

Information and Response to Cryptographic Evaluations Report – October 2022

Company Name and ABN	Red Piranha Ltd 63 160 631 505
Years in business	7
Years providing ICT deliverables	5
Background	<p>As part of ensuring Australian Signals Directorate (ASD) programs remain fit for purpose, Red Piranha offers this report to address standards used within the Crystal Eye XDR platform on the ASD Cryptographic Evaluations (ACE) program and Crystal Eye XDR cryptographic standards used within the platform.</p> <p>Crystal Eye XDR provides backwards compatibility with respects to older encryption standards so locking down your Crystal Eye XDR network to meet security controls will rely on end users understanding the needs and implementing the correct settings.</p> <p>This report is aimed at helping understand some of these requirements, the formal position around cryptographic standards, and for partners seeking assurances around cryptographic functionality.</p>
Details of ability to deliver the offered categories	<p>Red Piranha Limited’s services and contributions to the Information Security and Cybersecurity Industries with its Crystal Eye XDR Platform, Red Piranha Limited provides numerous other services both as standalone and integrated services with the XDR platform including, but not limited to:</p> <ul style="list-style-type: none"> • Vulnerability Assessments and Penetration Testing • Virtual Chief Information Security Officer (vCISO) and XDR Integrated eCISO engagements • Governance, Risk and Compliance (GRC) Audits and Consultancy • Digital Forensics Services • Managed Detection and Response • Threat Hunting and Threat Intelligence services • Incident Response Services • Threat Intelligence Analysis • Cyber Security Reviews and Assessment Services, and • Corporate and General Staff Security Awareness Training. <p>At Red Piranha Limited, all customers who have a Crystal Eye device within their environment automatically communicate and engage with Red Piranha Limited's Global Security Operations Centres.</p> <p>These Crystal Eye XDR devices are continuously monitored and maintained by Red Piranha Limited's Global Security Operations Centre personnel. These XDR devices are also inclusive of Security Information and Event Management (SIEM) operations and functionality.</p>

Details of Red Piranha's Risk Management Systems

The Red Piranha Risk Committee, chaired by Rosemary Milkins (Non-Executive Director), was established 2022. The Risk Committee advises the Board on enterprise and Cyber risks, including monitoring of Red Piranha's Risk Management Systems. The Risk Committee regularly reports to the Board on risk.

Within the domain of operational risk, Red Piranha holds an ISO/IEC 27001 certification and places great focus on continual improvement of its Information Security practices.

Red Piranha is ISO 9001:2015 certified for Quality Management systems thereby ensuring that our customers get consistent, good-quality products and services.

Red Piranha has undergone IRAP assessment and works to IRAP and ISM alignment, also subscribing to the Defence Industry Security Program (DISP) and has achieved DISP membership.

Red Piranha has been granted the Defence Export Permit by the Department of Defence, allowing it to export their technology to foreign governments (Defence Export Permit: DOD/DEP/20829572).

Red Piranha undertakes periodic and ongoing vulnerability testing on its service delivery network. Vulnerability scans within the most recent quarter were conducted on 1/08/2022, 07/09/2022, and 28/09/2022. The results of those tests were analysed by the Compliance Team and the CISO on submission, and requests for mitigation activities are made, based on the level of risk each vulnerability posed to Red Piranha at that time. As part of the ongoing process vulnerabilities are monitored by the Admin and Compliance teams on a weekly basis.

In addition, penetration testing on product change control and on new product releases as per our internal policies is being conducted. Penetration testing for Crystal Eye 4.5 and Orchestrate was completed on 30/08/2022.

In addition to that, Red Piranha also implemented an incident management system for both internal and client incidents. Measurable processes and metrics have been introduced for change control and vulnerability management. The outputs and mitigations from these processes are reviewed and managed by the Compliance Team in weekly risk meetings. Compliance attends weekly Infrastructure and Secops management meetings to ensure vulnerabilities, changes and mitigations are being tracked and managed in a timely fashion.

Red Piranha has achieved CREST ANZ (Council of Registered Ethical Security Testers) certification, providing assurance that testing conducted is of exemplary quality, conform to industry best practices and meets the highest ethical standards in penetration testing services.

Red Piranha has a security report submission page for the public to report security issues direct to the internal compliance team.

Red Piranha undertakes management for product development in the ISO domain ISO 15408 and aims to attain CC certification.

Red Piranha seeks to be listed on the Australian Government EPL list, subscribes to the ACE (ASD Cryptographic Evaluation) program, and aims to address ASD (Australian Signals Directorate) questions consumers may have around standards applied in its products in this report.

	Red Piranha Ltd complies with the ASX Risk Management Framework outlined in the ACH Clearing Rules Guidance Note No. 13.
--	--

FAQ's - Standards and Cryptographic Position

Is Perfect Forward Secrecy (PFS) supported in all TLS Communications?	Yes, all proxy and SSL-VPN TLS communications supports PFS
Does Crystal Eye support SNMPv3? Do we have the option to force disable SNMPv1 and SNMPv2 and are disabled by default?	Crystal Eye XDR does not support SNMP and so no requirements to disable SNMPv1 or SNMPv2 is needed
Are all web and TLS components on Crystal XDR forced to TLS 1.2/1.3 only with TLS 1.0 and 1.1 both Client and Server disabled?	While backwards compatibility is supported, Crystal Eye XDR has support to drop all TLS connections from clients with TLS 1.0, TLS 1.1, and TLS 1.2 allowing customers to force TLS 1.3 communications.
Is support for DES / 3DES and all other block ciphers with a 64-Bit Block Size disabled/blocked?	As AES has replaced DES and 3DES, the WebGUI still supports 3DES for backwards compatibility. Web Proxy and SSL communications has DES and 3DES disabled by default.
Are all weak ciphers disabled such as those that use RC4, MD5, or have key lengths of less than 128 bits or anonymous/unauthenticated DH Algorithms?	Yes, all weak ciphers are disabled.
Confirming all Telnet, FTP and TFTP services are disabled by default	In Crystal Eye XDR these are not supported and disabled
Confirming SSLv3 is forced disabled?	Yes, SSLv3 is disabled

Additional information

Red Piranha has a Security Operations team that can be called upon as required. Red Piranha operates 24/7 and has a maximum response time of 4 hours.

Red Piranha has other employees who live outside of Australia; however, Data Sovereignty is maintained inside Australia when required.

Red Piranha implements Multi-Factor Authentication wherever possible.

Red Piranha's cloud-based Crystal Eye XDR on TPG Cloud also implements the aforementioned cryptographic capabilities.

ISO 15408

Red Piranha follows processes and guidelines outlined in ISO 15408.

ISO 9001

Red Piranha is ISO9001 compliant.

Last audit date: 09th June 2022

Certificate number: 703236

ISO/IEC 27001

Red Piranha is ISO/IEC 27001 compliant.

Last external audit date: 17th February 2022

Last internal audit date: 9th September 2022

Certificate number: 781489

IRAP

Red Piranha has undergone IRAP assessment and works to the Australian Signals Directorate's Information Security Registered Assessors Program (IRAP) alignment.

ISM

Red Piranha works to the Australian Government Information Security Manual (ISM) alignment.

Crystal Eye 4.0

Crystal Eye 4.0 is the latest release of Red Piranha's Crystal Eye XDR with version 4.5 currently in the Beta testing phase.

Change Control Testing

All penetration testing is conducted following our defined change control process, which follows 4 key stages:

- Change Acceptance
- Change Implementation
- Change Approval
- Change Deployment

Each internal team involved in the change control process follows set SLAs and uses a common repository for all change requests.

We perform 3 types of penetration testing each quarter to ensure the maximum level of assurance:

- Blind test – simulates a typical cyber attack scenario
- Double-Blind – is an advanced version of the Blind test with particular attention on restricting information sharing
- Targeted/Lights-On – all personnel involved know that a test is being carried out

Statement of Accuracy

Red Piranha confirms the accuracy of the information provided in this document.



Product Manager



GRC Consultant