VINAYGOUD GANDI

San Antonio, TX |+1 (210) 868-1239 | gandivinay343@gmail.com

PROFESSIONAL SUMMARY

Results-driven Cybersecurity Engineer with 3+ years of experience in threat detection, SOC operations, incident response, IAM, and vulnerability management. Skilled in SIEM (Splunk, ELK, Azure Sentinel), SOAR automation, and EDR/XDR to strengthen defenses and reduce response times. Experienced in cloud security across AWS, Azure, and GCP with IAM enforcement, container security, and DevSecOps integration. Adept in threat hunting, penetration testing, and compliance (ISO 27001, NIST, SOC2, PCI-DSS, HIPAA, GDPR), enabling resilient, enterprise-grade security architectures.

TECHNICAL SKILLS

Cybersecurity & SOC: SIEM (Splunk, ELK, Azure Sentinel), SOAR (Cortex XSOAR, Swimlane), EDR/XDR (CrowdStrike Falcon, Microsoft Defender ATP, SentinelOne), IDS/IPS (Snort, Suricata, Zeek), Threat Hunting, Digital Forensics, Malware Analysis, Incident Response

IAM & Compliance: Identity & Access Management (RBAC, SAML, OAuth2.0, SCIM, MFA, PAM), Active Directory & Azure AD, Okta, Ping Identity, SailPoint, Zero Trust Architecture, Compliance Frameworks (ISO 27001, SOC2, NIST 800-53, CIS Benchmarks, HIPAA, PCI-DSS, GDPR, FedRAMP)

Cloud & Infrastructure Security: AWS (GuardDuty, Security Hub, KMS, WAF, Shield, IAM), Azure (Security Center, Sentinel, Defender for Cloud, Key Vault), GCP (Security Command Center, Cloud Armor, IAM), Container & Kubernetes Security (Falco, Aqua, Prisma Cloud, Trivy), Infrastructure Security Hardening

Vulnerability & Risk Management: Nessus, Qualys, OpenVAS, Rapid7 InsightVM, CVSS Scoring, Patch Management Automation, Exploit Testing (Metasploit, Cobalt Strike), Red/Blue Teaming, MITRE ATT&CK Framework

DevSecOps & Automation: Python (Threat Intel APIs), Bash, PowerShell, Terraform (Security as Code), Ansible, Jenkins, GitHub Actions, GitLab CI/CD, Secure SDLC, Automated Security Testing (OWASP ZAP, Burp Suite, Bandit, Snyk)

Networking & Monitoring: Firewalls (Palo Alto, Fortinet, Cisco ASA), VPN, Proxy, DNS Security, Wireshark, Nagios, Prometheus, Grafana, NetFlow/PCAP Analysis, TLS/PKI Management

Visualization & Analytics: Kibana, Splunk Dashboards, Grafana, Threat Intelligence Platforms (MISP, Anomali, Recorded Future)

PROFESSIONAL EXPERIENCE

Cybersecurity Engineer **Jun 2024 - Present**

CloudTech Innovations Inc | Dallas, TX

- Rolled out SIEM platforms (ELK, Splunk) across AWS, Azure, and on-prem servers, consolidating 10M+ daily logs into a unified view that accelerated anomaly detection and reduced MTTD by 40%.
- Built Python-driven SOAR playbooks to handle malware and phishing alerts automatically, which shortened MTTR by 35% and freed analysts to focus on advanced threat investigations.
- Strengthened edge defenses by integrating Snort and Suricata IDS/IPS with AWS WAF policies, effectively stopping 98% of injection and DDoS attacks before reaching production workloads.
- Improved identity posture by enforcing MFA, RBAC, and OAuth2 across multi-cloud environments, which cut down unauthorized access alerts by half and supported a Zero Trust framework.
- Launched a vulnerability management cycle with Nessus and OpenVAS, scanning 500+ endpoints monthly and ensuring critical CVEs were patched on time, which boosted audit compliance scores by 20%.
- Embedded Aqua and Trivy container scans into Kubernetes and Docker CI/CD pipelines, allowing vulnerabilities to be caught pre-deployment and resulting in zero misconfigured images in production.
- Carried out threat hunting missions with Splunk queries mapped to MITRE ATT&CK, exposing persistence techniques and lateral movement paths that had previously gone unnoticed, expanding SOC detection coverage by 30%.
- Activated AWS GuardDuty and Security Hub for continuous monitoring of IAM and cloud resources, which generated high-fidelity alerts that helped prevent multiple privilege escalation attempts.

Information Security Analyst **Nov 2021 - Nov 2023**

NextWave Software Solutions | Hyderabad, India

- Built Splunk dashboards that correlated firewall, endpoint, and user activity, which gave SOC analysts clearer visibility into anomalies and cut false positives by 30%.
- Integrated OWASP ZAP and Bandit scans into GitHub Actions so that insecure code was flagged before release, blocking critical vulnerabilities from reaching production.
- Rolled out CrowdStrike Falcon across enterprise endpoints, giving the SOC richer telemetry that improved malware detection by 45% and shortened investigation time.
- Ran phishing simulations with Python and Gophish, tracked click-through results, and used insights to refine training, which raised employee detection of phishing by 60%.
- Automated log enrichment pipelines in Python and Airflow, pulling threat intel feeds into Splunk, which enhanced detection of emerging IoCs and reduced alert fatigue.
- Applied CVSS scoring to vulnerability reports, worked with DevOps on prioritized fixes, and reduced the patch backlog by 40%, improving overall security posture.
- Led red-team exercises with Kali, Burp Suite, and Metasploit, uncovered exploitable flaws in web apps, and ensured all critical issues were remediated before client release.
- Hardened AWS and Azure workloads using CIS benchmarks, aligning identity, storage, and network controls, which boosted external audit compliance scores by 25%.

PROJECTS

Security Operations Center Automation

- Integrated SIEM (Splunk, ELK) with SOAR playbooks (Python, Ansible) to triage phishing, brute force, and malware alerts automatically, which reduced MTTR by 40% and boosted SOC response capacity.
- Augmented detection by feeding Threat Intel (MISP, VirusTotal, AlienVault OTX) into SIEM, which increased accuracy of correlation rules and cut false positives by 30%.
- Built incident dashboards in Kibana and Power BI to visualize SOC alerts, which gave managers real-time visibility into SLA breaches and security trends.

Advanced Penetration Testing Framework

- Executed penetration tests with Kali, Burp Suite, and Metasploit on enterprise web apps, then hardened code with Django/Flask security controls, which eliminated exploitable flaws before release.
- Embedded OWASP ZAP scans in CI/CD pipelines, shifting security left and reducing exploitable defects in production by 50%.
- Applied JWT hardening, Nginx rate limiting, and CSP headers to strengthen APIs, which ensured resilience against injection attacks and API abuse.

EDUCATION

Master of Science in Cybersecurity

Webster University | San Antonio, TX

CERTIFICATIONS

- Google Cybersecurity Professional Certificate - **Coursera**
- IBM Cybersecurity Analyst Professional Certificate - **Coursera**
- Microsoft Cybersecurity Analyst - **LinkedIn Learning**
- Cloud Security Fundamentals - **LinkedIn Learning**
- Identity and Access Management (IAM) Concepts - **Coursera**
- Introduction to Cyber Threat Intelligence - **IBM**