

# MONISH TEJA KOLLI

## Cyber Security Analyst | Cloud & SOC Security

Boston, MA, USA | +1 (617) 971-7835 | Email: [Kolli.m@northeastern.edu](mailto:Kolli.m@northeastern.edu) | [LinkedIn](#) | [Personal Website](#)

### SUMMARY

Cyber Security professional with 2+ years of experience protecting enterprise environments across on-prem and cloud platforms (AWS/Azure). Delivered effective SIEM detections, optimized EDR configurations, automated incident response workflows, and implemented CIS/NIST security controls to reduce operational risk. Supported audit readiness and compliance for ISO 27001, SOC 2, and HIPAA. Experienced in threat hunting, log engineering, IAM, network security, vulnerability management, and DevSecOps, recognized for clear documentation and strong collaboration with IT, DevOps, and Compliance teams.

### 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+ (SY0-701), Total Seminars, Udemy
- ISC2 Certified in Cybersecurity (CC)

### PROFESSIONAL EXPERIENCE

<b>Cyber Security Analyst   DXC Technology   USA</b>	<b>Sep 2025 – Present</b>
<ul style="list-style-type: none"><li>Engineered <b>SIEM detections</b> in Splunk and <b>Microsoft Sentinel</b> (KQL/SPL) for authentication anomalies, privilege escalation, suspicious PowerShell, and improved <b>true-positive rate by 31%</b> while cutting alert noise <b>28%</b> through rule tuning and risk-based alerting.</li><li>Built <b>SOAR playbooks</b> (Logic Apps/Power Automate + Python) for phishing triage, IOC enrichment (VirusTotal, AbuseIPDB), and containment via <b>EDR (Defender/CrowdStrike)</b>; minimized mean time to respond (<b>MTTR</b>) from <b>3.6h → 45m</b>.</li><li>Led <b>threat hunting</b> sprints using Sigma/MITRE ATT&amp;CK to identify living-off-the-land behaviors, suspicious scheduled tasks, and token theft; surfaced two credential-stuffing campaigns and a <b>previously undetected C2 beacon</b>.</li><li>Stood up <b>cloud security posture management</b>: <b>AWS GuardDuty</b>, <b>Security Hub</b>, <b>Config</b> rules and Azure Defender recommendations; implemented <b>least-privilege IAM</b> and SCPs, closing <b>200+</b> misconfigurations and lowering critical findings <b>&gt;60%</b>.</li><li>Drove <b>vulnerability management</b> program with <b>Tenable/Nessus + Qualys</b>, integrating with Jira for SLAs (critical: 7 days, high: 14 days); achieved <b>92% on-time remediation</b> and <b>brought down critical vulns 55%</b> in two quarters.</li><li>Performed <b>endpoint hardening</b> (CIS L1/L2) and application control; enforced <b>BitLocker</b> and <b>Device Control</b> policies across 1,800+ endpoints, improving measured device risk score by <b>40%</b>.</li></ul>	

<b>Cyber Security Analyst Intern   OESON Pvt. Ltd   USA</b>	<b>Jan 2024 – Apr 2024</b>
<ul style="list-style-type: none"><li>Partnered with <b>DevOps</b> to embed <b>SAST/DAST/Dependency scanning</b> (GitHub Advanced Security, OWASP ZAP) in CI/CD; blocked <b>32</b> vulnerable packages pre-prod and authored <b>secure coding standards</b> aligned to <b>OWASP ASVS</b>.</li><li>Conducted <b>tabletop exercises</b> and IR trainings; refined the <b>Incident Response Plan</b> and communication templates, meeting <b>HIPAA/SOC 2</b> evidence requirements; led post-incident RCAs with <b>5-Why</b> and <b>MITRE</b> mapping.</li><li>Built <b>data loss prevention</b> rules for M365 &amp; email (sensitive keywords/regex, labeling, auto-encrypt); decreased unintentional data exposure incidents <b>by 70%</b> quarter-over-quarter.</li><li>Authored <b>policies/SOPs/playbooks</b> (Access Control, Logging &amp; Monitoring, Vendor Risk, Secure Build Baselines), uplifting audit readiness; contributed to <b>ISO 27001</b> internal audit with zero major non-conformities.</li></ul>	

<b>Associate Security Analyst   Mphasis   USA</b>	<b>Oct 2021 – Aug 2023</b>
<ul style="list-style-type: none"><li>Operated <b>24x7 SOC</b> functions—triage, investigation, escalation, and closure—covering phishing, EDR alerts, DNS tunneling, and <b>brute-force</b> attempts; standardized enrichment using <b>Sigma rules</b> and IOC feeds to ensure consistent evidence collection.</li><li>Deployed <b>Azure Sentinel</b> connectors (M365, Defender, AAD, AWS CloudTrail) and curated <b>KQL</b> analytics to baseline user/app behavior; reduced undifferentiated informational alerts <b>by 35%</b>.</li><li>Enforced <b>network security controls</b> (NGFW policies, IDS/IPS, geo-IP blocking, URL filtering) and <b>Zero Trust</b> segmentation; supported <b>WAF</b> configs for public APIs, mitigating <b>OWASP Top 10</b> risks.</li><li>Assisted with <b>vulnerability scanning</b> (OpenVAS/Tenable) and <b>patch governance</b> for Windows/Linux and third-party apps; cut patch backlog <b>by 48%</b> and monitored KB deployments with compliance dashboards.</li><li>Hardened <b>Windows/Linux baselines</b> with <b>CIS Benchmarks</b> and <b>GPOs/Ansible</b>, enabling consistent secure configurations across dev/test/prod; lowered misconfig drift measured by Config/Azure Policy.</li><li>Supported <b>identity security</b> initiatives—<b>MFA rollout</b>, conditional access, <b>Okta</b> app onboarding, and periodic access reviews; decreased high-risk sign-ins <b>by 37%</b> within 90 days.</li><li>Contributed to <b>DevSecOps</b> adoption: added <b>secret scanning</b> (Gitleaks), <b>container image scanning</b>, and IaC checks (tfsec/checkov) to pipelines; prevented deployment of <b>20+</b> images with critical CVEs.</li><li>Helped build a <b>phishing simulation &amp; awareness</b> program (KnowBe4) and tracked metrics (failure rate, report rate), driving <b>employee click-rate down from 14% → 3.2%</b> in six months.</li><li>Performed <b>risk assessments</b> and <b>third-party reviews</b> using standardized questionnaires (SIG/CAIQ); documented compensating controls and fed risks to the register for <b>SOC 2/ISO 27001</b> evidence.</li><li>Wrote and maintained <b>runbooks</b> for common incidents (phish, malware, suspected account compromise), improving L1 handoffs and decreasing handle time <b>by 22%</b>.</li></ul>	

### 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