Kurudunje Deekshith Shetty

SOC Analyst | Security+ Certified

+17325080380 | k.deekshithshetty@gmail.com | Jersey City, NJ | LinkedIn | Github | Portfolio

SUMMARY

Dedicated Cybersecurity Analyst with almost 3 years of experience in security event analysis and incident response. Committed to enhancing organizational security posture through proactive monitoring and advanced defense strategies. Recognized for optimizing correlation rules and successfully reducing false positives by over **50%**, solving the case of massive Alert fatigue.

Currently pursuing a Master of Science in Cybersecurity and Privacy at NJIT with **3.95 GPA**, combining academic excellence with real-world experience. Passionate about network security, continuous learning, and empowering others through cybersecurity education and mentorship.

RELEVANT CERTIFICATIONS

- *CompTIA Security+*
- *Fortinet NSE 5 - FortiSIEM*

EDUCATION

M.Sc. in Cyber Security and Privacy, CGPA : 3.95/4.00 — Jan 2024 - Dec 2025

NJIT - Ying Wu College of Computing — Newark, NJ

- *Relevant Coursework:*
  - *Counter Hacking Techniques |Network Security Protocols | Cryptography and Security*
  - *Cloud Computing | Computer Security Auditing |Cyber Security Investigations and Law*
  - *Human Centered Privacy and Usability | Internet and Higher Layer Protocols | Security and Privacy in Computer Systems*

PROFESSIONAL EXPERIENCE

Graduate Teaching Assistant – Cryptography and Security — Jun 2024 - Present

New Jersey Institute of Technology — Newark, NJ

- Graded assignments and exams for over **200+** students per semester, mentored students, teaching them complex cryptographic concepts
- Assisted in practical labs and exam evaluations, contributing to student success in core security modules

Cyber Security Analyst — Sep 2021 - Dec 2023

Terralogic Software Solutions Pvt Ltd — Bengaluru, IN

- Monitored and triaged **500+** alerts monthly using LogRhythm SIEM, Stellar Cyber XDR, FortiGate firewall, Palo Alto Stratos, SentinelOne EDR, Darktrace NDR, Beyond Trust IAM,, identifying and escalating **150+** high-priority incidents
- Assisted with SOC2 Audit and re-configured technical and managerial controls based on industry best practices(NIST and CIS)
- Resolved **2** separate instances of **Ransomware** Attacks on managed clients with minimal downtime.
- Mitigated several DDOS attempts on managed clients using Radware **WAF**.
- Mapped **50+** correlation rules referencing **MITRE ATT&CK** framework, mapping over **50+** custom rules
- Analyzed security incidents, fine-tuned alerts, and reduced false positives by almost **50%**
- Managed incident tickets maintaining a **100%** adherence to SLAs with every client
- Collaborated with senior analysts to develop **30+** SOPs and playbooks for smoother operations and task automation
- Worked **12** hour shifts whenever necessary, primarily in the nights, always alert and responsive to incidents

Cyber Security Intern — Jun 2021 - Sep 2021

Terralogic Software Solutions Pvt Ltd — Bengaluru, IN

- Conducted phishing simulations, prepared **10+** monthly client reports, and supported SOC and NOC operations across multiple departments
- Designed **10+** dashboards and **35+** Query filters for enhanced detection and faster threat hunting
- Integrated various threat intelligence tools like Shodan, Virustotal, Talos into existing security tools

KEY SKILLS

Security operations: *Incident management, Triage and Response, Security Solutions Deployment, Event Correlation , Alert Fine Tuning, Log and Behavior Analysis, Vulnerability Management and Threat Detection, Data Privacy and Protection , Malware and Phishing Email Analysis, VAPT, Compromise and Risk Assessment, Auditing*

Network Operations: *Network Administration, Firewall Rule Optimization, Identity and Access Management, AWS Cloud Services*

Technical: *x86 Assembly, , Bash Scripting, GDB, HTML, Cisco IOS, JavaScript, Python, Java, Perl, Lucene query, SIEM, EDR, NDR, XDR, Kibana, Wireshark, Nessus, Cisco Packet Tracer, Jira, Latex*

Frameworks: *MITRE ATT&CK, NIST SP 800-61, ISO 27001, CIS Controls, OSINT, OWASP, Metasploit*

LEADERSHIP EXPERIENCE

- Instructor – STEMX Cybersecurity Bootcamp | NJIT - Ying Wu College of Computing | Jun 2024 - Aug 2024 | Jun 2025 - Aug 2025
  - Led bootcamp sessions for high school students at NJIT, teaching cybersecurity principles and hands-on labs

EXTRACURRICULAR ACTIVITY

- External Volunteer – JerseyCTF 2025 | NJIT - Ying Wu College of Computing | Mar 2025 - May 2025
  - Designed and reviewed cryptography challenges for NJIT's Capture the Flag competition

ACADEMIC PROJECTS

- **Examining User Behavior and Trust in Free VPN Services**| GitHub | *XeLatex, Likert scale, Thematic analysis, Stratified sampling*
  - This research study investigates user trust in free Virtual Private Network (VPN) services through a primary survey of 94 general users, complemented by a secondary survey of 16 security-aware users with cybersecurity expertise
- **Salesforce Application Audit Report** | GitHub | *XeLatex, Permission set analyzer, OWASP ZAP, Checkmarx vulnerability scanner*
  - Created a complete audit plan for a hypothetical Salesforce application including risk, compliance, and mitigation analysis
- **Energy Consumption Prediction on AWS** | GitHub | *MLlib, Apache Spark, Hadoop, AWS EMR, EC2, Pyspark, Python*
  - Designed energy prediction model using Apache Spark and Hadoop in EMR clusters (4-node parallel processing)
  - Utilized dockers to containerize the application
- **AWS Cloud Image Recognition**| GitHub | *AWS Rekognition, Textract, S3, EC2, Java*
  - Developed an AWS-based application using Rekognition and Textract APIs to detect faces and extract license text
- **Network defense simulation** | GitHub |*Kibana, Suricata/Snort NIDS, Lucene query, Metasploit framework, pfSense WAF*
  - Integrated Security Onion with pfSense in a virtual lab to simulate alert generation and traffic filtering
  - Utilized Kibana dashboards for visualization through custom Lucene queries
- **Buffer overflow assessments with GDB** | GitHub | *GNU Debugger, C++, x86 Assembly, Perl*
  - Investigated memory protection bypasses in binaries using GDB with DEP, ASLR, and SSP enabled