Threat Detection, Investigation and Response (TDIR)

Red Piranha
unified threat management

CYBER THREAT ALLIANCE

Australian Government Department of Defence

Australia

Defence Industry Security Program

Quickly and efficiently identify, assess and respond to all threats, with Red Piranha.

Up to **10x Increased Visibility** - Gain critical visibility and insight into network operations to deal with APTs and previously unknown attacks through network behavioural analytics.

Deploy fully **Operationalised and Contextualised Threat Intelligence** efficiently and receive Automated Actionable Intelligence to Protect, Detect and Respond to threats proactively.

24/7 access to our "village" of security professionals leveraging Human-machine teaming for improved alert prioritisation and incident response.

Flexible In-line Deployment to avoid disruptive infrastructure changes and eliminate the need for engineering overheads.

Threat Detection, Investigation and Response (TDIR)

- Advanced heuristics and ML anomaly detection with World-Class Threat Intelligence for contextualised, high confidence alerts.
- Push-button escalation to Red Piranha's SOC - Remove complexity, instantly escalate an event to the SOC team and enhance security operations.
- Receive instant alerts and after-action reports directly from the Red Piranha SOC team with Platinum SIEM.
- Proactive threat hunting and investigation to detect advanced APTs, LotL (Living off the Land) and other indicators to reduce dwell time.
- Multi-tenanted, single platform sensor deployment to improve detection engineering efficacy across East-West traffic flows.
- Industry-leading forensic log retention for 18+ months to help meet compliance.

With best-in-class Threat Detection Investigation and Response, effectively detect, correlate and respond to adversary activity on your networks including advanced lateral movement and other IOCs that are often left undetected.

Together with human-machine teaming and state-of-the-art technology, our clients get cohesive protection against advanced persistent threats (APTs) without the need for new specialist engineering teams, reducing the total cost of ownership for maximum security outcomes.

Red Piranha is Australia's leading developer, manufacturer, and official member of Team Defence Australia for advanced cybersecurity solutions.

24x7x365 protection for your organisation.

Meet your compliance challenges.

ISO 27001:2013 Certified Cert. No.: 781489

ISO 9001:2015 Certified Cert. No.: 703236

Our ISO 27001 and ISO 9001 Certifications demonstrate that our processes, tools, and systems adhere to a recognised framework.

Red Piranha
unified threat management

- Enhance Security Operations
- Thwart Sophisticated Attacks
- Detect all known Malware families and CnC call outs
- Reduce Total Cost of Ownership (TCO)

NEXT STEPS

1. Get in touch
2. Get a proposal
3. Get started

info@redpiranha.net

+61 8 6365 0450
+61 2 8089 1219

redpiranha.net