Crystal Eye MDR
Managed Detection & Response

Crystal Eye MDR allows you to reduce gaps in visibility, prioritize alerts and simplify investigations, all backed with Red Piranha's SOC team to enhance your security capability.

"Security teams can no longer fight the advanced cyberthreat detection and response battleground on their own. They need help. Between managing multiple complex security tools, triaging thousands of alerts and dealing with decentralized data, it's hard to stay on top of the real threats that require attention above the noise. That's where MDR comes in."

– Adam Bennett,
CEO of Red Piranha

With the proliferation of advanced cybersecurity attacks and the expansion of the cyber defence battleground, security teams must work harder than ever to secure their organisation's vast attack surface area across hundreds if not thousands of attack vectors. Most internal security departments can't keep up with the ever-expanding and complex workloads and lack the dedicated resources required to stay on top of these developments.

Red Piranha's Crystal Eye XDR (Extended Detection and Response) can play a vital role in reducing the burden on your security team by providing a single unified platform that intelligently and intuitively protects, detects and responds to threats across your entire digital footprint. This allows for the quick identification of real threats from the noise and initiates a rapid response strategy to minimize the overall impact felt by your business, all from one comprehensive and unified platform.

We provide a fully integrated MDR service to complement the XDR capabilities. Our certified security analysts within our 24/7/365 Security Operation Centres (SOCs) are available to investigate and resolve any security incidents in real-time across your network and help coordinate rapid response activities.

Our MDR service enables your team to focus on what matters most to you while letting us handle threat detection and response. We'll be an extension of your internal team, your partner against cybercrime and a key player in strengthening your overall security posture.

Learn more at: redpiranha.net/MDR

Managed Detection & Response

24x7 continuous cybersecurity monitoring drastically improves your threat visibility and gives you more time to spend on your security strategies.

The cybersecurity landscape has changed dramatically;

- Get the support you need to stay ahead

Meet your compliance & regulatory requirements;

- With plug 'n play, compliant Incident Response playbooks.

Minimize data breaches;

- Reduce the cost to your business.

Improve your Mean-Time-To-Respond;

- With Crystal Eye integrated incident response.

Knowing who your adversaries are;

- With integrated Crystal Eye XDR threat intelligence.

Instant Network Security Monitoring (NSM);

- To reduce your deployment overhead.

MDR SIEM Platinum Pricing

Crystal Eye XDR Series 10	25 Seats	$3,800 per year*
Crystal Eye XDR Series 20	50 Seats	$7,600 per year*
Crystal Eye XDR Series 25	75 Seats	$9,500 per year*
Crystal Eye XDR Series 30	75 Seats	$11,400 per year*
Crystal Eye XDR Series 40	75 Seats	$15,200 per year*
Crystal Eye XDR Series 50	150 Seats	$19,000 per year*

* Prices are ex GST. Speak to your account manager for prices on higher Series and Seat Ranges

- Full Network Event monitoring with 24/7 Eyes-on-glass
- System Integrity and Availability
- Service Monitoring

Three-tier analyst monitoring; giving you a compliant monitoring and Incident Response program with end-to-end protection, reducing your liability and risk. Effective human-machine teaming with dynamic interactions between human and machine control to reduce the manual load on security staff.

- Advanced event analysis and behavioural concerns
- Determination of importance of event categories
  - Escalation to customer
- Forcefield system logins processed and checked
  - Integrated Threat Intelligence with integrated actionable outcomes
- On Demand XDR Integrated Digital Forensics and Incident Response capability

Compliant Customer Communication & Reporting

- Email or direct call to customer - Formal SLAs and fast, compliant Incident Response capability
- File movement analysis and alarm response triggers
- Managed correlation directives and reporting
  - create and fine-tune as determined by advanced SIEM cloud processing backed by qualified service.
- Advance Investigation – analysis and forensic services for further investigation
  - based on AI alarms created in Crystal Eye
- Full NSM with Intrusion Detection and Prevention alerts and alarms
- Artificial Intelligence SMB and Kerberos detection, IDPS SID rule anomalies and advanced SSH detection alarms

MDR Service Tiers

	Device Montioring	Security Monitoring	Advanced Security Monitoring	
Services	**Silver**	**Gold**	**Platinum**	**Description**
Availability Checking	✓	✓	✓	Checking the up-time status of the CE device and the SIEM agent.
System Integrity Log Monitoring	✓	✓	✓	The mail logs, message logs and security logs are monitored to ensure system integrity.
System Integrity Rootkit Detection	✓	✓	✓	The CE system is monitored to ensure system integrity and prevent unauthorised or unexpected changes.
Web Configuration and Application Status	✓	✓	✓	The CE system and CE applications can be managed via web interface
Endpoint Protection Monitoring	✓	✓	✓	Alerting on malicious activity happening on the CEASR & DFIR endpoint apps.
Incident Response Escalation	✓	✓	✓	Escalating security incidents to the SOC and the nominated client contact.
Gateway Antivirus Monitoring		✓	✓	The central antivirus engine scans and blocks threats over the web, email, FTP and more.
Content Filter Monitoring		✓	✓	Enforce internet usage policies across an entire site, specific groups or individuals.
Forcefield Monitoring		✓	✓	Actively tracks attacks and the automated defense against the appliance that are identified as likely threats.
Data Loss Prevention Monitoring		✓	✓	Alerting on sensitive files being accidentally or maliciously shared with unauthorised parties.
Gateway Scan / Web Proxy / Content Filter Monitoring		✓	✓	Logging information related to the gateway scan, content filter, application filter and protocol filter engines.
Application Whitelisting Monitoring		✓	✓	Alarms for unauthorised applications running on the network.
Network UBA Anlomy Detection		✓	✓	Detecting User Behavious Analysis by machine learning on selected network protocols.
Network Security Monitoring via IDPS			✓	Advanced real-time scanning of the network identifies and blocks attempts to gain unauthorised access to the network.
Forcefield with Automated Actionable Intelligence Monitoring			✓	Automated Actionable Intelligence feeding Indicators of Compromise to the Crystal Eye platform.

Product Features

In addition to the above monitoring services, the below product features are available in all service tiers.

- Firewall
- SD-WAN
- IDPS
- Secure Web Gateway
- Secure Email Gateway
- Central Management
- Data Loss Prevention
- Network Access Control
- Endpoint Protection
- Threat Intelligence
- Managed IDPS Threat Hunting
- Integrated Risk Management
- Application Whitelisting
- DNS Control & DNS Insure
- Vulnerability Management
- VPN Clients

CRYSTAL EYE XDR

Red Piranha
unified threat management

www.redpiranha.net sales@redpiranha.net +61 8 6365 0450 | +61 2 8089 1219