Trustwave®

How Curtin University Partnered with Trustwave for Complete Cyber Insight and Response

CASE STUDY

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 cyber security capabilities, the University has partnered with Trustwave'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 cyber security incidents.

The Challenge

The University came to Trustwave 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, 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, Trustwave agreed to help enhance Curtin's cyber academic programs, develop an on-premises teaching Security Operations Centre and contribute to cyber research programs.

"Visibility is the key thing that we needed to bolster. This partnership with Trustwave 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 Trustwave's Managed Detection and Response (MDR) solution to help consolidate and strengthen its cybersecurity capabilities. The agreement with Trustwave 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 the cloud and on-premise environments and optimising the vulnerability management technology.

In addition to these services, Curtin will have on-site access to named Trustwave 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 to help continuously improve the University's cybersecurity capabilities.

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

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

Curtin University's partnership with Trustwave 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 defence in-depth strategy.

The partnership has allowed Curtin University's security team greater ability to pursue detailed incidents and accelerate incident response. The Trustwave 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.

Industry Threat

Cybersecurity is an ongoing concern for colleges and universities. Because colleges and universities store such large amounts of data, they are often a target of hackers and other cyber criminals. Additionally, many universities have diverse technology and networks, multiple locations, as well as sensitive research projects that can make them even more vulnerable.

Institutions of higher learning will need to take steps to prevent emerging threats. Understanding the risks that are most relevant to colleges and universities can help you develop an effective cybersecurity strategy.

Phishing

Student scam emails range from ransomware to visa deceptions. They can also be a method used by competitors to steal academic teaching resources and exam papers.

Data Breaches

Universities often have PII data from thousands of current students and alumni. Exposure of this data may result in fines and reputational damage. In addition, financial systems are also prone to attack.

Hacktavists and Internal Threats

Hacktavists can make a political point by defacing online systems. Internal threats include academic results tampering.

Nation States

Nation state actors may seek to exfiltrate research data from government funded programs including defence research. Interference by foreign bodies on academic programs can result in influence on research strategy or results.

Trustwave®

www.trustwave.com