HCLTech | Supercharging Progress™

Unlocking **security excellence** with HCLTech UMDR and Microsoft XDR

Introduction

In the current landscape of enterprise operations, the IT ecosystems have reached a point of unprecedented complexity, extending across multiple clouds and connecting with services and devices beyond secure network boundaries. Navigating this complexity requires a robust security approach. Organizations are increasingly adopting diverse security controls to safeguard hybrid and remote infrastructures, emphasizing the need for a centralized security monitoring platform. This platform is essential not only for detecting but also for effectively mitigating security threats and incidents.

Enter HCLTech Universal Managed Detection and Response (UMDR) service, a transformative solution powered by Microsoft XDR (Sentinel+ Defender). HCLTech UMDR provides a comprehensive suite of Managed Detection and Response services, enveloping the entire spectrum of IT landscapes — from Security Monitoring to Threat Detection and Response. Anchored in principles of inclusivity, collaboration, resilience, and adaptability, HCLTech UMDR is crafted to mitigate the impact of sophisticated threats. Its core mission is to empower enterprises to make informed decisions, optimize security operations, adhere to regulatory and privacy requirements, and scale their quantitative cyber risk management programs.

Business challenges

Lack of visibility:
Many organizations struggle to attain complete visibility into their expansive enterprise environments, extending beyond endpoints. Enhanced visibility is crucial for streamlined threat detection and response.

Lack of preventive threat hunting:
Relying on reactive measures leaves enterprises vulnerable. The absence of proactive threat-hunting hampers the ability to detect and respond to potential cyber threats before they inflict significant damage.

Complexity of threat landscape:
The ever-evolving cyber threat landscape introduces constant challenges. Staying ahead and ensuring protection against emerging threats becomes a never-ending challenge for organizations.

Shortage of skilled personnel:
Cybersecurity is a specialized field that needs an elevated level of expertise. Organizations struggle to find and retain skilled cybersecurity personnel, making managing an effective MDR solution challenging.
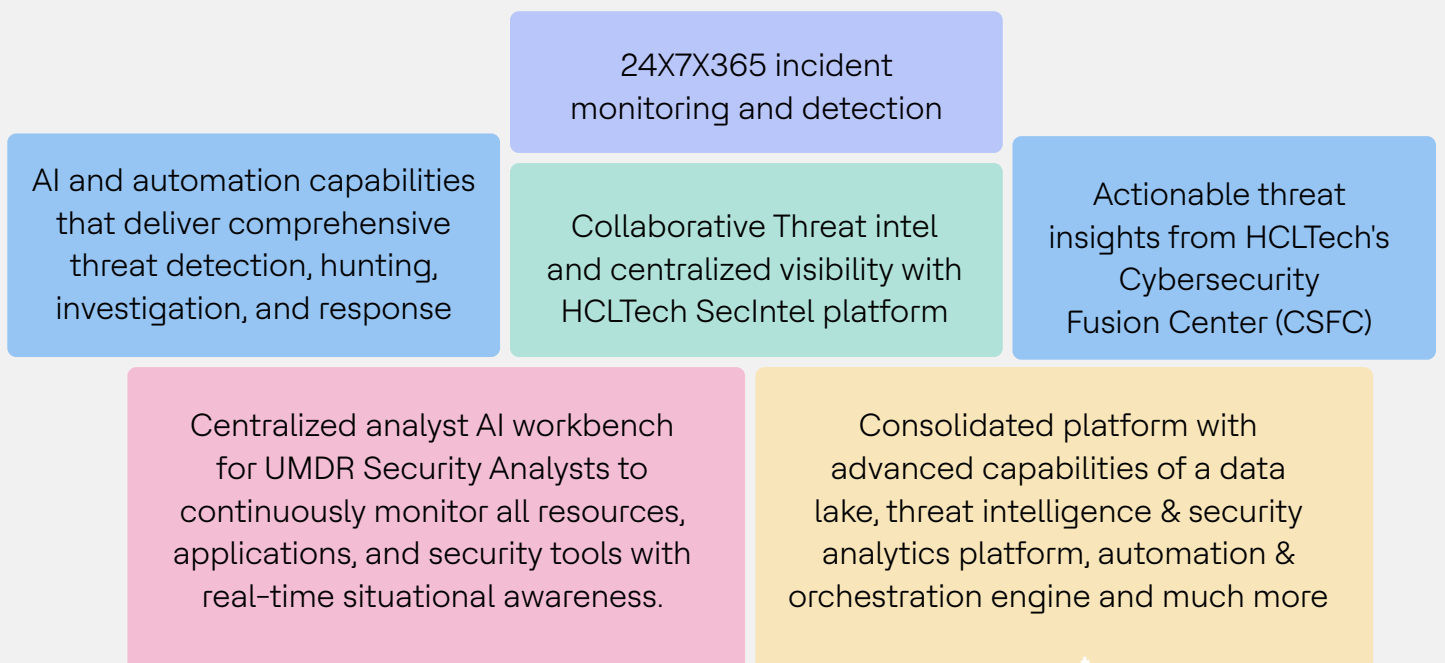
Diversified approach:
Enterprises use various security tools and technologies, which can lead to integration challenges and security gaps and give a disintegrated view of the security logs, making it hard for the monitoring team to detect and respond to security incidents.

Our solution

HCLTech UMDR service powered by Microsoft XDR addresses the existing and future security requirements. The solution offers Managed SOC and threat management with holistic coverage of security signals across the IT estate, including endpoints, networks, OT–IoT, cloud and applications for automated threat detection, investigation, triage, and mitigation on the same solution platform.
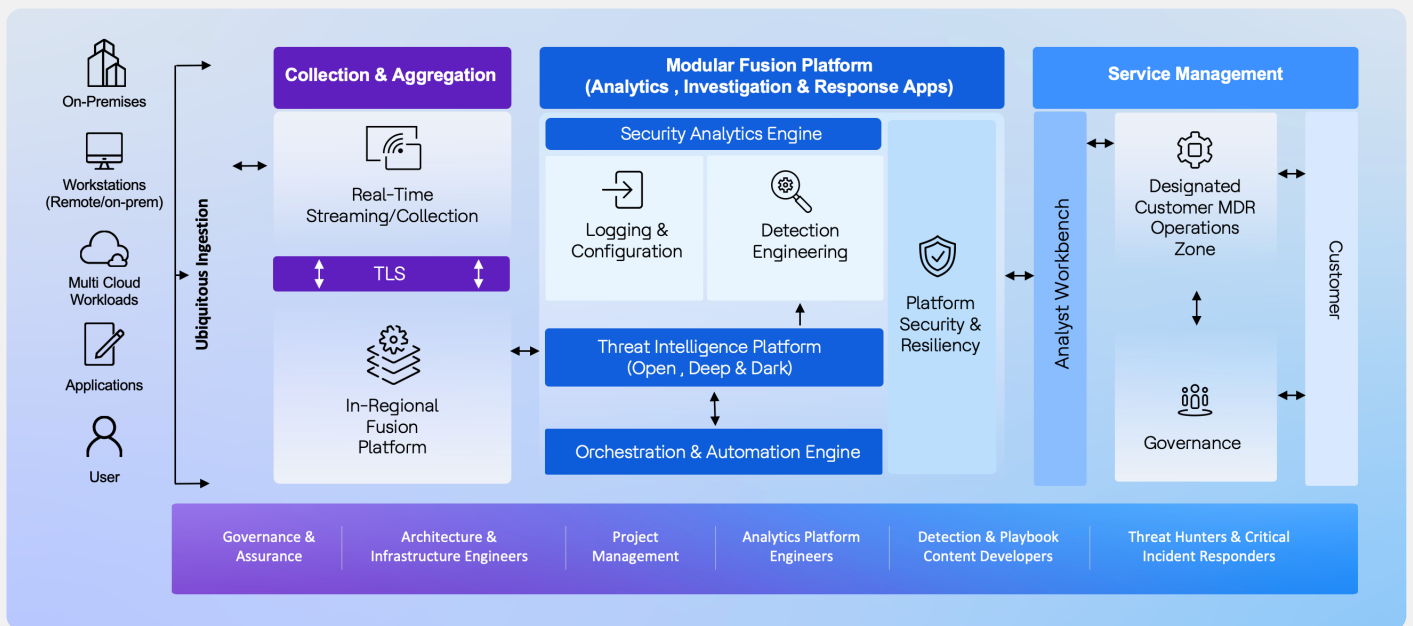
HCLTech UMDR, with its SecIntl Platform, amalgamates with Microsoft threat detection solutions, including Microsoft Defender for Endpoint (MDE), Microsoft Defender for Office 365 (MDO), Microsoft Defender for Coud Apps (MDCA) and Microsoft Defender for Cloud (MDC) , takes ownership of every incident with AI and automation first approach, providing a single security touchpoint for all security needs. The Key features of the HCLTech UMDR are:

24X7X365 incident monitoring and detection

AI and automation capabilities that deliver comprehensive threat detection, hunting, investigation, and response

Collaborative Threat intel and centralized visibility with HCLTech SecIntel platform

Actionable threat insights from HCLTech's Cybersecurity Fusion Center (CSFC)

Centralized analyst AI workbench for UMDR Security Analysts to continuously monitor all resources, applications, and security tools with real-time situational awareness.

Consolidated platform with advanced capabilities of a data lake, threat intelligence & security analytics platform, automation & orchestration engine and much more

Value delivered

Robust MDR solution that offers scalability, easy integration, customization, and enhanced threat protection

Efficient and effective Global delivery with 6 Cyber Security Fusion Centers (CSFCs) & multiple regional satellite SOCs

50% higher detections backed by custom detection logic and use cases

10-20% effort & cost saving

10-15% faster time to onboarding

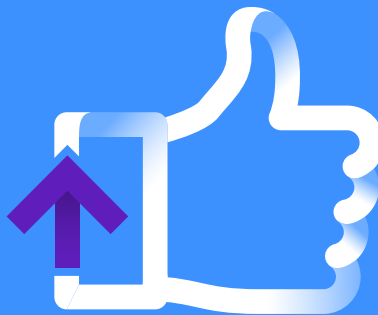## HCLTech UMDR Capability

1.

25+ years of experience in cyber security

2.

40+ collaborative threat intel sources

3.

150+ out-of-the-box custom integrations and **100+** automation playbooks

4.

120+ MDR customers

5.

HCLTech Positioned as a **Leader** in Everest Group MDR PEAK Matrix in 2022

HCLTech | Supercharging Progress™

hcltech.com