LevelBlue

CASE STUDY

How LevelBlue helped an Australian media client strengthen cybersecurity and eliminate false positives with Microsoft E5

The client is a well-established Australian company in the media and advertising sector. With operations across major cities, the organization connects with a broad audience through diverse advertising assets and channels.

The challenge

The client is a mature organization from a cybersecurity perspective with a CISO and a highly trained security operations team. The company had been using different security vendors for endpoint security and SIEM but was suffering from a high level of false positives that distracted its security team from focusing on important issues.

The client had brought Microsoft E5 on board just before its initial meeting with LevelBlue. Still, it remained dependent on its current security providers, had yet to fully implement all of E5 security tools, and was not gaining the highest return possible on its investment.

The client sought a cybersecurity solution that could seamlessly integrate with its Microsoft technology stack while addressing key challenges, including:

- Proactive threat detection and response
- Effective configuration guidance for robust defenses
- Continuous monitoring to ensure optimal system security

Additionally, the company needed a strategic partner to align its security approach with its business objectives and operational needs.

The solution

LevelBlue recommended the client move fully to a complete Microsoft E5 ecosystem, which the company accomplished. It then contracted with LevelBlue for several solutions late last year.

The initial move saw the LevelBlue team conduct a fast-track Microsoft Engagement/Workshop to bring the client's team up to speed on E5's capabilities and the process of moving to the Microsoft environment began.

The client opted to contract with LevelBlue to supply Managed Detection and Response for Microsoft Defender and Endpoint, Co-Managed SOC for Microsoft Sentinel, a Digital Forensics and Incident Response Retainer and Cyber Advisory services. All of which were up and running in a short period of time.

With all these solutions in place, the client had the following tools and support from LevelBlue in place:

- **24×7 Monitoring:** Ensuring continuous oversight of systems to detect and mitigate potential threats promptly.
- **Expert Guidance:** Assisting with configuration to optimize the Microsoft technology stack and enhance security posture.
- **Proactive Threat Management:** Employing advanced detection capabilities and human-led threat intelligence to counter emerging risks.

The result

Through its partnership with LevelBlue, the client achieved:

- **Enhanced Cybersecurity:** Strengthened operational resilience and elevated cyber maturity to industry-leading standards.
- **Operational:** Streamlined threat management processes, enabling focus on core business activities.
- **Competitive Advantage:** Instilled confidence among clients, advertisers, and stakeholders by demonstrating a commitment to security and reliability.

One of the issues plaguing the client's security team before partnering with LevelBlue was dealing with a high number of false positives that not only distracted staffers from their normal duties but sometimes proved difficult to confirm as truly being benign. The client immediately saw a decrease in false positives, and with LevelBlue handling the detail work with E5, those staffers could focus on other work.

The decrease in false positives and having LevelBlue's experienced team on hand paid almost immediate results. Several months after LevelBlue was on board, its Global Threat Operations (GTO) team picked up on several alerts coming into one of the client's outside databases. At first glance, these appeared to simply be more false positives, but LevelBlue GTO was not convinced and conducted additional research, which indicated the alerts were indeed hostile. LevelBlue immediately contacted the client while invoking DFIR, which confirmed the alerts were dangerous.

Once notified the client's security shut down the instance being impacted, stopping the threat before it could move laterally and cause any harm.

A satisfied client

When asked, the client highlighted several reasons it opted to select LevelBlue to manage the migration and subsequent management of its E5 solution.

Key factors included LevelBlue's long-standing partnership with Microsoft, the team's demonstrated expertise across various technology stacks, and LevelBlue's compelling case for Microsoft as a comprehensive solution. Additionally, LevelBlue's impressive in-person presentation, the strong relationship it built with the client, clear program governance, defined roles, and well-outlined project timelines were crucial in their decision.