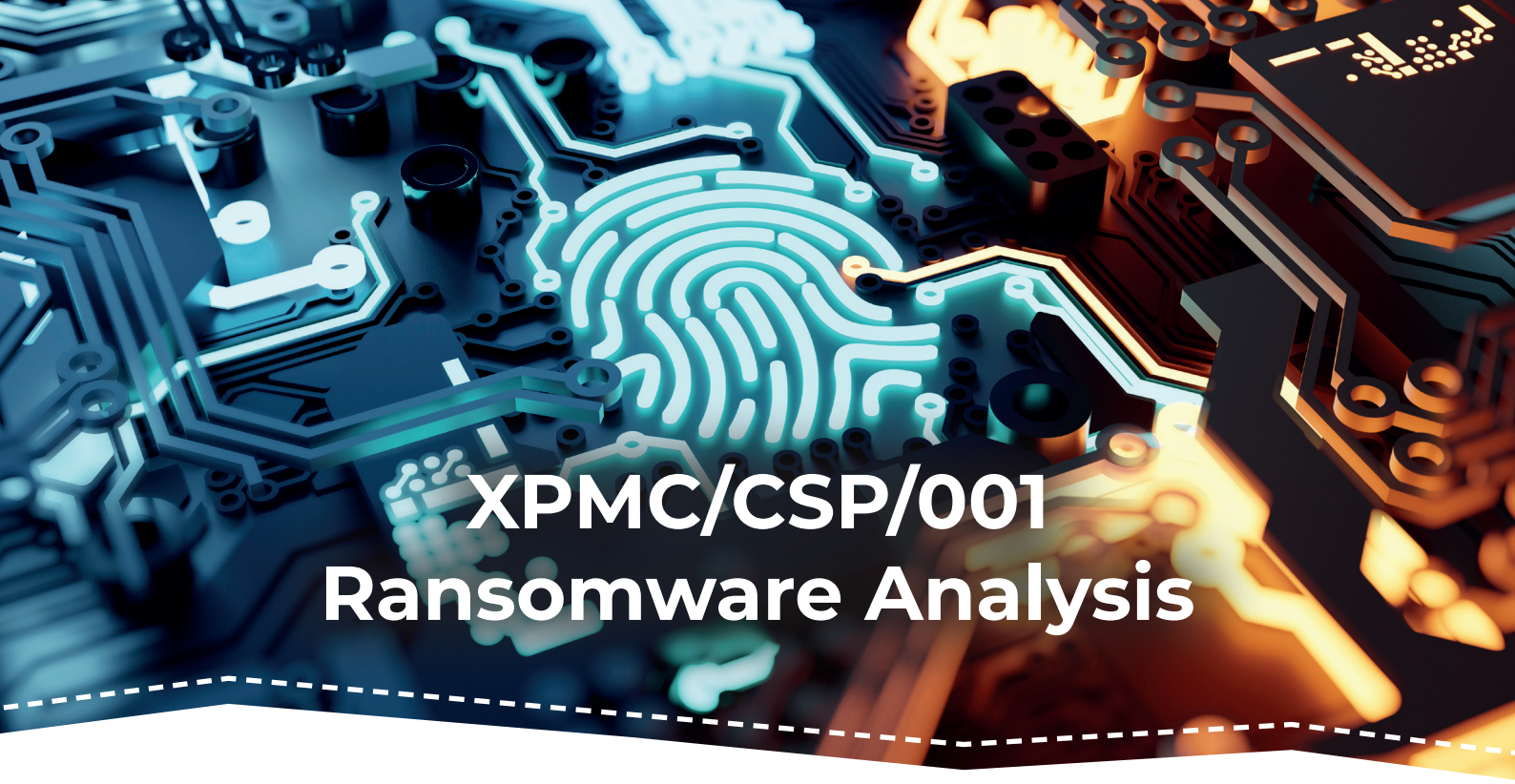

XPMC/CSP/001
Ransomware Analysis

Product Owner: Vinit Sinha, Director of Cyber Security, SME, APAC, Mastercard

Pre-req: Engineering / CS Third year

Team size: 5 to 6 members

This Cybersecurity XPMC aims to prepare Engineering students and other aspiring cybersecurity professionals on Ransomware Analysis and Detection. Working within the environment of cyber-security department, the teams will perform static and dynamic analysis of an identified ransomware, will gain an understanding of the process to conduct reverse engineering of ransomware. Understanding these processes will help learners in overcoming the most critical challenge faced by organisations in the fast-evolving digital era. The team will produce reports on their work and make their colleagues aware of potential vulnerabilities.

Structure

Sprint	Deliverable	Assessment
Sprint 1 (Week 1 – 4)	Static analysis of Ransomware	Report by the team on Ransomware code
Sprint 2 (Week 5 – 8)	Dynamic analysis of Ransomware	Report / Presentation on system vulnerability
Sprint 3 (Week 9 – 12)	Reverse engineering	Demonstration by the team on Ransomware prevention strategies

Meetings:

1. Daily project team meetings
2. Weekly review by Project Manager
3. Bi-weekly progress update to Product Owner
4. Sprint Review meetings (once a month) with full team, project manager & product owner