www.ballina.nsw.gov.au

Government | 400+ Employees

A Regional Council Stays Protected From Zero-Day Attacks

Ballina Shire is a picturesque region in the Northern Rivers area of New South Wales, Australia. The region is known for its beautiful beaches, scenic views, and vibrant community.

Ballina Shire Council, the governing body responsible for managing the local government area, faced significant cyber security challenges. In 2019, Ballina Shire Council faced the typical cyber security challenges experienced by local government organisations, such as being targeted by malicious threat actors due to high-value information held by government organisations. It had been increasingly difficult for the IT staff to quickly respond to modern threats like social engineering, sophisticated phishing campaigns, or zero-days. Therefore, the Council was looking to deploy a solution to address its cyber security challenges.

Ballina Shire Council partnered with ThreatDefence to implement security monitoring and cyber security assurance services. Through our always-on Security Operations Centre (SOC), the ThreatDefence SecOps platform enabled the Council to have advanced threat detection, deep visibility into their cyber security posture, ongoing incident response, and cyber risk management.

In December 2021, a severe log4j zero-day vulnerability was discovered and rapidly exploited by cybercriminals worldwide. Thanks to the ThreatDefence platform's capabilities, the Council could detect the zero-day within minutes of its discovery, ahead of many global cyber security vendors. This allowed them to take immediate action and protect their systems from potential attacks.

"When log4j exploits hit the headlines, like any other organisation, we had to quickly qualify if our environment was vulnerable and if any of our systems were exposed. The ThreatDefence team had already scanned all our systems for exposure, in addition to monitoring every single attempt against our systems in real-time. We got a call from the ThreatDefence Security Operation Centre (SOC) on the same day, reporting to us on the unexpected network sessions and providing the full outline of the attack. It is very difficult to protect from zero-day attacks, but with our level of visibility we feel comfortable and assured."

Stewart Littleford, Manager Information Services
Ballina Shire Council

> *"Although we already had mature controls, we needed another layer of security to get visibility into what was happening in our environment from the cyber security operations perspective. ThreatDefence included everything the Council needed for a comprehensive security operations function with several integrated tools and sensors. It was effortless to deploy and did not require a major investment or an implementation project from our side."*
>
> **Stewart Littleford, Manager Information Services**
> Ballina Shire Council

On the same day, Ballina Shire Council received a comprehensive report from ThreatDefence on all exposed systems and exploitation activity. ThreatDefence was able to provide complete assurance, identify vulnerable components, record all attack attempts, and effectively prevent compromise.

ABOUT THREATDEFENCE

ThreatDefence provides innovative security operations and cyber defence solutions to MSPs and Enterprises. Our SecOps Platform is designed to assist organisations of all sizes in implementing world-class detection and response, utilising all available data sources within their network, on the Dark Web, or concealed deep within their supply chain. We value open ecosystems and seamlessly integrate with any threat intelligence feeds and log sources, delivering immediate, actionable security insights.

For more information, visit
www.threatdefence.com

Phone:
1300 122 434

Email
sales@threatdefence.com

Address:
Level 11, 88 Pitt St,
Sydney, NSW 2000