# 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

## How SOC Prime integrates with Microsoft Sentinel to yield industry expertise capable of addressing custom use cases.

SOC Prime's Center of Excellence for Microsoft Sentinel SIEM & SOAR enables security teams to save up to 5 years of R&D effort on SIEM-native content development tailored to the needs of both large-scale enterprises and MDRs. SOC Prime's Detection as Code platform ensures complete threat visibility with the customers' Microsoft Sentinel solution to keep their SIEM continuously updated on the latest threats.

## Customer Benefits

- **Microsoft Sentinel-native content development.** Obtain out-of-the-box use cases, including SIEM-native Workbooks, Playbooks, Logic Apps, and Data Connectors.
- **Cost-efficient support and maintenance**. Have all data normalized and parsed with no extra costs for content development, integration, and fine-tuning.
- **Full threat context and ATT&CK® alignment**. Get ready-to-use Rules and Queries mapped to ATT&CK with threat context on any alert triggered and query matched.
- **Automated content streaming.** Automatically push detections that can instantly kick off SOAR Playbooks in Logic Apps directly in your environment.

### Learn More

Explore Now

https://tdm.socprime.com/login/azure

Contact

https://my.socprime.com/microsoft-sentinel/

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