

NEXT-GEN Cybersecurity Services



The new generation digital, software intensive and networked aircraft have resulted in a new challenge for the aerospace industry which is Cybersecurity.

Today the A&D ecosystem is interconnected and more open to the outside world than ever before. Open, interconnected systems bring new opportunities, better performances and passenger experience, and new cyber risks as threat surface and threat vectors increase. No computer system, including the systems used to fly aircraft or control air traffic, can ignore this fact, especially in view of the potentially devastating consequences of an attack.

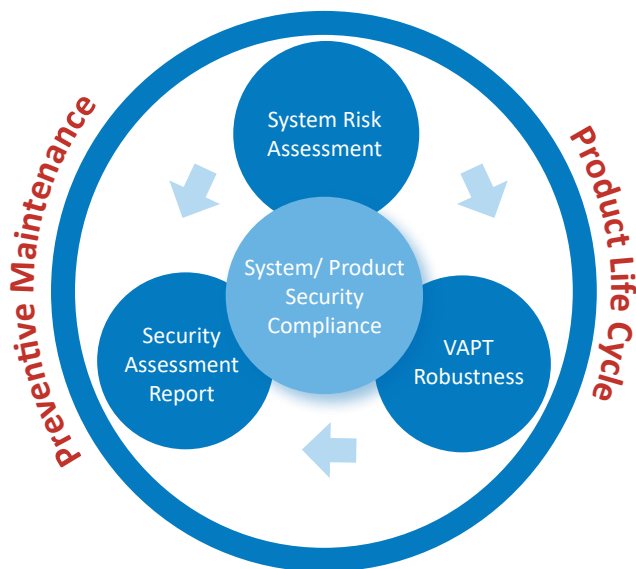
A major challenge that A&D industry would face going forward is due to their complex and highly distributed supply chain. The large interdependence between supply chain elements poses a challenge as composite systems are accessible and operated by multiple organizations. This places these highly sensitive systems in an extremely vulnerable position and ripe for cyber-attacks.

SECURITY - LIKE FLIGHT SAFETY - IS A BASIC REQUIREMENT IN THIS DIGITAL AGE

HCL CYBER SECURITY ADVISORY SERVICES

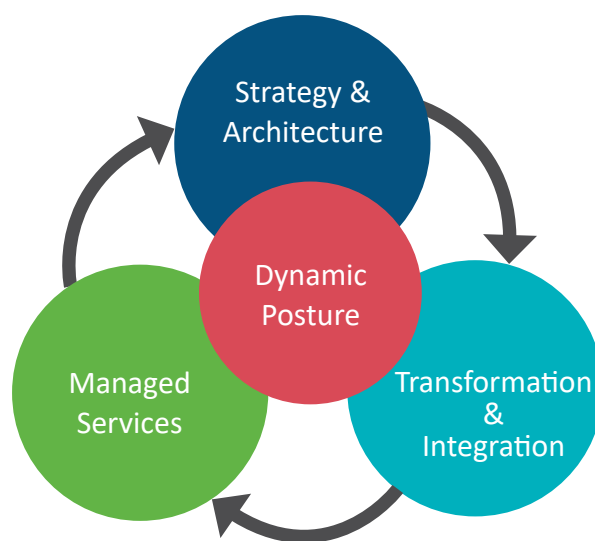
With an ever evolving threat landscape it becomes a necessity to assess the current state to define an adaptive & evolving cybersecurity posture for your organization. HCL's phased approach allows:

- Progressive evaluation of the security of the product or system under assessment



- Preventing Security Breaches from early stages
- Approaching security from design execution perspective
- Keeping the system/product up-to-date along their lifecycle
- Guaranteed security of the add-on features, maintenance interventions and obsolescence of software components through preventive assessment

HCL CYBER SECURITY SERVICES ACROSS DOMAIN



VAPT- VULNERABILITY ASSESSMENT AND PENETRATION TEST

Each phase comprises of several evaluation steps, which can be adapted and tailored according to the complexity of the assessment and applicable standard rules of the domain/ market.

RISK ASSESSMENT

Risk Assessment & Threat Analysis

- 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/ PENETRATION

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



CYBERSEC. ASSESSMENT REPORT

Security Assessment report

- Architecture Improvement
- Missing Security Requirements
- VAPT recommendations
- Stress Test Weakness report

Customer VALUE

- Security Accelerator to Hacking Prevention
- Proactive Approach to Security Compliance
- Suggestion of Mitigation Actions



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

- HCL has a large portfolio of commercial and open source security tools
- HCL security approach is the same, irrespective of the vertical domain, but the used assessment methodologies, tools and licenses are specific for the different areas



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

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

Managing Technology Transformation

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

Service Offering

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

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

HCL DIFFERENTIATORS

- ✓ Customer centric and world-class certified experts across different vertical technology landscape
- ✓ Ethical hacking approach - CEH, CISSP, ISO 27001 certified
- ✓ Multiple guidelines and best practices knowledge
 - CSA (Cloud Security Assessment)
 - OWASP (Open Web Application Security Project)
 - NIST SP 800 series
- ✓ Standard based – leveraging industry technology and process standards NIST, ISO/IEC, SANS/CSC, COBIT, EC-Council, FIPS, HIPAA, SAE, FAA
- ✓ Vendor agnostic- partnership with 40+ OEMs

1

Network system risk assessment and VAPT* for cabin service infrastructure

**VAPT- Vulnerability Assessment and Penetration Test a.k.a. Robustness Test*

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 exploits
- Final reporting as per aviation certification requirement (FAA/EASA)

2

Evaluate security weakness for an overall RAN backhaul data transmission solution

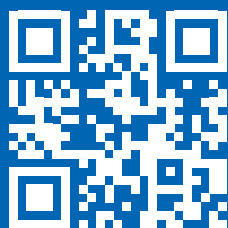
Solution

- 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



HCL Technologies (HCL) empowers global enterprises with technology for the next decade today. HCL's Mode 1-2-3 strategy, through its deep-domain industry expertise, customer-centricity and entrepreneurial culture of ideapreneurship™ enables businesses to transform into next-gen enterprises.

HCL offers its services and products through three lines of business - IT and Business Services (ITBS), Engineering and R&D Services (ERS), and Products & Platforms (P&P). ITBS enables global enterprises to transform their businesses through offerings in areas of Applications, Infrastructure, Digital Process Operations, and next generation digital transformation solutions. ERS offers engineering services and solutions in all aspects of product development and platform engineering while under P&P. HCL provides modernized software products to global clients for their technology and industry specific requirements. Through its cutting-edge co-innovation labs, global delivery capabilities, and broad global network, HCL delivers holistic services in various industry verticals, categorized under Financial Services, Manufacturing, Technology & Services, Telecom & Media, Retail & CPG, Life Sciences, and Healthcare and Public Services.



www.hcltech.com

As a leading global technology company, HCL takes pride in its diversity, social responsibility, sustainability, and education initiatives. As of 12 months ending on March 31, 2020, HCL has a consolidated revenue of US\$ 9.9 billion and its 150,423 ideapreneurs operate out of 46 countries. For more information, visit www.hcltech.com