**Habeeb Owais**

**Hawais9594@gmail.com**

**(732) 807 0276**

**Professional Summary**

* Cybersecurity Professional with over 10 years of experience across diverse security domains, including IAM, PAM, TVM, SOC operations, and cloud security in hybrid and multi-cloud environments.
* Proficient in container security and cloud-native platforms, integrating tools like Wiz.io, Aqua Security, and Twistlock for runtime protection, vulnerability scanning, and compliance enforcement in Docker/Kubernetes clusters.
* Specialized in implementing and managing enterprise Identity and Access Management (IAM) solutions using Okta, Ping Identity, ForgeRock, and Microsoft Azure AD.
* Deep experience in Privileged Access Management (PAM) platforms such as CyberArk, BeyondTrust, and Delinea (Thycotic), managing privileged credentials, session monitoring, and vaulting.
* Implemented Infrastructure as Code (IaC) security using Terraform and Terraform Cloud with automated drift detection, secrets management, and security baselines.
* Architected end-to-end PAM deployments in large enterprise environments, integrating with AD, LDAP, and SIEM platforms for complete visibility and control.
* Led vulnerability management programs utilizing Tenable, Qualys, and Rapid7 to reduce critical vulnerabilities through continuous scanning, patch lifecycle optimization, and remediation tracking.
* Designed and implemented comprehensive cloud security strategies on AWS, Azure, and GCP, utilizing native tools like AWS Config, Azure Defender, and GCP Security Command Center.
* Developed automated security workflows and playbooks in Python and PowerShell for threat hunting, alert enrichment, and incident response.
* Experienced in DevSecOps practices, embedding security gates in CI/CD pipelines using Jenkins, GitLab, and tools like SonarQube, Snyk, and Aqua Security.
* Proficient in designing and maintaining secure architectures using Zero Trust principles, network segmentation, and least privilege access models.
* Conducted Red Team vs. Blue Team exercises and simulated threat scenarios to test SOC readiness, incident response, and recovery procedures.
* Expert in SIEM solutions such as Splunk, QRadar, and Microsoft Sentinel for real-time monitoring, threat detection, and log correlation.
* Strong background in regulatory and compliance frameworks including NIST 800-53, NIST CSF, ISO 27001, PCI-DSS, HIPAA, SOX, and FedRAMP.
* Performed comprehensive risk assessments and Business Impact Analyses (BIA) to drive security roadmap planning and investment prioritization.
* Configured and managed endpoint detection and response (EDR/XDR) solutions like CrowdStrike Falcon, Microsoft Defender, and SentinelOne.
* Led cloud migration security assessments ensuring identity federation, encryption standards, and secure configuration baselines were met.
* Delivered security awareness training and phishing simulations, improving organizational resilience against social engineering attacks.
* Managed Security Operations Center (SOC) functions including triage, containment, eradication, and post-incident analysis of security events.
* Oversaw multi-factor authentication (MFA), Single Sign-On (SSO), and Role-Based Access Control (RBAC) implementations across platforms.
* Conducted vulnerability assessments with Wiz.io for CSPM and CNAPP use cases, identifying misconfigurations, privilege escalations, and lateral movement paths across AWS, Azure, and GCP environments.
* Led third-party risk assessments and vendor security reviews, integrating findings into broader governance, risk, and compliance (GRC) efforts.
* Utilized tools like ServiceNow GRC and Archer to document risks, manage controls, and automate compliance evidence collection.
* Built custom dashboards and reporting mechanisms to provide actionable insights to executive leadership and drive data-informed decisions.
* Collaborated with internal audit and legal teams to maintain data protection policies and ensure readiness for regulatory inspections.
* Developed Data Loss Prevention (DLP) policies across cloud and on-prem environments, ensuring sensitive data remained protected.
* Conducted forensic investigations using tools such as EnCase and FTK, tracing lateral movement and identifying data exfiltration methods.
* Experienced in token-based authentication, SAML/OAuth2/OpenID Connect protocols, and API security standards.
* Proven track record of influencing security culture and aligning technical controls with enterprise business objectives.

**Technical Skills**

|  |  |
| --- | --- |
| **IAM / PAM** | CyberArk (EPV, PSM, CPM, AIM, PTA), Okta, Ping Identity, BeyondTrust, SailPoint |
| **Cloud Platforms** | AWS, Azure, GCP |
| **Security Tools** | Splunk, QRadar, Wiz.io, Tenable, Nessus, Rapid7, CrowdStrike, SentinelOne, Aqua Security |
| **Authentication** | SAML, OAuth2, OpenID Connect (OIDC), SCIM, LDAP, RBAC, ABAC |
| **DevOps & Automation** | PowerShell, Python, REST APIs, Terraform, Git, Jenkins, Ansible, GitLab |
| **Compliance** | NIST 800-53, ISO 27001, PCI-DSS, HIPAA, FedRAMP |
| **SIEM & Monitoring** | Splunk, QRadar, Microsoft Sentinel |
| **EDR / XDR** | CrowdStrike, Microsoft Defender, SentinelOne |
| **Vulnerability Mgmt.** | Tenable, Qualys, IBM AppScan, Burp Suite, Fortify |
| **Operating Systems** | Windows Server, Linux (RedHat, Ubuntu), Unix |
| **Networking** | DNS, VPN, DHCP, Apache, IIS, Active Directory, ADFS |

**Professional Experience**

**Senior Cybersecurity Consultant**
**Vitol, Houston, TX.**  **Feb 2023 – Till date**

**Responsibilities:**

* Collaborated with OT Network and Application Engineers to assess existing process environments and gather infrastructure data across multiple industrial sites.
* Managed end-to-end implementation of security controls aligned with NIST 800-53 and FedRAMP frameworks, ensuring compliance for federal cloud environments.
* Assisted in evaluating site-level cyber readiness, identifying vulnerabilities, and supporting remediation initiatives in alignment with NIST and ISO 27001 frameworks.
* Developed security architecture designs and hardening strategies for AWS and Azure environments using CIS benchmarks and custom policies.
* Built secure Kubernetes workloads on EKS and AKS, applying pod security policies, network segmentation, and runtime threat detection using Aqua Security and Falco.
* Designed and operationalized Security Operations Center (SOC) dashboards using Splunk Enterprise Security for real-time threat detection and response.
* Installed and configured cybersecurity tools (such as endpoint protection and network monitoring solutions) on industrial control systems and operator workstations.
* Provided remediation guidance and patch management workflows across Windows, Linux, and network devices to reduce CVSS-based vulnerabilities by 80%.
* Implemented advanced threat hunting techniques using tools like CrowdStrike, Carbon Black, and Velociraptor.
* Led Red Team vs. Blue Team exercises to evaluate incident response capabilities and improve internal SOC effectiveness.
* Directed the deployment of Public Key Infrastructure (PKI) for access control and encryption in a highly regulated DoD environment.
* Collaborated with software development teams to integrate DevSecOps practices in CI/CD pipelines using GitLab, Jenkins, and Aqua Security.
* Authored risk assessment reports and security design documentation for Authority to Operate (ATO) packages under RMF process.
* Conducted cloud infrastructure hardening using Wiz.io findings and Terraform modules; mapped exposure paths to sensitive resources.Coached junior analysts on malware analysis techniques, SIEM rule creation, and log correlation strategies.
* Oversaw identity governance solutions using SailPoint and Okta, strengthening user provisioning and access certification processes.
* Conducted comprehensive third-party risk assessments and vendor security reviews to ensure alignment with ISO 27001 standards.
* Worked closely with legal and compliance teams to handle data breach response, ensuring adherence to HIPAA and FISMA regulations.
* Contributed to the development of site-specific documentation, standard operating procedures (SOPs), and user training materials for OT environments.
* Built security automation scripts in Python to enhance incident triage, log parsing, and threat intel enrichment.
* Participated in tabletop exercises simulating ransomware and nation-state attack scenarios for continuity planning.
* Reviewed and updated incident response plans, playbooks, and escalation procedures for both IT and OT environments.
* Developed custom Splunk dashboards ingesting container and Kubernetes audit logs for behavior-based threat detection.
* Created and maintained asset inventory using ServiceNow CMDB, enabling better vulnerability prioritization and patch lifecycle management.
* Supported the hyper care phase by delivering user training and addressing operational or security issues during early adoption.
* Utilized Nessus, OpenVAS, and Qualys for regular internal/external scans and created executive-level vulnerability reports.

**Sr. Cyber Security Engineer**
**Xceedtek INDIA Sep 2018- April 2022**

**Responsibilities:**

* Led the enterprise deployment of CyberArk suite, configuring EPV, PVWA, CPM, PSM, AIM, and PTA across 5,000+ privileged accounts including Windows, Unix, service, and domain admin accounts.
* Designed and enforced password rotation policies, session monitoring rules, and safe creation protocols for privileged accounts aligned with compliance mandates.
* Configured Azure Security Center for threat detection, compliance insights, and automated policy enforcement.
* Implemented MFA (Okta, DUO) for privileged access and critical SaaS platforms; configured conditional access and risk-based policies.
* Automated provisioning and de-provisioning workflows with SCIM, PowerShell, and REST APIs; integrated with Okta and Ping.
* Developed RBAC and ABAC models for identity governance across AWS, Azure, and GCP using IAM roles, groups, and permissions boundaries.
* Conducted vulnerability assessments using IBM AppScan, Fortify, Burp Suite; identified and remediated high-risk OWASP vulnerabilities.
* Monitored real-time network threats via QRadar SIEM; built custom rules, dashboards, and correlation logic for incident detection.
* Configured alert tuning and data enrichment for 100+ data sources including firewalls, EDRs, proxies, DNS, and cloud APIs.
* Created incident response playbooks for account compromise, lateral movement, and data exfiltration; led tabletop exercises.
* Hardened system and application configurations using CIS benchmarks and Azure/AWS Security Best Practices.
* Designed and implemented TLS encryption, BitLocker, and Azure Key Vault policies for data protection at rest and in transit.
* Delivered IAM/PAM architecture roadmaps, system documentation, SOPs, and runbooks for Tier 1-3 security operations.
* Provided SME support in audit reviews, internal controls testing, and evidence collection for PCI and HIPAA assessments.
* Maintained security governance by running monthly access certification campaigns and quarterly privileged user reviews.

**Network Security Engineer**
**Reliant Hyderabad, IN May 2015 – Aug 2018**

**Responsibilities:**

* Spearheaded CyberArk PAM implementation for internal infrastructure and third-party vendor accounts; achieved full compliance with corporate security policies.
* Deployed and managed over 4,000 privileged credentials including Windows, Linux, databases, and application admin accounts.
* Configured platform-specific settings for credential management, account reconciliation, and custom connectors.
* Integrated CyberArk with Splunk and QRadar for log ingestion, privileged activity monitoring, and alert generation.
* Migrated legacy IAM policies to Okta, implementing SAML-based SSO across 150+ SaaS applications.
* Customized Okta lifecycle management workflows (JML - Joiners, Movers, Leavers) using directory integration and event hooks.
* Designed authentication frameworks leveraging OAuth2, SAML, OIDC for federated login to internal and external apps.
* Implemented MFA for high-risk user groups using adaptive access and geolocation-based policies.
* Integrated Ping Identity with internal LDAP directories and ADFS for centralized identity brokering.
* Developed PowerShell scripts for automation of privileged account onboarding, API token rotations, and credential sync.
* Conducted penetration testing support and remediation tracking for externally facing applications.
* Provided endpoint protection via Palo Alto firewalls, SSL decryption, DNS filtering, and custom threat signatures.
* Collaborated with GRC teams to align PAM practices with ISO 27001 controls and conduct policy gap analysis.
* Participated in security incident response, root cause analysis, and retrospective reporting.
* Delivered training and workshops for security teams, application owners, and helpdesk staff on IAM best practices.