, AWS ALB, Azure AD, Azure Firewall, O365 / Office 365, Defender for cloud apps etc.
- Integrated various other data sources such as Checkpoint NGFW, SentinelOne EDR, Mimecast.
- Performed Securonix integration with Service now ITSM tool.
- Providing the requirements to the respective teams for implementations.
- Connecting weekly with the clients for providing updates and working on improvising the process.
- Defined SOC operations, Usecases creation workflow and the process.
- Enabling the Usecases as per the data sources integrated to Securonix SIEM.

EDUCATION

GIET College of Engineering, Rajahmundry, JNTUK, A.P. **2018**

B.Tech

DECLARATION

I do here by confirm that the information given in this form is true to do the best of my knowledge and belief.

Karumujji Rajesh Kumar