Security Engineer Intern

Toyota Tsusho Systems India (TTSI)

Toyota Tsusho Systems India (TTS-IN) is a key IT solutions provider within the Toyota Group, dedicated to supporting Toyota's operations and its ecosystem of suppliers, dealers, and partners. TTS-IN delivers cutting-edge IT services and digital transformation solutions, including enterprise resource planning (ERP), IT infrastructure management, cloud solutions, and cybersecurity, all tailored to the unique needs of Toyota's global business processes. With a deep understanding of Toyota's philosophy, such as Kaizen and Just-in-Time, TTS-IN ensures seamless integration of technology with Toyota's operational excellence. By fostering innovation and aligning with Toyota's vision of sustainable growth, TTS-IN plays a vital role in enhancing efficiency, productivity, and security across the Toyota network in India and beyond.

Culture

At Toyota Tsusho Systems India, the culture is rooted in the principles of the Toyota Way, emphasizing respect for people, continuous improvement (Kaizen), and teamwork. The organization fosters an inclusive and collaborative environment where innovation thrives, and employees are empowered to take ownership of their contributions. With a strong focus on professional growth, work-life balance, and ethical practices, TTS-IN nurtures a culture of excellence that aligns with Toyota's commitment to quality and sustainability.

Security Engineer Intern Responsibilities

- Conceive, design & develop industry-leading security products, system and/or frameworks. Analyse and improve efficiency, scalability and stability of the existing security systems and frameworks.
- Participate in the implementation, development and improvement of SOC processes and procedures.
- Contribute to the development of thought leadership content, whitepapers, and technical publications.
- Prepare Threat Intelligence reports for newly discovered threat agents, exploits, attacks.
- Assist in the investigation of security incidents by gathering and analysing log data, generating reports, and supporting the implementation of remediation actions.
- Collaborate with cross-functional teams to ensure the integration of security best practices into system design and development processes.
- Design and develop detection use cases based on threat intelligence, MITRE ATT&CK, and emerging threats.
- Write correlation rules, KQL queries, and analytics to identify suspicious or malicious behaviour.
- Research and stay updated on emerging cybersecurity threats, technologies, and best practices to contribute to proactive defence strategies.

Be the Right ONE

Technical Skills

- **Cybersecurity Fundamentals:** Strong understanding of networking, operating systems (Windows/Linux), and common protocols such as TCP/IP, DNS, and HTTP.
- **Threat Analysis Tools:** Hands-on experience with SIEM platforms, vulnerability scanners, and endpoint protection tools.
- **AI and Machine Learning:** Familiarity with applying AI/ML concepts to cybersecurity, such as anomaly detection, threat prediction, or behaviour-based analysis.
- **Incident Response:** Basic understanding of incident detection, triage, and remediation processes.
- **Detection Engineering:** Skilled in developing behavioural detections using KQL/SPL and mapping them to MITRE ATT&CK.
- **Scripting & Automation:** Proficient in Python, PowerShell, or Bash for parsing, enrichment, and automating detection logic.
- **AI Tools:** Experience with AI platforms like TensorFlow, PyTorch, or pre-trained models for tasks such as natural language processing (NLP) or predictive analytics.
- **Log Analysis:** Familiarity with log aggregation and analysis tools like Splunk, Sentinel, ELK stack, or Graylog for monitoring and troubleshooting.

Soft Skills

- **Analytical Thinking:** Ability to assess complex problems, identify patterns, and derive actionable insights.
- **Communication Skills:** Effectively convey technical information to both technical and non-technical stakeholders, including documentation and reporting.
- **Team Collaboration:** Work cohesively with cross-functional teams, fostering a collaborative and supportive environment.
- **Adaptability:** Quickly adjust to changing priorities, technologies, and security challenges in a dynamic environment.
- **Attention to Detail:** Maintain focus on critical details while analysing data, monitoring systems, or troubleshooting issues.
- **Problem-Solving:** Approach challenges with a proactive and innovative mindset to develop effective solutions.
- **Eagerness to Learn:** Demonstrate a passion for cybersecurity and a commitment to continuous professional development.

Educational Qualifications:

- Students Pursuing **MTech.** In Cyber Security / Artificial Intelligence or in a relevant field.
- Minimum of **7 CGPA** in subsequent semesters with **no active backlogs,** and no awaited results of Pre-Active Backlogs.