LevelBlue | Microsoft

LevelBlue Managed SIEM for Microsoft Sentinel

Modernize your security operations.

Expanding your digital footprint also expands the attack surface. Traditional security tools can't detect multi-layer attacks, correlate alerts, or keep pace with growing data.

Ransomware attacks are growing in sophistication and dominating headlines. At the same time, the average cost of recovering from a data breach is US$4.35M[1]. Security leaders are feeling the pressure – from macroeconomic headwinds to cybersecurity staff shortages – to do more with less.

Traditional security tools, like SIEMs, are not designed to keep pace with rapid growth in security data and analytics across a multi-cloud digital environment with a distributed workforce. This puts the burden on the organization's limited security team resources to fill the gaps and maintain complex setups.

Modernize your security operations - Microsoft Sentinel

Microsoft Sentinel is a modern, cloud native SIEM powered by AI, automation, and Microsoft's deep understanding of the threat landscape. Microsoft Sentinel provides coverage for both hybrid and multi-cloud systems and ingests data at scale and makes it even easier to bring in the data needed for complete security.

Microsoft Sentinel provides a unified set of capabilities to collect data, detect breaches and anomalies, investigate threats, and remediate issues. You get a modern SecOps solution that is both easy and powerful.

Microsoft enriches data with threat intelligence, uses machine learning to correlate alerts and provides SOAR capabilities to automate response to common issues. Not only does Sentinel make it easy to identify an issue, but it also provides incredible context including entity mapping to visualize how threats are moving across an organization. All of this is built on top of the Azure cloud, allowing for speed and scale that modern security operations teams need.

Getting started and turning on Microsoft Sentinel with your E5 license is the easy part, but having the right modern tools is only part of the people, process, and technology equation.

24×7 global security operations - LevelBlue Managed SIEM

LevelBlue Managed SIEM for Microsoft Sentinel service goes a few steps further by providing you the talent and resources required to operate a modern 24×7 threat monitoring, investigation, and response operation without incurring the cost or risk of doing it yourself.

Leveraging the advanced tools in Microsoft Sentinel with the addition of LevelBlue's field-proven use case content, Microsoft certified experts, and security operation prowess, uniquely positions your organization to stay ahead of sophisticated attacks and out of the headlines.

Benefits

- Modernize your security operations
- Augment your security team
- Get instant 24×7 global coverage
- Avoid the cost and risks from DIY
- Eliminate false positives
- Stop real threats before it's too late
- Stay protected from emerging threats

To maximize the benefits and returns from your investment with Microsoft Sentinel, LevelBlue's experts work in the background and become an instant extension of your team. You'll gain a global security operations team with decades of cumulative knowledge which has allowed us to sharpen our enterprise-proven processes and operational intelligence to deliver unrivalled results for our clients.

We know what great looks like for security operations. We augment your current capabilities, accelerate security readiness, and improve your overall ability to address the latest threats before damage is done.

LevelBlue will conduct 24×7 global, real-time threat monitoring, human-led incident investigations, provide actionable response recommendations, and update detection content to address the latest threats.

As an added layer, LevelBlue securty analysts will be armed with SpiderLabs curated threat intelligence to assist them in further identifying real threats and eliminating false positives, while only confirmed and investigated incidents that require your response will be sent to your security team for further action.

What's Included:

- Microsoft Sentinel Managed by LevelBlue certified experts
- Field-proven use cases and protection against emerging threats
- 24×7 global real-time threat monitoring
- Expert security analysts and threat investigators
- Targeted response actions and incident prioritization
- SpiderLabs threat intelligence
- Microsoft focused data sources

LevelBlue SpiderLabs Threat Intelligence – embedded

LevelBlue SpiderLabs is an elite, industry-recognized team of security researchers, ethical hackers, threat hunters, forensics investigators, pen testers, malware reverse engineers, and incident responders, with extensive security expertise and pedigree. The output from this team is the core of LevelBlue's proprietary curated threat intelligence which is integrated across our portfolio of offers to protect all our clients from the latest emerging threats.

Detection and response – LevelBlue MDR

In addition to LevelBlue Managed SIEM for Microsoft Sentinel services, LevelBlue Managed Detection and Response (MDR) service adds comprehensive threat response, threat hunting on the endpoint, remote incident response, and more.

LevelBlue MDR extends the ability of security analysts to investigate and respond to threats directly on endpoints and in multiple security controls. Analysts are able conduct advanced threat hunting and investigate the impact and blast radius of a threat more completely, allowing for faster responses with higher confidence.

Be sure to ask us about the added benefits of LevelBlue MDR.

Strategic alliance partner – LevelBlue and Microsoft

LevelBlue is one of the first Microsoft MSSP Partners to offer Managed SIEM services for Microsoft Sentinel. As a long time Microsoft partner, we're committed to Microsoft's forward-facing roadmaps to help your organization maximize your Microsoft investment well into the future.

- Microsoft Intelligent Security Association member
- Microsoft Managed XDR Solution Partner
- Microsoft AI Cloud Solution Partner
- Microsoft Solutions Partner Security Specialist:
  - Cloud Security
  - Threat Protection

Microsoft Intelligent Security Association

Microsoft Security

Microsoft Verified Managed XDR Solution

Microsoft Solutions Partner
Security
Specialist
Cloud Security
Threat Protection

Microsoft FastTrack Partner