Advanced Detection and Response

Perfect for small business

Automatically uncover and stop elusive threats with agility and precision

ADR provides businesses with continuous real-time monitoring of security services and automated threat visibility, detection, alerts with response to attacks and incidents. Currently available with Email Security, the technology is road mapped to be integrated through Web, Endpoint and Firewall providing real Extended Detection and Response (XDR) capability.

Currently it provides in-built advanced email protection against targeted phishing and impersonation attacks (Business Email Compromise (BEC), email account takeover, trusted relationship). It provides continuous threat hunting via retrospective analysis of URL/Links and attachments in delivered emails and threat containment via automated inbox message clawback to 'defuse' advanced persistent threats and targeted attacks by cyber criminals before any damage can be caused to SMBs' business.

'Defuse' advanced persistent threats and targeted attacks

Continuous threat hunting

Real-time monitoring and remediation

Unique application of **Security Information and Event Management (SIEM)** technology, security engineering & advanced threat research and intelligence to protect any size of business from the latest targeted phishing attacks.

Powered by world's leading solutions for small business

SHELT FirstWave

CyberCision

Advanced Detection and Response

Perfect for small business

Features

ADR Labs
ADR Labs is the global threat intelligence arm of FirstWave comprised of cybersecurity engineers and data scientists focused on discovering and collecting unknown threats. The Lab conducts innovative experiments including forays into the dark web to gather novel and behavioural data relating to emerging threat actors.

The advanced analytics applied to this data lies at the heart of creating countermeasures which safeguard users against sophisticated attacks.

Threat Intelligence Platform
Acquiring, aggregating and actioning threat intelligence shared by a large variety of well-regarded threat sources into a Threat Intelligence Platform to more quickly and accurately detect phishing threats targeting the business

Dark Web Monitoring
Gathering Threat Intelligence on phishing and malware activities of threat actors 'lurking' in the dark web to foster preparedness against phishing threats that could target the business in future

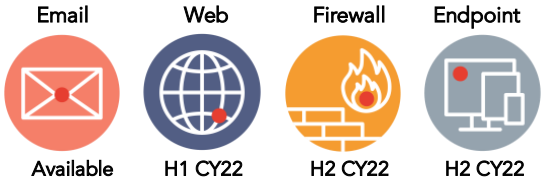
Threat Analysis Team
Security Engineering to continuously:

- Optimise, 'fine-tune' correlation rules
- Test and verify detection & response engine effectiveness

'Red/Blue team' expertise:

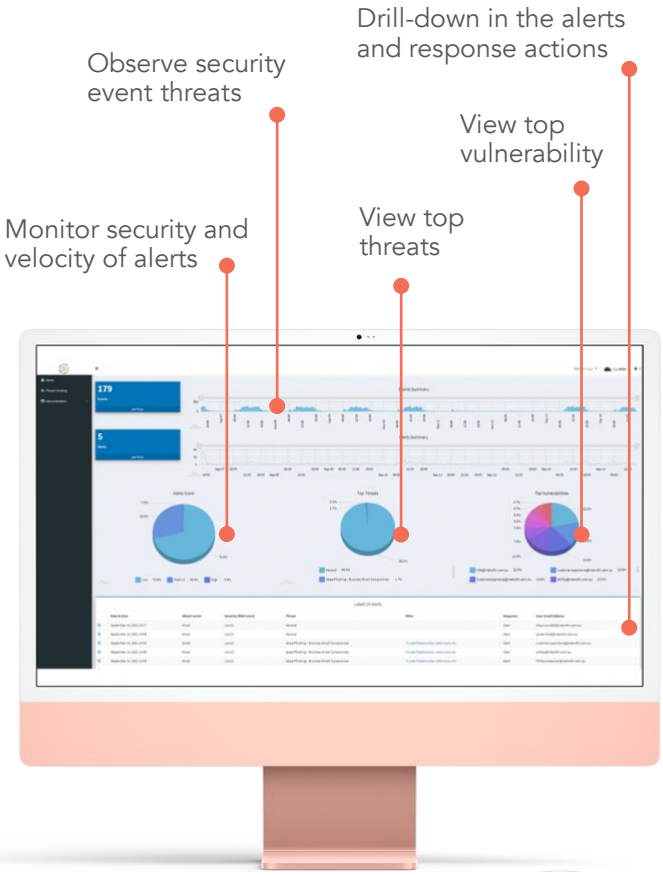
- Deep knowledge of critical phishing vulnerabilities e.g. Microsoft 365
- Monitor & emulate latest adversary/attacker threats
- Test and verify detection & response engine effectiveness

Security Service Integrations:



ADR Threat Dashboard

Full visibility and control of discovered threats



CyberCision