Nitya Singh

nityasingh1273@gmail.com
(+91) 87691 06094
Rajasthan, Inidia
-nitya-singh-
@nitya_singh
https://nitya-singh.netlify.app/

Threat Researcher specializing in threat intelligence, phishing and malware analysis, IOC investigations, campaign tracking, and detection validation. Experienced with Kibana, Elasticsearch, regex-based detections, URL/domain investigations, and non-PE malware analysis. Interested in evolving toward Threat Intelligence Engineering, security automation, and AI-driven security workflows.

PROFESSIONAL EXPERIENCE

Sophos Technologies Private Limited

Threat Researcher 1 *January 2024 - Present*

- Analyzed 100,000+ enterprise email submissions to identify abusive behavior and block spam, phishing, malware, BEC, Nigerian scam, Data Champions, and CS campaigns across large customer environments.
- Investigated and correlated IOCs across URLs and domains, resulting in blocking actions on 1,000+ malicious spam and phishing domains and URLs.
- Developed and validated regex-based detection rules to catch high-risk campaigns while tuning logic to reduce false positives.
- Monitored active and emerging campaigns using Kibana, LSP, and Elasticsearch, turning observed signals into repeatable detection and triage workflows.
- Analyzed 100+ malicious files (HTML, PDF, JavaScript, VBS, PowerShell, HTA, JAR) to extract attacker techniques, delivery patterns, and campaign relationships (TTPs).

Burgwalden, Horseshoe BG, Germany

Web Developer Intern *June 2022 - August 2022*

- Designed and developed an internal admin dashboard to view and manage customer and program data, adding login-based access and role-based restrictions so only authorized users could see sensitive information.
- Built search, filtering, and data-fetching features, ensuring inputs were validated and data remained accurate while being accessed or updated.
- Followed secure development practices, using encrypted API communication and proper session handling to keep data safe during day-to-day usage.

EDUCATION

Rajasthan Technical University - Bachelor's of Technology in Computer Science - 9.73 CGPA (2020 - 2024)
Saint Paul's Senior Secondary School - Class XII (CBSE): 92.20% (2020) | Class X (CBSE): 94.20% (2018)

SKILLS

- **Threat Intelligence:** Email Threat Analysis (Spam, Phishing, Malware, BEC), Domain & URL Reputation Analysis, IOC Analysis & Correlation, Campaign Tracking, Threat Hunting, OSINT investigations, MITRE ATT&CK
- **Detection Engineering:** Regex-based Detection Rules, YARA Basics, Detection Validation, False-Positive Reduction, Kibana, LSP, Elasticsearch.
- **Malware & File Analysis:** Non-PE Analysis (HTML, PDF, JavaScript, VBS, PowerShell, HTA, JAR)
- **Programming & Web:** JavaScript, React.js, Node.js, REST APIs.
- **Security Fundamentals:** OWASP Top 10, OSINT, Incident Response, Business Continuity, Disaster Recovery Concepts, Network Security, Access Control Concepts.

PROJECT

IOC Enrichment CLI

- Developed a command-line tool that accepts URLs, domains, IPs, and hashes, enriches indicators through external APIs, and exports normalized investigation reports.
- Implemented caching, error handling, rate-limit handling, and structured output for repeatable analyst workflows.

CERTIFICATIONS

- Academic Excellence Award (2022-2023) – Issued by SKIT, Jaipur
- Certified in Cybersecurity (CC) | ISC2

VOLUNTEERING

- Google Developer Student Club (GDSC WOW'23), Jaipur – Design Team
- GirlScript Summer of Code (GSSoC'22) – Open-Source Contributor