Microsoft Sentinel

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

Microsoft Sentinel is a modern, cloud-native SIEM powered by AI, automation, and Microsoft's deep understanding of the threat landscape empowering defenders to detect, investigate and respond to threats - quickly and efficiently. With in-built security orchestration, automation, and response (SOAR) capabilities, user and entity behavior analytics (UEBA) and threat intelligence (TI), customers get a comprehensive solution that is both easy and powerful. Microsoft Sentinel aggregates security data from all sources, including users, applications, servers, and devices running on-premise or in the cloud. By eliminating on-premises infrastructure, it lowers costs by 44% compared to legacy SIEMs, as found by the commissioned Forrester Consulting Total Economic Impact™ of Microsoft Sentinel study. With Microsoft Sentinel defenders can hunt and resolve critical threats quickly and efficiently.

Learn More
https://aka.ms/MISAproducts

How Sekoia intelligence integrates with Microsoft Sentinel

Combining Microsoft Sentinel detection capabilities with the Sekoia intelligence data allows the customers to extend the coverage of the detected threats. The integration between Microsoft Sentinel and Sekoia intelligence is seamless (more information here) because Microsoft and Sekoia comply with open standards (STIX 2.1). Sekoia intelligence can easily feeds Microsoft Sentinel with highly structured and contextualized Cyber Threat Intelligence (CTI) data to drastically increase the threats coverage. Thanks to a very strict life cycle management of the Indicators of Compromise (IoC) Sekoia Intelligence guarantees a very low false positives rate within Microsoft Sentinel and save the SOC analysts time.

Customer Benefits

- Extend the threats coverage by combining Microsoft Sentinel with the data provided by one of the European CTI leader

- Rely on highly contextualized CTI data to properly understand the detected threats

- Rely on two vendors which comply with open standards

Learn More

Product tour
https://www.sekoia.io/en/product/cti/

Contact
contact@sekoia.io

Member of
Microsoft Intelligent
Security Association

Microsoft Security