THREATDEFENCE:
EXECUTIVE OVERVIEW

ThreatDefence is an Australian cybersecurity company focused on modern Security Operations for enterprise, government, and critical infrastructure environments. We combine our unified SecOps platform with Australian-based 24×7 Security Operations Centre services to help organisations detect threats earlier, investigate faster, and respond with greater confidence.

Why Organisations Look at ThreatDefence

Australian organisations know they need protect themselves against advanced cyber threats, and understand the value of security operations centre and ongoing detection and response, but face the same core challenges:

Insufficient Resources

Internal teams often do not have the time, coverage, or specialist capability needed to run effective security operations.

Inefficient Service Providers

Attempts to outsource security operations often leave companies with limited visibility into what is happening and why.

Too Much Noise

A growing stack of separate products increases complexity, alert fatigue, and operational overhead.

Cost of Investment

Security solutions can take too long to deploy and expensive to maintain, costs grow exponentially.

Company at a Glance

Founded:

- 2014

Headquarters:

- Sydney, Australia

Focus:

- Security Operations Centre
- Managed Detection and Response
- SIEM, NDR and SOC Automation

Core Offering:

- Unified SecOps platform with 24×7 Australian SOC services.

What ThreatDefence Delivers

Our approach is built around a simple idea: security operations should reduce risk, not create more complexity. Instead of forcing organisations to manage disconnected tools, fragmented data, and alert overload, ThreatDefence brings together telemetry, SecOps toolset, threat intelligence, detection rules, automation, response and reporting in one operating model.

Our SecOps platforms ingest millions of events in real time from your environment, while our local team applies threat intelligence, detection logic, AI-driven automation and playbooks to build and maintain aligned to your unique security use cases.

Without reliance on legacy tools which are often difficult to scale and manage, we operate efficiently and keep costs predictable, while also ensuring Australian data sovereignty.

What ThreatDefence Delivers

ThreatDefence provides a unified platform for collecting, normalising, correlating, and analysing security telemetry across endpoint, identity, cloud, on-premises infrastructure, and network environments. This enables earlier detection of suspicious activity, faster triage, and stronger investigative depth.

Our Australian-based 24/7 SOC monitors and investigates around the clock, escalating high-confidence activity with clear evidence, impact context, and recommended response actions. Where deeper support is needed, the same operating model extends into incident response and forensic investigation.

For organisations with operational technology, ThreatDefence also supports OT-aware monitoring and network visibility, helping security teams detect threats in environments where uptime, safety, and operational continuity are critical.

Because ThreatDefence uses an integrated SecOps toolset, our customers avoid lengthy deployment cycles, accelerate onboarding, and begin integrating telemetry in hours or days rather than months, delivering value faster.

Key Capabilities

- ✓ **Managed SIEM and detection engineering**
  Centralised log collection, correlation, detection, enrichment, and alert triage across hybrid environments.
- ✓ **24×7 SOC and MDR**
  Continuous monitoring and investigation by Australian-based analysts with structured escalation and response coordination.
- ✓ **Network Detection and Response**
  Behaviour-based detection of lateral movement, anomalous communications, and suspicious network activity.
- ✓ **Dark Web Monitoring**
  Continuous discovery of exposed credentials, leaked data, and external threat activity relevant to your organisation.
- ✓ **Attack Surface Management**
  Continuous visibility of internet-facing assets, exposures, and security weaknesses that may increase risk.
- ✓ **Automation and Response Workflows**
  Playbooks for enrichment, case handling, notification, evidence capture, and controlled response actions.
- ✓ **Evidence-led Investigations**
  A case-driven approach that brings together timelines, artefacts, and supporting evidence so teams can act on facts rather than isolated alerts.
- ✓ **Integrated DFIR**
  Seamless escalation to deeper incident response and forensic investigation during major incidents.
- ✓ **OT and Critical Infrastructure Visibility**
  Integrated monitoring across industrial and operational environments, not just traditional IT estates.
- ✓ **Legacy SIEM Migration**
  Support for transitioning from other SIEM platforms including transfer of data and detection rules.

PROOF OF CONCEPT

A free Proof of Concept is a fast and low-impact way to see real value in your own environment. From day one, the platform starts uncovering hidden assets, unexpected communications, insecure access paths, and behaviours that may be increasing risk without being visible today.

If you are ready to validate our solution your organisation, the next step is simple. Contact us to arrange an initial discussion or technical walkthrough, and we will guide you through the deployment that delivers immediate visibility.

For more information, visit
www.threatdefence.com

Phone:
1300 122 434

Email
sales@threatdefence.com

Address:
17 Castlereagh St,
Sydney NSW 2000