HCLTech | Supercharging Progress™

Cyber defense for the cloud

HCLTech Managed SIEM powered by Microsoft Azure Sentinel

Business **challenges**

Complex security landscape

With cloud adoption the size of the IT environment increases. This leads to a large number of security point products in an enterprise. A non-integrated architecture can create complexity.

Unsecured data storage

Enterprises can easily lose track of sensitive data and databases.

Dependence on CSP

Cloud adoption and digital transformation cause enterprises to depend on CSP's IT infrastructures for their business processes.

Increased attack surface

Cloud and digital adoption increases attack surfaces with static security policies.

Sophisticated attackers

Attackers range from local hackers to sophisticated nation-state hackers

Acute lack of skilled talent

Global shortage of skilled cloud security talent and the challenge of retaining existing sta.

Risk and compliance management

Increasingly complex regulatory requirements related to cloud adoption require improved security services.

Lack of proper content

The alerts generated by security tools are not helpful without proper content relevant to an organization's cloud adoption.

Information overload

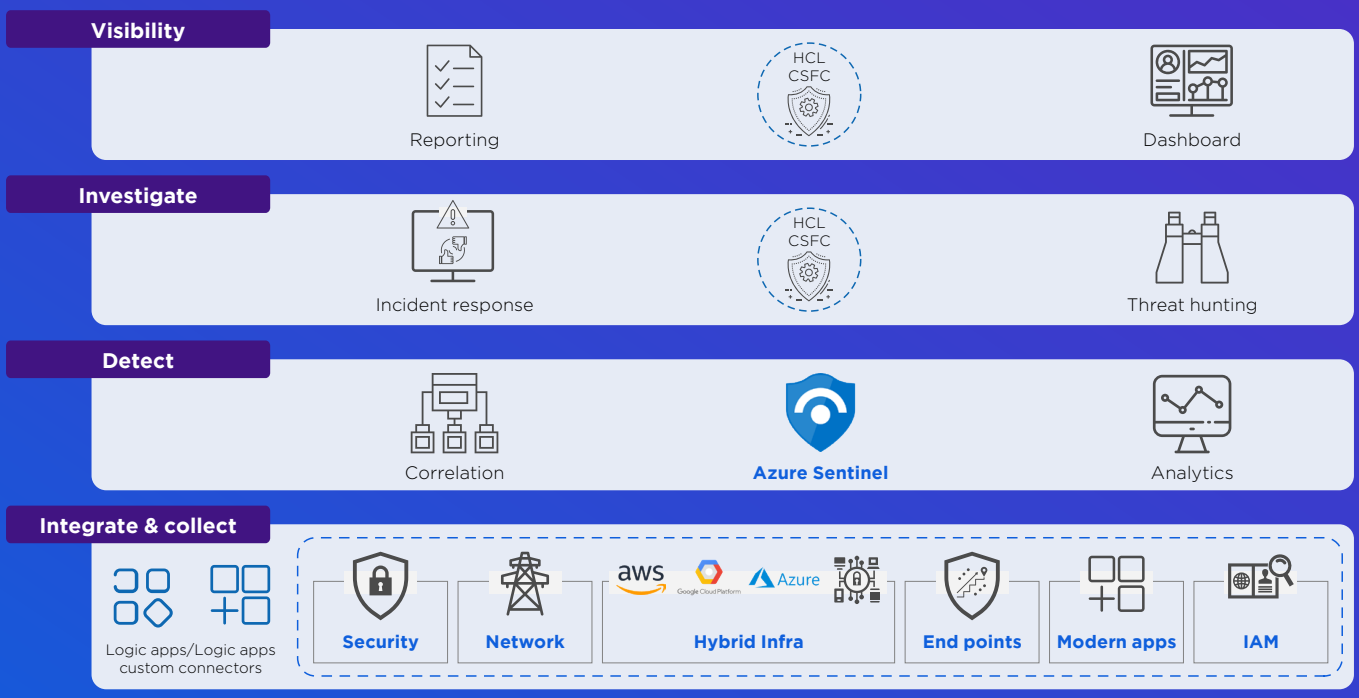
With too many alerts there is bound to be alert fatigue, which could lead to important actionable alerts being missed.

Solution **overview**

HCLTech's Managed SIEM services maximize the value and eectiveness of your SIEM investment by augmenting your IT security team with our centralized analyst workbench from the HCLTech CSFC Fusion Platform. Our experts manage and monitor industry-leading SIEM platforms, 24x7x365. This fully-managed service is delivered through resources that are certified and trained on leading SIEM platforms with years of experience in security monitoring and analytics. Our experts perform log data analysis, alerts triage and handling, custom use case development, standard reports creation, and incident response coordination to ensure the continuous enhancement of your cyber security posture.

With the enhancement of Azure Sentinel platform by Microsoft -- the leading SIEM & SOAR solution -- we help deliver next-generation threat intelligence and security analytics services across the enterprise environment. This provides a single platform for threat detection, threat response, and proactive threat hunting as well as granular visibility into the threat landscape across a hybrid/multi-cloud environment.

HCLTech's goal is to help customers manage their Azure Sentinel platform so they can monitor and detect any cyber threats to the enterprise environment more eectively, with timely alerts and response recommendations. HCLTech Cyber Defense for the cloud service takes the form of our global HCLTech CSFC's Managed Cloud SIEM solution that provides a birds-eye view across the enterprise, alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution time frames.



HCLTech Managed SIEM with Azure Sentinel

HCLTech Cyber Defense for Cloud service includes the following activities:

Design and deploy

Design the Azure Sentinel architecture with the right SIEM use cases and build the Sentinel cloud instance with corresponding configurations.

Integrate and develop

Integrate complete infrastructure with all the log sources using Azure Sentinel connectors. Develop additional threat-hunting templates and tune-in playbooks for automatic execution.

Analyze and mitigate

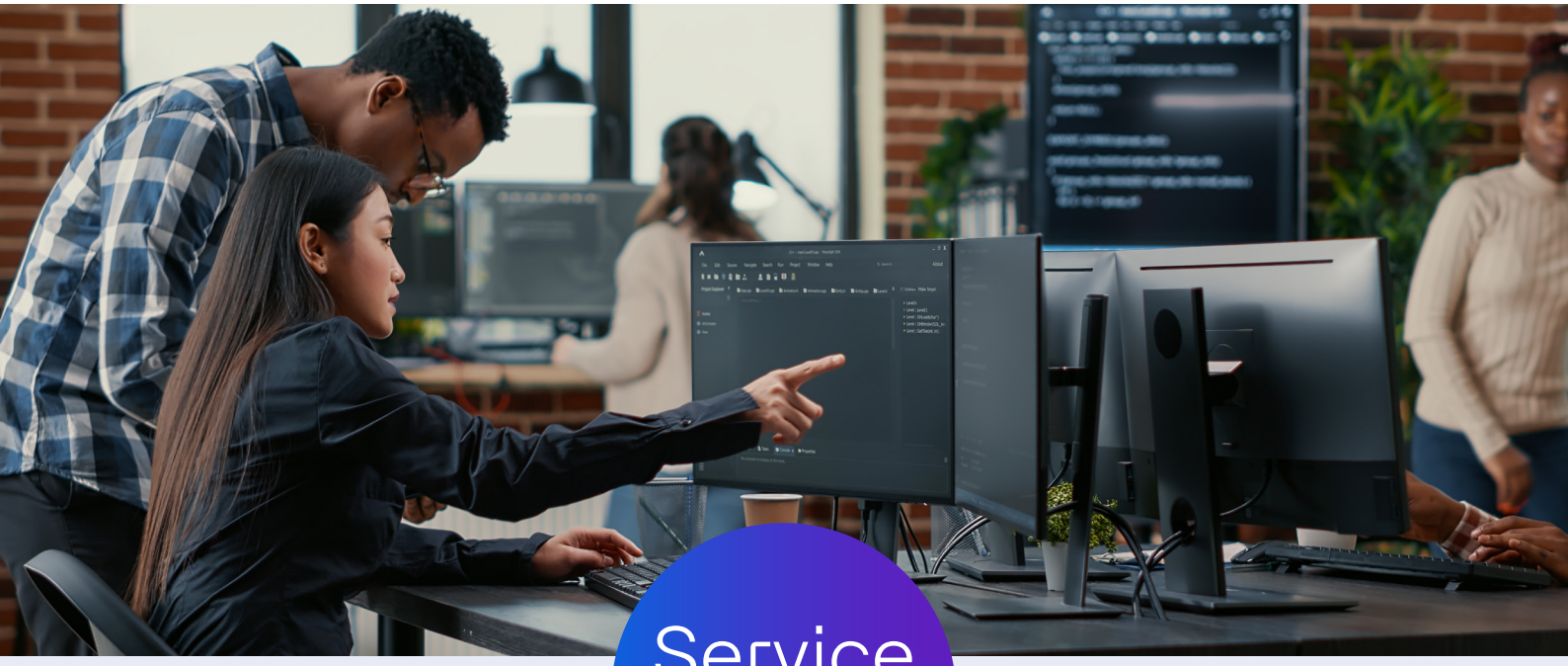
Threat analysis and investigation done by certified and skilled resources to detect and mitigate zero-day cyber threats. Brilliant analysis of the threat landscape and associated business risk for continuous fine-tuning of the Azure Sentinel environment.

Service **catalogue**

Standard package	Add-Ons
Tuning and optimization of customer's Azure Sentinel	Standard package +
Security event log processing	Client tailored use cases
24X7 security monitoring	Client focused digital threat intel
Collaborative threat intelligence	Incident response retainer services
Standard use case library	Custom reporting
Client tailored use cases (up to 10 per annum)	Custom solution integration (parser dev.)
Incident alerting & notification	
Incident response recommendation	
Cyber threat advisories	
Standard pre-defined reports	
Ongoing platform engineering	

Service **features**

- Azure Sentinel platform management
- Security event log processing
- 24x7x365 security monitoring
- Incident alerting and notification
- Incident response recommendation and support
- Cyber threat advisories
- Backed by industry-leading SLAs



Service **benefits**

- Improve operational eciency
- Minimize cyber risk
- Up-to-date visibility with Cyber Security Fusion Centre dashboard
- Gain from HCLTech's security expertise
- Gain situational cyber awareness at scale

Benefits of Azure Sentinel as SIEM **platform**

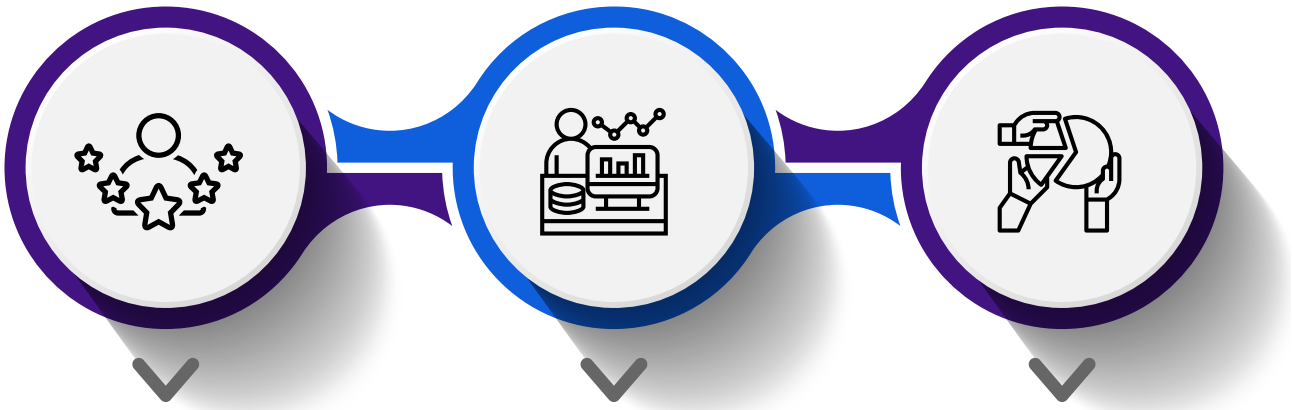
Improved SOC efficiency*
Azure Sentinel's AI-driven correlation engine and behavior-based analytics has reduced the number of false positives by up to 79%.

Ease of deployment*
Customers can save up to 67% of time needed to deploy a SIEM solution with Azure Sentinel's pre-built SIEM content and out-of-the-box functionality.

Cost effective*
Total costs for Azure Sentinel were 48% lower than the cost of the legacy solution including licensing, storage, and infrastructure costs.

Improved visibility with large coverage*-
With pre-built connections to many dierent applications and data sources in Azure Sentinel, the ingestion of new data is made as simple as a few clicks, even for a hybrid cloud environment.

HCLTech differentiators



22+ years
of experience
in security monitoring

Certified
engineers and
expert analysts

Enriched with
collaborative
threat intelligence
insights

Use **cases**

Use case	Qualifications	Solution and benefits
Faster detection of threats	Customers are looking for: • Faster detection of threats • Post detection, containment of threats without aecting the enterprise environment	• Integration of multiple security solutions in the enterprise infrastructure with single SOAR platform • Integration with centralized alerting platform with pre-defined security playbooks which can take action itself which helps remediate and contain the threats
Advanced incident/ Alert enrichment	Customers are looking for: • Enrichment of alerts/ incidents	• For the entities found in the respective alerts/ incidents, pre-defined playbooks are used to search for any historical data among other security solutions • Similar alert from dierent security solutions help categorize any true incident
Automatic triage of incidents/ alerts	Customers are looking for: • Automatic triaging of security incidents	Integration of Siemplify playbook, incidents/ alerts triaging is done automatically
Enrichment of knowledge database	Customers are looking for: • Integration of SOAR with knowledge bases for the enrichment of KB's	• Integration of SOAR platform with security knowledge databases • Security playbooks are pre-defined to search for known/ unknown activities or entities within the knowledge base
Integration with other cloud native/ third party security solutions	Customers are looking for: • Integration of cloud native and any/ all third-party security solutions with one single centralized SIEM platform	• Based on available API's, integration of SOAR platform with all the security controls, cloud native & third party, is enabled to have a centralized alerting, enrichment and remediation of security incidents.
Integration with ITSM Solutions	Customers are looking for: • Integration of security incident management platform with ITSM solutions	• Integration of security playbooks with ITSM solution • Defined playbooks can be used for automated incident life-cycle management through ITSM

HCLTech | Supercharging Progress™

BI-112AIAII734735745450-EN00GL

hcltech.com

HCLTech is a global technology company, home to 219,000+ people across 54 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 September 2022 totaled $12.1 billion. To learn how we can supercharge progress for you, visit hcltech.com.