Crystal Eye XDR Cryptographic Capability and Standards

Information and Response to Cartographic Evaluations Report

Company Name and ABN	Red Piranha Ltd 63 160 631 505
Years in business	5
Years providing ICT deliverables	5
Background	As part of ensuring ASD programs remain fit for purpose, we would like to offer 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. 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. 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.
Details of ability to deliver the offered category/ies	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; ▸ 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. 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. 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.
Details of Red Piranha's Risk Management Systems	Red Piranha manages risks on a number of levels. The Red Piranha Board meets every 6 weeks and risk management is a standing item for discussion. Risk issues involving operations, market, credit, liquidity, documentation, reputation, regulations and systems are reviewed. Within the domain of operational risk, Red Piranha holds an ISO 27001 certification and places great focus on continual improvement of its Information Security practices. Red Piranha has undergone IRAP assessment and works to IRAP and ISM alignment, also subscribing to the Department of Defence DISP program and has undergone DISP assessment. Red Piranha has been assessed and its Defense Export Permit is DOD/DEP/20829572 Red Piranha undertakes periodic and ongoing vulnerability testing on its service delivery network, penetration testing on product change control and on new product releases as per our internal policies. 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 program and aims to address ASD 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

Statements on Standards an 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 l.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 week 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 27001

Red Piranha is ISO 27001 compliant.
Last audit date: 17th February 2021
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

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.

Secops Manager

Security and Compliance Manager