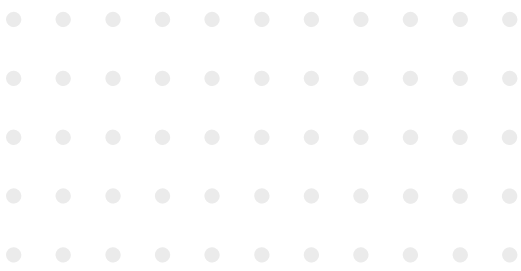




www.campbelltown.nsw.gov.au

Government | 1,000 + Employees



ThreatDefence Helps Campbelltown City Council Maintain A More Proactive Approach To Cyber Security



Campbelltown City Council is one of the largest councils in Australia, serving a significant population. In recent years, the Council has undergone a major transformation of its ICT environment, implementing numerous security controls to improve its security posture. However, the Council's stakeholders were aware that potential weaknesses and exposures still needed to be identified and addressed. As a result, they were seeking a local cyber security partner with expertise in identifying vulnerabilities and mitigating risks.

Previously, local government organisations like councils had little reason to worry about cyber risks. However, the threat landscape has changed dramatically in recent years, and poor cyber security management can expose these organisations to a range of risks, including financial loss, reputational damage, and data breaches. Ensuring robust cyber security practices is paramount for councils like Campbelltown City Council, which hold significant amounts of sensitive information about their communities.

The potential impacts for local government organisations might include:

- Theft of corporate and financial information and intellectual property or theft of money
- Third-party losses when personal information stored on government systems is used for criminal purposes
- Reputational damage associated with the loss of citizens' personal information
- Enormous incident response and investigation costs incurred due to a compromise.

Being concerned with the increasing number of cyber security attacks targeting local government organisations, the Council stakeholders were seeking to understand their level of readiness to tackle cyber security incidents, such as:

- Do we have complete visibility into our cloud infrastructure?
- Can we quickly detect account takeovers, contain a threat, and provide assurance to the organisation that attackers did not spread to other user accounts?
- Can our IT staff provide assurance that our systems are not currently compromised?
- Are we ready to respond to a security data breach associated with citizens' personal data exposure?
- How quickly can our team detect, investigate, and contain cyber threats?

The Council engaged ThreatDefence to perform a security review and analysis of its security posture and assess whether the environment had any indicators of compromise or significant security weaknesses and misconfigurations. During the assessment, ThreatDefence worked with the Council to review the entire organisation's environment and identify security weaknesses or exposures. ThreatDefence consultants focused on the practical aspects of cyber security to assist the Council in identifying tactical and strategic opportunities to enhance the maturity of cyber security and privacy programs.

“

ThreatDefence bridged the visibility and resource capability gap within our existing cyber security controls, resources and technology. We consume the complete cyber security as a service offering from ThreatDefence and the included products / services are excellent value for money for most budget conscious council teams (like ours). The ThreatDefence team truly operates as an extension to our in-house ICT team. The uplift in our cyber security posture means my team and I can sleep better in the current climate of persistent threats.”

Ari Aich, Head of Technology
Campbelltown City Council



ThreatDefence's network, endpoint, and cloud sensors were strategically deployed to analyse the Campbelltown Council's network traffic, collect security events from its infrastructure in real-time, and conduct system scans for any indicators of compromise. The comprehensive data collected was then meticulously analysed by ThreatDefence, utilising advanced security analytics to identify malicious indicators or suspicious and anomalous behaviours. By leveraging this innovative and holistic approach to cyber security, the Council significantly enhanced its overall security posture and created an actionable roadmap of remediations to be implemented as part of its ongoing cyber security program.

“

ThreatDefence equipped our IT Department with superior abilities to collect and analyse security events and proactively respond to data breaches if they occur. Being able to contain threats in real-time provides a tremendous value to our organisation.”

Ari Aich, CIO
Campbelltown City Council




Building upon the success of the initial assessment, Campbelltown Council made the proactive decision to enlist the services of ThreatDefence to provide ongoing cyber security management through a complete Cyber security as a service program (cSaaS). This robust program includes continuous security monitoring, threat detection, vulnerability management, and incident response services, ensuring that the Council is constantly fortified against the ever-evolving landscape of cyber threats. By partnering with ThreatDefence, the Council can rest easy knowing that its cyber security needs are being expertly managed and monitored by a team of seasoned cyber security professionals.



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