HCLTech | Supercharging Progress™

Maximize organizational security investment with HCLTech's 360° SecureOT

Delivering robust enterprise security with an adaptive OT framework through Microsoft Defender for IoT

Overview

As traditional measures such as establishing demilitarized zones (DMZs) and air-gapping lose their relevance, protecting operational technology (OT) systems has become increasingly complex. The rise of Industry 4.0 has effectively fused IoT and connected devices with AI/ML, Robotic Process Automation (RPA), additive manufacturing, advanced analytics, blockchain and similar technologies across new business models and solutions. And the integration of IoT within modern OT environments has also resulted in greater complexity due to the inherent reliance on cloud access and internet connectivity.

As OT and IT become irreversibly interlinked, OT security can no longer address the gaps between sophisticated IT threats and OT security, leaving vital systems vulnerable. In a few short years, traditional OT environments have been laid bare to global threats with critical applications becoming the prize target for bad actors. As a result, organizations need to reassess their security posture by seeking intelligent security solutions that can help them ensure close threat monitoring to minimize systems downtime and ensure operational resilience.

Business challenges

Today, the volume of attack surfaces often goes beyond the security perimeter of the existing organizational network. OT security is also plagued by diverse IoT systems spread across the enterprise, resulting in a lack of visibility and third-party access. The rising convergence of OT/IT and remote maintenance is increasing the threat and attack surfaces. With the advancements in the IoT layers of edge computing, physical devices and cloud applications, modern enterprises face challenges in security deployment.

- Lack of cybersecurity governance, security policies, risk management, resilience planning and cybersecurity strategy
- Lack of security threat monitoring and incident response capabilities (SOC)
- Absence of comprehensive cybersecurity training and awareness programs for employees
- Inadequate resilience planning for natural or man-made (cyber) disruptions.
- Unmanaged attack surface on OT networks
- Weak identity and access management practices including the use of static passwords and limited control over vendor/ contractor access
- Flat networks with minimal or no segmentation, allowing for convenient traffic movement

Our solution

Cyber-monitoring is necessary to detect, prevent and respond to disruptive incidents in an OT environment. It involves risk and threat baselining of OT asset inventories and conducting constant security checks of an organization's networks, systems and information. Continuous monitoring of ingress and egress network traffic can detect malicious activities in the OT environment.

HCLTech's 360° SecureOT framework has been specially designed to enable enterprises to assess, define, strategize and handle their OT landscape in accordance with industry-accepted standards and cybersecurity guidelines. The framework covers the 4 dimensions vital to any OT landscape- people, technology, assets, process and compliance. We specialize in deploying Microsoft Defender for IoT, an agentless monitoring solution to the digital infrastructure of enterprises with HCLTech's 360° SecureOT solution.

HCLTech's 360° SecureOT framework – Capabilities

Identification

- Asset discovery
- Network topology mapping
- Identifying unauthorized remote access and weak credentials

Protection

- Automated OT threat modeling
- OT vulnerability management and risk mitigation
- Native integration with firewalls and network access control (NAC)

Recovery

- Automated reporting to stakeholders
- Alerting on failed backups

Detection

Continuous OT monitoring with patented behavioral anomaly detection

Response

- Deep forensic and threat hunting tools
- Native apps for SIEM integrations
- Integration with IT service management (ITSM) and orchestration tools (SOAR)

Managed Services

- Support from a team of skilled and experienced security analysts
- In-built security analytics and detection engine for actionable threat intelligence
- 24/7 global coverage

HCLTech's 360° SecureOT framework – Features

IoT/OT asset discovery

- OT/IoT/ICS device discovery in the enterprise environment
- Communication between different OT/IoT devices

Risk and vulnerability management

- Identification of risks associated with major IT/OT assets
- Prioritization of risk management for major IT/OT assets

Constant IoT/OT threat monitoring, incident response and threat intelligence

- Identification of risks and zero-day vulnerabilities related to IT/OT assets
- Timely mitigation of identified risks

Operational efficiency

- Detection of malicious activities with IoT/OT-aware behavioral analytics, machine learning and threat intelligence
- Micro segmentation with zero-trust-based access to IoT/OT devices

Value Delivered

HCLTech's 360° SecureOT through Microsoft Defender for IoT delivers immense value to enterprise operations, as has been proven across our various client engagements. Some of the key benefits of this comprehensive solution include:

Risk-based visibility

- Real-time monitoring of anomalies in connected systems and data-flow communication
- Analytics-powered operations platform, improving detection times and providing granular reporting

Controls effectiveness

- Design and implementation of cybersecurity solutions aligned with industry standards and regulatory compliances -ISA/IEC 62443, NIST, NERC CIP, etc.
- Global pool of experienced OT/ Cybersecurity architects for pragmatic solution design and implementation

Execution excellence

- Planning and deployment of solutions into OT environments with minimal downtime, leveraging our OT experience across industry verticals
- Drive awareness with OT stakeholders and promote successful technology adoption with the help of SMEs with prior experience across OT environments

Contextual threat intel

- Management of security services as a MSSP for global customers for visibility and access to the latest threat vectors across geographies and industrial verticals
- In-house threat hunting and intelligence research teams for successful mitigation of threats

Delivery ecosystem

- Access to a mature partner ecosystem with global reach, across both OT automation and OT cybersecurity OEMs
- Access to a network of global field services organization, across 100+ countries, delivering complete local support at remote site locations

HCLTech | Supercharging Progress™

hcltech.com

HCLTech is a global technology company, home to 222,000+ 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 December 2022 totaled $12.3 billion. To learn how we can supercharge progress for you, visit hcltech.com.