RAVINDRA DHOLARIYA

United States | (551) 232-4991 | ravindrad@workmailit.com | LinkedIn | github.com/f1cti0nal

SUMMARY

- Cybersecurity Analyst with 4+ years of hands-on experience in SOC environments, securing financial and enterprise infrastructures using SIEM tools (Splunk, Wazuh), SOAR platforms (Shuffle, TheHive), and endpoint protection technologies (Suricata, Cisco AMP).
- Proven ability to detect, analyze, and respond to sophisticated threats by implementing alert triage workflows, log correlation rules, and behavioral analysis techniques mapped to MITRE ATT&CK.
- Adept in vulnerability scanning (Nessus, Qualys, OpenVAS), CVSS scoring, and patch validation across hybrid cloud (AWS, Azure, GCP) deployments, reducing security debt and exposure windows by up to 60%.
- Specialized in developing incident response playbooks and automation scripts using Python, PowerShell, and Bash to streamline repetitive tasks, accelerate MTTD/MTTR, and ensure audit-ready compliance with ISO 27001 and NIST 800-53.

SKILLS

Scripting & Automation: Python (NumPy, pandas, Matplotlib), PowerShell, Bash, SOAR workflows (Shuffle, TheHive)
Security Frameworks & Compliance: MITRE ATT&CK, NIST 800-53, ISO 27001, CIS Controls, GDPR, SOX
Threat Detection & Monitoring: Splunk, LogRhythm, Wazuh SIEM, Log Analysis, Alert Triage, Threat Hunting
Vulnerability & Risk Management: Tenable Nessus, Qualys, OpenVAS, Rapid7 InsightVM, CVSS Scoring
Network & Endpoint Security: IDS/IPS (Snort, Suricata), Palo Alto & Fortinet Firewalls, VPN, NAC, Cisco AMP, Zeek
Identity & Access Management (IAM): Okta, RBAC, SAML, OAuth2
Cloud Security: Amazon Web Services (AWS), Azure, Google Cloud Platform, Digital Ocean, Linode, SonarQube
Digital Forensics & Incident Response: Wireshark, Volatility, Autopsy
Collaboration & ITSM Tools: JIRA, Confluence, ServiceNow, Discord (alerts/webhooks)

EXPERIENCE

MetLife, United States | Cybersecurity Analyst **January 2025 – Present**

- Built and maintained 80+ custom correlation rules in Wazuh and Splunk for real-time monitoring of login anomalies, policy violations, and malware callbacks across MetLife's internal insurance systems.
- Investigated alerts and conducted threat hunting using MITRE ATT&CK mapping and log correlation from AWS (CloudTrail, VPC Flow Logs), identifying persistent lateral movement and rare beaconing behaviors from compromised assets.
- Developed and deployed automated incident triage workflows using Shuffle SOAR, integrating Discord webhooks, IP enrichment APIs, and internal IOC databases—cutting average triage time by 72%.
- Implemented Python-based log parsing scripts to extract and normalize security events from VPN, NAC, and firewall logs (Fortinet, Palo Alto), feeding into Wazuh for improved correlation accuracy.
- Collaborated with IAM team to monitor and validate Okta-based authentication policies, including SAML assertion logs, RBAC audits, and OAuth2 token refresh anomalies.
- Ensured compliance with NIST 800-53 and SOX controls by assisting internal audit teams in log integrity validation, alert documentation, and quarterly risk assessment reports.

Sage SoftTech, India | SOC Analyst **January 2020 – June 2023**

- Monitored 10,000+ daily logs across firewall, endpoint, and application layers using Wazuh SIEM, identifying brute-force attempts, privilege escalations, and DNS tunneling activities.
- Conducted in-depth analysis of alert payloads using Wireshark and Zeek, investigating traffic for encrypted command-and-control (C2) channels and abnormal HTTP/S behavior patterns.
- Managed and tuned IDS/IPS signatures (Snort and Suricata) to reduce false positives by 35%, enabling higher confidence alerting for key detection scenarios like SQL injection and malware dropper activity.
- Executed full-cycle incident response investigations—from alert verification to containment and recovery—documenting artifacts in TheHive and ensuring compliance with ISO 27001 IR protocols.
- Contributed quarterly vulnerability assessments using OpenVAS, working with sysadmins to close 200+ high-severity findings and implementing firewall-based segmentation strategies to contain exploitable services.
- Hardened web application infrastructure by integrating file integrity monitoring (FIM) tools with SIEM alerts, detecting unauthorized script injections and unauthorized PHP shell uploads.

EDUCATION

Master's in Cybersecurity **May 2023 – May 2025**
Pace University, New York

Bachelor's in Computer Application **April 2017 – February 2021**
Veer Narmad South Gujarat University, India

CERTIFICATIONS

- Certified Ethical Hacker
- CompTIA Security+ ce Certification
- Junior Penetration Tester