

Security services for semiconductor ecosystem



Securing manufacturing environments for decades

To match the rising semiconductor demands, foundries are adopting latest technologies, modern ways of supply chain operations and implementing smart manufacturing operations to improve the efficiency, leaving Fab/OSAT vulnerable and making it essential to tighten the cybersecurity practices. Semiconductor equipment's play vital role in foundries and it is critical to secure them from malware and threats in the smart manufacturing environment.

HCLTech has dedicated CoEs for cybersecurity to secure smart manufacturing, equipment and software product level. Our domain expertise and in-depth understanding help us innovate frameworks and solution accelerators, which leveraged us in addressing 1000+ security projects across multiple industries. We have established security partners, security alliances and IT security ecosystem.

We are the leading Engineering and R&D services (ERS) organization that offers engineering services to semiconductor OEM, Fab and OSAT, by leveraging over 22 years of experience in the semiconductor domain covering process, inspection and test equipment. Our services also include software development and testing, mechanical, electrical and digital transformation services such as cybersecurity, IoT and smart manufacturing.

Security propositions for Semi OEM, Fab and OSAT

Semi equipment is a complex environment which needs multiple layers of protection. Operational Technology (OT) cybersecurity services, Operating System (OS) hardening of equipment computers, equipment software (SW) application SecOps practices and different layers of protection techniques can help to secure the equipment and Fab environment against threats and vulnerabilities.

1 Secure smart manufacturing

- Endpoint protection
- System and security updates
- OS end-of-life counter measures
- Security Content Automation Protocol (SCAP) scanning
- Field service scenarios support
- Malware scanning
- Secure data handling
- Secure decommissioning guidelines

2 Secure equipment

- Malware scanning report
- SCAP scanning
- Access control and authentication
- Endpoint protection
- Network service hardening
- Network segmentation and connection
- Patch management

3 Secure product

- Security requirement definition
- Secured architectural design
- Secure coding practice
- OS hardening
- Penetration testing
- Threat modelling
- Vulnerability assessment



Security services



Information
technology



Operational
technology



Engineering
technology



Supply chain



Software



Third party



Manufacturing



Data



Equipment

Solutions and accelerators



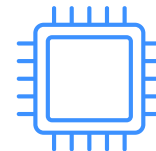
Engineering technology security services

- Device security CoE
- 350+ industrial security SMEs
- Secure engineering framework
- Unified vulnerability management
- DevSecOps, NSure automation framework
- Penetration testing



Operational technology security services

- 360-degree secure OT framework
- 1000+ OT security project executed
- IT – OT convergence cybersecurity strategy and architecture
- 4-dimensions of an industry addressed: Assets, People, Technology and Process/ Compliance

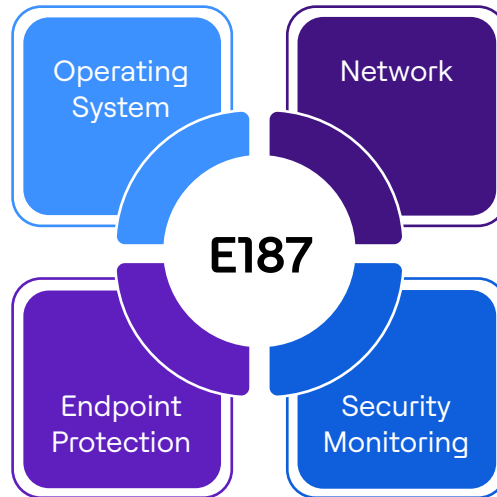


Information technology security services

- IEM – for security alerts and event monitoring
- Managed network security service
- Managed endpoint security service
- SOC advisory as a service
- Effective steady-state security operational support
- Effective security incident and event management

Enabling semiconductor security standards

- E187: Specification for Cybersecurity of Fab Equipment
- E188: Specification for Malware Free Equipment integration into FAB manufacturing environment

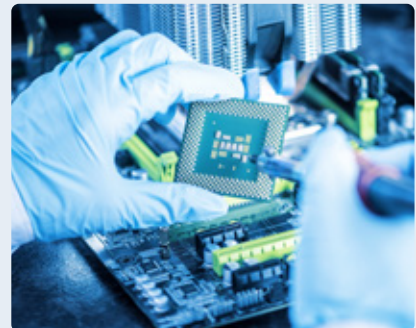


Case studies

1

Semiconductor Test Equipment (ATE) customer needs to provide their customers with a secure tester computer environment to resist malicious attacks.

- Established procedures and process for hardening images for seven tester platforms and industrial PCs.
- Automation framework for compliance verification and scan images at regular cadence.



2

Leading supplier of semiconductor process equipment required new Managed Security Service (MSS) provider for monitoring and management.

- Design and implementation services for end-to-end security architecture with network security, endpoint security, Security Information and Event Management (SIEM) and log management.



Over the years, our unique solutions, frameworks and domain expertise enabled us to build advanced security offerings for the semiconductor industry, helping us to successfully implement projects for OEM, Fab and OSAT. Learn more about how HCLTech can help you in supercharging your semiconductor innovation journey. Reach us at hclsemi@hcl.com.

HCLTech | Supercharging Progress™

HCLTech is a global technology company, home to 225,900+ people across 60 countries, delivering industry-leading capabilities centered around digital, engineering and cloud, powered by a broad portfolio of technology services and products. We work with clients across all major verticals, providing industry solutions for Financial Services, Manufacturing, Life Sciences and Healthcare, Technology and Services, Telecom and Media, Retail and CPG, and Public Services. Consolidated revenues as of 12 months ending March 2023 totaled \$12.6 billion. To learn how we can supercharge progress for you, visit hcltech.com

hcltech.com

