LevelBlue

CASE STUDY

# How Curtin University partnered with LevelBlue for complete cyber insight and response

*Curtin University is keenly aware of the potential cybersecurity risks facing the higher education sector and takes its responsibilities in this area very seriously. As part of Curtin's continual review and improvement of its in-house cybersecurity capabilities, the university has selected LevelBlue's Managed Detection and Response (MDR) solution.*

## Client spotlight

Curtin University in Perth, Western Australia, has more than 57,000 students and almost 4,000 equivalent full-time staff and is a leading public university ranked in the top 1% of universities worldwide. Curtin's continuous improvement focus means its cybersecurity team was keen to increase visibility of cyber threats within the Curtin network and make the best use of internal resources to detect and respond promptly to potential cybersecurity incidents.

## The challenge

The university came to LevelBlue with several problems it needed to solve. The first was increasing the cybersecurity team's visibility into suspicious events within the university's environment. Additionally, the institution needed to make the best use of its resources to detect and respond in a timely manner to any potential and actual security incidents.

Curtin wanted to partner with a company that would help the institution build new security capabilities, increase cyber resilience, and improve visibility and coverage of threats in the technology environment. In addition, the university wanted to use threat intelligence to enrich and augment the existing cybersecurity team and, most importantly, build a partnership that would deliver mutually beneficial commercial outcomes.

As an added benefit, LevelBlue agreed to help enhance Curtin's cyber academic programs, develop an on-premises Security Operations Center, and contribute to cyber research programs.

*"Visibility is the key thing that we needed to bolster. This partnership with LevelBlue will give us greater ability to see a threat from end to end, where it originated from, where it went, what systems it affected, to identify the advanced vectors more quickly and contain the threat," said Jason Cowie, CIO of Curtin University.*

## The solution

Curtin's evaluation team selected LevelBlue's Managed Detection and Response (MDR) solution to help consolidate and strengthen its cybersecurity capabilities. The agreement with LevelBlue has the company handling the 24×7 monitoring of the University's systems, co-managing the Security Information and Event Management (SIEM) solution for threat detection across cloud and on-premise environments, and optimizing the vulnerability management technology.

In addition to these services, Curtin will have on-site access to named LevelBlue team members who augment the Curtin cybersecurity team. These team members include an Information Security Specialist (ISS), who will deliver the technical know-how to correlate the signals coming from the security platforms already in place. Additionally, an Information Security Advisor will help continuously improve the university's cybersecurity capabilities.

Finally, the university engaged LevelBlue for Digital Forensics and Incident Response (DFIR) services. This retainer ensures the university has the expert skills required to respond rapidly if a major security incident occurs. The elite LevelBlue SpiderLabs team, which is comprised of ethical hackers, forensic investigators, and researchers, supports all these services.

*"The global capability and local expertise of LevelBlue, co-located with us, was a winning combination," Mr. Cowie said.*

Curtin University's partnership with LevelBlue allows it to focus on expanding the use of technology within its existing licensing agreements, giving Curtin greater value from its existing investments, and has allowed it to expand the coverage of its endpoint protection as part of a defense-in-depth strategy.

The partnership has enabled Curtin University's security team to pursue detailed incidents more effectively and accelerate incident response. The LevelBlue Fusion platform provides the university with a dashboard for measuring the health of its security environment. Linked with their existing SIEM and ticketing system, KPIs can be measured accurately, and a real-time snapshot of threat response activity is always visible.