threatdefence_

SOLUTION BRIEF

SOC as a Service for Managed Service Providers

Establish ongoing visibility and assurance for your customers with our SIEM/XDR platform

Detect cyber threats proactively and provide rich reporting and visualisations

Start providing advanced 24x7 cyber security services to your customers tomorrow.

ThreatDefence is the only Australian SOC-as-a-Service Managed Detection and Response provider using Australian-grown technology and providing comprehensive coverage across all parts of your enterprise. Take advantage of our scalable business model – get full access to our platform and our 24x7 team of security experts. We will provide you with everything you need to start and grow your cyber security business, from technology and 24x7 support to marketing collateral.

SIEM/XDR toolset

Cloud based technology ready to go from day one, full stack of endpoint/cloud/network security monitoring and threat detection.

Simple and cost effective

No need to start a new project or hire consultants. We will work directly with your team and will equip you with everything you need to get started.

Proven solution used by other MSP's

Partner with 100% Australian business. We thoroughly understand your needs and requirements, and your data always stays onshore.

24x7 SOC

Provide proactive monitoring and incident response with a 24x7 team of cyber security experts.

Our technology has been developed in Australia and we will work hard to make you successful. Start with us for free now and support local Australian business.

Visit https://threatdefence.com/demo to get started.

AUSTRALIAN MADE AND OWNED

FROM MSP TO MSSP OVERNIGHT

Cyber security threats are very realistic now, with many organisations being targeted by ransomware operators and other threat actors.

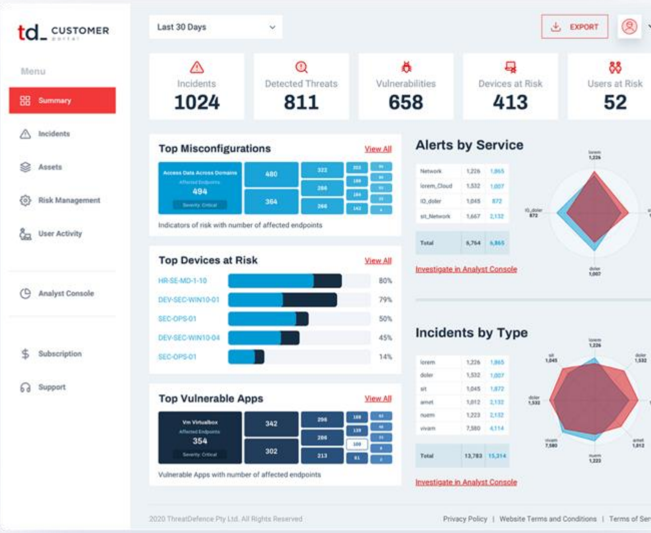
These days, MSP’s are often being asked if they can provide Security Monitoring, Incident Response and managed SIEM services. What can you do meet these demands, empower your people to detect and respond to cyber threats, and assure your customers that their environments are protected?

Implementing cyber threat prevention and detection services traditionally required large investments across staff, operational tools, implementation, maintenance and technology. As an Australian cyber security vendor, ThreatDefence has created an easy-to-implement solution specifically designed for MSP’s. Our MDR and SOC services will enable you to enhance your cyber security detection and response capabilities without conducting expensive staff training or investing in long-term implementation projects.

Deployed and operational in a fraction of the time and cost versus a do-it-yourself (DIY) model, ThreatDefence MDR and SOC services are designed to get you started immediately, providing scalable 24x7x365 threat detection and incident response.

Our flexible growth model allows you to start now and bring to market advanced Security Operations, Managed Detection and Response, and Threat Hunting services tailored to the specifics of your industry and your business.

We have everything ready to go for you – people, process & technology, as well as sales & marketing collateral and MSSP service packages to deliver to your customers.
Our cyber security experts will work with your team to launch your cyber security program and get you started. We do not require any minimum commitment from you, and ready to onboard your customers immediately.



Network	1,226	1,865
lorem_Cloud	1,532	1,007
IO_doler	1,045	872
sit_Network	1,667	2,132
Total	6,764	6,865

lorem	1,226	1,865
doler	1,532	1,007
sit	1,045	1,872
amet	1,012	2,132
nuem	1,223	2,132
vivam	7,580	4,114
Total	13,783	15,314

WHY PARTNER WITH THREATDEFENCE?

ThreatDefence is the only solution in the industry that 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, managed Threat Hunting and Incident Response services, ThreatDefence delivers unprecedented value to MSP's of any size.

SEE BEYOND the limitations of your current security tools

REPORT on any security metric and be able to analyse any security event

PREVENT BREACHES with continuous vulnerability management and device hardening

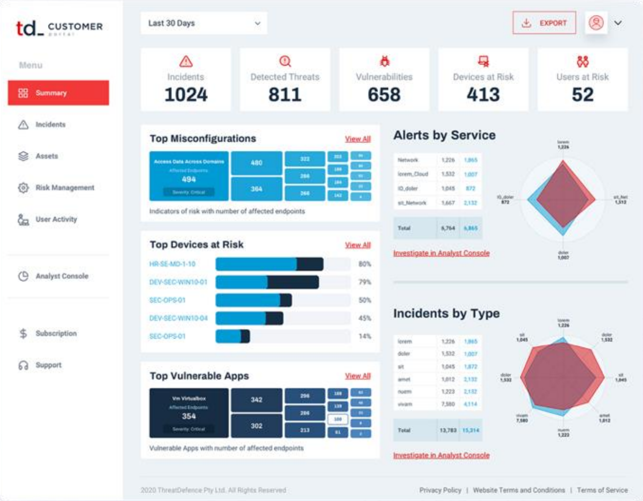
DETECT THREATS with automated detection and threat hunting

PREDICT COMPROMISES with Dark Web monitoring and digital brand protection

RESPOND TO INCIDENTS with 24x7 SOC and proactive incident response

We have been working with MSP's for a very long time and understand the challenges you and your customers have, as well as the criticality of providing effective cyber security solutions to your customers at a reasonable price.

Our MSSP Enablement program allows you to become a competitive security services provider overnight, delivering high-value cyber security solutions to your customer base. We support you with the definition of your service offerings and your go-to-market initiatives and provide a well-paved path for your growth with options to build your own in-house cyber security capabilities, integrating organically into your service delivery framework.



Indicators of risk with number of affected endpoints

Vulnerable Apps with number of affected endpoints

Alerts by Service

Network	1,226	1,865
lorem_Cloud	1,532	1,007
IO_doler	1,045	872
sit_Network	1,667	2,132
Total	6,764	6,865

Incidents by Type

lorem	1,226	1,865
doler	1,532	1,007
sit	1,045	1,872
amet	1,012	2,132
nuem	1,223	2,132
vivam	7,580	4,114
Total	13,783	15,314

2020 ThreatDefence Pty Ltd. All Rights Reserved

BUSINESS CASE FOR YOUR MDR AND SOC SERVICES

ThreatDefence is the only Managed SOC solution that allows you to easily move between service tiers and focus on what works the best for your business in any particular moment of time.

With ThreatDefence, you can start with our 24x7 SOC service and build your cyber security capability at your own pace. At any point in time, you can get your people to take over day-to-day security operations and continue using our platform with an in-house team of security analysts.

Mitigate your resource constraints and start delivering 24x7 SOC services now:

	ThreatDefence
Modern technology provisioning (SIEM, XDR, threat hunting)	+
End-to-end onboarding support	+
SaaS delivery model	+
Ongoing platform management	+
Build your own SOC	+
24x7 Incident Response	+
SIEM and SOC services	+
Real-time dashboards	+
Customisable Reports	+
MITRE ATT&CK mapping	+
24x7 alerts	+
Threat Hunting	+
Investigation and Incident Response	+
Network Traffic Analysis	+
Dark Web monitoring	+
Vulnerability Management	+
Cloud Monitoring and Assurance	+
Daily Compliance Checks	+
Log Management and Data Retention	+
Compliance Reporting	+
Customer Portal with real-time and historical data	+

DEPLOY OUR SIEM/XDR PLATFORM IN MUNUTES

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, ThreatDefence's Adaptive XDR platform embraces all your security data, from any environment.

Our 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 the 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.

_ENDPOINT

Advanced endpoint visibility, forensic analysis of endpoint telemetry, detection and response

_NETWORK

Detect insider threat and lateral movement with network-based intrusion detection and packet analysis

_CLOUD

Multi-cloud security insights, cloud workload vulnerability management and continuous risk assessment

_OSINT

Continuously integrated Open Source Intelligence, including indicators from Dark Web, social media, and third-party vulnerabilities

_ANYTHING

Any standard or custom application or log source, completely integrated into the platform

Our platform provides an unmatched capability to visualise your networks and systems and expose high-risk areas across cloud, on-premises, or virtual and delivers an end-to-end cyber security solution, with full cycle detection, investigation, and response across all areas of your enterprise. It provided you with capabilities to protect the entire enterprise, collecting information from all environments, including risks associated with your partners and suppliers. The platform correlates security events across all sources, and applies advanced machine learning to detect sophisticated threats and provide insights over the entire enterprise's digital footprint.

AUSTRALIAN TECHNOLOGY

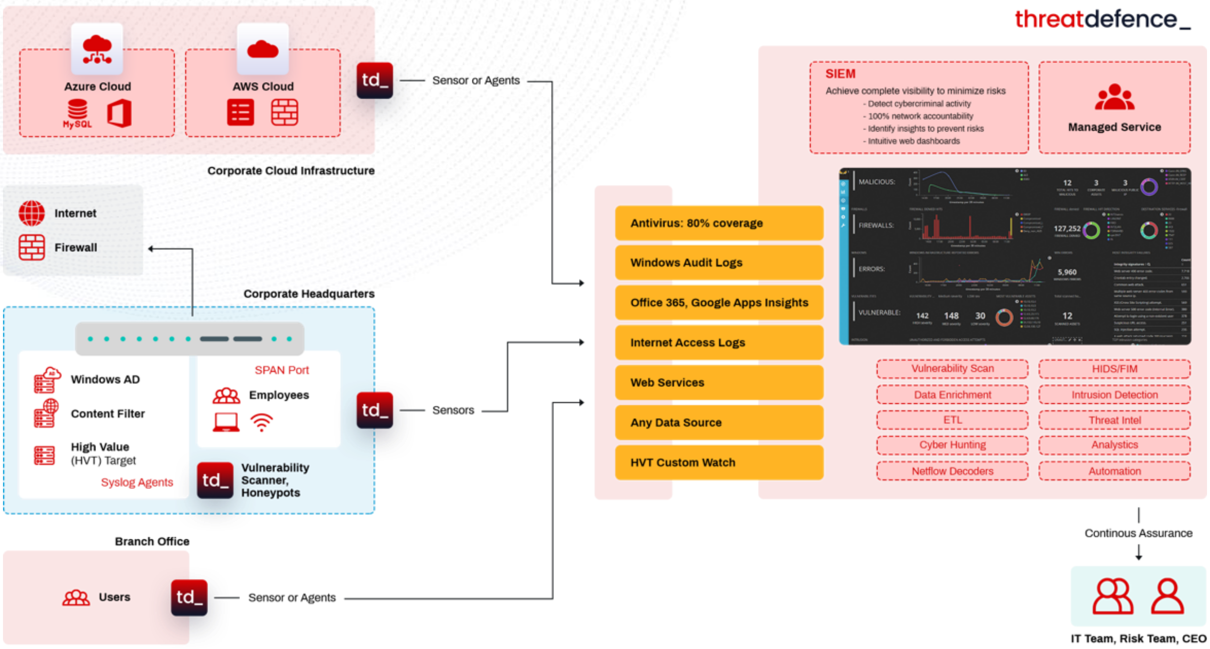
- Designed, developed, hosted and managed in Australia
- No minimum commitment for Australian MSP's
- Unrestricted integration capability, support for any log source or custom data
- 24x7 SOC based in Sydney

DEVELOPED FOR MSP's

- Easy installation, management, and support; 100% cloud-based platform
- Multi-tenant environment, search and report across all of your tenants
- Comes with integrated threat intelligence, dark web monitoring, vulnerability management, automated security assessment and many other features
- White-labelled Customer Portal and Analyst Console

EASY DEPLOYMENT

- A lightweight agent deploys in seconds without any impact on user productivity
- An extensive library of ready-to-go cloud and syslog integrations
- Automated deployment options.



WE BECOME PART OF YOUR TEAM

Deployed within minutes, our cloud-based platform provides immediate security backed by 24/7/365 SOC team - all through an affordable, subscription-based service.

We will pair our cyber security technology with trained and experienced security specialists who works 24x7x365 to deliver true defence to your business. Our Security Operations team detects and analyses attack patterns and alert your team as soon as possible.

We will completely integrate into your current workflows and will follow your escalation procedures so you can counter security threats before they cause any damage.

Our SOC-as-a-Service provides MSP's with scalable options to grow your cyber security business. We offer multiple options on how you can get started – you can completely outsource your service to us, or you can use us as the last line of your response capability and get your technical team to handle initial alerts and customer requests.

In any case, you will have direct access to our threat hunters, incidents responders and platform engineers, and will get your requests resolved in real time.

Whenever it comes to Incident Response, we work with your technical team to contain cyber threats as soon as possible. We support Incident Response lifecycle end-to-end, prioritising quick threat containment and root cause identification. As a breach is contained, we will work to collect evidence, determine instances of data exfiltration, conduct forensic analysis and prepare a detailed post-incident review.

Continious Monitoring

We monitor security events and detect threats in real time, 24 hours a day. Our system process your data non-stop and provide true correlation and detection in real time.

Security Geeks

We hire people who understand cyber security and love technology. They organicly extend your existing team to keep you secure.

Threat Intelligence

We understand cyber security and now how it works – we always consider real world detection scenarios, not just alerts and thresholds.

HOW IT WORKS

Our platform is 100% cloud-based and is available to be used immediate by you and your customers. It only takes few simple steps to start using our solution:

1 Integrate your security data sources into the ThreatDefence cloud XDR platform in minutes—all data is hosted in Australia. We can collect data from your endpoints, cloud accounts, dark web, syslog sources and applications.

2 Visualise your data and get security threats, vulnerabilities and weaknesses detected in real time.

Get immediate visibility into your on-premises systems, Office365, AWS, and many other systems and platforms.

3 Customise your report templates and activate SOC notifications and alerts. We can send alerts and reports to your IT team, or directly to your customers.

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

VALUE PROPOSITION TO YOUR CUSTOMERS

Based on the latest Australian Cyber Security Centre data, more than 60% of Australian SME's could not fully recover from a significant security breach and had to cease their operations due to significant financial or reputational damages.

Every business wants to get assurance that:

- Your computer is not compromised
- Your data was not stolen and used by your competitors
- Your credentials are not posted on Dark Web forums, and can be easily discovered by other hackers.

- On average it takes a business:
- 50 days to detect a cyber breach
- 30 days to contain a cyber breach
- Average cost of a cyber attack - $276,323

Australian Government, 2020

It takes 50 days on average for a business to detect a security incident, allowing attackers a lot of time to execute on their objectives.

If your customer organisation is breached tomorrow, do you know what you are going to do? Security Incident Response is a rather expensive activity, requiring weeks of security experts' time working on premium rates, and also burning an enormous amount of time from your business as well, as recovery efforts might be extremely time consuming.

Most businesses have no visibility into what is happening on their network, and therefore cannot confidently detect cyber threats, or easily understand the extend of the threat in case of a compromise.

The cost of being protected is not high – with our SOC as a Service you can provide your customers with:

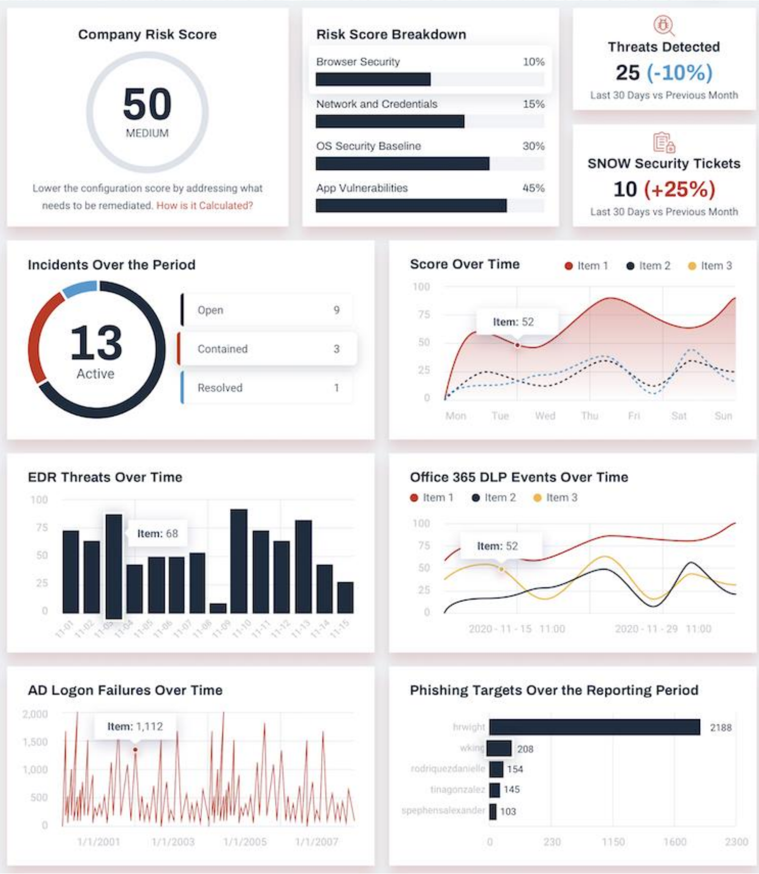
- Ongoing security monitoring of systems and networks, detecting any malicious activity
- Dark Web monitoring, providing proactive notifications if user accounts are compromised
- Continuous forensic recording of security events, allowing quick investigations and breach containment
- 24x7 Security Operations Centre, providing incident response and guidance in case of a data breach.

WHITE LABELED REPORTING

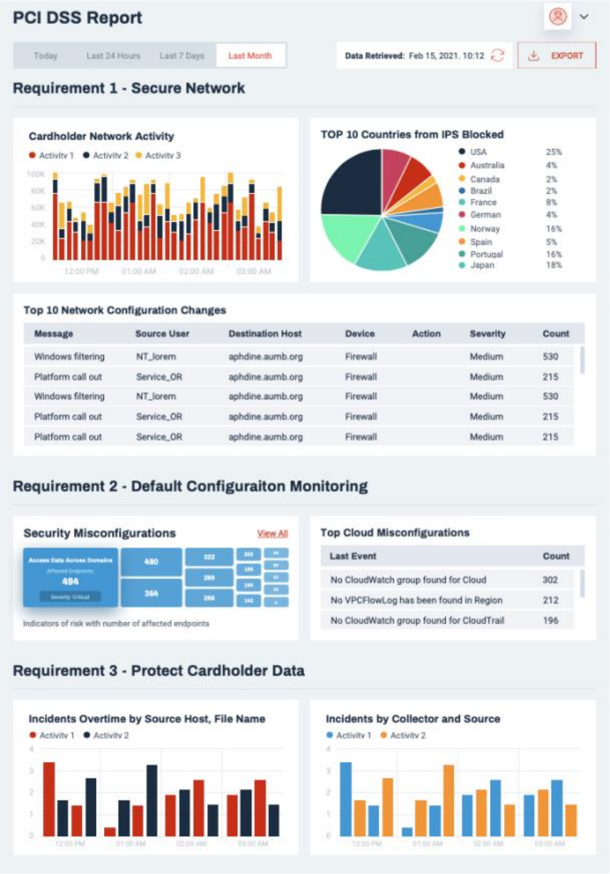
We provide automated weekly and monthly reporting to your partners based on their operational and compliance needs. We will work with you to customise your report templates based on your technology stack and will ensure your customers get all the information they need.

Our reporting covers security posture overview, ongoing operational issues, security trends over time, as well as various compliance frameworks such as ISO27001, APRA CPS 234, Essential Eight, PCI DSS and others.

Our 24x7 SOC reports also include analyst notes for notable security events and incidents, providing proactive advice on what can be improved or what remediation actions could be applied. All reports can be white labelled -just send us your logo, and we will do the rest.



Lower the configuration score by addressing what needs to be remediated. How is it Calculated?



Data Retrieved: Feb 15, 2021. 10:12

Requirement 1 - Secure Network

Top 10 Network Configuration Changes

Message	Source User	Destination Host	Device	Action	Severity	Count
Windows filtering	NT_lorem	aphdine.aumb.org	Firewall		Medium	530
Platform call out	Service_OR	aphdine.aumb.org	Firewall		Medium	215
Windows filtering	NT_lorem	aphdine.aumb.org	Firewall		Medium	530
Platform call out	Service_OR	aphdine.aumb.org	Firewall		Medium	215
Platform call out	Service_OR	aphdine.aumb.org	Firewall		Medium	215

Requirement 2 - Default Configuraiton Monitoring

Indicators of risk with number of affected endpoints

Top Cloud Misconfigurations

Last Event	Count
No CloudWatch group found for Cloud	302
No VPCFlowLog has been found in Region	212
No CloudWatch group found for CloudTrail	196

Requirement 3 - Protect Cardholder Data

© 2021 ThreatDefence all rights reserved

START TODAY FOR FREE

At ThreatDefence, we know that seeing is believing. Lots of products claim to do wonderful things but disappoint when the rubber hits the road. For us, the opposite is true. When people see ThreatDefence live on their security data, the potential suddenly comes alive, and the value appears.

A free Proof of Value (sometimes called a Proof of Concept) is the first step in the introduction of ThreatDefence to your team. In this carefully controlled and managed engagement, we connect ThreatDefence to your systems, collect security data, and then work with your team to produce meaningful insights on your cyber security posture. We highlight areas where your systems might be compromised, vulnerabilities might be present, and security configurations could be enhanced.

We can run a Proof of Value for your own infrastructure, as well as for 1-2 of your customers. We will create a multi-tenant instance for you and will onboard your data – you will get immediate access to all dashboards, alerts and reports, as well as to our 24x7 SOC team.

If you like what you see, you can continue using the service on a monthly basis – and your first month will be free!

ABOUT THREATDEFENCE_

PHONE:
1300 122 434

EMAIL:
team@threatdefence.com

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

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.