PRUTHVI RAJ DASARI

Sr. Security Analyst

Ph:9440610181
Email:pruthviraj.soc42@gmail.com

KEY SKILLS

QRadar, Arc Sight, and McAfee
Incident response Vulnerability Assessment Cyber Threat Analysis
Incident response
Installation and use of firewalls

Platforms – Windows 7/8/10
Networking – TCP/IP, OSI, VPN
Security Tools – Splunk,Aisaac QRadar,Arcsight ESM/Logger

Security Devices - Check Point, -Palo Alto, Imperva WAF, Symantec Mail Gateway.
Ticket and Reporting tools: BMC Remedy and Service Now.

PROFESSIONAL SUMMARY:

- **4+** Years of experience across SIEM tools, SOAR, Intrusion Prevention System,Vulnerabilities and remediation,Antimalware and firewall.
- **1** year of experience across configuring, operating, optimization and troubleshooting of network security devices.
- Familiarity with firewall implementation and SOC monitoring with best practices.
- Agile in investigating security threats such as Malware Outbreaks, **DDOS, OWASP T-10**
- Familiarity with cyber security regulations, including cybersecurity standards and implementing best practices.

EXPERIENCE:

TCS PVT LTD

March 2017-Current

- Optimizing, managing and monitoring real-time events from devices like firewalls, web proxy, antivirus vendors, DCs using ArcSight , QRadar and DLP data loss .
- Aligning **MITRE** framework to the threat or Use Case and plotting the relevant TTP and analyze further mitigations
- Perform Security Incident Event Management (SIEM) console monitoring and correlation.
- Oversee and ensure P1 and P2 incidents are handled according to operational procedures. Document areas of improvement through after-action reports.

EDUCATION

BE/BTECH ,PRAGATI ENGINERING COLLEGE.

Intermediate Education from Sri Chaitanya Junior college.

I.C.S.E from ST.Ann's School,Rajahmundry.

- Detecting potential data breaches/data ex-filtration transmissions and prevents them by monitoring.
- Designated systems detect and prevent unauthorized attempts to copy or send sensitive data, intentionally or unintentionally, mainly by personnel who are authorized to access the sensitive information
- Authentication Manager includes an administrative user interface called the Security Console For example,you use the Security Console to: Add and manage users and user groups.
- RSA Authentication Manager from RSA Security is a multifactor authentication software tool that adds additional security measures (via smartphones and biometrics) to standard username and password logins fora number of services and servers.
- RSA provides both SecurID hardware and software tokens.
- Initially, the Security Console and Operations Console both use the user name and password that you specified during Quick Setup. If you change the user name or password for either Console, the user name and password for the other console remains unchanged.

ROLES AND RESPONSIBILITIES:

- Analysing the security advisories for taking preventing measure for vulnerabilities and malwares.
- Escalating the security incidents based on the client's SLA and providing meaningful information related to security incidents by doing in-depth analysis of event payload, providing recommendations regarding security incidents mitigation which in turn makes the customer business safeand secure.
- Co-ordinate extensively with networking teams to maintain and establish communication to remote **QRadar** Collectors/Processors
- Clear the risk-based authentication (RBA) device history to unregister devices
- Responding to various security alerts for various client and scanning for vulnerabilities using tools like **NESSUS.**
- Configure security questions for identity confirmation
- Manage their RSA SecurID PIN
- Security questions cannot be used as a primary authentication

method to access the Self-Service Console.Primary methods are RSA Password, LDAP Password, On- Demand Authentication, and SecurID.

- Responsible to preparing the root cause analysis reports based on the analysis.
- Troubleshooting SIEM dashboard issues when there are no reports getting generated or no data available.
- Determine the scope of security incident and its potential impact to Client network recommend steps to handle the security incident with all information and supporting evidence of security events.
- Handling multiple customers globally analyzing the customer networks for potential security attacks.
- Finding false positive,fine tuning and escalating Security events.
- Analysing weekly and monthly reports.

PERSONAL DETAILS:

DOB: 20th June 1994
Address: Rajahmundry
Languages:
English,Telugu,Hindi.