# GANDHAM JOTHISH

Nashik, Maharashtra, India | +91 8374754009 | jothishgandham2@gmail.com
LinkedIn: linkedin.com/in/jothish-gandham | GitHub: github.com/jothish-blip | Portfolio: webjothishanalyst.site

## PROFESSIONAL SUMMARY

B.Tech Computer Science student specializing in Cyber Security & Forensics, focusing on SOC operations and Blue Team defense strategies. Certified Google Cybersecurity Professional with hands-on experience in incident response, threat hunting, network traffic analysis, and SIEM configuration. Engineered defense mechanisms, analyzed threat intelligence, and remediated vulnerabilities to harden enterprise architectures against 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 |

## PRACTICAL EXPERIENCE & PROJECTS

### Detection & Response Operations

- Remediated 50+ phishing incidents within threat scenarios 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 and flag anomalous payload signatures.
- Configured Suricata IDS rulesets to monitor live network streams, reducing false-positive alert volume by 15% during controlled intrusion testing.
- Executed complex SPL queries in Splunk and Google Chronicle to parse 5,000+ security events and reconstruct attack kill chains for rapid triage.
- 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 to facilitate stakeholder review.

### Enterprise Vulnerability Assessment

- Orchestrated qualitative risk assessments adhering to NIST SP 800-30 guidelines across 30+ virtualized enterprise assets.
- Quantified threat likelihood and business impact metrics, prioritizing 10 critical vulnerabilities for immediate patch deployment.
- Formulated actionable remediation strategies projecting 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 allowlists and enforce strict network 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 the 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 to guide cross-functional engineering teams in remediation efforts.

## EDUCATION

**Sandip University** **Nashik, Maharashtra**

Bachelor of Technology (B.Tech) - Computer Science & Engineering

Specialization: Cyber Security & Forensics (CSF) Expected Graduation: 2028

## CERTIFICATIONS

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