**Name: Premaja P Sr. Cyber Security Engineer**

**Email ID:** [**premap0699@gmail.com**](mailto:premap0699@gmail.com)

**Cell: +1 727-777-4945**

**LinkedIn:** [**http://linkedin.com/in/prema-cyber**](http://linkedin.com/in/prema-cyber)

**Professional Summary:**

* Professional with 8+ years of extensive experience in the areas of **Risk Analysis**, **SIEM, Endpoint Security, DLP**, Network Security, Email Security, Web Gateway, **Vulnerability Assessment, Pen testing**, Windows Server, Domain technology, and Antivirus servers.
* Expert in Vulnerability Assessment using **Qualys, Nessus, and Nexpose** tools to evaluate attack vectors, identify system vulnerabilities and develop remediation plans and security procedures.
* Assisted in integrating regulatory compliance requirements (e.g., PCI, NIST) into the organizational security roadmap.
* Hands-on experience with Forcepoint and Knowledge of distributed Splunk installation with Forwarders, Clusters, and Search head clusters.
* Possess a well-balanced understanding of business relationships, business requirements, and technical solutions with the ability to work collaboratively with business analysts, software testers, developers,
* Hands-on experience in the development, implementation, and administration of information security policies, standards, and procedures, adhering to industry best practices for clients.
* Assisted in ensuring that the corporate IT environment is secure and complies with all external audit requirements and federal standards.
* Responsible to triaged EDR incidents forward from the SoC team .
* Experience in integrating operations of SIEM and EDR.
* Designed and facilitated new cloud security architecture at **Bluemix data centers** for the ECMoC product offering using Vyatta 5400/5600, Juniper vSRX, and **Fortinet/FortiGate series firewalls**.
* Efficient and Expert in EIGRP, and OSPF, with knowledge of MPLS, and BGP (including configuration and troubleshooting)
* Acunetix, Microsoft Project, **Tripwire/IP360**, Tenable, Project Libre, **Visio**, Pac2000, SharePoint, Peoplesoft & Nexus, Continuous monitoring, GIS Ware, Cloudera, Hadoop, Apache, Microsoft application, endpoint, Security APIs, shodan API + Nmap, and others.
* Perform Risk Assessment, Gap analysis & create a Risk Mitigation plan.
* Strong understanding of enterprise, network, system/endpoint, and application-level security issues and risks. Oversee Vulnerability assessment/penetration testing of scoped systems and applications to identify system vulnerabilities.
* Experience in Azure Cloud Services (PaaS & IaaS), Storage, Web Apps, Active Directory, Application Insights, Logic Apps, Data Factory, Service Bus, Traffic Manager, Azure Monitoring, OMS, Key Vault, Visual Studio Online (VSO), Cognitive Services (LUIS) and SQL Azure.
* Excellent knowledge of **FISMA, HIPAA and NIST, PIA** Compliance usage, rules, and regulations.
* Use IBM QRadar Security Manager to identify threats and assigned categories.
* Processed daily security operations and log analysis. Processed daily security operations and log analysis.

**Technical Skills:**

|  |  |
| --- | --- |
| * **Networking** | * Packet Analysis (TCPDUMP, Wireshark), IDS (Bro, Snort), Splunk, Firewall, IDS/IPS, Access Control. |
| * **Systems Administration** | * Active Directory, DNS, FTP, SSH, DHCP, SMB, HTTP, Virtualization (ESX). |
| * **Vulnerability Assessment** | * Nmap, Nessus, Ettercap, Metasploit, Honeypots (HoneyD, INetSim), Burp Suite |
| * **Endpoint Security** | * McAfee Suits (VSE, HIPS & HDLP), McAfee MOVE AV, Symantec McAfee Email Security Gateways GUI & CLI, McAfee Network Data Loss Prevention, McAfee NITRO SIEM Security Information, and Event Management. |
| * **Platforms/Applications** | * Continuous Monitoring Vulnerability Management, Web Application Scanning, Threat Protect, Policy Compliance, Cloud Agents, Asset Management, Governance, Risk Management and Compliance, SolarWinds, Nexpose, Rapid7 Event Management RSA Archer, Blue Coat Proxy, IBM QRadar, NTT Security, LogRhythm, Pen Test Tools Metasploit, Burp Suite, NMAP, Wireshark and Kali. |
| * **Security Software** | * Nessus, Ethereal, NMap, Metasploit, Snort, RSA Authentication, PIA. |
| * **Programming Languages** | * C, C++, Java, Python, JavaScript, Linux, PowerShell. |
| * **Networking** | * LAN, WAN, Wi-Fi, DNS, WINS, DHCP, TCP/IP, ISCSI, Firewalls/IPS/IDS |
| * **Protocols** | * TCP/IP, L2TP, PPTP, IPSEC, IKE, SSL, SSH, UDP, DHCP, DNS, NetBIOS, SNMP, TLS, etc. |
| * **Domain Knowledge** | * Risk Management, BCP/DRP, ISO 27001, COBIT, Vulnerability * [SWOT analysis, Cryptography, Incident Response, Penetration Test, Risk Assessment, SCADA Security, SCADA Audits, SIEM, NIST, FIPS]. |

**Work Experience:**

**ARAMCO, Houston, TX April 2019 to date**

**Sr. Cyber Security Engineer/Analyst**

Responsibilities:

* Establish a strong GRC (Governance, Risk, and Compliance) practice to ensure adherence to best practices, regulatory requirements, and ISO 27001.
* Adept with Radar, Symantec PCAP, Symantec CloudSOC, PAN Firewall, PAN WildFire, PAN TRAPS, PAN Redlock, FireEye, ThreatQ, Microsoft SCEP, Microsoft O365 Security and Compliance Portal, ProofPoint,
* Working with McAfee ePO for managing clients' workstations for providing endpoint security.
* Facilitate implementations of information security policies, account security policies, and standards for logical and physical security.
* Worked on SIEM, as well as solar winds, and Symantec end-to-end point security for malware detection and threat analysis.
* Executed cybersecurity assessments on internally and externally hosted solutions, including internal, SaaS and cloud hosted solutions.
* Experience with national, international, and/or sectoral cloud security assurance/compliance regimes and frameworks such as Federal Risk and Authorization Management Program (FedRAMP), Federal
* Responsible for performing application penetration testing on the web, thick client, and other types of applications to identify significant vulnerabilities that threaten the confidentiality, integrity, and availability of customer systems.
* Implementation and configuration of the network infrastructure in the Business environment.
* Experience with managing SOC engagements and Incident Handling efforts for EDR and to optimize EDR operations at Zoox.
* Installation and maintenance of McAfee Drive Encryption used to encrypt all workstation hard drives in the environment to secure the data stored on them.
* Installation, maintenance, and monitoring of McAfee Data Loss Prevention Endpoint, one piece of the Removable Media Encryption suite
* Experienced with Linux/UNIX operating systems (Red Hat Enterprise Linux, Solaris, HP UX, IBM AIX).
* Installation "maintenance and monitoring of McAfee File and Removable Media Protection, the second piece of the Removable Media Encryption suite
* Implemented and configured CASB solution including Netskope to secure the enterprise with a cloud.
* Implementing OS patches on Red Hat Enterprise Linux (RHEL v6, 7 & 8) Advance servers.
* Tested and certified new software such as Tanium Protect (an access control software) and PEGA trouble ticketing software.
* Audit Support: Facilitated the PCI DSS external audit for the client and took charge of end-to-end coordination and support during the onsite assessment.
* Oversee the design and development of security solutions and manage cross-platform integration of a range of on-premises and public cloud security designs and configurations, Amazon CloudFront, and Amazon Route 53.
* Troubleshooting day-to-day issues in IT infrastructure in Business Environment tools like Splunk, ServiceNow, ArcSight, Solutionary, PIA, LogRhythm, SCCM, Altiris, LanDesk, BigFix, McAfee/Symantec.
* Automated DLP Incident metrics using Splunk. Developed monthly, and weekly metrics and dashboards using Splunk.
* Provided leadership in architecting and implementing security solutions towards Qualys and SIEM tools like Splunk, ArcSight, Solutionary, LogRhythm, SCCM, Altiris, LanDesk, BigFix, and McAfee/Symantec.
* Configured Advance CyberArk integration with AD through LDAP, 2-factor authentication & email integrations.
* Utilizing Tanium Endpoint Security to create reports to resolve various information security issues.
* Experience with Risk assessment, Cobit I help Malware Analysis.
* Working as a dedicated resource for a Scrum Project to provide timely firewall support and configuration for ongoing high-priority Scrum Projects.
* Vulnerability Assessment and Management (Nessus & Qualys), Security risk analysis; reporting using SPLUNK.
* Leading a SOC team for cyber incidence and compliance towards PCI DSS, NIST framework.
* Installed, configured, and administered Splunk Enterprise Server and Splunk Forwarder on Redhat Linux and Windows servers.
* Configuration and Maintenance of MPLS between satellite locations and Datacenter. Rule Management for MPLS routers.
* Tracks all the incidents that happened in all the stores and are used for recovery and settlements using RSA Archer.

**Bank of America, Agoura Hills, CA Oct 2017 – Mar 2019**

**Sr. Cyber Security Engineer**

Responsibilities:

* Experienced with DLP, Bluecoat Websense, Proofpoint, Trend Micro, and IBM QRadar Enterprise SIEM security tools to monitor network environment.
* Worked on tools like Information security and Group Policy, Symantec Data Loss Prevention, Symantec End- Point Protection Manager, Symantec Endpoint Encryption, Windows Server Update Service, Bluecoat Proxy, Syslogs, and GFI.
* Experienced primary Voltage secure data encryption engineer heading up International Project encryption servers worldwide.
* Oversee Vulnerability assessment/penetration testing of scoped systems and applications to identify system vulnerabilities.
* Application support for tripwire, research and understand all aspects of tripwire and troubleshooting as well as find other ways to automate practices. Would help other teams in cyber security as well for any projects dealing with Nessus tools vulnerability management, risk, and compliance in NERC standards.
* Lead a team of cloud security engineers in various areas of expertise to execute complex solutions to meet delivery timelines.
* Recognize, adopt, utilize, and teach best practices in cloud security engineering.
* Internal Network Vulnerability Assessments to enhance the Information Security culture of an organization through identifying, analyzing, and reporting the gaps which may be used to threaten the CIA of information.
* Converting existing AWS infrastructure to a serverless deployed via Terraform or AWS Cloud formation.
* Frameworks used ISO 27001 ISMS, PCI DSS, SSAE16, OWASP, SANS, and Forcepoint.
* Monitored and researched Cyber Threats with a direct & indirect impact on the organization internally.
* Experience on Nessus VA and Burp Suite PT with implementing RSA SecurID.
* Multi-model Consulting on different frameworks & standards like ITIL, COBIT, SDI, CMMI & ISO 2000, and ISO 9001.
* Security Consultant specializing in Data Loss Prevention and large infrastructure encryption. Security Engineer for Proof Point Email Gateway Security.
* Develop reference architectures and proof of concept implementations of cloud security environments.
* Responsible for architecting, implementing, and supporting cloud-based infrastructure and its solutions.
* Manage all repeated threats to all systems and perform vulnerability tests.
* Responsible for the design, development, and implementation of new and innovative solutions to protect lucid sensitive data and strengthen data protection capabilities.
* Support IT teams based on the latest risks and possible remediation Vulnerability remediation of VBlock Infrastructure. Involved in the integration of Splunk with ServiceNow, Active Directory, and LDAP authentication.
* Experienced with Handling Cloud environments (AWS and Cloud)
* Experience with managing SOC engagements and Incident Handling efforts for EDR and to optimize EDR operations at Zoox.
* Simplified knowledge sharing by creating and maintaining detailed and comprehensive documentation and necessary diagrams.
* Managing the enterprise infrastructure of the System Security team, such as the configuration of File Integrity Monitoring systems, Data Loss Prevention (DLP) toolsets, enterprise Antivirus solutions, and endpoint encryption.
* Assisted internal users of Splunk in designing & maintaining production-quality dashboards, assisted the team to understand the use case of business and provided technical services to projects, user requests & data queries.

**GEICO, Chevy Chase, MD Aug 2016 – Sep 2017**

**Cyber Security Engineer**

Responsibilities:

* Experience with many of the following technologies/roles: Privileged Account Management, Two-Factor Authentication, Web filtering, Web Application Firewalls, Virtualized computing environments, Encryption-at-rest and encryption-in-transit, and Vulnerability Management.
* Installation and configuration of networks and network devices such as web application firewalls, network firewalls, switches, checkpoint firewalls, squid firewalls, blue coat proxy, and routers.
* Network Security configuration, audit, and management of Windows servers. Installation, configuration, audit, and management of security tools.
* Security configuration, audit, and management of applications and databases. Leading security incident investigations, including basic forensic analysis and reporting. Deploying, automating, maintaining, and managing AWS cloud-based production system, to ensure the availability, performance, scalability, and security of production systems.
* Maintenance and monitoring of the network and host intrusion detection and prevention technologies. Implementing security controls. Experience with using a broad range of AWS technologies (e.g., EC2, RDS, ELB, EBD, S3, VPC, Glacier, IAM, CloudWatch, KMS) to develop and maintain an Amazon AWS-based cloud solution, with an emphasis on best practice cloud security.
* Implemented physical and procedural safeguards for information resources within the facility. Communicate effectively with senior management, peers, staff, and customers both inside and outside the corporation.
* Administered access to information resources and makes provisions for timely detection, reporting, and analysis of actual and attempted unauthorized access to information resources.
* Proposed and assisted with the acquisition of security hardware/software. Develops and maintains access control rules. Experience with VOIP systems.
* Maintains user lists, passwords, encryption keys, and other authentication and security-related information and databases.
* Responsible to triaged EDR incidents forward from the SoC team and integrating operations of SIEM and EDR.
* Experience using DAST tools to detect potential vulnerabilities such as HP Webinspect, SolarWinds, Zap, Burp, Tenable, Splunk, ServiceNow, Alertlogic, Symantec Endpoint Protection, Zscaler, McAfee security, Portswigger, Fiddler, Wireshark, Nmap, JIRA, Sonatype, Coverity. Experience in Palo Alto Networks and Firewall. Experience in maintaining local and remote networks.
* Lead the design, implementation, and migration of enterprise infrastructure and application services to software-defined networks. Experience in Palo alto networks and a firewall. Configure and manage AWS/Azure cloud infrastructure.
* Develops and leads procedures for testing disaster recovery plans. Provides help-desk-style assistance.
* Administered MS Windows Server, Red Hat Linux Server, and Network/Security Administration.

**Client: Indus Net Technologies Pvt. Ltd, Hyderabad Oct 2014 –Dec 2015**

**Jr. Security Analyst**

Responsibilities:

* Responsible for detection and response to security events and incidents within global fortune 500 client networks; utilizing ArcSight, ServiceNow, Splunk, Tipping Point, Virus Total, IPVOID, FireEye, Jira, 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 the 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 before engineers made permanent threshold changes.
* Facilitated and operated direct telephone communication 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.

**Client: Virtusa, Chennai, India May 2014 –Sep 2014**

**Junior Network Engineer (Intern)**

Responsibilities:

* Involved in complete local area network (**LAN**) and wide area network (**WAN**) development including designing, installation, configuration, and maintenance.
* Designed the network infrastructure for 25 remote sites and the central office considering the user requirements at each location.
* Installed Cisco Catalyst 2960 Switches and **Cisco ASA 5505 Firewalls** at remote locations.
* Performed the switching technology administration by configuring **Cisco switches** (Cisco catalyst 2960, CISCO SF300-24P, and Cisco SG200-26P switches).
* Maintained stable STP topology using Port fast, BPDU guard, root guard, and UDLD.
* Configured Virtual LANs (VLANs), VLAN Trunking, **Inter VLAN routing**, Port security, and LAN security on Cisco Switches.
* Performed troubleshooting for VLAN misconfiguration and port security issues.
* Deployed and maintained the network security infrastructure by Configuring Cisco ASA 5510 security appliance.
* Configured Cisco **2960 routers** as **DHCP** **servers** to distribute dynamic IP addresses.
* Established Remote-Access **Virtual Private Network (VPN)** between 25 remote site offices and the central office.
* Created IKE Phase 1 tunnel and **IPsec tunnel** between remote offices and central offices for the e Confidential data traffic.
* Applied Access Control List (ACL) as a part of **VPN** cryptography policy on Cisco ASA 5505 and 5510 Firewalls.
* Installed secure and scalable Cisco WAP150 Wireless access points and documented all network set-ups.
* Installed Yealink and Cisco 7941 **VoIP phones** and implemented the telephony infrastructure on Elastic servers.
* Documented the network designs and data flow representations using the tool **Microsoft Visio**.
* Maintained LAN user documentation including hardware and software applications and support logs.
* Configured dynamic routing protocol OSPF on Cisco Core Router and redistributed routes from **EIGRP to OSPF** and **OSPF to EIGRP**
* Provided desktop support to corporate users and technical staff including configuration and installation of Software and Hardware and providing internet and intranet support.