MONISH TEJA KOLLI

Cyber Security

MA, USA | +1 (617) 971-7835 | Email: | LinkedIn

SUMMARY

Detail-oriented **Cyber Security professional with 3+ years of experience** protecting enterprise environments across on-prem and cloud (**AWS/Azure). Proven track record building SIEM detections, tuning EDR**, automating incident response, **hardening infrastructure with CIS/NIST controls, and driving audit readiness for ISO 27001, SOC 2, HIPAA.** Skilled in threat hunting, log engineering, IAM, network security, vulnerability management, and DevSecOps. Known for measurable risk reduction, crisp documentation, and cross-functional collaboration with **IT, DevOps, and Compliance**.

TECHNICAL SKILLS

- **Security Operations:** SIEM engineering (Splunk/QRadar/Azure Sentinel), EDR (CrowdStrike, Defender for Endpoint), SOAR playbooks, threat hunting, incident response, malware triage, phishing defense
- **Cloud & Identity:** AWS Security Hub/GuardDuty/CloudTrail/Config, Azure Defender/Defender for Cloud, IAM, Okta, SSO/SAML/OAuth2, least privilege, key management (KMS)
- **Vuln & Hardening:** Nessus, Qualys, OpenVAS, OS patching, CIS Benchmarks, NIST 800-53/171, OWASP Top 10, container security (ECR/ACR, image scanning)
- **Network Security:** Firewalls (Palo Alto, Fortinet), IDS/IPS (Snort/Suricata), WAF, TLS/PKI, DNS security, VPN, micro-segmentation
- **DevSecOps & Automation:** Python, Bash, PowerShell, GitHub Actions/Jenkins, IaC (Terraform), policy-as-code, secret scanning (TruffleHog/Gitleaks)
- **Governance & Audit:** Risk assessments, third-party, SOC 2/ISO 27001 controls mapping, HIPAA, PCI DSS, data classification & DLP
- **Observability & Data:** Log pipelines (Fluent Bit/Beats/Kinesis), KQL/SPL/SQL, dashboarding, detection-as-code

CERTIFICATIONS

- Google Cybersecurity Specialization, Google
- CompTIA Security + Exam SY0-701, Total Seminars, Udemy
- ISC2 Cyber Security

PROFESSIONAL EXPERIENCE

Cyber Security Analyst | DXC Technology | USA — Jan 2024 – Present

- Engineered **SIEM detections** in Splunk and **Microsoft Sentinel** (KQL/SPL) for authentication anomalies, privilege escalation, suspicious PowerShell, and improved **true-positive rate by 31%** while cutting alert noise **28%** through rule tuning and risk-based alerting.
- Built **SOAR playbooks** (Logic Apps/Power Automate + Python) for phishing triage, IOC enrichment (VirusTotal, AbuseIPDB), and containment via **EDR (Defender/CrowdStrike)**; reduced mean time to respond (**MTTR**) from **3.6h → 45m**.
- Led **threat hunting** sprints using Sigma/MITRE ATT&CK to identify living-off-the-land behaviors, suspicious scheduled tasks, and token theft; surfaced two credential-stuffing campaigns and a **previously undetected C2 beacon**.
- Stood up **cloud security posture management**: **AWS GuardDuty, Security Hub, Config** rules and Azure Defender recommendations; implemented **least-privilege IAM** and SCPs, closing **200+** misconfigurations and lowering critical findings **>60%**.
- Drove **vulnerability management** program with **Tenable/Nessus + Qualys**, integrating with Jira for SLAs (critical: 7 days, high: 14 days); achieved **92% on-time remediation** and **reduced critical vulns 55%** in two quarters.
- Implemented **endpoint hardening** (CIS L1/L2) and application control; enforced **BitLocker** and **Device Control** policies across 1,800+ endpoints, improving measured device risk score by **40%**.
- Partnered with **DevOps** to embed **SAST/DAST/Dependency scanning** (GitHub Advanced Security, OWASP ZAP) in CI/CD; blocked **32** vulnerable packages pre-prod and authored **secure coding standards** aligned to **OWASP ASVS**.
- Conducted **tabletop exercises** and IR trainings; refined the **Incident Response Plan** and communication templates, meeting **HIPAA/SOC 2** evidence requirements; led post-incident RCAs with **5-Why** and **MITRE** mapping.
- Built **data loss prevention** rules for M365 & email (sensitive keywords/regex, labeling, auto-encrypt); decreased unintentional data exposure incidents **by 70%** quarter-over-quarter.
- Authored **policies/SOPs/playbooks** (Access Control, Logging & Monitoring, Vendor Risk, Secure Build Baselines), uplifting audit readiness; contributed to **ISO 27001** internal audit with zero major non-conformities.

Associate Security Engineer | Mphasis | India — Oct 2021 – Aug 2023

- Operated **24×7 SOC** functions—triage, investigation, escalation, and closure—covering phishing, EDR alerts, DNS tunneling, and **brute-force** attempts; standardized enrichment using **Sigma rules** and IOC feeds to ensure consistent evidence collection.
- Deployed **Azure Sentinel** connectors (M365, Defender, AAD, AWS CloudTrail) and curated **KQL** analytics to baseline user/app behavior; reduced undifferentiated informational alerts **by 35%**.
- Implemented **network security controls** (NGFW policies, IDS/IPS, geo-IP blocking, URL filtering) and **Zero Trust**segmentation; supported **WAF** configs for public APIs, mitigating **OWASP Top 10** risks.
- Assisted with **vulnerability scanning** (OpenVAS/Tenable) and **patch governance** for Windows/Linux and third-party apps; cut patch backlog **by 48%** and monitored KB deployments with compliance dashboards.
- Hardened **Windows/Linux baselines** with **CIS Benchmarks** and **GPOs/Ansible**, enabling consistent secure configurations across dev/test/prod; reduced misconfig drift measured by Config/Azure Policy.
- Supported **identity security** initiatives—**MFA rollout**, conditional access, **Okta** app onboarding, and periodic access reviews; decreased high-risk sign-ins **by 37%** within 90 days.
- Contributed to **DevSecOps** adoption: added **secret scanning** (Gitleaks), **container image scanning**, and IaC checks (tfsec/checkov) to pipelines; prevented deployment of **20+** images with critical CVEs.
- Helped build a **phishing simulation & awareness** program (KnowBe4) and tracked metrics (failure rate, report rate), driving **employee click-rate down from 14% → 3.2%** in six months.
- Performed **risk assessments** and **third-party reviews** using standardized questionnaires (SIG/CAIQ); documented compensating controls and fed risks to the register for **SOC 2/ISO 27001** evidence.
- Wrote and maintained **runbooks** for common incidents (phish, malware, suspected account compromise), improving L1 handoffs and decreasing handle time **by 22%**.

EDUCATION

Masters in Informatics – Information security and Management | Northeastern University Boston, USA — **Sept 2023 – July 2025**

Bachelor in Computer Science and Engineering | GITAM Deemed to be University, India — **June 2019 – April 2023**