LevelBlue

CASE STUDY

Higgins Coatings leverage LevelBlue's SIEM and SOC experts to transform their security operations

LevelBlue aggregates and enriches Higgins security data from their existing Microsoft XDR environment, together with the range of other security non-Microsoft products in use, including their firewalls to deliver complete visibility of what is occurring in their environment. LevelBlue Co-Managed SOC services help them to leverage the investment made in their existing security technology to strengthen their cyber visibility, and respond quickly.

Client spotlight

With nearly 75 years experience, Higgins Coatings is Australia's go-to provider for commercial painting and maintenance needs across a broad range of industries. Headquartered in Melbourne, the company has 23 branches throughout Australia and a team of 1300 employees and subcontractors. They paint a lot of buildings, including the iconic Flinders Street Station, and are Australia's largest family-owned commercial painting contractor.

With a commitment to work, health and safety, quality and the environment, Higgins Coatings has an industry-leading ISO Tri-Certification Accreditation. The Higgins business spans general repainting, maintenance painting, new construction painting and building services for a variety of industry sectors including government, education, and healthcare.

The challenge

Safety is a priority, both when painters are abseiling buildings with a paintbrush in their hand, and in their head office, keeping their people and business secure is essential. The continued digitization of their business to support growth and additional systems to streamline operations means that securing their IT environment from cyberattacks is a priority.

Higgins is supported by a very busy 6-person, internal IT team – and did not have enough resources to monitor their IT security logs and alerts 24×7, 365 days per year. They knew that attackers were getting more sophisticated, and that if a breach occurred, they would need to be able to respond quickly to limit damage. They had recently deployed Microsoft Defender and Microsoft Sentinel in their security environment and wanted to maximize the return on this investment.

Reviewing the latest Gartner and Forrester analyst reports, they identified that LevelBlue was well-positioned to help them lift their cyber maturity and get the coverage they needed across multiple aspects of their security program.

The solution

Higgins engaged LevelBlue to provide Managed Detection and Response (MDR) services over the next three years. LevelBlue aggregates and enriches Higgins's security data from their existing Microsoft XDR environment, together with the range of other security non-Microsoft products in use, including their firewalls to deliver complete visibility of what is occurring in their environment. LevelBlue Co-Managed SOC services help them to leverage the investment made in their existing security technology to strengthen their cyber visibility.

'The expertise found in LevelBlue people was the key difference between other SOC services in the market. We knew that having access to cyber specialists who had a wealth of experience within all of our key existing technologies was a massive advantage,' says Revasan Govender, Head of IT at Higgins Coatings.

LevelBlue global threat analysts monitor their environment continuously and if an incident occurs, they can take action on behalf of the Higgins security team using a traffic light protocol (TLP), predefined to meet Higgins's business needs. LevelBlue's Traffic Light Protocol enables agreed actions and the necessary client approvals by asset (or asset group). It allows for automated responses initiated by LevelBlue experts like isolating a host, killing a process, blocking traffic, or changing a firewall configuration, dependent upon the relevant technology deployed. The result is that security risk is decreased as security incidents are actioned fast, in accordance with the business's priorities.

The 'defense in depth' approach also includes incident response services.

"Safety and security are a big concern for our business. You don't know what's around the corner. LevelBlue Incident Response Services have our back, should we suffer any major incident. And on a daily basis, LevelBlue has been pivotal in identifying even small anomalies – from bad links clicked through to suspicious activity," says Panos Michanetzis, Security Systems Administrator at Higgins Coatings.

Michanetzis has confidence that the LevelBlue team will alert him of key incidents as they occur; whether that be in the middle of the night or on weekends – he'll be informed quickly – an essential capability given they were not staffed to do that level of monitoring themselves.

LevelBlue has helped to improve their cyber resilience while reducing the load on their IT and security team. The technology team at Higgins Coatings are looking forward to focusing their work on further cloud migration to support the growing needs of their expanding business.

Advice for teams embarking on a new security partnership:

- **Patience** – configuring your systems and managing deployment requires your best work. Don't rush this.
- **Checks and due diligence** – closely manage your time constraints and resources. Having more eyes on your change management environment will ensure important things are not missed.
- **Engaging senior business management** – make sure they understand the full value of your engagement with a managed security services provider, and how this fits with a detailed security strategic plan to uplift your cyber capability.