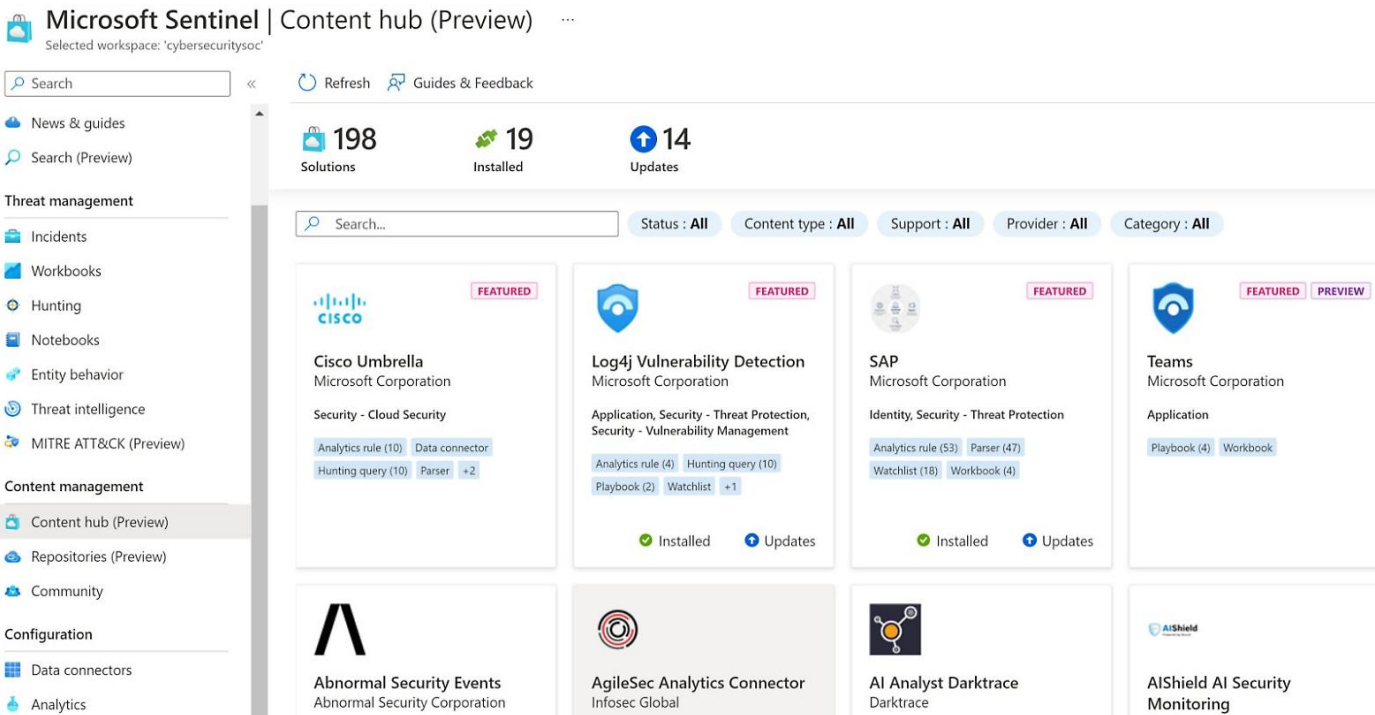


Microsoft Sentinel in 30

Intelligent Security Analytics and Threat Intelligence

Microsoft Sentinel in 30 offers an intelligent, comprehensive SIEM solution for threat detection, investigation, response, and proactive threat hunting, enabling you to modernize your security operations.



The screenshot displays the Microsoft Sentinel Content Hub interface. At the top, it shows the workspace name 'cybersecuritysoc' and statistics: 198 Solutions, 19 Installed, and 14 Updates. The main content area is a grid of solution cards, each with a 'FEATURED' badge and details about its capabilities and status. The cards include:

- Cisco Umbrella** (Microsoft Corporation): Security - Cloud Security. Includes 10 Analytics rules, 1 Data connector, 10 Hunting queries, and 2 Parsers.
- Log4j Vulnerability Detection** (Microsoft Corporation): Application, Security - Threat Protection, Security - Vulnerability Management. Includes 4 Analytics rules, 10 Hunting queries, 2 Playbooks, and 1 Watchlist.
- SAP** (Microsoft Corporation): Identity, Security - Threat Protection. Includes 53 Analytics rules, 47 Parsers, 18 Watchlists, and 4 Workbooks.
- Teams** (Microsoft Corporation): Application. Includes 4 Playbooks and 1 Workbook.
- Abnormal Security Events** (Abnormal Security Corporation): No specific details shown.
- AgileSec Analytics Connector** (Infosec Global): No specific details shown.
- AI Analyst Darktrace** (Darktrace): No specific details shown.
- AIShield AI Security Monitoring** (AIShield): No specific details shown.

Microsoft Sentinel in 30 at a Glance:

Long View offers you:

- The development of a recommended high-level data flow and architecture
- Deployment of Microsoft Sentinel as a pilot
- Deployment of a Sentinel Syslog Collector
- The enablement of Security Operations Center (SOC) Operations Efficiency and Data Collection Health Monitoring
- Validation and testing of each collection type
- Up to two (2) 2-hour workshops for training and knowledge transfer
- Recommendations for further deployment or migration next steps

By choosing Long View we enable your business to:

- Understand how Microsoft Sentinel can help modernize your security operations
- Define and accelerate your organization's security strategy
- Collect relevant data from a few sources as a pilot
- Review Microsoft Sentinel's threat detection and response capabilities to discover and mitigate threats

Optional Services Available:

- **CSI Engagement*** (* Microsoft Funding may be available)
- Microsoft Sentinel Engagement