|  |
| --- |
| **ROSHAN ABDUL PH : 984-329-2610**  **Email Id :** [**roshan.abdul90@gmail.com**](mailto:roshan.abdul90@gmail.com) |

****

**PROFESSIONAL PROFILE**

* Epxertise experience in Network Security Operations, content authoring, design, installation, administration, upgrades, monitoring, implementation, integration operation of an IBM Qradar /Splunk/Nessus/Rapid 7/McAfee EPO.
* Expert level understanding of Qradar Implementation & its Integration with other N/W devices and Applications and the troubleshooting work.
* Expert Understanding to develop the complex Use Cases, Universal device support Modules on the QRadar SIEM.
* Integration of different devices/applications/databases/operating systems with QRadar SIEM.
* Knowledge of cleaning up log auto-discovered sources in Qradar by identifying duplicates, correcting misidentified log sources, and identifying log sources from their logs.
* Expertise in Creating Scripting for Configuration Backup, Report backup, Qradar Device Reports and for Metric Generation.
* Experience in editing building blocks to reduce the number of false positives that are generated by IBM SecurityQRadar and writing co-relation rules.
* Develop processes and perform investigations on all identified attacks via IPS, IDS, Firewall, Antivirus, and Data Loss Prevention Tools.
* Analyze security logs generated by Intrusion Detection/Prevention Systems (IDS/IPS), Firewalls, Anti-Virus, and/or other security logging sources and SIEM aggregators.
* Authored, directed the SOC Analyst and Engineering playbooks for functional areas such Threat Intelligence operations (collection, analysis, and dissemination), malicious code analysis, custom Sourcefire IDS signature analysis, Sourcefire ThreatFeeds.
* On-site Security/Risk Assessments, McAfee Web Gateway, McAfee ePO and Endpoint Security deployment including Virus Scan enterprise, endpoint security 10.x, HIPS, DLP, whitelisting with Solidcore (File Integrity Manager, Application Manager),FireEye MTP and Proofpoint.
* Providing recommendations within the incident-management system.
* Review and analyze pcaps using Wireshark.
* Conduct vulnerability scanning using Nessus
* Involved in the administration of F5 ASM and Bluecoat SSL6v and responsible for writing rules and policies.
* Experienced in building Automation frameworks related to Application Security and proficient in Java,Python and Unix shell scripts and PowerShell.
* Expertise in Kerberos, DNS, Load Balancers, Active Directory.
* Cyber vulnerability assessment and remediation as part of NERC Standard CIP-007.   
  Access review and reporting for physical and electronic security controls as part of NERC StandardsCIP-005 & CIP-006.
* Experience in developing the vulnerability assessment report for the vulnerabilities and non-compliance issues that were detected. Recommend possible mitigating measures (Rapid7, Nessus, Qualys Guard).
* Provide PKI support and subject matter expertise for application developers in enabling their applications to support PKI.
* Experience in working with various web filters and web security gateways likeBluecoat Secure web gateway, McAfee Web Gateway, F5 Secure Web Gateway.
* Experience with network security technologies such as Palo Alto, Check Point, and Sourcefire and The SANS Investigative Forensic Toolkit ("SIFT").
* Implemented Symantec DATA Loss prevention to secure all end points. Configured and instrumented Symantec management console, Symantec management server and Symantec database on Oracle.
* Experience with enterprise-class security products such as web proxy, reverse proxy, load balancing, IDS/IPS, DLP, Firewall, IPsec/SSL VPN, WAN/LAN, wireless and remote connectivity.
* Extensive knowledge of security controls (ISO/27002, NIST 800-53) used to implement regulatory compliance (NERC CIP, PCI, SOX, HIPAA) with IBM Qradar products.
* Analyze network traffic with Splunk and IBM Qradar tools on network traffic, firewall (Source Fire defense center) and AV (McAfee) logs.

**AREAS OF EXPERTISE:**

|  |  |  |
| --- | --- | --- |
| * [IBM QRadar](http://www-01.ibm.com/support/docview.wss?uid=swg21651118) | * Linux | * Unix |
| * Splunk 5.x and 6.x | * Firewalls-Checkpoint,PaloAlto | * IPS-Sophos,PaloAlto |
| * Bluecoat Proxy * IDS– Snort,Tripwire * PCI,SOX,HIPAA | * Symantec DLP and SEP * Mcafee EPO * Rapid-7 Nexpose |  |

**PROFESSIONAL EXPERIENCE**

**Patheon Inc, Durham, North Carolina. (April 17 to Present)**

**Role: Security Analyst.**

**Roles & Responsibilities:**

* Initial set-up, installation, and implementation of new SIEM solution (IBM Qradar).
* Migrating existing Reports and Alerts from RSA envision to IBM Qradar.
* Aggregate, correlate and analyze log data from network devices, security devices and other key assets using QRadar.
* Created SIEM dashboard for Qradar and reconciliation with Storage, Database Server,Workstation and Server and Network Devices.
* Along with creating custom views, reporting and automated alerting for both operational and security use using IBM QRadar.
* Assist multiple security projects with the goal of exceeding compliance objectives. Responsible for maintenance, administration, and configuration of the log aggregation solution.
* Experience working with Bluecoat WAN Accelerator, Bluecoat Packet shaper and Bluecoat Proxy.
* Developed, evaluated, and documented specific metrics for management purposes in Splunk
* Developed, evaluated, and documented management reports and dashboards in Splunk.
* Prepared, arranged, and tested Splunk search strings and operational strings in Splunk.
* Ensure the integrity and protection of networks, systems, and applications by technical enforcement of organizational security policies, through monitoring of vulnerability scanning devices.
* Use Splunk for log, report, and alert gathering.
* Responsible for maintaining availability, reporting and communication of the SIEM between it, its event-sources and the endpoints. Analysis of various use cases in the Qradar console like Malware, AD-related issues.
* Responsible for the creation of the logic to correlate attacks across multiple event sources and attempt to make a determination of the possible outcome.
* Responsible for creating weekly, ad hoc and monthly reports using exposeRapid 7 vulnerability tool to analyze reports using excel to create pivot charts to show trends.
* Using Symantec DLP monitored the transmission of confidential data contained in corporate emails that were sent using Microsoft Exchange and downloaded to mobile devices.
* Assisted in themonitor and set policies in EPO server, maintain updates on HBSS server, domain servers, and domain workstations, push McAfee policies to required computers, and Symantec to servers.
* Used consultative selling skills to prospect, identify opportunities, overcome objections, and, Compliance (HIPPA, PCI, SOX), and Vulnerability software technology.
* Assist in development and implementation of an information security vulnerability management policies, procedures, and standards based on National Institute of Standards and Technology (NIST) 800-53 standards, best practices, and compliance requirements.
* Created reusable and auditable automation test scripts to evaluate the entire financial transaction process through the BST application during the SDLC process from business requirements review, design, development, final system testing, and release readiness testing.
* Given the authority to build and lead the effort towards the improvement and development of the Incident Response Program. Also co-opted into the Symantec Data Loss Prevention (DLP) program to keep track of potential breaches of PCI and other sensitive data in the environment.

### Environment: IBM Qradar, Splunk, Windows, Nessus Scanner, Rapid 7 Nexpose,[McAfee Network Security Platform](http://www.mcafee.com/us/products/network-security-platform.aspx) (NSP),Java and Python Shell scripting, Bluecoat, SymantecDLP, and SEP.

**Bristol-Myers Squibb, Princeton, New Jersey. (Feb 16 to March 17)**

**Role: Security Analyst ( SOC )**

**Responsibilities:**

* QRadar SIEM v7.2 Administration with SIEM EPS tuning, distributed deployment architectures.
* Part of deployment team where parsing several Log sources are integrated into QRadar through mid-layer such as F5 for PCI and Syslog services.
* IBM QRadar Vulnerability manager and Threat Manager (QVM and QTM).
* Added few Custom Log Sources via Universal DSM/LSX - QID adding/mapping and creating building blocks/rules.
* Created custom searches, custom reports, rules, reference sets and reference maps.
* Experience in Security Incident handling SIEM using RSA Envision and IBM Qradar products Identifying the critical IT infrastructure that requires 24/7 monitoring.
* Expert level understanding of Qradar Implementation & its Integration with other N/W devices and Applications and the troubleshooting work.
* Performed CERT/SOC operations, including IDS event monitoring and analysis, security incident handling, incident reporting, and threat analysis. Performed security incident handling, incident reporting, and threat analysis.
* Perform vulnerability, configuration and compliance scan with Rapid7 to detect deficiencies and validate compliance with information systems configuration with organization's policies and standards.
* Create test scripts for computer network device, such as: Implemented a test web UI by Perl, Python, TCL/Expect.Analyze network traffic by Perl, python.
* Experience on working with Integration of UNIX and LINUX with Active Directory using Certify Tool Provided 24x7 on-call Support for Production Environments.
* Review and updating System Security Plan (SSP) based on findings from Assessing controls using NIST SP 800-18 rev1, NIST SP 800-53a rev4, and NIST SP 800-53.
* Actively monitored and responded to activity impacting various enterpriseendpoints facilitating network communication and data handling (McAfee End Point Security, DLP, Splunk)
* Worked on Cisco Routers, Active /Passive Hubs, Switches, Cisco PIX Firewall, Cisco ASA, NOKIA Firewalls, Nortel VPN Concentrators TCP/IP, NAT and Checkpoint ESX/GSX firewall.
* Responsible for identifying and validating indicators of threat from multiple intel sources (i.e. Crowdstrike, FS-ISAC, BlueCoat, etc.) against internal assets to determine an accurate threat landscape and remediation targets (i.e. Splunk endpoint analysis, Vulnerability analysis (Qualys, Nessus, Metasploit).
* Worked on Palo Alto Firewalls (50+ firewalls) PA-3020, PA-3050, PA-5020, PA-5050, PA-5060 series.

**Environment:** IBM QRadar, Linux, Splunk, Rapid 7 Nexpose,Symantec DLP and SEP,SYSLOG-NG,Java and Unix shell scripting,Bluecoat Proxy.

**Client: Surya Technologies Inc.,Cary, North Carolina. (Nov 13 to July 15)**

**Role: SIEM Engineer/Cybersecurity consultant**

**Responsibilities:**

* Installation of Connectors and Integration of multi-platform devices with IBM Qradar.
* Configuring log generation and collection from a wide variety of products distributed across categories of servers, network devices, security devices, databases, and apps.
* Integration of IDS/IPS to IBM Qradar and analyze the logs to filter out False positives and add False negatives into IDS/IPS rule set.
* Categorize the messages generated by security and networking devices into the multi-dimensional IBM Qradar normalization scheme.
* Develop content for IBM Qradar like correlation rules, dashboards, reports and filters, Active lists, and Session list.
* Review and updating System Security Plan (SSP) based on findings from Assessing controls using NIST SP 800-18 rev1, NIST SP 800-53a rev4, and NIST SP 800-53.
* Scheduled enterprise vulnerability scans to ensure there is no impact on client facing or critical information assets. (Internal Nessus, Nexpose and Metasploit scans in coordination with the enterprise Red Team, and external scans (Qualys)). This role required the ability to configure scanning tools and identify the scope of the scans being performed (target range, expectations, support role delegation).
* Serves as a team member that properly prepares for and address incidents across the organization, a centralized incident response team is formed and is responsible for analyzing security breaches and taking any necessary responsive measures.
* Implementation, configuration, and support of Checkpoint and ASA firewalls for clients.

### Environment: IBM QRadar, Splunk, UNIX, HP TippingPoint NX Next-Generation Intrusion Prevention System,Bluecoat secure web gateway, Symantec DLP, and EndPoint.

**HCL Technologies,Hyderabad, India. (May 11 to Oct 13**

**Role: IT Engineer**

**Environment: Windows, Linux, LAN, WAN, Antivirus.**

* Performed vulnerability scanning on web applications and databases to identify security threats and vulnerabilities.
* Responsible for analyzing, detecting, preventing malware with security analysis tools and compliance tools.
* Audit of Cisco ACL, Active Directory, and rules in F5 ASM.
* Conduct penetration testing & Auditing of the organization network by using tools.
* Footprinting, Scanning, Sniffing and monitoring Network activities by using Open source & commercial tools like (Wireshark, Nmap).
* Expertise in virtual server technology (VMWare, ESXi, VSphere).
* Installing, Configuring of Networking Equipment’s: Routers and Switches and LAN/WAN design, implementation and optimization using Cisco routers and switches.
* Used Layer 3 protocols like EIGRP and BGP to configure Routers in the network.
* Configure and Implement Remote Access Solution: IPSEC VPN, Remote Access.
* Conducted evaluation of intranets and firewalls on a regular basis.
* Worked closely with project team members to document current PCI requirements and instructed team members on appropriate control rationalization and test evidencing

techniques.