Microsoft Sentinel

Modernize security operations and focus on what matters most with cloud-native SIEM, powered by AI.

Microsoft Sentinel is a cloud-native security information and event management (SIEM) platform that uses built-in AI to analyze large volumes of data across an enterprise—fast. Microsoft Sentinel aggregates security data from all sources, including users, applications, servers, and devices running on-premise or in any cloud. By eliminating on-premises infrastructure, it lowers costs by 48% compared to legacy SIEMs, as found by the commissioned Forrester Consulting Total Economic Impact™ of Microsoft Sentinel study. What's more, it reduces alert fatigue by 90% with machine-learning (ML) and analytics. With Microsoft Sentinel, your team can focus on what matters most: protecting your organization.

Learn More

https://aka.ms/MISAproducts

Senserva integrates with Microsoft Sentinel to provide automated, detailed insights about user and application security for enriched correlation of high risk events

The Cloud is inherently complex, dynamic and disjointed making it challenging to secure. To help the industry meet this challenge, Senserva's cloud-native technology automates security governance associated with Azure Active Directory, by monitoring and aggregating intricate security data, helping to enable a zero trust environment. This automation within Microsoft Sentinel accelerates the protection of your organization's Azure environment against entitlement breaches, highly sophisticated and otherwise undetectable attacks as well as helping companies ensure they meet compliance requirements. Senserva Simplifies the Complex.

Customer Benefits

- **Stay One Step Ahead**: Senserva's Prologue data intelligence engine sorts through volumes of non-relevant data providing automated insights and enriched correlation for alerting and remediation in Microsoft Sentinel – Saving Time and Cost.

- **Cloud Security is Complex. Senserva Makes it Simple:** Senserva's Prologue automates the complex task of visualizing user and application governance in Azure Active Directory by leveraging Jupyter Notebooks. This allows organizations to quickly prioritize risks, manage cloud entitlements, and remediate in Microsoft Sentinel – Better Utilizing Human Resources and Reducing Alert Fatigue.

Learn More

No Cost Trial

Click on the link below to participate in a fully supported 90-day complimentary program
https://info.senserva.com/

Contact

Kevin Rich
Kevin@senserva.com

The Microsoft Intelligent Security Association (MISA) is an ecosystem of independent software vendors and managed security service providers that have integrated their security solutions with Microsoft to better defend against a world of increasingly sophisticated, fast-moving threats. aka.ms/MISA

Member of
Microsoft Intelligent Security Association

Microsoft