**Saichand Pothana**

**Mail**: [saichand.pothana@gmail.com](mailto:saichand.pothana@gmail.com) | **Mobile:** +1(916) 620-5210

**LinkedIn**: <https://www.linkedin.com/in/saichandpothana/>

**Cyber Security, Network Security, Cloud Security, Information Security, GRC**

**SUMMARY:**

* **Information security expert with 14 years of proven track record in delivering enterprise grade security solutions** with major strengths in both infrastructure security and compliance framework.
* **Experienced in compliance audits, control testing, establishing standards, and setting up information security controls** by leveraging on various tools and technologies ensuring data security and privacy.
* **Expertise in ensuring the protection of organization’s networks, computer systems, and data against security breaches.** Proven abilities in identifying security gaps and providing optimum solutions, developing combat strategies for cyber threats, develop Resiliency exercises test scenarios, disaster recovery planning, data backup systems, create baseline configurations as per CIS benchmarks, Implement NIST 800-53, NIST CSF frame works, performing risk & vulnerability assessments, penetration testing for on-prem & Cloud (AWS, Azure, GCP) servers, and implementing the threat management frameworks.
* **Experience on multiple IRM and GRC tools** like ServiceNow GRC, RSA Archer, Audit board and Onetrust.
* **Experience on various security assessments tools and tech** like Nessus, Acunetix, Rapid7, Burp Suite, OWASP Zap, Qualys vulnerability and PCI ASV scanner, Kali Linux tools, Parrot OS tools, NMAP, Wireshark, Metasploit and MITRE ATT&CK frameworks.
* **Cloud and Network Security Architect** with strong experience in designing enterprise level Zero trust network access(ZTNA), three tire, collapsed core network architectures, ODC/Clean room infrastructure setup with security controls at various layers and implement robust distributed Network Monitoring systems. Have good experience on Linux, Docker, Kubernetes, and cloud environments (Azure, AWS & GCP), Change, Incident, Problem management process as per ITIL standards.
* **Demonstrated competencies as a Cyber Security Architect** in designing and implementing various security products in On-prem and Cloud infrastructure like Zscaler Proxy and Zero trust solutions, implement and manage ELK, Splunk SIEM, SOAR, Endpoint Security, Data Leak Prevention products, Malware analysis tools, threat intel, sandboxing, Case and threat management solutions.
* **Deft in analysing security events** from host-based/perimeter IDS, firewalls, switches, Servers, application, and database logs with various SIEM tools like ELK stack, Splunk SIEM, Azure Sentinel along with SOAR solutions like Phantom and Demisto.
* **Strong understanding of OWASP, ISO:27001, ISO:31000, PCI DSS, NIST 800-53, NIST CSF, ITGC and other compliance security frameworks**. Established processes & procedures and fix gaps to get aligned to ISO, PCI DSS, DISA STIG and NIST standards.
* **Worked on networking technologies like Firewalls, WAF, IPS/IDS, Switches, Routers, VPN Gateways and Server administration (Windows/Linux/Mac platforms).** Experience in design and implementing multiple Open-source and commercial Infrastructure and Security solutions of Cisco, PaloAlto, Fortinet and Juniper firewall/switches, implemented MDM (Mobile Device Management) solutions.
* **People-centric leader with proven abilities in leading & training teams on several SOC (Security Operations Centre) and Cyber Security tools,** implementing security strategies, ensuring adherence to the regulatory requirements and continually focusing on improving organization’s security posture.
* **Leadership in Audit and Compliance,** lead cross-functional audit initiatives and technology innovations that improved compliance by 20%, reduced financial risks, and enhanced operational efficiency. Orchestrated end-to-end adherence to multiple regulatory frameworks including ISO27001, SOC, GDPR, PCI DSS, HIPAA and NIST, while pioneering data analytics in audit reporting for predictive insights.
* **Experience in Penetration Testing** on Web applications covering OWASP Top10 vulnerabilities, On-Prem and cloud infrastructures and suggest mitigation/remediation techniques/plans for the identified gaps/exploits/vulnerabilities.

**CORE COMPETENCIES:**

|  |  |  |
| --- | --- | --- |
| * Information Security Strategies * Cloud Computing * Security Team Management * Threat Management * Network Security Architecture * Splunk and ELK SIEM, SOAR * Firewall, Endpoint Security, IDS, IPS, EDR, NDR, XDR | * Compensation controls * Process Automation * Project Planning * Strategic Planning * Technical Consulting * Client Relationship Building * Internal Audit | * External Compliance Audit’s * Vulnerability Assessment and Penetration Testing * SOC2, HIPAA, PCI DSS, ISO 27001, NIST 800-53, NIST CSF, CIS, DISA STIG, ITGC * Identity and Access Management * Computer Forensics * Malware Analysis |

**EXPERIENCE:**

**Client: - PayPal, CA Jan 2022– Present**

**Role: - GRC Lead – IT Security**

* Responsible for drafting and testing controls of IT Security risk processes to ensure design and operational effectiveness of the controls.
* Responsible for assessing risk against IT Security Controls for PayPal and their subsidiaries.
* Responsible for managing, testing, and maintaining Control Lifecycle management for TPX (Technological Platform Experience) domains across PayPal and their subsidiaries under First Line of Defence in accordance with PCI DSS standards.
* Understanding and applying the enterprise policies, standards, and framework for governance, risk & compliance (GRC).
* Partnering with different stakeholders and external auditors to maintain up to date documentation for scoping, testing and remediation of IT controls. Validating the key controls to provide an early warning to management for timely correction and remediation action.
* Assessing audit findings/ gaps including control weaknesses in coordination with different stakeholders and assisting the management with the development of strategic action plans.
* Review Zscaler client enforcing configuration, review forwarding policies, access user access re-consolation and reporting.
* Review DLP configuration, validate polices and updating frequency as per the PayPal standards.
* Review Palo Alto network firewalls and WAF access policies, assess firewall, IPS, Endpoint security, DLP and FIM configurations.
* Providing control consulting services to control owners and redesigning the effectiveness to improve/automate the control environment.

**Accomplishments:**

* Created comprehensive and in-depth test procedures for all PCI DSS controls, which was subsequently added to PayPal’s testing bible and standards. This process helped organizations validate their hidden risks/gaps and take remedial actions before they breakout and lead to potential risks.
* Enhanced efficiencies and minimized dependence on multiple teams by developing automation dashboard in SIEM (SPLUNK) to fetch the real time data whenever required. This saved a lot of time and effort in reaching multiple domain owners for reports and was helpful in speeding up the control testing process for few security controls.

**Client: - Photon Interactive, India Sep 2014–Jan 2022**

**Role: - Senior Manager Information Security and SOC**

* Spearheaded the development and implementation of a comprehensive GRC framework to align with the company’s business objectives by defining, implementing, and managing a comprehensive IT security program.
* Performed periodic Internal audits across various domains, review security controls and counter measures to ensure right practices are established and adhered to.
* Conducted enterprise-wide risk assessments and audits to identify vulnerabilities and compliance gaps, developed actionable mitigation plans.
* Facilitated collaboration and follow-ups with internal and external contacts on remediation of security incidents. Responsible for managing relationships with stakeholders and communicating with senior leaders through regular reporting.
* Authored and updated governance policies, procedures, and guidelines in accordance with industry best practices and regulations.
* Designed and delivered GRC training programs to educate staff and stakeholders on compliance requirements and risk management best practices.
* Scoping, design, implementation, and operation of PCI DSS, ISO 27001, SOC2 and related Information Security framework/ standards.
* Assessed in-depth device configurations like Firewalls policies review, perform internal vulnerability assessment on Infrastructure devices and Servers. Assess Wireless Infrastructure on regular interval scans to identify any security breaches.
* Experience in ITGC and cybersecurity controls, with a special emphasis on securing digital work environments this includes Endpoint Security, Collaboration & Communication Systems Security, Data Security & Rights Management, and Identity & Access Management. Strengthened operational controls, developed & integrated all SOC, threat intelligence and other related processes.
* Mitigated the cyber security risks and strengthen the attack detection and response processes. Worked on Cyber Security attacks, tools/techniques and gained experience in Advanced Threat management.
* Implemented Symantec SEPM, Sophos, and CrowdStrike Endpoint protection solutions.
* Implemented McAfee DLP and CrowdStrike Falcon XDR configure policies as per the organization-defined policy and configure DLP’s to forward the events to SIEM solution and monitor the attacks/ potential threats.
* Implemented several open source solutions for the requirements like Eramba for GRC, ELK stack along with Wazuh and rsyslog for SIEM.
* Implemented Splunk Enterprise SIEM with Splunk SOAR (Phantom) and hand knowledge on Demisto.
* Deployed Layer 7 WAF’s like Imperva, AWS WAF and Mod Security WAF solutions to safeguard organization web applications exposed to internet.
* Implemented, managed and monitored Cloud Proxy solutions like Zscaler Internet Access, Zscaler Private Access and connectors.
* Deploy ZPA Connectors in required networks/subnets as required; create user/group-based access policies in ZPA for definite service/destinations.
* Integrate Azure AD with SCIM, create local accounts/groups to quickly remove, manage, or add users to ZSLogin. Integrated with ZIA with OKTA IAM for user access provisioning and MFA.
* Hosted PAC file creation, updating and as per the organization Secure browsing/ Internet access policy.
* Configure SSL inspection bypass for specific/internal websites, update PAC file to bypass Zscaler proxy as required to make traffic originated from the organization exit point instead of Zscaler DC.
* Configure and review NGFW access policies in ZAPP portal, Update ZAPP to latest versions through ZIA portal.
* Create and streamline ZIA and ZPA access policies. Update PAC file as per requirements to bypass Zscaler proxy.
* Implemented and managed Zscaler’s secure web gateway.
* Plan and deployed PaloAlto firewalls in On-prem and in AZURE infrastructures. Establish S2S tunnels from On-Prem to Azure.
* Implement Network Zoning; create access policies, web content filtering policies as per the CIS and organization-defined standards.
* Deployed Panoroma and integrated all Palo Alto firewalls for centralised management.
* Integrate Palo Alto firewalls with Active Directory, SCIM. Perform log review and t.shoot issues with packet captures.
* Proficient in creating managing workloads EC2 instances in AWS and VM’s in Azure, harden base operating systems images as per the NIST/CIS, organization defined standards.
* Deployed Imperva, AWS WAF and Mod Security WAF solutions to safeguard organization web applications exposed to internet.
* Perform penetration testing and vulnerability assessment on Web applications, on-premises infrastructures, cloud infrastructures, and provide remediation plans for the identified exploits/vulnerabilities.
* Setup and managed Centralized Log collectors, FIM’s (File Integrity Monitor) and OS patches. Implemented and managed Cisco MERAKI MDM solution organization wide.
* Architect secure connectivity and setup infrastructure includes Network, Wireless, servers, security controls for ODC, Clean room.
* Design secure network architect for lift and shift of workloads from on prem to Azure, AWS cloud infra.
* Develop automate scripts to perform specific tasks, fetch data from various sources for further analytics.
* Administrate OKTA, an Identity Access Manager for day-to-day activities and perform user access privileges review from compliance perspective. Have

**Accomplishments:**

* As a Network security architect, assessed and designed a fully resilient three-tire modular enterprise level network topology and revamped the entire organization-wide infrastructure. Aligned all branch offices to single standard design and connected them securely to head offices with Star, Hub and Spoke topologies.
* Connected and centralised administrate all branch offices network traffic by Leveraging NGFW feature in Zscaler. Replaced UTF firewalls in all branch offices with legacy routers, establish GRE tunnels to Zscaler, created filtering polices in ZAPP portal for branch office interesting ingress/egress traffic. This helps the organization to reduce the complexity of branch office network management and get insights in central dashboard.
* Implemented ZPA on ad-hoc for enabling WFH for all employees during covid pandemic, deployed ZPA Connectors in various ODC’s and client networks and create necessary access policies. This helps the organization to seamlessly transition from onsite to remote work model without any business impact.
* As a cyber-security architect, masterminded and successfully deployed the end-to-end Security Operations Centre environment with various cyber security tools covering Vulnerability, threat hunting, malware analysis, endpoint security, IDS/IPS, SIEM, SOAR and case management.
* Built the new Security Operations Centre team from scratch, trained team on several SOC and Cyber security tools to continuously monitor cyber threats to the organization round the clock, took the required action to form defence strategies, and applied them on the devices.

**Client: - Accenture Services, India Aug 2012–Sep 2014**

**Role: - L3 Network Security**

* Responsible for Design, Implement, configure and maintenance of new and existing network devices.
* Hands on experience in Incident management, Change management process.
* Monitoring and managing Cisco/Juniper routers, Fortinet/Cisco/Juniper/PaloAlto Firewalls and Cisco/Juniper/HP/ Avaya Switches.
* Create access policies in Cisco, Juniper and PaloAlto firewalls and the delivery needs.
* Device configuration hardening/Baseline configuration as per organization policy.
* Hardening Cisco, Juniper, PaloAlto network devices according to the IT security policy.
* Experience in setting end-to-end network infrastructure setup for a new facility.
* Hands on experience on RIVERBED WAN Accelerators and Blue Coat Packet Shapers.
* Hands on experience on Static and Dynamic Routing Protocols, Policy based routing and Access Control Lists.

**Accomplishments:**

* Designed and implemented a free open-source Linux-based log management system that served as an effective replacement for the paid version of Solar Winds. The solution was rolled-out by Accenture in all branch offices across the globe. Trained the staff on its implementation and management and awarded with "Innovative Excellence Award”.
* Saved several hours of team effort and streamlined the work by creating a shell script to automate of taking 4K devices configuration backup daily with user input function to add new devices into the existing devices list and added several new features.

**Client: - Cameo Corporate Services, India May 2010–Aug 2012**

**Role: - Senior Network Administrator**

* Designed and deployed a secure VPN solution for CAMEO that allowed the subcontract vendors to access the internal application servers in the CAMEO network and share data securely with each other. This helped CAMEO expand business opportunities, increase subcontract vendors, open new branch offices in Uganda, and increase revenue flow for the organization.
* Introduced enhancements in the network and server infrastructure by designing and deploying a collapsed core topology network infrastructure with redundancy to handle high network volume. Successfully designed and deployed NLB (Network Load balancer) to distribute the load across several application servers in the server farm.

**QUALIFICATIONS:**

* PG Diploma in Cyber Crime & Information Security | University of Madras | Apr 2010
* Bachelor of Engineering in Electronics and Communication | Anna University | Apr 2008

**CERTIFICATIONS:**

* CEH (Certified Ethical Hacker) v11, Certificate ID: ECC5973864102, Valid through Aug 14 2026
* CCNA Certified, Cisco ID: CSCO12609412, Valid through Apr 26 2017
* Salesforce Administrator, Credentials ID: 3743441, Issued on Oct 20 2023
* Undergoing CISSP Certification.