

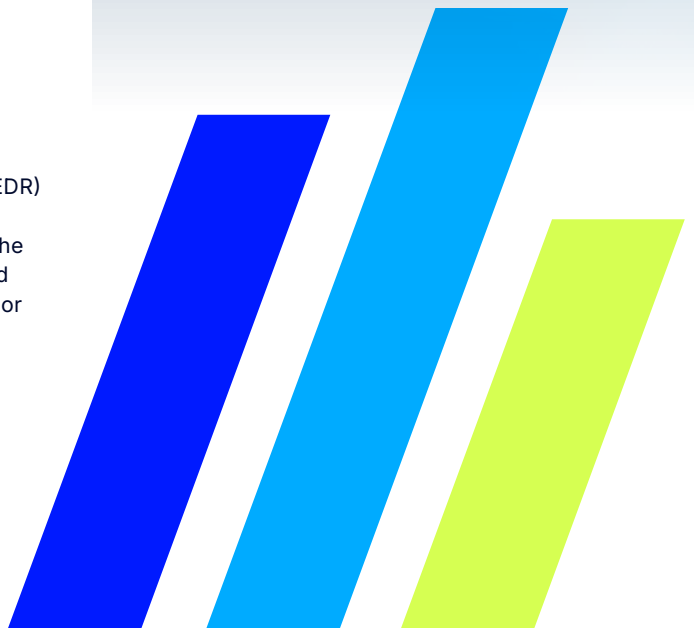
CASE STUDY

From compliance to resilience: how an automotive firm transformed its security with LevelBlue MDR & SIEM

An automotive manufacturing company facing increasing cybersecurity threats and stringent insurance requirements sought to enhance its IT security posture. Following a comprehensive Microsoft Threat Protection Engagement and Sentinel Engagement Workshop, the company selected LevelBlue to implement tailored solutions and address its unique challenges.

The challenge

The organization was under significant pressure to meet a critical insurance mandate requiring the deployment of an Endpoint Detection and Response (EDR) tool. The client had a lean internal cybersecurity team and needed to ensure adequate log retention and daily review to comply with industry standards. The overarching challenge was implementing a robust security solution that could fulfill the insurance requirements without overburdening the existing IT staff or disrupting operations.



The solution

To address these challenges, LevelBlue implemented a suite of Managed Detection and Response (MDR) and Co-Managed Security Information and Event Management (SIEM) services. Leveraging Microsoft Sentinel and Microsoft Defender for Endpoints, the solution was designed to align with the company's compliance requirements and operational needs.

Key Components of the Solution:

- 1 LevelBlue Managed Detection and Response (MDR):** The MDR service provides 24x7 monitoring, threat detection, and incident response. This continuous monitoring ensured that any security threats were promptly identified, the client was notified, and mitigation efforts were defined and started.
- 2 LevelBlue Co-Managed SOC (SIEM Services):** By integrating Microsoft Sentinel, the client gained access to a powerful log management and analytics platform. This facilitated real-time monitoring and historical data analysis, which is critical for compliance and proactive threat management.
- 3 Microsoft Defender for Endpoints:** LevelBlue deployed this advanced endpoint protection to safeguard the company's devices, ensuring comprehensive coverage against malicious activities.
- 4 Microsoft Engagement Workshop:** A dedicated workshop demonstrated the seamless integration of these tools with the company's existing IT systems. This no-cost initiative underscored LevelBlue's commitment to delivering value and ensuring client success and helped convince it that LevelBlue was the partner of choice.
- 5 Information Security Advisor (ISA):** The client was assigned an experienced LevelBlue ISA. ISAs provide day-to-day support and strategic guidance for addressing complex security issues. LevelBlue believes this personalized approach ensured the client received expert assistance throughout the implementation process.

The results

Implementing Microsoft Sentinel and Defender for Endpoints significantly enhanced the company's IT security posture. The solutions met the insurance provider's requirements and provided the organization with a reliable and scalable security framework.

Key Benefits Realized:

- 1 Enhanced Security Posture:** The client achieved advanced threat detection and response capabilities, bolstering their defense against cyberattacks.
- 2 Compliance Achieved:** The solution fulfilled all insurance and compliance requirements, alleviating regulatory pressures.
- 3 Improved Operational Efficiency:** With 24x7 monitoring and incident response handled by LevelBlue, the internal IT team could refocus on core business activities.
- 4 Strategic Expertise:** Ongoing support from the ISA ensured the client could navigate evolving cybersecurity challenges effectively.
- 5 Cost Savings:** The no-cost engagement workshop and co-managed services provided a cost-effective path to achieving an advanced security framework without additional staffing requirements.

By implementing a comprehensive cybersecurity solution that included LevelBlue MDR, LevelBlue Co-Managed SOC (SIEM) services, and Microsoft Sentinel and Defender for Endpoints, the automotive manufacturing company successfully met its insurance requirements and fortified its IT security posture.

The collaboration allowed the client to concentrate on its primary business objectives, confident that a reliable partner was expertly managing its cybersecurity needs. This case highlights the importance of tailored cybersecurity solutions in meeting both compliance demands and operational goals.