**Bhanu Prathap**

**Ph No. +1** 732-338-8659 **| Mail ID:** **nag.velpula24@gmail.com**

**PROFESSIONAL SUMMARY:**

* Result driven Cyber Security Analyst with 10+ years of experience in implementing and reviewing Policy documents and remediating POAMs/Incidents as well as vulnerability scanning with extensive experience with network devices (switches, routers, hubs) and continuous monitoring (SIEM). I thrive under pressure in fast - paced environment while directing multiple projects from concept to implementation and working to prevent cyber-attacks especially in business and corporate settings.
* Experienced in Vulnerability management and remediation.
* Experience configuring and deploying McAfee modules and products like McAfee ePO, McAfee VSE, McAfee HIPS, McAfee Endpoint Encryption, McAfee Network DLP, McAfee DLP Endpoint, McAfee SIEM.
* Experience with SIEM tool like Qradar, Splunk.
* Experience in planning, developing, implementing, monitoring and updating security programs, and advanced technical information security solutions, and sound knowledge in SOX and PCI compliance requirements and understanding of NIST and ISO standards.
* Experience with industry recognized SIEM (Security Information and Event Management) solutions such as SNORT, Splunk, Log Rhythm and many other tools.
* Worked on McAfee HIPS product for Get the broadest IPS coverage, Safeguard against malicious threats, Get automatic security updates, Protection around the clock.
* Experienced in SIEM tool such as ArcSight to manage security events and big data analytics.
* Manage and perform Nessus and Nmap scans before all production releases and analyze vulnerabilities and report to all stakeholders.
* Performs vulnerability assessments and penetration testing using automated tools on web applications.
* Switching tasks include VTP, Trunking, VLAN Change, ISL and 802.1q, IP and GRE Tunneling, VLAN, Ether Channel, STP, PVSTP and RSTP. Network security including NAT/PAT configuration, ACL, IDS/IPS and ASA/PIX Firewalls.
* Implementation and troubleshooting of technologies such as MPLS VPN, IPsec VPN, DMVPN, LDAP, AAA
* Well Experienced in Protocols HSRP, GLBP, VRRP, ICMP, IGMP, PPP, PAP, CHAP SMTP and PoP3. Expertise in IP Addressing, Sub netting, VLSM and CIDR. Implemented traffic filters using Standard and Extended access-lists, Distribute-Lists, and Route Maps.
* Experience in installing and troubleshooting DNS, DHCP server. Experience in configuring VPN: Site-to-site, Site-to-SOHO, remote access VPN solutions (SSL). Experience testing Cisco routers and switches in a lab environment and deploying on site for production.
* Hands on Experience in Riverbed Steelhead appliances, Riverbed Cascade Profiler, Gateway and Sensor.
* Experience with configuration, installation, testing, deployment of networking devices.
* Working knowledge of Solarwind Network Management software.
* Configuration and Maintenance of Aruba wireless controller and access points.
* Experience in installation and configuration of Splunk Enterprise.
* Working experience in Checkpoint Smart dashboard, Smartview Tracker, Smartview Monitor, Smartview Report.
* Experience with Palo Alto, Checkpoint, Cisco ASA, Juniper SRX, FWSM, SSL VPN (SA VPN) firewalls.
* Source fire IPS, AIP-SSM Modules on ASA, Checkpoint IPS Blades etc.
* Experience with Bluecoat Proxy, F5 Load balancer LTM and GTM.

**CORE COMPETENCIES:**

Vulnerability Scanning and Management | Risk Analysis | Incident Response | Threat Remediation | Endpoint Security | Process Improvement | Project Management | Training & Documentation | Windows, Linux, Cisco, IIS, Apache, Mcafee, ArcSight, Blue Coat, Nessus, Metasploit, Nmap, Burp Suite, Maltego, Wireshark, Powershell, Python, Ruby.

**TECHNICAL SKILLS:**

|  |  |
| --- | --- |
| **Category** | **Technologies / Tools** |
| **Routing Technologies** | RIPV1, RIPV2, IGRP, EIGRP, IS-IS, OSPF, BGP |
| **Network Products – Routers** | Cisco 1700, 1800, 2500, 2600, 2800, 3600, 3800, 7200, 12010, 12404 |
| **Network Products – Switches** | Cisco 1900, 2950 (listed twice), 2960G, 3550XL, 4948 Core, Catalyst 4503, 4507 RE, 6500/6503/6507, Nexus 2000, 5000, 7000 series |
| **Antivirus & Endpoint Protection** | Cisco CSA, Symantec Enterprise, McAfee Enterprise |
| **Security & VPN** | ASA 5505 Firewall, AIP SSM, CSC SSM, FWSM, FortiGate, Cisco CSM, ACL, IPS/IDS, NAT, PAT, Cisco ACS, Juniper NetScreen, Palo Alto Firewalls, WSUS |
| **Security Tools / Devices / Software** | SEPM, Websense, Wireshark, IronPort, FireEye, QualysGuard, FireMon, Splunk, SolarWinds, Algosec, Cisco ISE, NAC, Cisco ASA 5512/5525/5525-X, Firepower, Cisco IOS, NX-OS, Akamai (CDN/WAF), F5 Networks WAF, Cisco IPS, Palo Alto IPS, StealthWatch, SIEM Tools, ESA, WSA, MFA, Cisco Umbrella, Cisco AMP, Bluecoat Proxy, AWS, Azure, GCP |
| **LAN Technologies** | IEEE 802.11, Token Ring, Workgroup, Domain, HSRP, DNS, Static, VLAN, STP, VTP, EtherChannel, Trunks |
| **WAN Infrastructure** | Leased Line, ISDN/Dial-Up, Frame Relay, Metro Ethernet |
| **Scripting** | Bash, Unix, Python (Firewall configuration scripts) |
| **WAN Technologies** | HDLC, PPP, ATM, SONET, MPLS, VPN, IPsec-VPN |
| **Wireless & Wi-Fi** | Canopy (P2P/PTMP), DLink Wireless/AP, Cisco 1200 AP, Linksys Wireless Router |
| **Operating Systems & Tools** | Cisco IOS, Windows NT 4.0, Windows 2000/2003/2008 Server, Windows XP/7/8, Linux, Solaris, Active Directory, Apache, MS Exchange, VERITAS Volume Manager |

**CAREER EXPERIENCE AND HIGHLIGHTS:**

**Healthfirst**

**Cyber Security ENGINEER and Cyber Security Analyst Aug-2023 To till date**

**Responsibilities:**

* Managed database assets (inventory) and vulnerability management scans utilizing Tripwire Compliance Configuration Manager (CCM), IP360 and Nessus.
* Responsible for the planning and deployment of Nessus within the organization.
* Managing the enterprise infrastructure of the System Security team, such as configuration of File Integrity Monitoring systems, Data Loss Prevention (DLP) toolsets, enterprise Antivirus solutions, and endpoint encryption.
* Supported customers on various implementation of Windows Azure AD, MS office 365, Azure Single Sign On, On-premise, Single Sign On, Windows Azure.
* Provided expertise with incident response, security event monitoring, vulnerability management, asset security compliance and Data Loss Prevention utilizing McAfee Nitro (SIEM), McAfee ePO, McAfee DLP
* Managed Security and Compliance Dashboard inside Office 365 Tenant.
* Administration of Cyber Ark Privilege Accounts and Vaulting services.
* Build Safes and add servers into the safes as needed. Troubleshoot and fix all problems that arose in Cyber Ark due to ill-usage of the cyber ark from different users.
* Reviewed security logs (LogRythm SEIM) to ensure compliance with policies and procedures and identifies potential anomalies.
* Integrated IDS/IPS to ArcSight ESM and analysed the logs to filter out False positives and add False negatives into IDS/IPS rule set.
* Well versed in both remote and on-site user Splunk (SIEM) Support.
* Centralizing the storage and interpretation of logs using Splunk (SIEM) System.
* Worked in Security Incident and Event Monitoring SIEM platform - IBM Qradar, and Splunk.
* Responsible for applying standards for each platform (Windows, Unix, Middleware etc.) with application like Symantec Control Compliance Suite.
* Experience in SOC (Security Operation Center) to facilitate strong planning as per security protocol needed Analyse main Steps in IT Governance & Familiar with Cyber Security Process and ISO/NISI/ANSI Standard.
* Successfully completed Version upgrade projects of the existing SIEM platforms - LogRhythm and FortiSIEM.
* Created installation and configuration and test case scenarios documents for each specific device Connectors.
* Experience Configuring and managing AzureAD Connect, AzureAD Connect health, Microsoft Azure Active Directory.
* Configured and resolved Azure AD Connect sync issues.
* Having Experience of Creating and Managing the users and groups in Azure AD.
* Successfully established and tested Azure AD Tenant for production.
* Cyber Ark Vault Maintenances. Building CyberArk safes and adding different applications/portfolios in the safes.
* Active Directory group/user authentication and maintenances.
* Conduct risk assessments regularly; ensure measures raised in assessments were implemented in accordance with risk profile, and root-causes of risks were fully addressed following NIST 800-30 and NIST 800-37.
* Authentication and Authorization of Privilege users working with Cyber Ark and Access Management.
* General managing of Cyber-Ark Security that offers any enterprise a wide range of services and support options to making digital vault solution a success; these services include implementation, consulting, training, maintenance, online support and vault scripting, SIEM, and Digital Certification supporting.
* Experience with Symantec DLP and RSA DLP architecture and implementation for enterprise level. Designed Symantec DLP architecture, implemented Symantec DLP. Worked with Symantec DLP upgrades and patches. Implemented Symantec DLP Policy and Content Blade creation and tuning. Provided input into customer's operational and processes and procedures.
* Performed Serialization Validation - Antares System (Print & Check System - serialize and aggregate products) validation and testing of customer communication (Serial Number Management) with PCI.
* Provide onsite Symantec ™ DLP technical service and support to a Large Enterprise customer base.
* Conducted threat hunting analysis in ArcSight SIEM during each shift per shift report requirements.
* Utilized ArcSight to investigate incoming cases and create detail report of events during shift.
* Responsible for monitoring and detecting security incidents in Arcsight (SIEM).
* Develops rules, lists, and active channels in ArcSight ESM.
* Experience in SOC team delivery using security analysis, investigations, reporting, Mitigation, and tuning efforts.
* Configured Nessus Scanner with latest security centre version.

**Southwest Airlines Texas, United States**

**CYBER SECURITY ENGINEER March- 2020 To July 2023**

**Confidential, Boston, MA**

**Responsibilities:**

* Utilize Nessus/Tenable, Nmap, OWSAP and Web Inspect to scan all ports, access points, devices, software and Servers.
* Identifies security risks, threats and vulnerabilities of networks, systems, applications and new technology initiatives. Provides technical support in the development, testing and operation of firewalls, intrusion detection systems, and enterprise anti-virus and software deployment tools.
* Install, Troubleshoot, Monitor ASP.NET Web Applications.
* Utilize PowerShell, SCCM for scripting, patching, Application Testing and Imaging Windows OS, 7 & 10 machines.
* Monitored, Configured, Scan/Patch Network TCP/IP, DNS, Telnet and DHCP.
* Managed/Secured and Scanned devices, software, Web applications following NIST protocol & FIPS 140-2.
* Auditing and documenting systems using DISA auditing tools, Assured Compliance Assessment Solution (ACAS), DISA STIG, and SCAP tools.
* Responsible for monitoring and, providing analysis in a 24x7x365SecurityOperation Center (SOC) using Splunk SIEM, IDS/IPS tools.
* Lead in implementing security solutions towards SIEM tool using Splunk, and work on setting up the dashboard. Operate closely with data security teams.
* Used Splunk Deployment Server to manage Splunk instances and analyzedsecurity-based events, risks & reporting.
* Provide support of Splunk integration and deployment, configuration and maintenance.
* Integration of data feeds (logs) into Splunk.
* Managing various industries standard IPS, PIA, CASB, Firewalls, Gateways, VBlock, Rapid7 Virus and Endpoint Managers.
* Audit and validate configurations of network devices based on DISA STIGs.
* Utilize RSA Archer platform 6.1.

**State Street--Boston, Massachusetts**

**CYBER SECURITY ANALYST NOV-2018 To Feb-2020**

**Responsibilities**:

* Responsible for detection and response to security events and incidents within global fortune 500 client networks; utilizing ArcSight, Splunk, Tipping Point, VirusTotal, IPVOID, FireEye, Wireshark, etc. to gather, analyze, and present forensic evidence of cyber malware and intrusions.
* Review System and firewall logs based on individual preset client policies, rules, and standards; also review all host activity for specified timeframe.
* Work directly with ESM engineers and Account Information Security Officers to adjust alert criteria.
* Coordinated escalations to Forensic Analyst Team with recommendations for remediation
* Acted as liaison and interacted with leadership, account management teams, and engineers to further define the risk and remediation plan.
* Evaluated and fulfilled requests from the Account Information Security Risk & Compliance Officers for each client and aligned with the appropriate runbook procedures to attain Client Service Level Objectives and Agreements.
* Adjusted network alerts temporarily to suppress excessive alerts prior to engineers making permanent threshold changes.
* Facilitated and operated direct telephone communication in order to perform the immediate required escalation requests or engagements of required teams to support clients.
* Researched McAfee Threat Center, Symantec, and other vulnerability and threat libraries to identify and formulate remediation plans.
* Processed approved dataset access request and user id request for internal EDS and client platforms using ACF2, RACF, UNIX, and Windows.
* Participated in off-site quarterly Disaster Recovery Drills, providing access to the model office environment and troubleshooting dataset access issues, account creations, and password resets.
* Managed onboarding of external clients (health care, banking, telecom, etc.).
* Participated in annual audits of critical data to ensure we were PHI, PII, PCI, and SOX compliant.

**Reliant Hyderabad INDIA**

**Firewall Security Engineer Aug 2012 to Oct 2016**

**Responsibilities:**

* Hands on experience in configuration of VPN technologies (i.e. PPTP, L2TP, IPSEC, DMVPN).
* Worked on Cisco 7200, 3825, 890, Cisco Catalyst 6509E, 6513, 3750, Cisco Nexus 5K, Cisco 2800 Series Router.
* Worked on design and implementation of Cisco Meraki MX64, MX400, MX320 for specifically DMVPN with split tunnelling.
* Responsible for Palo Alto configuration and troubleshooting of User-ID, APP-ID, Content-ID through Panorama.
* Managed Fortigate 50,500 and 1000 series through Fortimanager.
* Worked on design and implementation of Cisco Cloud Web Security with Cisco 1800,1900,2800 series routers with split tunnelling.
* Worked on configuration of Bluecoat Threat Pulse Cloud web proxy in all field sites.
* Implemented DMVPN connecting to Head Office and the branch offices. Configured remote access VPN solutions for remote user using Juniper SSL VPN.
* Configured NAT, Security Policies, and SNMP in SRX for CCTV sites.
* Working experience in EIGRP, BGP, OSPF.
* Advanced knowledge, design, installation, configuration, maintenance and administration of CheckPoint Firewall R75 up to R77.20 version, SecurePlatform Installation, VPN.
* Responsible to manage Checkpoint cluster and troubleshooting experience with Smartview tracker, Smartview monitor, kdebug and zdebug.
* Experience in Aruba Wireless controller, i.e. Provisioning AP, Troubleshooting Wireless issue with users, Wireless profiles, etc.
* Conducted interviews with Process Owners, Administrators and Functional Heads to document how Information Security processes are performed.
* Provided information assurance support to TISOs and I TAOs to form, evaluate and maintain all security agreements according to required standards.
* Provided policy clarification, guidance and procedure interpretation to managers, data owners, project leads, application development teams, system operators and users.
* Assisted in the implementation of controls to ensure the appropriate level of protection and adherence to the goals of the overall information security strategy.
* Assisted in the development of access-controls and SOD.
* Assisted in the testing of Sarbanes-Oxley (SOX), Service Organization Control (SOC) SSAE 16 Review.
* Participated in the development and maintenance of global information security policy.
* Researched and reported on information security events and incidents.
* Helped maintain and support the organization's security requirements/infrastructure and other components of the Information Security Program.
* Reviewed security waivers for security technology or practices that deviate from established architecture and standards.
* Reviewed and documented practices and procedures on technical processes for a development project of a target operating model.
* Flowcharting as is/to be procedures for security domains for target operating model.
* Worked on Netscout packet sniffing tool for troubleshooting.
* Worked on JUNOS Space to integrate all CCTV site for monitoring and Configuration purposes.
* Upgraded about 900 Juniper devices using JUNOS Space to recommended code.
* Extensive knowledge in troubleshooting Juniper SRX210he & EX2200, EX4200 and EX4550 Switches.
* Working knowledge on Network Management tool SOLARWINDS to support all field and CCTV sites.
* Responsible for configuration and maintenance of Riverbed Steelhead appliances, Riverbed Cascade Profiler, Cascade Gateway and Cascade Sensor.
* Experience of Network Physics to get reports for troubleshooting purposes.
* Hands on experience in Splunk Enterprise for Alert throttling and troubleshooting of incident.
* Worked on Juniper SSL VPN appliance for troubleshooting issues for remote users.
* Have experience with Nessus scan which gives Vulnerability scan of network and provided detailed report and its mitigation.
* Cisco AMP for endpoint installation, managing policies, exclusions, Vulnerability report, threat detection and mitigation.
* Managing AV defender solution from RMM which is Solarwind’s product to monitor all server’s, Workstation’s or Network device’s health.
* Installation and configuration of Cisco Umbrella, which is Web filtering solution from Cisco. This includes installation of VAs and registering all Domain controller to cloud to gather all security events and apply policies accordingly.
* Coordinate and perform the implementation of Cisco’s Integrated Security Engine (ISE) across the Sutter Health System.
* Configuration, implementation, and integration of Cisco ISE for Guests, and staff Confidential over 300 hospitals.
* SME to provide guidance to the organization and team in selecting strategic options, and draft professional reports and present technical findings to a business audience.
* SME to provide security technology Confidential an architectural level, as well as Project Management.
* Responsible for performing Wireless 802.11 Site Surveys with AirMagnet survey software and installations Confidential.
* Responsible for documenting and engineering 802.11 Wireless and Wired High Speed Internet access infrastructure in assigned Confidential properties.
* Responsible for installing and configuring 802.11 Cisco Access points, Switches, Routers and Billing gateways.
* Management of crew (Wiring contractors, Technicians).
* Daily communication of project status with Hotel Management and Confidential Management.
* Management of Handoff Meetings to Handoff sites to Confidential NOC.