LAUNCH YOUR OWN SECOPS IN A DAY

Get your security data to work for you.

Businesses now understand that to be secure they cannot rely on traditional SOC and MDR providers anymore. They are seeking to deploy internal, bespoke Security Operations capability, establishing control over their security data as well as implementing customized detection and response mechanisms.

At ThreatDefence, we believe in giving you unrestricted access to your security data and providing comprehensive visibility across your entire IT stack. Our platform empowers you to establish an effective and sustainable Security Operations capability by transforming your data into actionable evidence. We work with you to integrate people, processes, and technology that align with your unique needs and budget, so you can confidently implement a capability that works for you.

ThreatDefence is the only SecOps as a Service company providing broad coverage across your entire technology stack with provable, evidence-based security. Our vision is to allow any business in the world to get their security data to work for them. We provide security teams with full-stack SecOps infrastructure - you get deep visibility from day one, gain control over your security data, and get access to a comprehensive set of ready-to-use tools, detections, workflows, playbooks and scenarios.

Collect Evidence, Not Noise

Gain complete visibility into all enterprise services, record and analyze all security events and see what is important.

Augment Your Security Tools

Get a single pane of glass for all security events and alerts, and detect threat actors with high confidence with our SecOps toolset.

Get Full Coverage

Utilize our SecOps platform to get end-to-end coverage for your environment, including NDR, deception, cloud visibility and SOC automation.

Leverage Our 24x7 SOC

Partner with our team of cyber security experts for advanced threat hunting, incident response and digital forensics.

Solution Brief

threatdefence_

Why Partner With ThreatDefence?

Everyone is being hacked despite spending millions on cyber security.

It seems like every vendor has a solution on how to protect your business. The promise is a simple and reliable cyber security. So why are organizations still getting breached?

The main reason is lack of visibility – most solutions in the market provide limited coverage, and at the same time operate as a black box – your security data is being sent somewhere to a cloud, however you can't ever see what is being collected and what is not.

Visibility + Evidence = SecOps

An alternative is to build to your own, customized Security Operations which will employ a variety of tools to provide you with end-to-end visibility, putting you in control over your data. This process normally takes months and requires a significant investment across technology and people domains.

ThreatDefence provides security teams with ready to use, end-to-end SecOps solution, including a full stack platform able to capture and correlate all types of security data, supported by Next-Generation SIEM, NDR, endpoint visibility, integrated threat intelligence, automation, SOC workflows and 24x7 team of cyber security experts.

We exist to evolve your cyber security approach from 'promise-based' to 'evidence-based' security, from 'probably secure' to 'provably secure'.

Our evidence-based approach to cyber security provides you with deep, forensic-like visibility in your environment. Our cloud SecOps platform can be deployed in minutes, transforming your data into evidence, and detecting active and dormant threats in your environment.

At the same time, it integrates with your existing security stack from day one. You can select your current security products from the list of hundreds of pre-built integrations and use our lightweight sensors across your on-prem and cloud environments.

Deep Visibility and Next Generation SIEM	**Full enterprise coverage, simple pricing model** Deploy in hours with full content and threat intel. Get comprehensive coverage from day one and avoid additional licensing costs in 1-2 years.
Recorded Evidence - Foundation for Premium SOC and IR	**Everything is recorded and can be inspected in real-time on any scale** In-depth, forensic-like visibility for breach detection, real-time forensics and incident response.
Premium SecOps - NDR, Deception, SOC Automation	**Cover your entire attack surface with premium capabilities** Deploy all SecOps tools from the same platform and detect threats in secods.
Evolving Cyber Security	**Stay ahead of threat actors with evolving SecOps** We continuously update and improve our tools to provide you with the latest SecOps capability, keeping attackers at bay.

Our Next Generation SecOps Platform

Our SecOps Platform is designed to assist businesses of all sizes in implementing world-class detection and response, utilizing all available data sources, whether it be within their network, on the Dark Web, or concealed deep within their supply chain.

The platform 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 organization, automatically correlating data from multiple sources and investigating anomalies.

With our SecOps infrastructure, you will have an integrated, comprehensive suite of threat detection and incident technology, creating a single cyber security context across all your systems and networks.

Mitigate your resource constraints and launch your fit-for-purpose SecOps now:

✔ Complete SecOps Suite (SIEM, XDR, NDR, TI, Automation)	✔ MITRE ATT&CK Mapping
✔ SaaS Delivery Model	✔ Playbooks and Automation
✔ Ongoing Platform Management	✔ Digital Forensics Toolset
✔ Detection Use Cases - Daily Updates	✔ Network Detection and Response
✔ Machine Learning and User Behavior Analytics	✔ Vulnerability Management
✔ Curated Threat Intelligence	✔ Cloud Monitoring and Assurance
✔ SIEM and 24x7 SOC services	✔ Inventory and Security Configuration Benchmarking
✔ SOC Workflows for Alerting and Escalations	✔ Attack Surface Management
✔ Real-Time Dashboards	✔ Log Management and Data Retention
✔ Customizable Reports	✔ Compliance Reporting
✔ 24x7 Incident Response	✔ Customer Portal with Real-Time Reports
✔ Threat Hunting Artefacts	✔ Hacker Deception
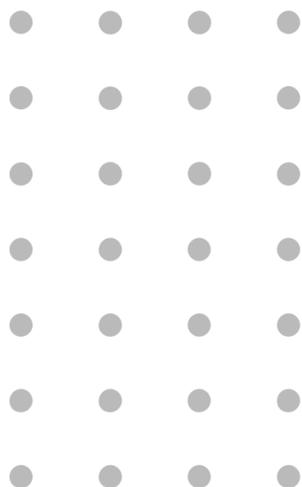
Fit-For-Purpose Security Operations

At ThreatDefence, we put a lot of value in your security data. Our SecOps infrastructure tools can be deployed into your cloud, network or endpoints to provide deep, forensic-like visibility. Every security event is being recorded and can be inspected in real-time or historically on any scale.

With ThreatDefence, you will not have any blind spots — all data can be operationalized and used for your analytics, hunting, detections and incident response. Equipped with our SecOps infrastructure tools and deep visibility, you can build and continuously evolve your own, customized Security Operations capability.

Deploy in Minutes

- Easy installation, management, and support; 100% cloud-based platform
- Comes with numerous integrations to support your existing tech
- Supplied with threat intel, hundreds of detection use cases and playbooks.

Enterprise-Grade SecOps

- Evidence-based security with NDR, endpoint DFIR, deception
- Next-Generation SIEM, integrated automation and Threat Hunting
- Cyber risk management with Dark Web, multi-cloud visibility, attack surface monitoring threat intel and more.

Evolving Cyber Security

- All-inclusive pricing model
- Continuously updated behavior analytics and ML detections
- New SecOps features based on the community feedback.
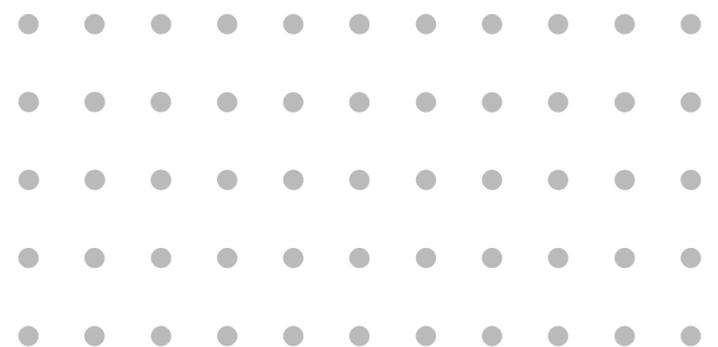
ABOUT THREATDEFENCE

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

For more information, visit
www.threatdefence.com

Phone:
1300 122 434

Email
team@threatdefence.com

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