Security Modelling

Design / Development Phase

Threat Modelling

- Design Specifications
- System Integrator/ OEM
- System Owner / Operator

- Threat identification
- Risk assessment
- Risk mitigation strategies

Deployment / Implementation Phase

Attack Modelling

- Attack Simulations
- Cybersecurity Analysts
- Penetration Testing

- Vulnerability and red-teaming assessment
- Threat intelligence and incident analysis
- Corrective controls and actions

Operation / Maintenance Phase

Security Monitoring

- Security Operations
- Attack Surface Management
- Threat Hunting

- 24x7 security monitoring
- Digital forensics and incident response (DFIR)
- Continuous improvement based on feedback loop from threat and attack modeling

Real-world incidents inform future threat and attack models