**Cyber security Analyst**

**Name: Sai Pavan Raj**

**Cell: 469-490-0344**

**Email:** [**vsaipavanraj@gmail.com**](file:///C:\Users\gopal\Downloads\vsaipavanraj@gmail.com)

**LinkedIn:** [**www.linkedin.com/in/pavan-raj-v-750069283**](http://www.linkedin.com/in/pavan-raj-v-750069283)

Professional with Good experience of **8+years** in the field of Information and **CYBER SECURITY** with a strong aptitude in Network SECURITY, seeking good time opportunity to enhance my knowledge and contribute to overall development of the organization.

* Self-starter with very good logical skills suitable for process design, data modeling and development. **CYBER SECURITY** Engineer with good experience in Implementation, Administration, Operation and Troubleshooting of enterprise data networks.
* Experience in vulnerability assessment and penetration testing using various tools like **Burp Suite**, **Dir - Buster**, **OWASP ZAP proxy**, **NMAP**, **Nessus,** **HP Fortify, IBM App Scan enterprise, Kali Linux, Metasploit**
* Conducted periodic scans and on demand scan as and when new network devices are introduced, or configurations are updated in the windows servers with **Qualys Guard**
* Responsible for setting up configuration files in **Splunk**.
* Huge knowledge of managing information assurance evaluation tests.
* Performed vulnerability scans using **HP Web Inspect, IBM App Scan, Qualys Guard, Retina, Nessus, Burp Suite, and Metasploit auxiliary** modules.
* Sound knowledge and industry experience in **Vulnerability Assessment and Penetration**.
* Testing on **web-based applications** Mobile based application and **Infrastructure penetration testing**.
* Conducted penetration testing and security tests and formulated scripts to test systems.
* Worked extensively on **Splunk Enterprise** and **Splunk Cloud**, having experience in Installation, developing Splunk alerts and Dashboards for analyzing application related data as per the business requirement.
* Supported for **Security Operations Center (SOC).** Monitor security system and diagnoses malware events to ensure no interruption of service. Identify potential threats, anomalies, and infections and provide reports to the customers.
* Experience as a **Splunk Engineer** configuring, implementing, and supporting Splunk Server Infrastructure across Windows, UNIX, and Linux environments.
* Extensive knowledge of SECURITY controls (**ISO/27002, NIST 800-53)** used to implement regulatory compliance (**NERC CIP, PCI, SOX, HIPAA) with IBM QRadar products**.
* Dedicated, multifaceted, and detail-oriented professional with progressive experience in CYBERSECURITY operations complemented with wide-ranging knowledge of **McAfee ePolicy** Orchestrator and networking technologies such as **firewalls, switches, and routers**.
* Experience with Risk assessment using Industry standards like **HIPAA, PCI/DSS** and develop SECURITY policy as per these standards.
* Conducts vulnerability scans and penetration tests to meet **PCI** requirements.
* Management and administration of Juniper and **ASA Firewalls** at various zones including **DMZ**, Extranet (Various Business Partners) and internal.
* Configure, maintain, and design network SECURITY solutions including firewalls (**Checkpoint, Cisco ASA, and Fortinet)**, **IDS/IPS (Cisco, Checkpoint and Sourcefire)**, **VPN, ACLs, Web Proxy**, etc.
* Work closely with clients Information Assurance analysts to oversee the preparation of a comprehensive and executive Certification and Accreditation (C&A) packages for approval of an Authorization to Operate (ATO); generate, review and update System SECURITY Plan (SSP) against **NIST 800-18 and NIST 800-53** requirements.
* Perform Risk Assessment, Gap analysis & create Risk Mitigation plan.
* Experienced with Proxy and Malware-mitigation (**Bluecoat, Radware/ApplXcel/Alteon, FireEye**), threat detection and data leakage protection (**Network DLP/Vontu/Symantec, Bluecoat SECURITY Analytics.**
* Experience in **Palo Alto Firewall, VPNs**, and networking with protocols i.e., **NetBIOS, SNMP, telnet, SSH, ARP, etc.**
* Configured Data leakage and protection policies to prevent data leakage of end client.
* Expert Understanding to develop the complex Use Cases, Universal Device Support Modules (DSM’s) on the Q Radar SIEM.
* Involved in Integration IBM Resilient IRP with IBM Q Radar SIEM.
* Knowledge of Authentication, End Point Security, Internet Policy Enforcement, Firewalls, Database Activity Monitoring (DAM), Identity and Access Management (IAM) solutions.
* Responsible for integration of Q Radar with Carbon Black Endpoint Security.
* Configured Tenable security center with latest version of Nessus scanner.
* Configured and involved in setting up architecture several internal tools such as vulnerability tracking reporting tool with including various ETL processes to monitor intrusion events and identify latest vulnerability.
* Analyze the results of penetrations tests, design reviews, source code reviews and other security tests. Decide on what to remediate and what to risk accept based on security requirements.
* Worked on manual and automated Vulnerability assessments and penetration testing for Web or Mobile Applications.
* Worked on Static Application Security Testing tools like Fortify, AppScan Source edition, Veracode, Checkmarx and HCL.

**EDUCATION:**

Bachelor’s: Computer Science, JNTU 2014

**TECHNICAL SKILLS**

|  |  |
| --- | --- |
| Port/Vulnerability Scanning | Nmap, Nessus, Rapid7, Qualys |
| SIEM Tools | Splunk, ELK, Azure Sentinal, Qradar |
| Network Security Testing | Symantec DLP-1 year, End-point Protection-1 year, Checkpoint-1 year, Palo Alto-1 year, Cisco, IDS/IPS-1-year, Anti-virus-1 year |
| Password Cracking | Hydra, Rainbow Crack, BladeLogic, Remedy, Ophcrack, John the Ripper, Pyrit |
| Security Tools | ZED attack proxy, SQLMAP, Wireshark, WebScarab, Paros, Nmap, Nessus, Rapid7 Nexpose, Arcsight SIEM, Varonis, Alien vault USM (SIEM) |
| DAST and SAST Tools | IBM AppScan Enterprise (ASE), Standard & Source editions, HP WebInspect, Burpsuite Pro, Acunetix |
| Operating Systems | UNIX, RedHat Linux 4/5, Windows Server2003/2008 |
| Programming Languages | SQL, Spring Framework, Java, J2EE, Python, C/C++, C#, .NET, Perl |

**PROFESSIONAL EXPERIENCE**

**Client: Visa, New city, NY Oct 2021- Till date**

**Cybersecurity Analyst**

**Responsibilities:**

* Use **SIEM** tools (**Splunk/LogRhythm**) to identify threats and patterns for security incident response.
* Tune **SIEM Al Engine** rules to create better alerting, establish security baselines for configuration to tune out unnecessary alerts.
* Performed risk assessments to help create optimal prevention and management plans.
* Analyze and troubleshoot logs in a timely manner.
* To deploy systems to incident investigation, remediation and PIR procedures for all **DLP/ILMS** cases.
* Developed security strategy and performing IT risk assessment, **vulnerability assessment** and working with the business to mitigate risks.
* Implemented **Splunk** arrangements in exceptionally accessible, repetitive, conveyed figuring situations.
* Provide 2nd level support to resolve escalation producers.
* Tracking reports for unauthorized websites and push the cases for escalations **End Point DLP**.
* Monitor threats and alerts affecting customer networks and triage responses to remediate the alerts.
* Create vulnerability reports using **CVEs** and devise plans to patch or x affected devices.
* Responsible of administrative role and duties of cyber security applications **like FireEye, Network intrusion detection system, McAfee policy orchestrator, Symantec** data leakage and protection, Confidential, Symantec control compliance suite, Netflow integrator.
* Integrated **IDS/IPS** to Confidential ESM and analyzed the logs to filter out False positive and add False negatives into **IDS/IPS** rule set.
* Responsible for applying standards for each platform (Windows, Unix, Middleware, etc) with applications like **Symantec Control Compliance Suite**.
* Created installation and configuration and test case scenarios documents for each specific device Connectors.
* Configured **Nessus Scanner** with latest security center version.
* Integrated different devices data to **Splunk** Environment and created dashboards and reports in Splunk.
* Monitored and identified any suspicious events using the Confidential **ESM** console and raised a ticket.
* Responsible for monitoring traffic status, appliance, and server health check to verify functionality.
* Entirely responsible for performing production changes/upgrades via informing to all responsible teams and stakeholders.
* Involved in weekly and monthly meetings with other teams to review and discuss upcoming production changes and policy modifications.
* Maintain and responsible to assess compliance score of each network asset in the infrastructure to align with government configuration policy.
* Create Policies, procedures, reports, Metrics and provide network and host-based security to each host within the organization.
* Work under the direction of the Team Leader to maintain security devices and show practical experience in managing SIEM environments, Fire Eys standalone devices such as NX, EX and HX, **NIDS, UNIX** servers and packet capture devices.
* Analyze logs and events from the solution and provide threat analysis reports and build custom security policies and application signatures.
* Review and ongoing assessment of malware analysis techniques, intrusion **detection/intrusion prevention, SIEM** application access control, Antivirus, and other network component policies.
* Configure, implement, and maintain all security platforms and their associated software, such as Linux based standalone devices, windows servers, **UNIX** servers, intrusion detection, intrusion prevention, SIEM.
* Ensure network security best practices are implemented through auditing: database servers, traffic analyzer sensors, firewall rules, change control and monitoring.
* Configured Intrusion policies, health policies and system policies in for network traffic analysis.

**Client: Central Bank, St louis, MO May 2018 – Sep 2021**

**Cybersecurity Analyst**

**Responsibilities:**

* Monitored system logs, **SIEM** tools and network traffic for unusual or suspicious activity.
* Interpret such activity and make recommendations for resolution.
* Excellent communication skills.
* Ability to work with the most to least computer literates.
* Performing regular penetration testing and vulnerability assessment/remediation using Nessus, IBM app scan and meta sploit.
* Detected/Analyzed and reported **DLP** Suspicious Incidents for end-users.
* Responsible for troubleshooting various indexing issues by analyzing **splunk** logs such as splunkd.log, metrics.log ingested as internal index.
* Administer and maintain end user accounts, permissions, and access rights.
* Developed and maintained documentation for security systems and procedures.
* Monitored the security and information technology infrastructure, including hardware, software, and to protect the confidentiality, integrity and availability of systems.
* Security incidents to provide management oversight to the incident process.
* Perform tuning of the Security Incident and Event Manager (**SIEM**) filters and correlations to continuously improve monitoring.
* Network and host **DLP** monitoring and logging.
* Performed Monthly and quarterly scans using **Symantic DLP** and doner the escalation of critical data found on Share devices and Shared drives. Created and Managed DLP policies.
* Utilized Security Information and Event Management (SIEM), Intrusion Detection and Prevention Systems (**IDS/IPS**), **Data Leakage Prevention (DLP)**, forensics, sniffers and malware analysis tools.
* Monitoring and remediating daily security alerts generated by end users with the tools like **Intel/ McAfee SIEM, Force Points Websense, and Intel/ McAfee EPO 5.X** and responsible for effectiveness of tools and scans, as well as assessing and tracking risk of exposure.
* Manage Splunk (SIEM) configuration files like input, props, transforms etc.
* Centralizing the storage and interpretation of logs using Splunk (SIEM) System.
* Worked to develop **CIRT** within organization to handle a potential future breach instance.
* Vulnerability Management: Configured **Qualys Guard** Tool for Vulnerability Analysis of Devices and Applications. Monitored them consistently through the dashboard by running the reports all the time.
* Installed, Configured Symantec End Point Protection on laptops used for remote connectivity.
* Familiarity with security and testing tools such as **Brup Suite, Nmap, Zenmap, OpenVAS, Nessus**.
* Used remediation techniques for all collected vulnerabilities and if it is very high severe Vulnerability.
* Maintains network performance by performing network monitoring and analysis, and performance tuning, troubleshooting network problems. Skilled using **Brup Suite, NMAP, Qualys guard, Nessus.**
* Provide Approvals for Software/ Application Installations, Site review for web access, **McAfee EPO** exceptions, and Vulnerability exceptions.
* Prepared, arranged, and tested Splunk search strings and operational strings. Created and configured management reports and dashboards.
* Expertise in the utilization, configuration and implementation of industry capabilities including web content filters, email security capabilities, **IDS, IPS**, Host Based Security System **(HBBS), SEIM** security practices.

**Client: ASCENA RETAIL GROUP, Columbus, OHIO Aug 2016 – Mar 2018**

**Security Engineer**

**Responsibilities:**

* Performed the review of a newly implemented Security Incident and Event Management **(SIEM)** system. Reviewed technical specifications for SIEM, logging and proposed recommendations to improve the overall deployment of the solution.
* Have experience on conducting application and **network penetration testing**.
* Used Sourcefire/ Firepower management console to monitor, validate and remediate attacks/ incidents.
* Deployed and monitored **Cisco AMP** for malware protection.
* Have worked in consulting on application security.
* Conduct periodic network, system, application, and physical security audits.
* Have managed large appsec programs.
* Maintain a set of policy documents, security standards, and process and procedure documents for the Technologies Division
* Have experience in working on **DevSecOp**s pipeline.
* Responsible for monitoring and providing analysis in a 24x7x365 Security Operation Center **(SOC)** using various **SIEM** (Splunk), **IDS/IPS** software tools.
* Responsible for Data loss prevention **(DLP)** and service interruptions.
* Exposure to wildfire advanced malware detection using IPS feature of **Palo Alto.**
* Monitor critical infrastructure including firewalls, **IDS/IPS** devices, virtual networks, vulnerability scanners, VPNs, WANs, and disaster recovery sites.
* Managed and maintained various network security systems including firewalls, IDS systems, central authentication systems, application proxies, and general support systems.
* Engineering, configuring, and deploying Enterprise SIEM/SEM solutions.
* Manage **Splunk** (SIEM) configuration files like inputs, props, transforms, and lookups. Upgrading the Splunk Enterprise and security patching.
* Worked extensively with software development teams to review the source code, triage the security vulnerabilities generated by **IBM AppScan, Burp Suite, HP Fortify, White Hat** and eliminated false positives.
* Performed penetration testing for external facing web applications. Security areas covering **DMZ architecture**, threat modeling, secure coding practices (i.e., OWASP standards) and vulnerability analysis were assessed.
* Initiated projects to create disaster recovery plans for identified gaps.
* Established disaster recovery plan testing and auditing cadence.
* Create policies, alerts and configure using SIEM tools (Splunk)
* Assisted Intelligence Team with indicators associated with different Actor groups to combat cyber-attacks performed identification of connectivity issues through PING and Traceroute.

**Client: Unisys, Bangalore, India July 2014 – Oct 2015**

**Security Analyst**

**Responsibilities:**

* Provided project planning, guidance and technical expertise in program, policy, process, and planning; risk management, auditing, and assessments; A&A; and quality planning and control.
* Researched and analyzed known hacker methodology, system exploits and vulnerabilities to support Red Team Assessment activities.
* Assisted with the update and administration of all **SOX** **audit** requirements from an IT internal controls perspective.
* Provided with Threat profiling of the application to the client and prepared combined reports of level of risks, their trend, and frequency to the client.
* Conducted white/gray box penetration testing on the financial systems using Kali, Linus, Cobalt Strike for **OWASP top 10 Vulnerabilities like XSS, SQL Injection, CSRF, Privilege Escalation** and all the test-case of a web application security testing.
* Threat and Virus scanning using **Malwarebytes** from centralized console Enforcement of policies and procedures for users, admins, and management.