LINTU OOMMEN

📧 oomensusan@gmail.com • 🌐 linkedin.com/in/lintu-oommen-909b2a118/

🌐 https://oomensusan.github.io/

SUMMARY

Cybersecurity professional with hands-on experience in SIEM operations, ML-driven threat detection, and automotive security. Skilled in security analytics, phishing investigation, and vulnerability assessment. Currently leading a team of 3 engineers performing technical reviews, fuzz and static testing. Actively expanding expertise in malware, forensic, and network analysis through practical challenges on TryHackMe. Seeking a Threat Research or Detection Engineering role to apply technical depth, scripting expertise, and analytical mindset to identify and mitigate evolving cyber threats.

SKILLS

- Threat Analysis: MITRE ATT&CK framework, phishing investigation, Trend Micro report analysis, Kaspersky log analysis
- Security Integration: AUTOSAR security modules, Microsoft Sentinel with on-premises infrastructure
- Vulnerability Management: Threat modeling, risk assessment, automotive security vulnerabilities
- Security Tools: Microsoft Sentinel, Splunk, Kaspersky Console, Phishing tools
- Technical Documentation: TARA documentation, Security Requirement Specification (SRS)
- Programming / Scripting: Python (for ML and security), C, PowerShell
- Networking & Analysis Tools: Wireshark, Malware analysis tools, Forensic analysis tools

WORK EXPERIENCE

Senior Engineer — Tata Elxsi (May 2023 – Present)

- Lead a team of 3 engineers conducting fuzz testing and static testing.
- Performed SAST for the source code to check for vulnerabilities using Klockwork tool.
- Lead integration of security libraries with AUTOSAR-compliant software, implementing cryptographic services.
- Automated hardware testing, reducing manual testing time by 40%.
- Automated FuSa activities using ML techniques, reducing manual effort by 50%.

- Conducted and documented TARA (Threat Analysis and Risk Assessment) using STRIDE.
- Built and maintained an automotive vulnerability database to track and prioritize vehicle system security issues.

Senior Systems Engineer — RMESI (Aug 2020 – Sep 2021)

- Implemented and maintained Microsoft Sentinel integration with on-premises infrastructure.
- Triaged and resolved security alerts in Sentinel, reducing MTTR by 30%.
- Created and maintained custom KQL-based detection rules from threat intelligence in Azure Sentinel
- Conducted analysis of Trend Micro reports to identify threat patterns and potential vulnerabilities.
- Collaborated with SOC team to fine-tune alert thresholds, reducing false positives by 25%.
- Documented incidents and developed standardized incident response procedures.

IT Support Officer — Flydubai (Feb 2018 – Aug 2020)

- Conducted phishing mail analysis and provided initial triage for suspected email threats using mail header checking tools.
- Performed log analysis using data from Kaspersky Security Console to identify endpoint-based anomalies.
- Assisted with software patching and vulnerability remediation as part of EDR activities using ManageEngine Desktop Central.
- Provided technical support for network and system issues, ensuring minimal downtime.
- Supported vulnerability scanning and network system analysis for endpoint protection using the Kaspersky EDR.
- Participated in end-user cybersecurity awareness programs.

RESEARCH & PROJECTS

- Medical Image Classification: Developed deep learning models for multi-label classification of lung diseases with imbalanced datasets.
- Security Data Analysis: Created data pipelines and visualization solutions for large-scale alert analysis.

EDUCATION

- M.Tech., Computer Science and Data Analytics — NIT Andhra Pradesh (CGPA: 9.18, Rank Holder, Computer Science & Data Analytics Department)

- B.Tech., Computer Science and Engineering — Cochin University of Science and Technology (CGPA: 8.2 / 10)

CERTIFICATIONS & PROFESSIONAL DEVELOPMENT

- Microsoft Azure Fundamentals
- MCSA Certified (MS ID: MS0616955030)
- Ongoing: TryHackMe Learning Path — Hands-on experience with:

PUBLICATIONS & ONLINE PRESENCE

Medium Blog: https://medium.com/@oomensusan

LinkedIn Profile: https://linkedin.com/in/lintu-oommen-909b2a118/

TryHackMe Profile: https://tryhackme.com/p/oomensusan

Journal Publication: 1239: Emerging Trends and Applications of Deep Learning for Biomedical Data Analysis, Published: 08 November 2024 : https://link.springer.com/article/10.1007/s11042-024-20363-z