

Dinesh Melimi

Email: melimidinesh2168@gmail.com

Mobile: +19405979837

LinkedIn: linkedin.com/in/dinesh-melimi | GitHub: github.com/Dinesh-Melimi

Cybersecurity Engineer | Cloud Security · Incident Response · DevSecOps

PROFESSIONAL SUMMARY:

Cybersecurity Engineer with 4+ years of experience securing enterprise cloud and hybrid environments across AWS, Azure, and Microsoft 365, including a regulated healthcare company. Investigates and responds to incidents across endpoint, identity, cloud, and network using Microsoft Sentinel, Splunk, Microsoft Defender XDR, and CrowdStrike Falcon, and tuned Sentinel detections to cut false positives by 25%. Reduced critical cloud exposure by 31% through Tenable-driven remediation, and secures AWS with least-privilege IAM, AWS Config, Security Hub, and GuardDuty against CIS Benchmarks and NIST. Integrated SAST/DAST gates into CI/CD pipelines and led a penetration testing program that found 50+ critical and high-severity vulnerabilities. Builds security automation in Python and PowerShell that cut manual effort by 40%, and writes Terraform, threat models, and runbooks.

TECHNICAL SKILLS:

- **SIEM & Security Operations** - Microsoft Sentinel, KQL, Splunk, ELK, Log Analytics, Alert Triage, Detection Tuning, Correlation Rules, SIEM Dashboards.
- **Incident Response & Threat Detection** - Incident Response Lifecycle, Digital Forensics, Evidence Handling, Root Cause Analysis, Threat Hunting, MITRE ATT&CK, IOC Analysis, Phishing and Malware Analysis, IR Playbooks.
- **Endpoint Security** - Microsoft Defender XDR, Microsoft Defender for Endpoint, Microsoft Defender for Office 365, CrowdStrike Falcon.
- **Cloud Security & CSPM** - AWS IAM, GuardDuty, Security Hub, CloudTrail, AWS Config, Inspector, KMS, VPC, Security Groups, S3; Microsoft Azure, Microsoft Defender for Cloud, Azure Monitor.
- **Identity & Access Management** - Microsoft Entra ID, Active Directory, Conditional Access, MFA, RBAC, SSO, PAM, Least Privilege, Access Governance.
- **Vulnerability Management & AppSec** - Tenable, Qualys, Nessus, Burp Suite Professional, OWASP ZAP, OWASP Top 10, VAPT, CVSS, API Security Testing, Threat Modeling (STRIDE).
- **DevSecOps & CI/CD** - GitHub Actions, SAST, DAST, SCA, Secret Detection (Gitleaks), IaC Scanning (Checkov), Container Scanning (Trivy), SBOM, Secure SDLC.
- **Infrastructure as Code & Containers** - Terraform (AWS, Cloudflare), AWS CloudFormation, Docker, Kubernetes.
- **Network & Web Security** - Firewalls, Cloudflare WAF, Rate Limiting, VPN, DNS, Proxy, IDS/IPS, TCP/IP, HTTP, SSL/TLS, Network Segmentation.
- **Automation & AI Security** - Python, PowerShell, Bash, REST APIs; LLM output validation and sensitive-data redaction.
- **Compliance & Tools** - NIST CSF, CIS Controls, ISO 27001, SOC 2, Audit Support; ServiceNow, Jira, Git/GitHub.

PROFESSIONAL EXPERIENCE:

Johnson & Johnson

March 2025 – Present

Cybersecurity Engineer

Responsibilities:

- Monitor and investigate security alerts across Microsoft Sentinel, Splunk, Microsoft Defender XDR, AWS GuardDuty, and Security Hub in a regulated healthcare environment, escalating confirmed incidents for response.
- Tune Microsoft Sentinel analytics rules, detection logic, and alerts, reducing false positives by 25% and improving analyst efficiency.
- Investigate endpoint, cloud, identity, and network incidents by correlating AWS CloudTrail, Defender XDR, and firewall, VPN, DNS, and proxy logs to determine scope and impact.
- Validate Defender XDR endpoint detections, collect and preserve forensic evidence, and coordinate containment, remediation, and recovery with infrastructure teams.
- Perform vulnerability assessments with Tenable and drive remediation with application and platform owners, reducing critical exposure by 31% across cloud assets.
- Configure least-privilege AWS IAM policies, security groups, and AWS Config rules, evaluating production configurations against CIS Benchmarks and NIST.

- Analyze phishing campaigns and suspicious email activity in Microsoft Defender for Office 365 to protect users and reduce organizational risk.
- Automate recurring log collection, reporting, and analysis with Python and PowerShell, reducing manual effort by 40%.
- Validate AI-assisted security recommendations through manual investigation, support NIST and ISO 27001 compliance, and perform MITRE ATT&CK-aligned threat hunting.

PURVIEW

January 2022 – June 2024

DevSecOps Engineer

Responsibilities:

- Integrated automated SAST/DAST security quality gates into CI/CD pipelines for mobile application platforms with development teams, intercepting malicious dependencies and non-compliant code before release.
- Led design and deployment of an automated Vulnerability Assessment and Penetration Testing (VAPT) program across production web applications and internal subnets using Nessus, Burp Suite Professional, and OWASP ZAP, identifying 50+ critical and high-severity vulnerabilities.
- Routed CVSS-scored findings into ticketing workflows with assigned owners and tracked remediation to verified closure.
- Served as a core incident responder: analyzed telemetry, authored post-incident reviews, and drafted incident response playbooks that reduced Mean Time to Resolution (MTTR).
- Triageed 1,500+ SIEM alerts monthly across Microsoft Sentinel, Splunk, and ELK, and investigated phishing, malware, and compromised accounts with Microsoft Defender for Endpoint.
- Built SIEM dashboards and alert rules that reduced investigation time by 20%, and Python and PowerShell automation for alert enrichment, ticketing, and reporting that cut manual effort by 35%.
- Hardened AWS resources with IAM, VPC, and CloudFormation, and enabled continuous monitoring with Security Hub, GuardDuty, and CloudTrail.
- Validated vulnerability remediation through Azure security processes, improving compliance coverage by 26%, and supported audits with incident records and compliance documentation.
- Reviewed privilege changes in Active Directory to enforce least privilege, and ran phishing awareness programs that cut simulated click-through by 30%.

Projects:

Cloud Security & DevSecOps Platform - github.com/Dinesh-Melimi/vuln-triage-ai

- Built a Python vulnerability triage tool and FastAPI service with XXE-safe parsing, API key authentication, and an AI validation layer that rejects invented CVEs, unknown hosts, and severity downgrades, with host and IP redaction before any LLM call.
- Built an 11-stage GitHub Actions pipeline: SAST, SCA, secret detection, IaC scanning, container scanning, SBOM, API fuzz testing, and a hardened Kubernetes deployment with smoke tests.
- Wrote Terraform for a KMS-encrypted, TLS-only S3 bucket and for Cloudflare WAF (managed and OWASP rulesets, custom rules, rate limiting, strict TLS), plus a STRIDE threat model and a cutover and rollback runbook.

Enterprise Security Lab

- Built a segmented Windows AD and Linux lab across production, DMZ, and management networks, centralizing Sysmon and syslog into Splunk and ELK to tune detections and investigate anomalies.

Educational Details:

Master of Science in Cyber Security - University of North Texas (2026)

Bachelor of Technology in Cybersecurity - VNR Vignana Jyothi Institute of Engineering & Technology (2024)

Certifications:

CompTIA Security+ (In Progress) | ISC2 Certified in Cybersecurity (CC) | AWS Certified Cloud Practitioner (CLF-C02) | Microsoft Cybersecurity Analyst Professional Certificate | Cloud Computing – NPTEL (2023) | Introduction to Cybersecurity – Cisco (2022)