

HCLTech UMDR powered by Google



Modern businesses face a multitude of cyber threats that can disrupt operations and compromise sensitive data. To effectively combat these threats, organizations require robust Managed Detection and Response (MDR) services that provide comprehensive security coverage. HCLTech, in partnership with Google Cloud Security, offers a unique MDR solution that addresses these needs and much more.



Drivers for MDR Services

The need for MDR services arises from several key factors:



Cost optimization leveraging best practices, accelerators and IPs.



Elimination of blind spots caused by data silos, tool sprawls, and/or cloud shift.



Vendor & technology consolidation through a robust MDR service.



Access to cutting-edge security technologies such as AI and ML for context-driven security.



Access to skilled in-house IT talent on tap.








Strong integration within the enterprise security stack for comprehensive data analytics.



Automation-led detection & response techniques and proactive threat hunting.

HCLTech Supercharges Your E2E MDR Adoption Journey

 Assess	 Plan & Design	 Migrate / Deploy	 Integrate and Optimize	 Run
<p>SOC (Process/Tech) Assessments</p> <hr/> <p>Enabling customers to gain insights into current state, develop an overall strategy /A detailed cost-benefit analysis and a roadmap for enterprise wide implementation</p> <hr/> <p>Indicative Services Include</p> <ul style="list-style-type: none"> • Strategy Workshop • SOC As-Is Assessment • Breach Likelihood assessment • Technology Consolidation/ Migration Assessment 	<p>TD&R Planning, Design & Transformation</p> <hr/> <p>Assists Customers with process or technology related to architectural, orchestration & automation and other tasks necessary for faster and more vigilant threat detection & response</p> <hr/> <p>Indicative Services Include</p> <ul style="list-style-type: none"> • Discovery & Analysis • HLD & LLD custom architecture design Build • Detection rules & Automation playbooks design • Platform management & orchestration planning 	<p>TD&R Platform Migration and HCLTech Platform deployment</p> <hr/> <p>Enabling customers to deploy a robust Threat Detection & Response platform quickly for modern enterprise environments and enable end-to end visibility</p> <hr/> <p>Indicative Services Include</p> <ul style="list-style-type: none"> • Deploy Platform stacks and modules offer as a service • Migration of legacy to HCLTech Platform • Technology Evaluations/POC 	<p>TD&R Platform integrations</p> <hr/> <p>Allows Customers the flexibility to integrate & leverage existing tools, processes & legacy systems aligned with HCLTech's open platform approach</p> <hr/> <p>Indicative Services Include</p> <ul style="list-style-type: none"> • Fusion Platform Implementation & Integration • Tools & Processes integration 	<p>TD&R Regular Business as usual</p> <hr/> <p>Leverage our proven Managed Threat Detection & Reponse services capabilities to proactively monitor your dynamic environment and hunt down threats</p> <hr/> <p>Indicative Services Include</p> <ul style="list-style-type: none"> # Fusion MDR Services # Service level measurement and improvement # Platform Management # Proactive Threat Hunting # Remote Incident Response Services

IPs

Fusion Platform | SecIntAI | VERITY | CSaaS | MiDaaS | 360° SECUREOT | CSFC

Accelerators

SOC Reference Architecture

Threat Simulations

Detection Use case catalog

Log Configuration and onboarding guides

Automation playbook Catalog

Analyst workflows and Incident handling Run books

Threat Hunting query libraries

Pre-configured persona based dashboards

Value Delivered



A balanced blend of technology and human-informed decision-making providing a reliable overlay for threat management powered by Google Security Suite.



A flexible, modular approach to threat detection and response designed to prevent vendor lock-in and facilitate easy consumption.



Comprehensive detection and response coverage for complex environments including OT/ICS, cloud, Identity and Apps.



Support throughout the lifecycle of an incident. We don't merely alert; we take ownership of the incident.



Continually updated threat intelligence for automated alert enrichment and contextual threat advisories.



Proactive exploration and hunting against persistent threats.



Access to a dedicated security advisor and a team of experienced experts.



Rapid deployment and protection from day one with customized detections for unique use cases enhancing security operations efficiency.

UMDR and Google Security: A powerful combination

Threat detection and response can be challenging! However, we've been enhancing the security posture of global enterprises and have been a trusted partner for over 25 years. Harness the power of HCLTech's expertise and experience coupled with Google's robust suite of security products and cloud scale:

1. A robust technology stack powered by Google Chronicle analytics, orchestration and automation engines.
2. Streamlined SOC processes supercharging uMDR security analysts and boosting productivity.
3. An open platform approach that allows you to scale Security Operations as your business expands.
4. Scalability and predictability with continuous service improvements.
5. Deep knowledge with experienced experts, IPs and service accelerators that help us start on the right foot.
6. Global Cyber Security Fusion Centre delivery presence with flexible and modular consumption models.

