HCLTech | Supercharging Progress™

Managed Detection and Response for AWS

Leverage cutting edge security expertise with HCLTech's CyberSecurity Fusion Center

Overview

Enterprises are rapidly accelerating the pace at which they're moving workloads to Amazon Web Services (AWS) for greater cost, scale, and speed advantages. With AWS you can leverage the latest technologies to experiment and innovate more quickly. AWS continues to be the preferred choice among enterprise public cloud providers and is a leader in cloud infrastructure and platform services.

Challenges

Organisations using more multi-cloud and hybrid environment, Security Operations face challenges to have a holistic view of cloud environments.

Attackers developing new attack vectors to circumvent the detection and response measures.

Multiple security tools to secure the cloud and hybrid environments often in silos

Lack of skilled security analysts to be able to rapidly pull information from across multiple sources and provide accurate analysis

HCLTech Solution

HCLTech's AWS Managed Detection and Response service helps enterprises achieve a 360-degree visibility of their cloud operations. This helps organizations enhance their IT resilience and ensure a seamless management of their AWS cloud infrastructure. The key capabilities enabled by HCLTech include:

1. **24/7 Response**

   HCLTech detects, triages, and alerts customers of high priority security findings on a continuous uninterrupted basis, 24 hours a day and 7 days a week.

2. **Monitoring**

   HCLTech enables the proactive and constant monitoring of an enterprises' AWS environment for any threats or vulnerabilities.

3. **Triage**

   HCLTech can assess and enrich the security findings in a customer's AWS Environment by providing additional context and actionable information that helps reduce false positives and effectively respond to incidents while also assessing degree of urgency of each vulnerability.

4. **Remediate**

   Once a vulnerability or threat has been found, HCLTech supports customers with remediation guidance to help resolve the issues within their environment.

5. **Engage MSSP Support**

   Alternatively, customers can also empower HCLTech with the ability and permissions to perform the remediation steps directly or deploy an automation solution for the customer.

HCLTech's CyberSecurity Fusion Center

HCLTech's Cybersecurity Fusion Center (CSFC) integrates with AWS resources to consume the logs which further get correlated, enriched, and contextualized for appropriate response actions through CSFC's central work bench 24X7, 365 days a year. This includes critical features such as:

- Providing a much-needed unified approach by integrating several different components of cybersecurity operations into one centre that operationalizes a comprehensive cybersecurity lifecycle powered by CSFC Fusion Platform.

- Enabling security analysts to qualify, prioritize, automate, and respond to AWS alerts with appropriate integration with AWS components (Cloud Trail/GuardDuty/Security Hub).

- Executing predefined security playbooks from CSFC that are built-in to the workflow based on the attack type and pattern which can be executed by the SOC analysts for triaging & notification.

- Providing dedicated apps that support the direct integration of key AWS security components which makes easier to trigger response actions directly based on appropriate business
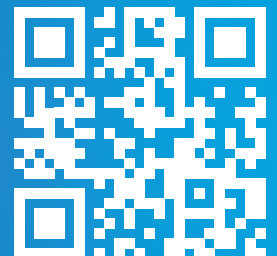
Value Delivered

- Next Gen platform delivering comprehensive threat detection and response

- Actionable threat insights with 24x7 coverage by CSFC security analysts

- Build on the foundations of HCLTech's SecIntAI platform

- Detection content and reporting mapped to MITRE ATT&CK

HCLTech | Supercharging Progress™

hcltech.com

HCLTech is a global technology company, home to 211,000+ people across 52 countries, delivering industry-leading capabilities centered around Digital, Engineering and Cloud powered by a broad portfolio of technology services and software. The company generated consolidated revenues of $11.79 billion over the 12 months ended June 30, 2022. To learn how we can supercharge progress for you, visit hcltech.com.