GANDHAM JOTHISH

LinkedIn: linkedin.com/in/jothish-gandham | GitHub: github.com/jothish-blip | Portfolio: webjothishanalyst.site

labs.vercel.app

PROFESSIONAL SUMMARY

B.Tech Computer Science student specializing in Cyber Security & Forensics with expertise in SOC Operations and Blue Team defense. Certified Google Cybersecurity Professional skilled in incident response, threat hunting, network security, and SIEM configuration. Proven ability to engineer defense mechanisms, analyze threat intelligence, and remediate vulnerabilities to harden enterprise architectures against sophisticated cyber threats.

TECHNICAL SKILLS

Security Operations: Incident Response, Threat Detection, Phishing Analysis, Malware Investigation, Log Analysis

SIEM & Security Tools: Splunk, Google Chronicle, Wireshark, TCPDump, Suricata, VirusTotal

Networking: Network Security, TCP/IP, Network Traffic Analysis

Frameworks & Standards: NIST Cybersecurity Framework (CSF), NIST SP 800-30, MITRE ATT&CK

Programming & OS: Python, SQL, Linux

PROJECTS

Detection & Response Operations

- Remediated 50+ simulated phishing incidents by parsing SMTP/IMAP email headers to extract Indicators of Compromise (IOCs) and isolate attack vectors.
- Engineered packet capture analysis workflows using Wireshark and TCPDump, inspecting over 10,000 TCP/UDP packets to identify anomalous payload signatures.
- Configured Suricata IDS rulesets to monitor live network streams, reducing false-positive alert volume by 15% during simulated intrusion tests.
- Executed complex SPL queries in Splunk and Google Chronicle to parse 5,000+ security events and reconstruct attack kill chains.
- Synthesized threat intelligence from VirusTotal and OSINT frameworks to classify 20+ malware variants based on behavioral heuristics.
- Authored 15+ standardized incident response reports mapping threat actor techniques to the MITRE ATT&CK framework for stakeholder review.

Enterprise Vulnerability Assessment

- Orchestrated qualitative risk assessments adhering to NIST SP 800-30 guidelines across 30+ simulated enterprise assets.
- Quantified threat likelihood and business impact metrics, prioritizing 10 critical vulnerabilities for immediate patching.
- Formulated actionable remediation strategies that projected a 40% reduction in overall exploit surface area.

Automated Access Control (Python)

- Programmed an automated Python script utilizing regular expressions (Regex) to dynamically update IP allow lists and enforce access controls.
- Automated file processing and string manipulation operations, decreasing manual firewall configuration time by 80% and eliminating human syntax errors.

NIST Compliance & Security Audit

- Audited organizational security controls across 5 core domains of the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover).
- Pinpointed 12 key compliance gaps and engineered step-by-step security hardening plans for cross-functional engineering teams.

EDUCATION

Sandip University **Nashik, Maharashtra**

Bachelor of Technology (B.Tech) - Computer Science & Engineering **Expected Graduation: 2028**

Specialization: Cyber Security & Forensics (CSF)

CERTIFICATIONS

- Google Cybersecurity Professional Certificate
- Google Network Security Specialization
- AI Prompt Engineering Certificate