HCLTech | Supercharging Progress™

Cybersecurity in Aerospace & Defense, maximized!

Transform your cybersecurity landscape with cutting-edge security solutions

The emergence of new-generation digital, software-intensive, and networked aircraft has presented the aerospace industry with a pressing challenge: cybersecurity.

In today's interconnected Aerospace and Defense (A&D) ecosystem, open and interconnected systems offer exciting possibilities for improved performance, passenger experiences, and new opportunities. However, they also expose the industry to cyberattacks that are growing in number and sophistication. To tackle these threats, it is crucial to first acknowledge them and then improve our aircraft operations and air traffic control systems.

Looking ahead, the A&D industry will face a big challenge in the form of an increasingly complex and highly distributed supply chain. High interdependence among supply chain elements present a challenge because various composite systems are accessible and operated by multiple organizations. Consequently, these highly sensitive systems find themselves in an exceedingly vulnerable position, prone to cyberattacks.

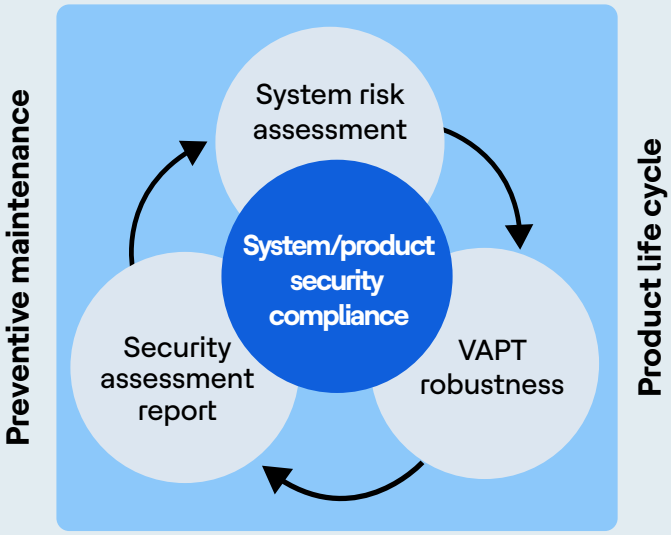
Cybersecurity is fundamental in this digital age

HCLTech's comprehensive cyber security advisory services

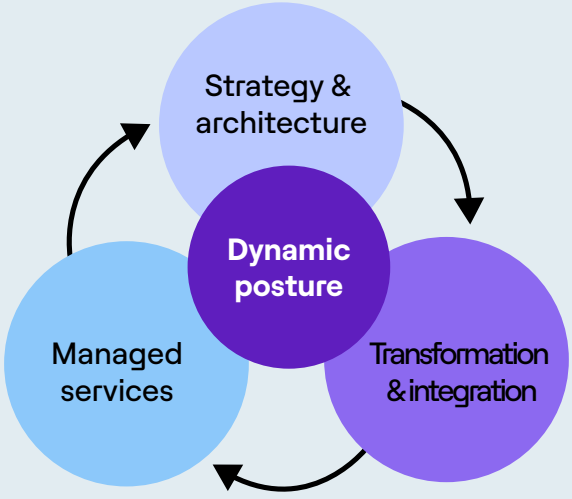
In a dynamic threat landscape, A&D organizations need to assess the current state and establish a cybersecurity posture that adapts and evolves to effectively mitigate emerging risks.

Our phased approach enables organizations to:

- Evaluate the security of the product or system under assessment
- Prevent security breaches in early stages
- Approach security from a design execution perspective
- Keep the system/product up-to-date throughout their lifecycle
- Avail add-on features, maintenance interventions and obsolescence of software components through preventive assessment



HCLTech integrated cyber security services



Enabling cyber protection at scale across the A&D ecosystem

Specific team competence

World-class certified expertise across different vertical technology landscape

- Ethical hacking
- Information security
- Cloud security
- Best practices:
  - CSA (Cloud Security Assessment)
  - OWASP (Open Web Application Security Project)
  - NIST SP 800 Series

Managing the ecosystem

- HCLTech has a large portfolio of commercial and open source security tools
- HCLTech security approach is the same, irrespective of the verticals, but the assessment, methodologies, tools and licenses used are specific to different areas

Managing technology transformation

- Security robustness in network transformation to prevent new types of threats in areas such as cloud & SDN
- IoT: Network architecture security assessment for preventing vulnerability threats in huge and distributed networks
- Telecom OEMs: Core competence and knowledge for securing application, network or product

Service offering

Anticipate and identify security threats before customer enters new services or delivers an E2E solution:

- TARA: Threat Analysis and Risk Assessment
- VAPT: Vulnerability Assessment Penetration Test
- Robustness testing
- Security improvement guidelines
- Security s/w feature development

Assessing customer applications

Security assessment as well as penetration tests can be carried out:

- Remotely - working through internet connections to access customer's applications
- Local lab installation

Multi-customer support

Assess the security level, the vulnerability risk and enforce the security robustness for each customer's application, domain or service, independently if local or cloud-based

VAPT- Vulnerability Assessment and Penetration Test

Discover. Assess. Fortify.

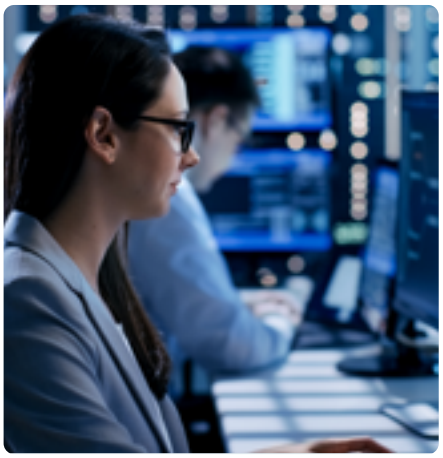
In each phase of the test, a series of evaluation steps are undertaken, allowing for customization and alignment with the assessment's complexity and domain/market-specific regulations.

Risk assessment and threat

- Security architecture identification
- Requirement analysis
- System threat identification
- Requirements GAP analysis

Customer value

- Preventive threat identification
- Security requirement fulfilment
- Proactive security design
- Predictive/protective maintenance of system security



Vulnerability and penetration testing

- Security test procedure and plan
- Vulnerability assessment
- Penetration testing
- Robustness/stress
- Predictive/protective maintenance of security
- Testing for improved protection

Customer value

- Preventing security breaches from early stages
- Business continuity when under attack

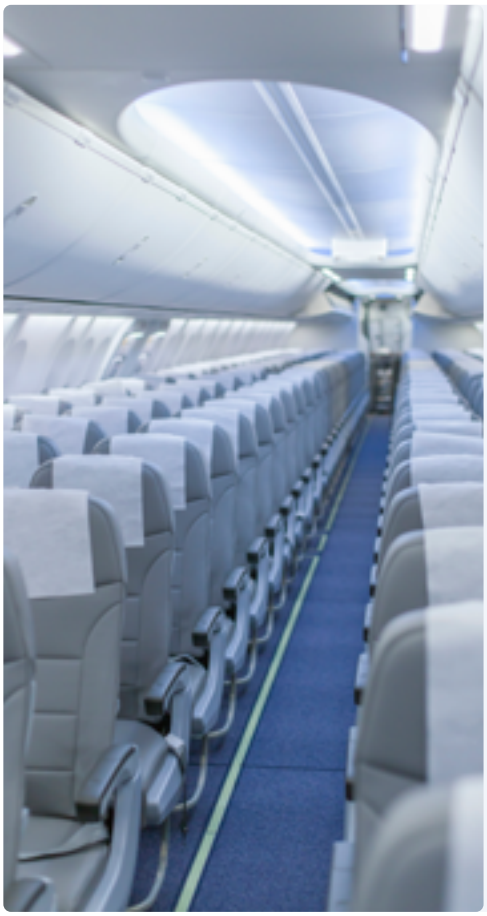
Security assessment report

- Architecture improvement
- Missing security requirements
- VAPT recommendations
- Stress test weakness report

Customer value

- Security accelerator for hacking prevention
- Proactive approach to security compliance
- Suggestion of mitigation actions

Success stories cementing our expertise



Network System Risk Assessment and VAPT* for cabin network infrastructure

Solution

- Analysis of system network configuration
- Assessment of security architecture and completeness of security requirements
- Threat assessment of the system to evaluate weakness of overall solution
- Identification of threats and vulnerabilities
- Assessment by penetration testing (VAPT)
  - Protocols and interfaces (man in the middle) and brute force tests on proprietary protocol
  - Full vulnerability scanning; patch auditing
  - Robustness tests
  - CVEs (Common Vulnerabilities and Exposure) exploits
- Final reporting as per aviation certification requirement FAA (Federal Aviation Administration) /EASA (European Aviation Safety Agency)

*VAPT – Vulnerability Assessment and Penetration Testing

Evaluate security vulnerabilities for an overall RAN backhaul data transmission solution

Solution

Threat analysis and risk assessment

- Analysis of architectural and system configuration.
- Gap analysis for Identification of vulnerabilities
- Assessment for penetration testing (VAPT)
- Robustness testing executed on Telco protocols
- Assessment reporting

The HCLTech advantage

Standard based – leveraging industry technology and process standards NIST, ISO/IEC, SANS/CSC, COBIT, EC-Council, FIPS, HIPAA, SAE, FAA

Multiple guidelines and best practices knowiedge

- CSA (Cloud Security Assessment)
- OWASP (Open Web Application Security Project)
- NIST SP 8OO series

Customer-centric and world-class certified experts across different vertical technology landscape

Ethical hacking approach – CEH, CISSP, ISO 27001 certified