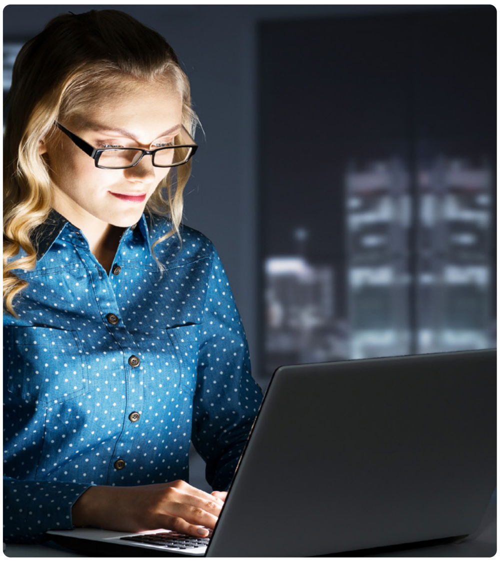
HCLTech | Supercharging Progress™

Elevate security with HCLTech Sentinel Bridge solution

Seamlessly transition to Microsoft Sentinel for advanced threat management

HCLTech Sentinel Bridge solution



In today's rapidly evolving cybersecurity landscape, legacy SIEM solutions like Splunk often struggle to keep pace with modern threats. Traditional SIEMs typically suffer from scalability issues, high operational costs and limited integration capabilities. These systems generate a high volume of alerts, often leading to alert fatigue and missed critical threats. Additionally, the lack of advanced analytics and automation hampers the ability to respond to incidents swiftly and effectively. As a result, security teams find themselves overwhelmed, unable to efficiently manage and mitigate security risks.

Why move to a next-gen SIEM like Microsoft Sentinel

Next-generation SIEM solutions, such as Microsoft Sentinel, address these challenges by offering robust, cloud-native security information and event management capabilities. Sentinel leverages the power of artificial intelligence and machine learning to provide enhanced threat detection, investigation and response. Its scalability ensures that it can handle large volumes of data without compromising performance. Sentinel's deep integration with the Microsoft ecosystem, along with its support for a wide range of third-party applications, ensures comprehensive security coverage. By adopting Sentinel, organizations can benefit from advanced analytics, automated responses and reduced operational costs, enabling a more proactive and efficient security posture.

Advanced features of Microsoft Sentinel

Microsoft Sentinel stands out with its advanced features designed to empower security teams. Key capabilities include:

AI and ML-Powered Threat Detection: Sentinel uses advanced machine learning models to detect anomalies and potential threats, reducing false positives and enhancing accuracy.

Scalability and Flexibility: As a cloud-native solution, Sentinel can effortlessly scale to meet the demands of growing data and evolving threats.

Automated Response and Orchestration: With built-in SOAR (Security Orchestration, Automation and Response) capabilities, Sentinel automates routine tasks, allowing security teams to focus on critical issues.

Cloud-native SAAS solution: The solution features benefits like automatic updates, low maintenance (no on-premises infrastructure to set up and maintain) and elastic scalability.

Subscription Pricing: Pay-as-you-go model allows you to pay only for the data you ingest.

Integration and Extensibility: Sentinel seamlessly integrates with other Microsoft products and numerous third-party tools, providing a holistic security environment.

When combined with HCLTech's cloud-native SAAS solution, Microsoft Sentinel offers significant return on investment (ROI) and operational benefits. Organizations can achieve a 200% ROI over three years, driven by a 79% decrease in false positives and an 80% reduction in investigation efforts. Management effort for infrastructure and SIEM is reduced by 56%, and overall costs are 48% less compared to legacy SIEMs. Additionally, Sentinel enables a 67% decrease in time to deployment with its prebuil SIEM content and out-of-the-box functionality, allowing for faster and more efficient implementation.

HCLTech Services: Your trusted partner in migration and support

HCLTech is dedicated to helping organizations transition from legacy SIEMs like Splunk to next-generation Microsoft Sentinel SIEM. Our comprehensive services include:

Assessment and Planning: We conduct a thorough assessment of your current SIEM environment and develop a tailored migration plan to ensure a seamless transition.

Migration and Deployment: Our experts handle the entire migration process, from data transfer and configuration to integration with existing security infrastructure.

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 investigation and analysis performed by certified, skilled resources to detect and mitigate even zero-day cyber-threats and associated business risks for a continuous fine-tuning of Azure Sentinel environment.

24/7 Monitoring and Support: Our CSFC experts provide round-the-clock monitoring, threat detection and incident response to ensure continuous protection.

HCLTech boasts robust Sentinel capabilities, having developed 30+ playbooks for cross-platform migrations tailored to various clients. We have fine-tuned 200+ detection rules to enhance security for multiple clients using Microsoft Sentinel. Our team of 3,000+ experienced and Microsoft-certified engineers, 35+ years of partnership with Microsoft and membership in the Microsoft Intelligent Security Association (MISA) reflect our commitment to delivering best-in-class security solutions.

HCLTech | Supercharging Progress™

hcltech.com