orro®
Cyber Security

Managed Detection & Response Services

Our managed detection and response (MDR) services provide security assurance via modern, remotely delivered, 24/7 Security Operations Centre (SOC) capabilities to increase your business's digital maturity.

orro.group

Securely Connected Everything™

With technology integrated across every aspect of your business, you must consider your company's security position.

Technology is pervasive, connecting us to customers, giving people access to multiple digital platforms, anywhere, any time.

As such, your business is susceptible to security weaknesses and the threat actors who attempt to exploit and leverage access to your environment and data. Therefore, maintaining secure operational integrity is critical to minimising financial loss and reducing the risk of business continuity and reputational damage.

Protecting your digital assets requires a strategic approach. Our MDR services are delivered leveraging our Security Operations Centre (SOC) to promptly detect, analyse, investigate, and actively respond to threats. Using visibility and intelligence systems, we provide you with a comprehensive overview of the cyber threat landscape that allows your organisation to gain back control of what is happening in your digital environment.

Key benefits of MDR.

- Leverage intelligence about your cyber threat landscape via our comprehensive reports packed with insights and recommendations.
- Remove the need to use internal resources and increase cost efficiencies via our processes and procedures.
- Our scalable and flexible solution allows effective management and remediation of security incidents with a successful and faster recovery period.
- Through prioritisation and risk assessment, protect your most valuable assets by investing only in tools that align with your policies and procedures.
- Our expertise in complex digital environments enables your business to be aware of ongoing compliance and security information changes.

orro®

How we help you.

SIEM & Threat Intelligence

- Secure private cloud-hosted SIEM management and comprehensive use case library
- Threat management from aggregated intelligence sources
- Visibility through live dashboarding of security events
- 24/7 monitoring and real-time dashboarding with added operational visibility
- Advanced alerting and reduced time to detect security incidents

Endpoint-as-a-Service

- Trained and certified security engineers
- Endpoint management methodology to meet modern mitigation requirements
- Ongoing monitoring of alerts via our SIEM solution
- Automate response and isolate impacted devices before a significant incident occurs
- In-house ability to hunt threats and respond to a cyber incident
- Battle-tested approach to policy creation

Phishing-as-a-Service

- Delivery of quarterly phishing campaigns for your organisation's staff to measure the effectiveness of user aware programs
- Defined target list to ensure data capture for any phishing exercise
- Reporting and recommendations for staff to prevent phishing attacks

Vulnerability Management-as-a-Service

- Dedicated onboarding engineer working collaboratively with your project team to reduce onboarding time to a matter of weeks
- Visibility into your most vulnerable systems through proactive and scheduled scans
- Tailored guidance for your organisation to understand the risks and remediations associated with recently disclosed vulnerabilities

Dark Web Intelligence

- Ability to proactively search extensive dark web sources to identify threats and unique risks
- Access to over 40 top-tier intelligence feeds (open and commercial) across the dark web
- Delivery of context-specific actionable intelligence from technical, open and proprietary sources
- Regular cyclic scanning to monitor for changes to organisational risk
- Early warning of potential environment compromise

Incident Response

- Certified and experienced response handlers
- Complete cyber incident event management
- Cyber attack identification and analysis of systems to understand malicious activity
- Executive communications management and post-incident reporting
- Extensive experience in responding to high-impact security incidents, including ransomware, phishing, and account compromise

Revolutionary thinking, *evolutionary defence.*

We are a multi-disciplinary team of innovative thinkers who use a no-nonsense approach to always find the right network security solution for your business, which means playing chess, not checkers to achieve the right outcomes.

Technology & People

Our strong customer relationships stem from a commitment to always advise on fit for purpose technology, and doing right by our customers.

Accurate & Proactive

We deliver real-time alerts and reports to help you achieve proactive transformation and monitoring to mitigate issues in alignment with attack surface management to maintain business-as-usual across your digital environment.

Strategic Partnerships

Through our strong business and vendor partnerships, we have the breadth of knowledge and expertise to help you deal with any scenario as soon as it happens. We provide you with the expertise and flexibility to get the results you need through a strategic approach.

Mitigate risk with intelligently secure services.

To learn more about our managed detection and response services or discuss your technology and business needs, reach out to the Orro team today.

CONTACT US

1300 900 000
sales.enquiries@orro.group

Sydney | Melbourne | Brisbane | Perth | UK | Philippines

orro.group