**Name: Anil Botla**

**Phone: +1 (405) 595-0249**

[**Email:**](mailto:jaiminpatel55@yahoo.com)**-** [**botlaanil19@gmail.com**](mailto:botlaanil19@gmail.com)

**Professional Summary:**

* Professional with Good experience of **9+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.
* CYBER SECURITY Engineer with good experience in Implementation, Administration, Operation and **Troubleshooting of** enterprise data networks**.**
* 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.
* 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.
* 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** (ePO) 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.

• Implemented **FireEye** **security** to avoid **malware** and **cyber-attacks** on the system.

* 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**.
* Experience with Manual Security Testing & Dynamic Application Security Testing tools like **BurpSuite, IBM AppScan, WhiteHat and WebInspect and Qualys Web Application Scanning**.
* Experience on Sub-Domains with **SIEM, Thread Modeling, PCI/HIPAA auditing and Risk assessments**, as well as onsite and offshore team management.
* Demonstrating flexibility in prioritizing and completing tasks and working collaboratively with the client to identify and solve **key constraints, vulnerability and risks**.
* Coordinate with dev team to ensure closure of reported vulnerabilities by explaining the ease of exploitation and the impact of the issue.
* Worked on Static Application Security Testing tools like **Fortify, AppScan Source edition, Veracode, Checkmarx and HCL**.

**Education:**

BE(ELECTRONICS) India- 2014.

**Areas of Experience:**

|  |  |
| --- | --- |
| 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 |

**Client: Crowdstrike, Sunnyvale, CA Oct 2022 - Till date**

**Role: Cybersecurity Analyst**

**Responsibilities:**

* Responsible of **administrative** role and **duties** of cyber security applications like **FireEye**, **Network intrusion detection system**, McAfee epolicy 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**, **FireEys** 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.

**Company: Verizon, Tampa, FL Nov 2020- Sept 2022**

**Role: Information Security Analyst**

**Responsibilities:**

* Experience in security Incident handling **SIEM** using **RSA Envision** and **IBM QRadar** Products.
* 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, ForcePoints 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 **Vulnarability 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 Installation**s, 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.**

**Company: Facebook, Seattle, WA Sep 2017- Oct 2020**

**Information Security Auditor/ Cybersecurity Incident Responder**

**Responsibilities:**

* Assist in research and development of security systems, processes and procedures following industry best practices.
* Track, review and analyze security alerts and **vulnerabilities from vendor and other sources**.
* Respond to **information security** incidents on an as needed basis.
* Knowledge of payment card industry data **security standards (PCI DSS) and ISO27001**.
* Experienced in **reviewing POA&M and ATO packages** to ensure compliance.
* Experienced in the **development** of policies and procedures following NIST 800-53 control document. Manage and support all information security projects, policies and procedures.
* Identify, Investigate, and report on **events** generated by security tools.
* Perform information **security risk & vulnerability assessment**s.
* Managed the **development of System Security Authorization Agreements.**
* Ability to work under difficult and fast paced terrain and meet deadlines in required time frames.
* Maintain excellent working relationships with both internal and external customers using communication skills.
* **Risk Assessment and Vulnerability assessment,** generating reports and responding to critical and severity of vulnerability.
* Experience in reviewing third party suppliers to ensure they comply with the company’s information security standards. Also, in carrying out security audit, security assessment and continuous auditing and monitoring third party hosting servers, replicating backups, data and information.
* Work **with ISSOs** to ensure documenting and remediating audit findings, security planning and reporting and mitigation of security vulnerabilities are completed in a timely manner.
* Knowledge of data protection and **GDPR**. Conducting seminar and workshop, presenting security weakness to stakeholder and employee. Also, advised the business on data protection and privacy requirements to protect customers **data and information** and to comply with **GDPR**.

**Company: Illumio, India Aug 2015 – Jan 2017**

**Role: Information Security Analyst**

**Responsibilities:**

* Monitored system logs, **SIEM** tools and network traffic for unusual or suspicious activity. Interpret such activity and make recommendations for resolution.
* Performing regular penetration testing **and vulnerability assessment/ remediation using Nessus, IBM app Scan and Metasploit.**
* Detected/ Analyzed and reported **DLP** Suspicious Incidents for end-users.
* Responsible for troubleshooting various indexing issues by **analyzing Splunk logs such as splinked.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.
* Managing Palo alto appliance for **IPS, URL filtering, Anti-Virus, DLP, Malware**, Denial of service and vulnerability protection.
* Experience in setting up dashboards for senior management and production support required to use **Splunk**.
* Daily activities included installation, upgrades, troubleshooting, configuration, migrating user profits and data, maintaining third party software applications, servers, and workstations.
* Manages **and facilitates information security related projects**.
* Conducting periodic vulnerability scans of systems, wireless and network devices.
* Monitoring of events from **Data Loss Prevention (DLP**) and other information security tools and determining appropriate next steps using knowledge of corning businesses or processes.
* Policy and **Rule Management in Symantec DLP**. Experience **with Symantec Vontu DLP** product Experience with deployment of Symantec **DLP – Endpoint Prevent**, Network Prevent for Email, and Network Prevent for Web, Network Discover, and ITA.
* 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 constantly 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 Burp Suite, Nmap, Zenmap, OpenVAS, Nessus.**
* Provide Approvals for Software/ application Installations, Site review for web access, **McAfee EPO** exceptions, and Vulnerability exceptions.
* Expertise in the utilization, configuration, and implementation of industry capabilities including web content filters, email security capabilities**, IDS, IPS, Host Based Security System (HBSS),** SEIM security practices.

**Client: HSBC Group, Hyderabad, India July 2014 to Aug 2015**

**Role: Security researcher**

**Responsibilities:**

* Performed **vulnerability assessments, threat assessment**, mitigation and reporting activities in order to safeguard information assets and ensure protection has been put in place on the system.
* Found common web site security issues (CSRF, XSS, application logic, SQL injection, information leakage, session fixation etc.) across various platforms.
* Preparation **of security testing checklist** to the company.
* Investigating **logs** and **payloads** for server **crashes/core dumps, DDoS attacks, SQL/XSS** etc.
* Prioritizing and managing multiple tasks in accordance with high level objectives.
* Performed live packet data capture with **Wire Shark** to examine security flaws.
* Performed dynamic and static analysis of web application using **HCL AppScan and HP Fortify**.
* Information gathering of the application using websites **like Shodan, ReverseDNS**.
* Network scanning using tools **like Nmap and Nessus**.