**Email:**

**Phone:**

**Senior Cybersecurity Engineer**

## **Professional Summary**

* Over 10 years of experience designing and implementing enterprise-grade cybersecurity frameworks to secure cloud, on-premises, and hybrid infrastructures.
* Architected multi-cloud security strategies, implementing zero-trust network segmentation, secure access policies, and identity controls.
* Automated threat detection and incident response workflows using SIEM platforms such as Splunk, QRadar, and Sentinel with custom Python scripts.
* Developed vulnerability management programs using Nessus, Qualys, and OpenVAS to reduce exposure to critical security risks.
* Built and maintained secure CI/CD pipelines with Jenkins, GitLab CI, and Azure DevOps, integrating SAST, DAST, and automated compliance checks.
* Integrated endpoint protection solutions with CrowdStrike, Carbon Black, and Microsoft Defender for proactive threat mitigation.
* Deployed identity and access management systems with MFA, SSO, and RBAC policies across hybrid environments.
* Implemented encryption for data at rest and in transit using TLS, SSL, AES, and PKI standards.
* Migrated legacy security infrastructure to modern cloud-native solutions while ensuring continuity and compliance.
* Optimized firewall, IDS/IPS, and network segmentation using Palo Alto, Cisco ASA, and Check Point to prevent unauthorized access.
* Conducted penetration testing and red-team exercises with Metasploit, Burp Suite, and Kali Linux to identify vulnerabilities and remediation strategies.
* Developed and enforced security policies, SOPs, and governance frameworks aligned with regulations.
* Led employee security awareness programs and phishing simulations to strengthen cybersecurity culture.
* Implemented monitoring and observability solutions with AWS CloudTrail, Azure Monitor, and ELK stack for proactive intelligence.
* Collaborated with development and DevOps teams to integrate secure coding practices throughout the software development lifecycle.

## **Technical Skills**

| **Category** | **Key Technologies & Expertise** |
| --- | --- |
| **Cloud Platforms & Security** | AWS, Azure, GCP, AWS GuardDuty, Azure Security Center, GCP Security Command Center, CloudTrail, Azure Monitor, Hybrid Cloud Security. |
| **Security Engineering & Architecture** | Zero-Trust, Multi-Cloud Strategy, Network Segmentation, DevSecOps, Secure CI/CD, Terraform, IAM, SSO, MFA, RBAC. |
| **Threat & Vulnerability Management** | Penetration Testing, Red-Team Exercises, Nessus (Tenable), Qualys, OpenVAS, Metasploit, Burp Suite, Kali Linux, Threat Modeling. |
| **SIEM & Incident Response (IR)** | Splunk, QRadar, Azure Sentinel, ELK Stack, SOC Workflows, Automated IR Runbooks, Python/PowerShell Scripting. |
| **Application & Pipeline Security** | CI/CD (Jenkins, GitLab CI, Azure DevOps), SAST, DAST, Secure Coding Practices, API Security (OAuth2, JWT). |
| **Endpoint & Data Protection** | CrowdStrike, Carbon Black, Microsoft Defender, DLP, Data Classification, Encryption (AES-256, TLS, SSL, PKI). |
| **Network Security** | Firewalls (Palo Alto, Cisco ASA, Check Point), IDS/IPS (Cisco Firepower, Snort), VPN. |
| **Compliance & Governance** | HIPAA, HITECH, GDPR, ISO 27001, SOC 2, Security Policies, SOPs, Audit Readiness. |
| **Scripting & Automation** | Python, PowerShell, Ansible Playbooks, Custom Scripting. |

## **Professional Experience**

### **Client:**

Senior Cybersecurity Engineer**| Oct 2018 – Present**

**Responsibilities:**

* Designed and deployed multi-layered security architecture across hybrid cloud platforms, implementing zero-trust network segmentation and access controls.
* Automated SOC workflows leveraging Splunk, QRadar, and custom Python scripts to accelerate threat detection and incident response.
* Implemented vulnerability scanning and remediation programs using Qualys, Tenable, and Ansible playbooks across cloud and on-premises systems.
* Integrated cloud-native security tools such as AWS GuardDuty, Azure Security Center, and GCP Security Command Center to monitor and mitigate risks.
* Built secure CI/CD pipelines with Jenkins and GitLab, integrating static and dynamic code analysis tools for continuous security validation.
* Deployed endpoint protection using CrowdStrike and Microsoft Defender for proactive threat mitigation.
* Managed IAM services with Okta, Azure AD, and role-based policies, enforcing MFA and SSO across multiple applications.
* Developed encryption strategies for databases and storage using AES-256, TLS, and PKI to safeguard sensitive data.
* Conducted penetration testing and red-team simulations with Burp Suite, Kali Linux, and Metasploit to identify and remediate security gaps.
* Monitored cloud security events using ELK Stack, CloudTrail, and Azure Monitor for real-time intelligence.
* Implemented DLP and data classification policies to protect sensitive business information.
* Led incident response investigations, coordinating with technical teams to mitigate breaches and restore secure operations.
* Developed comprehensive security documentation, SOPs, and best practices manuals for technical teams and management.
* Collaborated with developers and DevOps to enforce security in application lifecycles and release pipelines.

**Environment:** AWS, Azure, GCP, Jenkins, GitLab, Splunk, QRadar, CrowdStrike, Microsoft Defender, Nessus, Qualys, Ansible, ELK Stack, Burp Suite, Metasploit, Python, Terraform, Azure AD, Okta, IAM, CI/CD, Agile, DevSecOps

### **Client:**

**Senior Security Analyst | Jan 2016 – Sep 2018**

**Responsibilities:**

* Implemented security frameworks for healthcare and enterprise applications to protect sensitive data and comply with regulatory requirements.
* Designed and automated vulnerability assessment workflows using Nessus and OpenVAS, integrating remediation pipelines for cloud and on-premises systems.
* Built secure cloud environments on Azure, configuring encryption, network security groups, and logging policies.
* Conducted threat modeling and risk assessments for applications, databases, and cloud environments.
* Integrated SIEM solutions using Azure Sentinel and Splunk for centralized monitoring and threat reporting.
* Developed endpoint security strategies using CrowdStrike and Carbon Black to prevent malware and ransomware incidents.
* Automated incident response runbooks using Python and PowerShell scripts to accelerate containment and recovery.
* Implemented IAM and SSO solutions to control access to critical applications and data.
* Conducted employee cybersecurity awareness training to improve organizational security posture.
* Performed penetration testing and ethical hacking exercises to validate security controls and remediation effectiveness.
* Collaborated with DevOps teams to integrate security into CI/CD pipelines using Azure DevOps and Jenkins.
* Monitored compliance with HIPAA, HITECH, and GDPR through policy enforcement and audit readiness.
* Designed secure APIs for internal and external integrations using OAuth2 and JWT tokens.
* Led cloud migration security strategy for legacy systems to modern platforms.

**Environment:** Azure, AWS, Jenkins, Azure DevOps, Splunk, Sentinel, Nessus, OpenVAS, CrowdStrike, Carbon Black, Python, PowerShell, CI/CD, DevSecOps, HIPAA, HITECH, API Security, Agile

### **Client:**

**Cybersecurity Consultant | Mar 2013 – Dec 2015**

**Responsibilities:**

* Designed enterprise security architecture for web and mobile applications with secure access and authentication protocols.
* Implemented IDS/IPS solutions using Cisco Firepower and Snort for real-time network monitoring.
* Developed automated vulnerability scanning processes using Nessus, OpenVAS, and custom scripts.
* Integrated cloud-native monitoring and alerting using AWS CloudTrail, CloudWatch, and ELK Stack.
* Conducted penetration testing using Burp Suite, Metasploit, and Kali Linux to identify vulnerabilities.
* Deployed endpoint protection solutions using Symantec and Microsoft Defender for proactive mitigation.
* Managed IAM policies and SSO integrations for enterprise applications.
* Developed encryption protocols for databases and cloud storage to protect sensitive information.
* Automated SOC dashboards using ELK Stack and Splunk to provide real-time security insights.
* Performed security audits aligned with ISO 27001 and SOC 2 frameworks.
* Implemented secure coding guidelines in collaboration with development teams.
* Developed incident response playbooks and documentation for technical and management teams.
* Conducted employee training and phishing simulation exercises to enhance security awareness.
* Provided recommendations for cloud migration and modernization of security infrastructure.

**Environment:** AWS, Jenkins, Git, Splunk, ELK, Cisco Firepower, Snort, Nessus, Burp Suite, Metasploit, Symantec, Microsoft Defender, CI/CD, Python, Agile, DevSecOps

### **Client:**

**Information Security Engineer | Jan 2011 – Feb 2013**

**Responsibilities:**

* Designed secure network architecture and implemented firewall, VPN, and IDS/IPS solutions for enterprise environments.
* Conducted penetration testing and vulnerability assessments using Kali Linux, Metasploit, and Nessus.
* Managed automated vulnerability scanning and remediation using OpenVAS and custom scripts.
* Implemented IAM and SSO solutions to control access across enterprise applications.
* Deployed endpoint protection solutions to detect and mitigate advanced threats.
* Built automated incident response workflows using Python and PowerShell scripts.
* Developed security policies, procedures, and governance frameworks aligned with regulatory requirements.
* Monitored network and application security events using SIEM tools.
* Conducted security awareness training programs for technical and non-technical staff.
* Integrated encryption mechanisms for data at rest and in transit.
* Collaborated with DevOps teams to incorporate security into network automation pipelines.
* Audited third-party vendors and partner integrations for security compliance.
* Provided technical reports and recommendations for security improvements to management.
* Implemented cloud security monitoring and assessment for hybrid deployments.

**Environment:** Kali Linux, Metasploit, Nessus, OpenVAS, Python, PowerShell, VPN, Firewalls, SIEM, IAM, SSO, CI/CD, Agile, DevSecOps

### **Client:**

**Cybersecurity Specialist | June 2014 – Dec 2010**

**Responsibilities:**

* Designed and deployed security controls for enterprise systems and critical infrastructure.
* Implemented endpoint detection and response solutions to monitor and mitigate threats.
* Conducted threat assessments and risk analysis using structured methodologies.
* Built automated vulnerability scanning workflows using Nessus and custom scripts.
* Integrated SIEM and monitoring solutions to provide centralized security intelligence.
* Developed IAM and access control policies to secure corporate systems.
* Enforced encryption protocols for sensitive data and communications.
* Performed penetration testing and red-team exercises to validate security measures.
* Implemented patch management strategies across enterprise systems.
* Collaborated with IT teams to integrate cybersecurity into operational workflows.
* Developed incident response plans and playbooks for threat mitigation.
* Conducted security training for personnel to ensure awareness and compliance.
* Managed compliance audits aligned with ISO 27001 standards.
* Recommended modernization strategies for legacy security systems to cloud-integrated solutions.

**Environment:** Nessus, Python, PowerShell, SIEM, EDR, IAM, Encryption, Patch Management, CI/CD, DevSecOps, Agile