Red Piranha

Network Detection & Response Q&A

CRYSTAL EYE NDR

CRYSTAL EYE TDiR

CRYSTAL EYE DAS

1. What NDR form factors do you have? e.g. physical, virtual sensors and cloud networks to analyse raw network packet traffic or traffic flows. NDR must also monitor north-south traffic and east-west traffic.

Crystal Eye NDR is available as both hardware and cloud deployments to suit various deployment needs. On-premises, it comes in multiple form factors from a small desktop appliance, 1RU and 2RU rack-mounted units as well as a specialised datacentre model for very large-scale deployment.

We have also developed a PCIe Cyber Security card in conjunction with Intel specifically for our large Private Cloud customers to deploy in high-density rack environments.

In addition, Crystal Eye can be deployed as a cloud native virtual appliance on our 16 global PoP Private Cloud instances or platforms such as Amazon AWS, Microsoft Azure. This flexibility means organisations can implement NDR sensors physically within their network or in the cloud, as needed.

North-South and East-West Traffic Monitoring: Crystal Eye NDR monitors all network traffic flows, providing visibility into both north-south traffic (incoming and outgoing network perimeter traffic) and east-west traffic (lateral movements inside the network). Unlike traditional perimeter-only tools, Crystal Eye's sensors can be deployed across the network to capture internal communications between hosts (east-west) as well as gateway traffic (north-south).

Our solution has demonstrated significantly enhanced visibility of up to 10 × more than comparable products in its class, by prioritising complete coverage of all known malware and C2 communications with integrated threat intelligence to contextualize threat actor activity across east-west and north-south channels. In practice, this means stealthy tactics like lateral movement or internal reconnaissance are detected by Crystal Eye's NDR, not just the obvious inbound attacks.

Multi sensor deployments and in-line/out-of-band options further ensure improved detection for internal east-west traffic without requiring major infrastructure change.

In summary, Crystal Eye can be positioned to watch every corner of the network, providing comprehensive threat visibility and protection across both the network edge and internal network segments.

2. Baseline normal network traffic and highlight unusual traffic activity that falls outside the baseline range. NDR must also provide detection based on behavioural techniques. How?

Baselining Normal Traffic: Crystal Eye NDR employs advanced behavioural analytics to learn what "normal" network activity looks like in your environment, and then continuously monitors for deviations. It builds baselines by observing patterns in network flows, protocols, and user/device behaviours over time. Using machine learning (ML) models and User and Entity Behaviour Analytics (UEBA), the system establishes a profile of typical network usage for different entities. This allows Crystal Eye to detect anomalies that could indicate malicious activity, even if they don't match any known signature.

Anomalous Behaviour Detection: The platform uses a combination of heuristics and ML-driven anomaly detection to flag unusual network behaviours. For example, it can detect when a device suddenly begins communicating with an unusual host or using an atypical protocol for that network segment. Behavioural indicators such as traffic spikes, rare connections, or policy violations are identified by ML algorithms that have learned the normal baseline. Crystal Eye correlates these anomalies with contextual data (like time, location, user identity) and threat intelligence to determine if they are benign changes or potential threats. This behavioural approach enables detection of stealthy threats (including zero-days and insider attacks) that may not trigger traditional static rules. Notably, advanced heuristics and machine learning techniques are integrated with world-class threat intelligence to improve alert accuracy and context. In essence, Crystal Eye's NDR "learns" the environment's usual state and raises alerts when something deviates in a risky way providing early warning of suspicious behaviour such as lateral movement, data exfiltration attempts, or misuse of legitimate tools.

Crystal Eye's behavioural analytics are significantly enhanced through Red Piranha's superior threat intelligence, enabling precise detection of anomalous activity within the network. By continuously profiling normal traffic patterns and user behaviours, Crystal Eye establishes dynamic baselines and uses advanced machine learning to flag deviations. However, what sets it apart is how these anomalies are enriched and validated through a live fusion of global threat intelligence particularly from our position as one of only 2 Australian members of the Cyber Threat Alliance (CTA) and the only vendor.

Through our high-volume contributions and active membership in the CTA, Red Piranha receives real-time access to threat actor tactics, malware signatures, and high-fidelity indicators of compromise from a consortium of global cybersecurity leaders. This intelligence is automatically ingested into Crystal Eye's Automated Actionable Intelligence (AAI) engine, which correlates anomalies with current attack campaigns giving alerts context, reducing false positives, and enabling rapid prioritisation. Customers benefit from detection that not only identifies something as suspicious but can often link it directly to known adversarial behaviour.

This fusion of local behavioural insights with global threat context delivers exceptional accuracy in identifying threats like C2 communications, lateral movement, and data exfiltration, even when they involve novel or low-and-slow techniques. In effect, Red Piranha's threat intelligence gives Crystal Eye the situational awareness of a global SOC network with automated, intelligence-driven responses tailored to your environment.

3. When you detect an incident, how doyou respond? Is it automatic or manual?

Automated vs Manual Response: Crystal Eye NDR is designed with a strong focus on automation in incident response, while still allowing expert human oversight effectively a hybrid approach. The platform includes integrated Security Orchestration, Automation and Response (SOAR) capabilities that can automatically take action when a threat is confirmed. For instance, if Crystal Eye detects malware or an active attack on a host, it can immediately trigger containment measures thereby isolating the affected host at the network level, cutting off its VPN or network access, and even blocking malicious IPs or domains enterprise-wide all in an automated fashion. These automated responses occur in real-time, significantly reducing reaction time and limiting damage. Crystal Eye's automated containment and remediation can neutralise many threats within seconds, without waiting for human intervention.

Human-Machine-Teaming: While automation handles the immediate actions, Red Piranha's approach emphasises human-machine-teaming. Our 24×7 SOC (staffed by certified security experts) continuously monitors the alerts via our MDR service and can step in for detailed investigation, verification, and complex response actions. Analysts receive prioritised alerts (with false positives minimised by AI) and can decide whether to let the automated actions stand or to adjust as needed. This hybrid model ensures critical incidents are never missed and mundane tasks are automated, but human experts remain in the loop for oversight and incident handling that requires judgment. In practice, many incidents are handled through automated playbooks (for speed and consistency), with our SOC team ready to perform additional forensic analysis, threat hunting, or coordination with the client's IT team for full remediation. Crystal Eye's incident response thus combines the best of both worlds, machine-speed reactions with expert validation to effectively contain threats before they escalate. This greatly reduces dwell time and damage from attacks, as threats are contained often within minutes (or even automatically in real-time), rather than hours or days.

4. How do you detect intrusions? IDPS signatures, rule-based heuristics, AI/ML etc?

Crystal Eye uses a defence in depth approach to detect intrusions, combining professionally updated signature-based methods, heuristic rules, and cutting-edge AI/ML analytics in one unified system:

Intrusion Detection/Prevention Signatures: The platform includes a best in class Intrusion Detection and Prevention System (IDPS) with an extensive library of signatures (Currently over 74,000 up-to-date IDS/IPS rules as of recent counts). These signatures enable Crystal Eye to immediately recognise known threats such as specific malware signatures, exploit payload patterns, or command-and-control (C2) beacon traffic (e.g. detecting tell-tale indicators of Cobalt Strike or other tools). Red Piranha continuously updates these rules (from in-house research and community feeds) so that the latest known Indicators of Compromise (IoCs) are covered. This signature-based detection provides a first line of defence for known attack techniques and malware strains.

Protocol & Heuristic Analysis: Crystal Eye parses network traffic at a deep level, understanding over 3,200 protocols out-of-the-box (with ability to add custom decoders, including for SCADA/ICS protocols). It applies heuristic rules and anomaly detection per protocol, for example, flagging protocol misuse or policy violations (such as an HTTP session on a non-standard port, suspicious DNS queries, or malformed packets indicative of exploits). Traditional Next generation firewall and content filtering rules are also integrated. The appliance inspects raw traffic across multiple engines (firewall, IDS/IPS, web content filter, data loss prevention, etc.) including performing SSL/TLS decryption when configured. By correlating events across these engines, Crystal Eye can catch complex intrusion patterns (for example, an email-borne threat detected by content filtering that then triggers an outbound connection caught by the firewall/IDS).

AI/ML and Behavioural Analytics: Beyond signatures, Crystal Eye employs advanced machine learning and behavioural analytics to detect intrusions that are novel or highly sophisticated. As discussed, the system learns normal behaviour and then identifies abnormal patterns that could indicate threats. This includes detecting unusual network beaconing, lateral movement, or data exfiltration attempts that do not match known signatures. Behavioural anomaly detection is coupled with User and Entity Behaviour Analytics (monitoring user account activities for suspicious deviations) to catch insider threats or compromised accounts. In summary, rule-based matching, heuristic anomaly spotting, and ML-driven pattern recognition work in tandem within Crystal Eye. For example, if an attacker is using previously unseen malware or living-off-the-land techniques, Crystal Eye's behavioural detectors may flag abnormal network behaviour, even if the binary isn't recognised by antivirus signatures. This layered detection stack (signatures + heuristics + ML) gives Crystal Eye very high fidelity in identifying intrusions at various stages of the kill chain – from initial compromise to C2 communications and lateral spread.

Integrated Threat Intelligence: Underpinning these techniques is integrated Cyber Threat Intelligence (CTI). Threat intel feeds are continuously fed into Crystal Eye's detection engines, so it is aware of current malicious IP addresses, domains, file hashes, and tactics being used in the wild. This ensures that signature and indicator-based detection stays current with emerging threats. When a new threat is identified by Red Piranha's threat research team or our threat-sharing partnerships, detection rules and IoCs are quickly updated in the platform. The fusion of real-time threat intelligence with both pattern-matching and anomaly-detection means Crystal Eye can detect known bad activities as well as "unknown unknowns." This unified, multi-method approach is a key advantage of Crystal Eye, delivering best-in-breed high-fidelity threat detection across a wide range of attack types.

Crystal Eye's inbuilt Vulnerability Scanning and Management: This capability plays a crucial role in detecting intrusions by identifying weaknesses before attackers can exploit them. By continuously scanning systems, applications, and network assets for known vulnerabilities mapped against databases like CVE and vendor advisories Crystal Eye highlights exposure points that may serve as entry vectors for threat actors. These proactive findings are tightly integrated into the platform's TDIR engine, allowing it to correlate attempted exploits against real-time vulnerability data. This means when malicious traffic or suspicious behaviour is detected, Crystal Eye can immediately determine if the targeted system has an unpatched vulnerability, elevating the severity of the alert and enabling rapid, risk-informed response. This proactive visibility drastically improves an organisation's ability to prevent, detect, and contain intrusions early in the attack lifecycle.

5. How are you improving your LOTL detection? e.g. AI/ML etc?

LOTL Threats Overview: "Living off the land" refers to attackers using legitimate, built-in system tools or benign software to carry out malicious activity. These techniques (e.g. abusing PowerShell, WMI, command-line tools, etc.) are hard to detect because they blend in with normal administrative operations. Red Piranha is acutely aware that advanced persistent threats (APTs) often employ LOTL techniques to evade traditional defences. Therefore, Crystal Eye's development has placed heavy emphasis on detecting these subtle, behavioural threats through advanced analytics and machine learning.

Behavioural Detection of LOTL: Crystal Eye NDR continuously monitors for the tell-tale signs of LOTL attacks. Rather than relying on a single indicator, it looks at behaviour chains and context. For example, if an attacker is using PowerShell in an unusual way, Crystal Eye will notice anomalies such as a surge in PowerShell script executions on a server that doesn't typically use them, or a script making network connections it normally wouldn't. Our platform specifically analyses commands and usage of tools like PowerShell, WMI, or PsExec within network traffic and logs. When usage deviates from the baseline or matches known malicious patterns (e.g. encoded PowerShell commands, lateral movement via SMB, etc.), Crystal Eye will generate alerts. It also detects known malicious use of these tools by their signatures or IoCs, for instance, it can catch when a PowerShell command corresponds to a known malware family's behaviour or when a C2 beacon is hidden in otherwise legitimate-looking traffic. Crystal Eye's NDR component is complemented by endpoint telemetry (if Endpoint component is deployed) to get a full picture of LOTL tactics on hosts.

AI/ML Enhancements: To keep ahead of evolving LOTL tactics, Red Piranha continuously enhances Crystal Eye with artificial intelligence and machine learning improvements. The platform uses advanced ML algorithms to identify unusual patterns in network behaviour that may indicate LOTL attacks. This includes detecting abnormal internal data transfers, odd authentication flows, or sequences of events that don't fit typical operational profiles (for example, a workstation suddenly initiating domain controller-like behaviour). These ML models are trained on both global threat data and environment-specific data, so they can adapt to new LOTL techniques as they emerge. Additionally, Crystal Eye's threat hunting tools and dashboards allow our SOC analysts to proactively search for subtle indicators of LOTL activity (like scanning for any usage of tools known to be abused, but in contexts they normally wouldn't be used). Red Piranha's threat research team actively follows emerging LOTL heavy threat actors, for example, our intelligence monitoring of the Volt Typhoon group (a known APT that heavily uses LOTL tactics) feeds directly into product updates. By analysing such threats, we update Crystal Eye's detection logic (both signatures and anomaly models) to recognise similar patterns. The platform supports full packet capture and deep forensic analysis, which means even heavily disguised LOTL activity (like hidden commands in encrypted traffic) can be uncovered, notably, Crystal Eye fully supports encrypted traffic inspection and analysis for this purpose.

Log retention: In direct response to the Australian Signals Directorate's (ASD) recommendation to retain security logs for a minimum of 18 months or longer (ASD Best practices for event logging and threat detection), Red Piranha's Crystal Eye has been engineered to provide deep, long-term visibility across an organisation's entire attack surface. This extended log retention is not simply a compliance checkbox; it's a critical enabler in detecting, inspecting, and deterring LOTL attacks that leverage legitimate tools and processes to remain covert within an environment.

Crystal Eye leverages its 18-month log storage via its MDR service across network, endpoint, application, and identity layers to build detailed behavioural baselines and identify anomalies over time. This is especially vital for uncovering LOTL techniques, which often unfold slowly and evade traditional security controls. By retaining rich telemetry data, Crystal Eye empowers security teams to perform retrospective threat hunting, trace long-dwell adversary movement, and correlate seemingly benign actions that over weeks or months reveal malicious intent.

The platform's integrated Threat Detection, Investigation, and Response (TDIR) framework works in tandem with MITRE ATT&CK aligned analytics, machine learning models, and Red Piranha's sovereign threat intelligence feeds to expose LOTL behaviours such as PowerShell misuse, credential harvesting, lateral movement via legitimate admin tools, and command-and-control via encrypted channels.

Ultimately, Crystal Eye's log retention and LOTL-focused detection capabilities align with ASD's vision for proactive cyber defence, enabling organisations to go beyond compliance and into genuine resilience. This approach not only satisfies regulatory obligations but strengthens an organisation's ability to detect sophisticated, stealthy attackers operating under the radar.

Ongoing Enhancements: In summary, detecting LOTL attacks is an area of ongoing innovation for us. We leverage AI/ML to refine baselines and highlight the slightest deviations in system usage. We incorporate threat intelligence on LOTL techniques directly into our detection engines. And we champion a Zero Trust philosophy: Crystal Eye integrates with identity and access controls (e.g. Entra ID/Azure AD and our Declarative Authorization Service) so that unusual uses of legitimate credentials or tools are both detected and constrained by policy. This multi-layered, continuously improving strategy ensures that even when attackers "live off the land" to hide in plain sight, Crystal Eye will illuminate their activities. Our goal is to catch those subtle fingerprints of an attack such as a job scheduled via a system tool at an odd hour, a spike in clipboard or registry activity, an unexpected remote PowerShell session and we are constantly updating Crystal Eye to recognise and stop these LOTL behaviours using advanced analytics and machine learning.

6. Air gapped environments? Where have you deployed this?

Air-Gapped Capabilities: Crystal Eye is well-suited for deployment in air-gapped or highly isolated networks. Because the solution is delivered as a self-contained appliance (or set of appliances) that run on-premises, it does not require continuous Internet connectivity to function. All core detection engines (IDS/IPS, ML anomaly detection, etc.) and logging functions run locally on the appliance, meaning an organisation can deploy Crystal Eye entirely within a closed network environment. Updates (such as new threat intelligence, signatures, or software updates) can be applied manually or through controlled means (for example, via offline update packages or through a temporary controlled connection), so that even classified or sensitive networks can keep the system up to date without exposing the environment to the internet. In live operation, Crystal Eye in an air-gapped setting will still capture and analyse all internal traffic for threats, store logs/events for compliance, and enforce security controls, just as it would in a connected environment.

Real-World Deployments: Red Piranha has successfully deployed Crystal Eye in environments with strict isolation requirements, including government, defence, and critical infrastructure sectors. While specific client deployments are often under NDA, we can note that our company is an official member of Team Defence Australia and holds a Defence Export Control permit, meaning our Crystal Eye technology is approved for export to foreign government and defence customers. This is a strong indicator that Crystal Eye meets the stringent requirements of high-security and air-gapped scenarios. In Australia, for example, defence and sensitive government agencies have evaluated and, in some cases, implemented Crystal Eye for protected networks (taking confidence in the product's sovereign Australian origin and security certifications). We have also tailored solutions for industrial control system (ICS) networks (such as in mining and utilities) which are often segmented from the internet. Crystal Eye's ability to support custom SCADA protocols and operate offline has been invaluable in those cases.

One deployment case we can mention generally is in the mining industry. Mining operations often involve remote, isolated networks for operational technology. Red Piranha's focus on mining SOC services has shown that Crystal Eye NDR, deployed on-site at mine operations, can continuously monitor operational networks that have minimal external connectivity, detecting threats and enforcing policies without requiring cloud dependency. In summary, Crystal Eye can run in air-gapped environments with full functionality. All detection and response capabilities are available on-premise, and our team works with clients to provide offline update methods. Our status as a trusted provider to defence and critical industries stands as real-world evidence of Crystal Eye's suitability for highly secure, isolated deployments. (Do you automate responses, such as host containment or traffic blocking?

7. What direct integration do you have with other cybersecurity tools? e.g. End Point's etc?

Crystal Eye is designed as a unified cybersecurity platform, with extensive direct integrations across various cybersecurity and IT tools. These integrations enable Crystal Eye to operate as a centralised orchestrator for visibility, control, and response across an organisation's digital estate. Below is a detailed breakdown of the direct integration points Crystal Eye supports, grouped by category, with real-world examples where applicable:

Endpoint Security Tools Supported Integrations:

- Microsoft Defender for Endpoint
  - Ingests endpoint telemetry, correlates alerts in TDIR
  - Pushes block policies and quarantines from Crystal Eye
- SentinelOne (via API and log ingestion)
  - Collects EDR alerts, behaviour telemetry
  - Enables shared threat intelligence correlation
- CrowdStrike Falcon (via SIEM connectors or log forwarding)
  - Receives detection events and incident metadata
- Crystal Eye Native Endpoint Agent (Lightweight)
  - Used for host-based telemetry (Windows/Linux/Mac)
  - Collects logs, user activity, and performs DLP and host firewall controls
- OSQuery/GRR Rapid Response (Advanced agentless support for endpoint forensics)

Network and Perimeter Security Tools Supported Integrations:

- Cisco ASA / Meraki / Fortinet / Palo Alto firewalls
  - Log forwarding into Crystal Eye SIEM
  - Passive network monitoring for east-west and north-south visibility
- Aruba ClearPass / Cisco ISE (Network Access Control)
  - Context-aware access decisions
- Zeek/Bro
  - Deep packet inspection (DPI) feeds into NDR module
- SNMP/NetFlow/sFlow for routers and switches
  - Provides visibility for segmentation and anomaly detection

Identity and Access Management Supported Integrations:

- Microsoft Entra ID (Azure AD)
  - Ingests login activity, conditional access logs
  - Declarative Authorisation Service (DAS) applies policy logic using identity context
- Okta / Ping Identity / Auth0
  - Correlates IAM activity in TDIR
  - Informs enforcement policies via DAS
- LDAP / Active Directory (On-Prem)
  - User activity logs
  - Used for asset/user risk scoring and SSO
- Multi-Factor Authentication Logs
  - MFA bypass attempts and anomalies are flagged

Threat Intelligence Platforms (TIPs) and Feeds Supported Integrations:

- Cyber Threat Alliance (CTA)
  - Real-time global threat intelligence ingestion
- AlienVault OTX / MISP
  - Shared IOC enrichment and correlation
- VirusTotal API
  - File, URL, and hash analysis with verdicts
- Recorded Future / Anomali (Commercial TIPs)
  - Optional integrations via API or STIX/TAXII
- Australian Cyber Security Centre (ACSC) advisories
  - Automates mapping of CVEs and threat actor techniques

Security Operations and Incident Response (SOAR & SIEM) Supported Integrations:

- Crystal Eye TDIR & SIEM (Native)
  - Correlates logs from all sources for real-time threat detection
- Splunk / QRadar / LogRhythm / Elastic SIEM
  - Forward events via Syslog, Kafka, or API for hybrid setups
- TheHive + Cortex
  - Used for case management and enrichment
- ServiceNow Security Operations
  - Integration with incident management workflows

Cloud and SaaS Platforms Supported Integrations:

- Microsoft 365 / Exchange Online / OneDrive / Teams
  - Monitors user activity, email logs, and file sharing
  - Enforces controls via DLP and DAS
- Google Workspace (Gmail, Drive)
  - Ingests login and file access logs
- AWS CloudTrail / Azure Monitor / Google Cloud Logging
  - Cloud security monitoring across all major IaaS platforms
- Salesforce / Dropbox / Slack
  - Supported via API or proxy-based monitoring

Vulnerability and Patch Management Supported Integrations:

- Crystal Eye Vulnerability Scanner (Built-in)
  - Continuous vulnerability assessment and correlation with attack surface
- Nessus / OpenVAS / Qualys
  - External scan data ingestion and prioritisation via TDIR
- Microsoft WSUS / SCCM / Intune
  - Patch deployment coordination and status checks
- Red Hat Satellite / Canonical Livepatch
  - Linux patch visibility

Application and Asset Management Supported Integrations:

- Crystal Eye CMDB (Native)
  - Maintains authoritative inventory of assets, applications, and configurations
- ServiceNow CMDB (via API sync)
  - Mirrors asset state and risk levels
- Jira / Zendesk / Freshservice
  - ITSM integration for alerts, tickets, and compliance workflow

Data Loss Prevention (DLP) & Compliance Supported Integrations:

- Crystal Eye Native DLP Engine
  - File scanning, structured data detection, and policy enforcement
- Microsoft Purview (DLP Suite)
  - API-level integration for extended policy visibility and control
- Symantec DLP / Forcepoint (Data exchange via SIEM/logs)
  - Cross-policy mapping and incident correlation

Other Tools and Technologies Miscellaneous Integrations:

- Syslog/CEF/GELF Support for broad interoperability
- Kafka and Webhooks for modern data pipelines
- STIX/TAXII 2.1 for threat intel exchange
- API-first Architecture for custom integration with internal tools and dashboards
- SOC Dashboarding Tools like Grafana and Kibana (via data export)

8. What threat detection / Intelligence feeds do you use?

Threat intelligence is a vital component of Crystal Eye's detection capability. Red Piranha leverages multiple threat intel sources and feeds to keep Crystal Eye armed with the latest knowledge of adversaries:

Red Piranha Threat Intelligence Team: We have an in-house threat intelligence team that continuously researches new threats, malware, and vulnerabilities. Findings from our team (including Indicators of Compromise like malicious IPs, URLs, file hashes, and tactics gleaned from incident investigations) are fed directly into the Crystal Eye platform for all clients. For example, if our analysts identify a new phishing domain or C2 server in the wild, that indicator can be quickly added to Crystal Eye's blocklists or detection rules.

Cyber Threat Alliance (CTA): Red Piranha is proud to be the first (and currently only one of two) Australian/ Oceania member of the global Cyber Threat Alliance, a consortium of cybersecurity vendors that share threat intelligence in real-time. We are in fact one of the top contributors to the CTA. This membership gives us access to a rich stream of curated threat intelligence from major industry peers. All relevant intel from CTA – such as new malware signatures, threat actor techniques, and IoCs – is incorporated into Crystal Eye's threat feed. Being a CTA member greatly expands our visibility into emerging threats globally, beyond what any single team could gather.

Automated Threat Feeds and IOC Databases: Crystal Eye integrates a variety of threat feeds (both open-source and commercial). This includes feeds for known malicious domains/IPs (for botnets, spam, DDoS, etc.), threat actor fingerprints, vulnerability exploit indicators, and more. In total, Crystal Eye processes an enormous number of IoCs over 19 million indicators of compromise daily to generate automated defence rules. These come from sources like virus signature databases, honeypot networks, dark web monitoring, etc. The platform's Automated Actionable Intelligence engine sifts through these millions of IoCs to apply those relevant to each customer environment in real-time, updating blacklists and detection triggers accordingly.

IDS/IPS Signature Updates: As noted earlier, Crystal Eye maintains a repository of 70k+ IDS/IPS signatures. These signatures are updated frequently (at least daily, often multiple times per day) from both community rule sets (like Emerging Threats) and our proprietary rules. This ensures known attack patterns (exploits, malware command sequences, etc.) are always up to date. For example, when a new critical vulnerability (zero-day) is announced, our team quickly deploys or updates signatures to detect any attempted exploitation of that flaw, leveraging both our own research and shared industry intel.

Threat Intelligence Platform Integration: The Crystal Eye platform itself serves as a threat intel aggregator. It correlates incoming alerts with known threat actors and campaigns. When an alert fires, the system can show if the involved IP or file hash is known from threat intel and what threat group or malware it's associated with. We use multiple intelligence feeds (including OSINT sources, commercial feeds, and government CERT advisories) to tag alerts with context. This helps analysts prioritise and understand incidents e.g. knowing that an IP is associated with a ransomware gang's infrastructure immediately raises the severity.

External Intelligence Partnerships: Red Piranha has partnerships with organisations such as AustCyber and Team Defence Australia, and we contribute to national threat intelligence initiatives. We also subscribe to vulnerability intel (e.g. NVD, vendor advisories) to feed our vulnerability management module.

In practice, these feeds and intelligence sources enable Crystal Eye to have up-to-the-minute threat knowledge. The system can, for instance, detect a callback to a malicious domain that was first seen only hours ago by another alliance member. Or it can flag an incoming file that matches a hash from yesterday's malware batch. All told, Crystal Eye's detection is bolstered by a continuous stream of curated threat intelligence and indicator feeds, giving it a far-reaching view of the threat landscape. This significantly boosts detection of known threats (reducing false negatives) and provides context that improves alert fidelity. We consider our integrated CTI a major advantage – it's like having a global radar that feeds into each Crystal Eye deployment, so our customers are protected with collective insight, not just what their own environment has seen. As a result, Crystal Eye delivers comprehensive threat coverage, identifying everything from common malware to advanced targeted attacks using the latest intelligence.

9. Where are your SOC's located? Are they a 24x7x365 operation? Does your SOC only monitor CE?

As above the SOC is located in Australia is in 24/7 operation and staffed with Australian analysts.

ISO/IEC 27001:2022 Certified Cert. No.: 781489

ISO 9001:2015 Certified Cert. No.: 703236

Red Piranha is one of the few security organisations with ISO 27001 Certifications to demonstrate that our processes, tools, and systems adhere to a recognised framework.

Red Piranha
unified threat management

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