BRIEF

/ Microsoft Sentinel Deployment Accelerator

LevelBlue | Microsoft

Modernize your SOC with Microsoft Sentinel

$0 expert-led assessment, modernization, and deployment support for Microsoft Sentinel.

LevelBlue helps you understand your current SIEM environment, define the target state, and accelerate your move toward modern security operations.

Security operations environments evolve over time. Data sources are added, analytics rules accumulate, retention grows, integrations change, and operational processes become increasingly complex.

The Microsoft Sentinel Deployment Accelerator helps organisations review their current SIEM/SOC environment, identify opportunities to modernise the platform, and accelerate the deployment or expansion of Microsoft Sentinel.

What we assess

- Existing SIEM / SOC architecture and operating model
- Microsoft Sentinel workspace design
- Data connectors and log-source coverage
- Data ingestion, retention and tiering
- Analytics rules and detection coverage
- Microsoft Defender XDR and unified SecOps integration
- Automation and SOAR opportunities
- Workbooks and operational visibility
- Cost and ingestion optimisation
- Third-party logs, integrations and data lake readiness
- Migration dependencies and technical risks

Our approach

LevelBlue combines architecture, engineering and security operations experience to turn the assessment into practical technical actions and a clear roadmap, delivered in four phases.

1

Assess
Understand the current environment, business priorities, SOC requirements, data sources, platform health and operational challenges.

2

Modernize
Define the target Sentinel architecture, identify quick wins, prioritise technical changes, and agree on the migration or optimisation approach.

3

Deploy
Configure or optimise relevant Sentinel capabilities: connectors, analytics, automation, ingestion, retention and Microsoft Security integrations.

4

Validate
Confirm data flow, analytics, incidents and operational readiness, then document the next actions for your SecOps journey.

Built around your environment

This is not a generic Sentinel presentation. The engagement is shaped around your existing security environment, Microsoft investments, data sources, operational model and priorities. LevelBlue focuses the work on practical improvements that strengthen visibility, detection, investigation and response.

From current state to modern SecOps

A structured approach to assess, modernise, deploy and validate Microsoft Sentinel, based on your environment and priorities.

Microsoft-supported engagement – $0 cost to eligible customers. This engagement may be fully funded by Microsoft*.

Assess	Modernize	Deploy	Validate
Understand today	Design the path	Build the capability	Prove it works
• Current environment • Architecture • Data sources • Detection coverage • Operational priorities	• Target architecture • Quick wins • Migration approach • Retention strategy • Technical priorities	• Data connectors • Analytics rules • Automation • Retention configuration • Microsoft integrations	• Data flow • Detection results • Incident visibility • Operational readiness • Next-step roadmap

Benefits

- Improve security visibility across Microsoft and third-party data
- Accelerate deployment & increase adoption
- Reduce operational blind spots and detection gaps
- Align ingestion and retention with business requirements
- Identify opportunities to reduce unnecessary Sentinel cost
- Identify unused, failing or duplicated content
- Automate repetitive SOC processes and response actions
- Modernise integration with Defender XDR and unified SecOps
- Establish a practical roadmap for further Sentinel adoption

What you receive and why LevelBlue

- Current-state Sentinel / SIEM assessment
- Prioritised findings and quick wins
- Target-state architecture recommendations
- Migration or optimisation approach
- Deployment activities aligned to the agreed scope
- Validation of data ingestion and detection operation
- Prioritised recommendations and next-step roadmap

LevelBlue combines Microsoft security architecture, engineering, and security operations experience to move you from assessment to practical implementation.

- Sentinel architecture, engineering, and SIEM migration
- Detection engineering and automation capability
- Global security operations and threat intelligence experience

Microsoft credentials and certifications

LevelBlue is endorsed and validated by Microsoft as a leading cybersecurity partner:

Certified Microsoft AI Cloud Solutions Partner:

- Microsoft Specializations: Cloud Security, Threat Protection, Infrastructure & Security Solutions Partner
- Microsoft Intelligent Security Association (MISA) Member
- Microsoft Verified MXDR Partner

Microsoft Certified Experts:

- Microsoft MVP 'Most Valuable Professional' (Azure Security)
- Azure Security Architect Expert
- Azure Administrator
- Azure Security Engineer

*Subject to Microsoft qualification and approval.

LevelBlue

Talk to us about your Microsoft Sentinel environment

levelblue.com