Cyber Threat Detection and Response Local Government Organisations

Establish in-depth security monitoring across your whole ICT footprint.

Detect & prevent cyber threats without spending fortunes on incident response.

Support local Australian technology.

As an Australian cyber security vendor, we always wanted to make our platform easy-to-use and affordable for local government organisations. Our solution provides ongoing security monitoring, threat detection and incident response, and can be implemented in hours without the need to deploy any additional infrastructure.

Our platform provides the following benefits:

Visibility and assurance

Enable continuous visibility and threat detection across your entire ICT footprint, detecting malicious activity, threats, and security incidents.

Simple and cost effective

Our platform is cloud-based and can be and does not require any extra infrastructure. It can be deployed in few hours to protect your entire network.

Used by other councils

Benefit from a 100% Australian business. We thoroughly understand your needs and requirements, and your data always stays in NSW.

Threat Detection & Risk Reporting

Use your data to identify and manage cyber risks, getting real-time reporting on the maturity of security controls such as Essential Eight.

"ThreatDefence equipped our IT department with superior abilities to collect and analyse cyber security events proactively, and quickly respond to security incidents if they occur. Being able to contain threats in real time provides a tremendous value to our organisation."

-CIO, a large council in NSW

Web: https://www.threatdefence.com/start-for-free/

Email: team@threatdefence.com

Phone: 1300 122 434

LOCAL GOVERNMENT CHALLENGES

If you're in charge of IT security for a local public sector organisation, you might find yourself in a **difficult situation at the end of 2021**:

- Security threats are very realistic these days, and many public sector organisations are being targeted
- The guidance and support provided by the state government is still very limited
- Your business stakeholders are increasingly using cloud applications, and you are struggling to maintain 100% ownership and accountability of the increasing cloud footprint
- You do not have visibility into your network and your endpoints
- Your budget is limited, and your resources are constrained.

What can you do to **empower your people, prepare to detect and prevent cyber threats, and assure the business that your network is not compromised**? These days, cyber threats can expose local government organisations to a broad range of risks, including financial loss, reputational damage, and data breaches. The potential impacts may include:

- Theft of corporate and financial information and intellectual property, or theft of money
- Legal fees or legal action from losses arising from denial-of-service attacks causing downtime in critical systems
- 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.

> "
> - *67% of councils have not recently performed penetrations testing (cyber-attack simulation);*
> - *84% of councils do not have separate cyber security budget;*
> - *78% of councils do not maintain a centralised register of cyber incident."*
>
> ***-Audit Office NSW, 2020***

Incident response capabilities could lead to a destruction of your reputation and an inability to deliver services to citizens and communities. In recent years, we saw many cases when state and local government agencies in the UK and the US have had to spend millions to deal with the consequences of cyber-attacks. Such attacks are increasing more than 100% year on year, and it is only the matter of time before Australian local government organisations are targeted.

The big question is, **"Are you prepared to detect and respond to such attacks?"** Your answers to the following questions can help you determine your level of preparedness:

- Do you have complete visibility into your cloud accounts, and can you quickly detect account takeovers, contain a threat, and provide assurance to the business that attackers did not spread to other user accounts?
- Can your IT staff provide assurance that your systems are not currently compromised?
- Are you ready to respond to a security data breach associated with citizens' personal data exposure?
- If your systems become compromised tomorrow, how quickly would your team be able to detect, investigate, and contain the threat, and how much would you need to spend on external consultant fees?
- If you were to receive an advisory from your overarching cyber security function at the state government telling you to review all of your systems for specific events and indicators or compromise, how quickly would you be able to do it?

"…86% of councils in NSW are experiencing a skill shortage and 69% are experiencing skills gaps…"

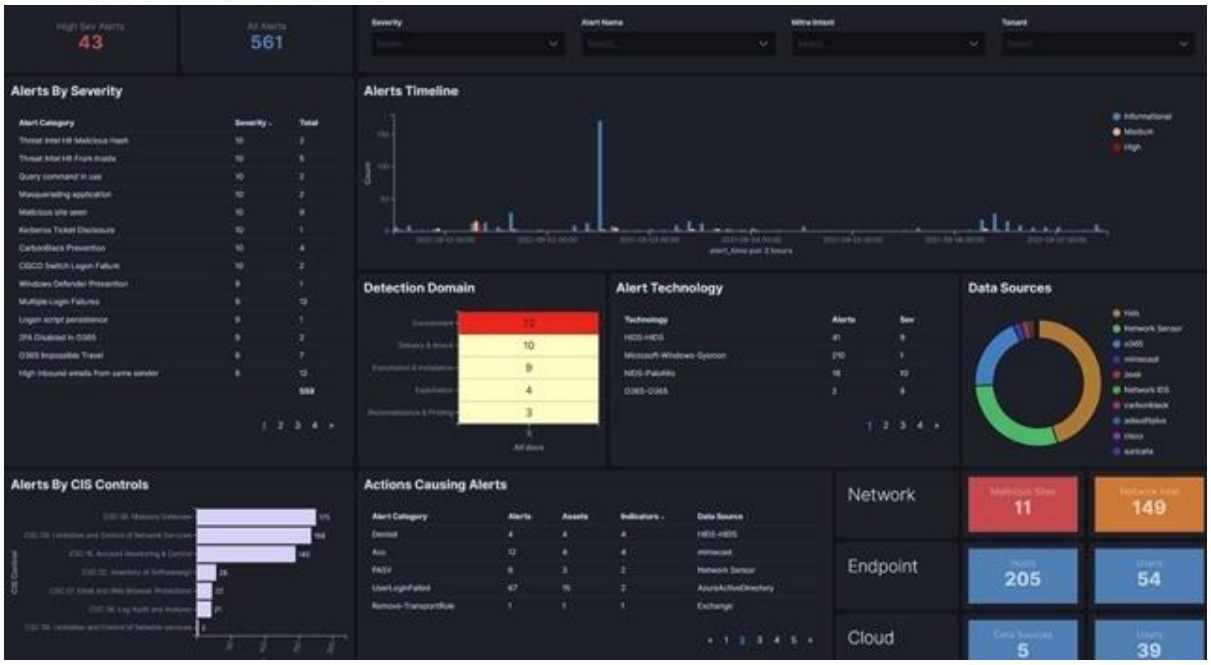
-Local Government NSW, 2020

OUR SOLUTION

As an Australian cyber security vendor, ThreatDefence has created an easy-to-implement solution focused on the needs of Australian local government organisations. Our XDR platform will enable you to enhance your cyber security detection and response capabilities without conducting expensive staff training or investing in long-term implementation projects.

While most security solutions try to solve the threat detection problem from a particular angle, implementing detection capabilities either at the network, cloud, endpoint, or perimeter level, our platform embraces all your security data, from any environment: cloud, SaaS, network, on-premises, remote, or virtual.

ThreatDefence provides a fully managed, plug & play experience, transforming machine data into actionable insights and executive-friendly reports. You do not need to maintain multiple security tools and run complex investigations with endless cross-system integrations, as ThreatDefence establishes context for all security events in your organisation, automatically correlating data from multiple sources.



HOW IT WORKS

It takes minutes to deploy our cloud, network and endpoint sensors which will feed your security data into our cloud platform hosted in Sydney. We offer 30-day free trial will full access to all features – you can start now and see your data coming into the platform in real time.

1 Integrate your security data sources into the ThreatDefence cloud XDR platform in minutes—all data is hosted in Australia.

2 Get your security controls assessment and report in real time, including Essential Eight maturity levels. Get immediate visibility into your on-premises systems, Office365 and AzureAD.

3 Receive detailed onboarding training and ongoing training sessions for your IT team—your IT system administrators will become experienced security analysts over time.

4 Receive a complimentary monthly meeting to get expert advice on your security posture, cyber risks, preventive technologies, etc.

5 Comply with ISO27001 and NSW Government Cyber Security Policy for detection and response capabilities. Support Australian owned and made cyber security business.

SOLUTION HIGHLIGHTS

ThreatDefence delivers continuous assurance across all your cyber security functions and enables your security operations with rich threat context and unbeatable visibility across endpoints, servers, cloud, and SaaS applications.

Paired with our 24x7 SOC as a Service, proactive Threat Hunting, and Incident Response services, ThreatDefence delivers unprecedented value to organisations of any size.

SEE BEYOND the limitations of your current security tools

BLOCK ATTACKS with automated response capability and incident playbooks

BE ABLE to answer any questions about your environment and report on anything

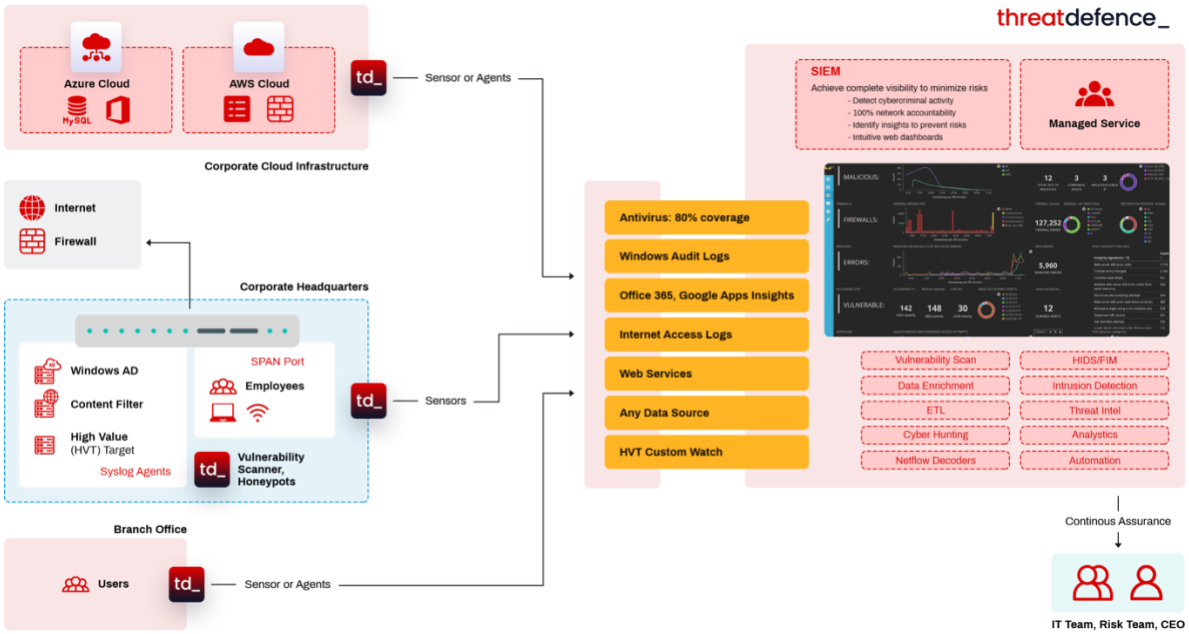
DETECT THREATS with automated detection and threat hunting

MANAGE RISKS with third-party cyber risk protection

PREDICT COMPROMISES with Dark Web monitoring and digital brand protection

PREVENT BREACHES with continuous vulnerability management and device hardening

RESPOND TO INCIDENTS with 24x7 SOC and proactive incident response



WHAT SHOULD I EXPECT?

Our solution provides ongoing cyber assurance – you can always be confident that your environment is not compromised, can detect cyber threat proactively, and quickly respond to security incidents leveraging deep security visibility that our platform provides. You will get deep visibility and detailed reporting on all security events you have, and essential important security controls such as ACSC Essential Eight.

You will be able to deploy professional SOC and SIEM services in one day, meeting all your compliance obligations and recording and storing logs from all your systems. In addition to this, you will get vulnerability management, Dark Web monitoring, integrated threat intelligence, security posture management for your cloud accounts, and many other features delivered to you as an integrated solution.

The platform will provide valuable insights from day one, and was used on multiple occasions in government organisations to reveal:

- Compromised legacy workstations used by hackers on your network
- Compromised Office365 accounts
- Unexpected software
- Exposed and vulnerable systems
- Files with passwords in plain text stored by your users
- Insecure external connections
- User accounts targeted by hackers, and many other exposures and risks.

Our platform is delivered as a fully managed service, and our team will look after you. In additional to automated 24x7 alerting, our experts will conduct weekly in-depth security reviews (threat hunting) and will report on any unexpected events and other anomalies. We also will host a monthly review & training session, reviewing your cyber risks from the operational perspective and providing our recommendations.

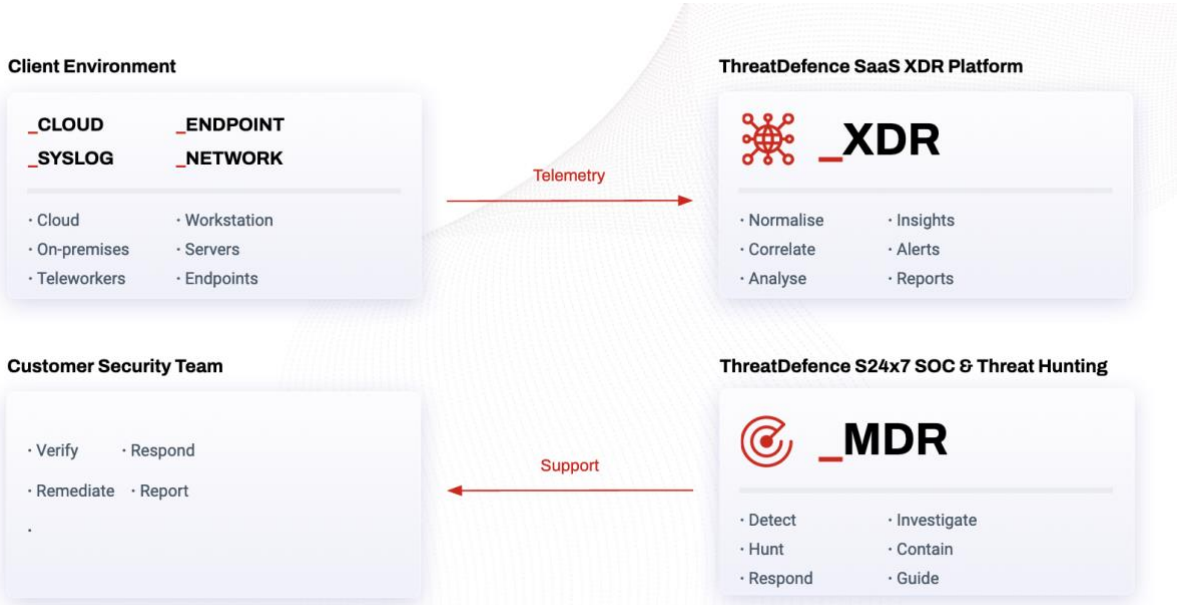
WE BECOME PART OF YOUR TEAM

Our XDR platform provides full enterprise coverage, integrating all the security data you can possibly reach into, including data that directly resides within your network and on your endpoints, as well as external data such as cloud workloads, SaaS applications, Dark Web breaches, compromised credentials, external vulnerabilities, and weaknesses and exposures related to third-party organisations in your supply chain.

Our Managed Detection and Response (MDR) get real-time threat detection, 24×7 threat hunting, thorough investigations and full incident response lifecycle support.

We pair our threat detection technology with trained and experienced security specialists who work 24x7x365 to deliver true cyber resilience capability to your business. Our Security Operations team detects and analyses attack patterns and alerts your team as soon as possible. We will completely integrate into your current workflows and will follow your escalation procedures so you can counter a security threat before it causes any damage.

Our focus is not on raising alerts, but on delivering great security outcomes and defending your business from disruptions and data breaches



ACSC ESSENTIAL EIGHT REPORTING

Our Customer Portal provides ongoing reporting, delivering a snapshot of your security posture in real time.

We have hundreds of security metrics in our platform, and we can report on any of them. Our reporting covers security posture overview, ongoing operational issues, security trends over time, as well as various compliance frameworks such as ISO27001 and ACSC Essential Eight.

BUSINESS CASE FOR YOUR CYBER DETECTION AND RESPONSE

In addition to continuous, context-rich detection and response, our platform also brings a real-time security assurance capability to your organisation. It provides ongoing monitoring of security configurations on-premises and in cloud, as well as detection of vulnerabilities and weaknesses in your external perimeter and your partner organisations to give important context and help predict external threats before they get a chance to reach your environment.

You can choose between one of our service plans below depending on if you'd to get our 24x7 SOC involved or not – in either case, you will get a full set of cybersecurity tools, deployed, managed and supported for you.

Mitigate your resource constraints:

	Cyber Essentials	24x7 SOC
Modern technology provisioning (SIEM, XDR, threat hunting)	+	+
End-to-end onboarding support	+	+
SaaS delivery model	+	+
Ongoing platform management	+	+
Log management	+	+
SIEM, detection rules and correlations	+	+
Vulnerability management	+	+
Dark Web monitoring	+	+
Email monitoring	+	+
Endpoint visibility and threat detection	+	+
Cloud monitoring (AWS, Azure, GCP)	+	+
Network and syslog monitoring	+	+
Application monitoring	+	+
24x7 alerts	+	+
Monthly security review	+	+
Weekly/monthly reporting	+	+
Essential Eight reporting	+	+
24x7 Eyes-on-Glass SOC		+
Threat hunting		+
Proactive Incident Response		+

PRICING

Our pricing is based on the number of permanent users in your organisation. To estimate your monthly subscription cost, you just need to choose between our cyber assurance (TD-XDR) and 24x7 proactive detection & response (TD-SOC) subscriptions, and multiply per-unit price to the number of active users in your organisation. All non-permanent users (such as contractors) with limited access to your environment can be monitored under a discounted identity monitoring license (TD-ID).

Service	Description	Active Users			
		50 - 199	200 - 499	500-999	1,000+
CYBER ESSENTIALS	Our essential security assurance package includes: - Premium cloud XDR subscription, including endpoint, cloud, email, syslog and network monitoring - 3-month data retention - Threat intelligence - Vulnerability management, - Dark Web monitoring, real - time alerting, monthly threat - hunting and monthly - customer review session, - weekly reporting and 24x7 support per user per month (permanent staff members).	$12.00	$10.00	$8.50	$7.00
24x7 SOC	Our cyber security 24x7 detection & response package includes: - all TD-ESSENTIAL features - 24x7 SOC, Managed Detection & Response - Continuous threat hunting, proactive threat detection and incident response per user per month (permanent staff members).	$20	$18.00	$16.50	$15.00
TD-ID	Additional security monitoring for email and cloud accounts, per user per month (non-permanent staff such as contractors).	$2.00	$2.00	$2.00	$2.00

FREE PROOF OF CONCEPT

Starting With ThreatDefence is Easy.

We give you a free month of personalised experience when our team can work with you to ensure that your environment is fully integrated. It will take minutes for your team to deploy our sensors and start received data in real-time.

- See how your data can empower your cyber capabilities
- Experience a fully managed service from ThreatDefence
- Reduce your security operations costs by up to 80%

Contact us today to start for free or to see a live demo:

Web: https://www.threatdefence.com/start-for-free/

Email: team@threatdefence.com

Phone: 1300 122 434

ABOUT THREATDEFENCE_

ThreatDefence provides innovative MDR, SOC-as-a-Service, and proactive cyber defence solutions to MSPs and Enterprises. Our Adaptive XDR Platform was created to help companies of any size to deploy a world-class detection and response, embracing all information that businesses can reach to, would it be within their network, on the Dark Web, or hiding deep into their supply chain. We believe in open ecosystems and connect you to any and all threat intelligence feeds and log sources, instantaneously providing you with actionable security insights. For more information, visit www.threatdefence.com.