Red Piranha

Technology Report

Red Piranha's Crystal Eye Platform

Peter Hannay & Clinton Carpene

peter@hannay.id.au, clinton@carpene.id.au

16th October 2017

Updated Review

Red Piranha's Crystal Eye XDR Platform v4.0

Kenneth Tan – ktch37@gmail.com

Meidi van der Lee – meidiz@outlook.com

Rossa Risdiana – rossarisdi@gmail.com

4th September 2020

The statements made and opinions expressed in this report are believed to be correct by the authors, however the authors assume no responsibility or liability for any errors or omissions in the content of this report. The information contained in this report is provided on an as-is basis with no guarantees of completeness, accuracy, usefulness or timeliness.

Any discussion of projections or future performance are subject to interpretation and it must be noted that past performance is not a reliable indicator of future results, as such no responsibility can be accepted for decisions made based on this report.

Executive Summary

Red Piranha Limited is a public unlisted company registered in Australia and currently based out of Perth and Sydney, developing information security products called the Crystal Eye Extended Detection and Response (CE XDR) platform with the immediate target market being small and medium businesses in Australia and exporting to global markets.

The Crystal Eye platform integrates a collection of security technologies to provide multiple layers of cybersecurity protection, giving the benefit of defence-in-depth with comprehensive features even without optional functions installed. Clients can add more functionalities from the Marketplace as required according to each business' inherent risks and requirements. Additional functionality can be included mostly at no additional cost.

The features work together within a single console to provide a comprehensive view into system information, network activities and real time threats, all graphically displayed on user-configurable dashboards.

During the review, the team found that the product has evolved since its initial audit in 2017 to include updated cybersecurity protection technologies and further integrated services, taking it from the former Unified Threat Management system to a more comprehensive XDR platform. It incorporates Identity and Access Management (IAM), Security Orchestration, Automation and Response (SOAR) and a Threat Intelligence Platform (TIP). The appliance performs extensive logging and reporting on wide variety of security events which are useful for threat intelligence, forensics and auditing. Multiple functionalities are included, including integration with managed security services, making it a Managed Detection and Response (MDR) system.

Through leveraging multithreading and CPU affinity, the appliance supports simultaneous resource-intensive applications including Firewall and IDPS functions. This allows the Crystal Eye platform to continue to deliver the full suite of cybersecurity protection without slowing the end user experience.

For clients who want to incorporate cybersecurity compliance and best practices the platform includes compliance controls which includes Integrated Risk Management (IRM), Data Loss Prevention (DLP), Vulnerability Management and Incident Response (IR).

At the conclusion of the review, the team continues to agree with the initial auditors that the CE XDR platform is an advanced, all-encompassing approach to cybersecurity that is cost-effective and resource-efficient for small and medium businesses and beyond.

Table of Contents

1. Introduction

Red Piranha Limited (“Red Piranha”, “the Company”, “RP”) is a public unlisted company registered in Australia and currently based out of Perth and Sydney. Red Piranha is the sole owner of the Crystal Eye (CE) appliance system, previously known as Crystal Eye Next Generation Firewall Operating System, now referred to as Crystal Eye Extended Detection and Response (XDR) platform. To complement the CE XDR appliance, Red Piranha also offers a range of services such as eCISO and vCISO. eCISO (Electronic Chief Information Security Officer) is an automated service that integrates directly with Crystal Eye platform and complemented by remote consulting services help clients developing detailed information security plan going towards fully compliance on clients’ required standards. VCISO (Virtual Chief Information Security Officer) is an on-site and remote access to Red Piranha’s pool of highly experienced security experts that helps clients in security planning and reporting requirements.

Red piranha is one of the few cybersecurity organisations in Australia to have achieved the highly regarded International Standards Organisation (ISO) certification, namely ISO/IEC 27001:2013 for their Security Operation (SecOps) side of the Crystal Eye appliance. Red Piranha’s target market is the small and medium businesses (SMB) in Australia and the global market.

Cyberattacks have become more sophisticated than ever. According to the Cybersecurity Ventures in 2019 (Morgan, 2019), worldwide spending on information security products and services exceeded $114 billion in 2018 and that is an increase of 12.4 % from 2017. Furthermore, Gartner, Inc also forecasted that the market would grow to $170.4 billion in 2022. This is where the Red Piranha CE XDR comes into the SMB community and large enterprises as a game changer when compared against competing products in the industry.

Cyberspace is growing twice as fast as the global economy, in financial year 2019 / 2020 alone the Australia Cyber Security Centre responded to 2,266 cyber security incidents which is the rate of more than six per day. This does not include other incidents referred to the police and other support organisations (Australia’s Cyber Security Strategy, 2020). As the cyber threat landscape continues to evolve, SMB are more vulnerable to cybersecurity issues due to the lack of comprehensive secure infrastructure that should be in place to help prevent and overcome any security incidents (Australia’s Cyber Security Strategy, 2016). This is where Red Piranha is making a difference as Red Piranha’s vision is to create an easy to manage, full-featured security solution that is affordable to the SME. Red Piranha continues to develop, build, and distribute its cutting-edge technology to all its clients, placing RP at a substantial advantage over the rest in the cybersecurity community (Hannay & Carpene, 2017).

2. About the Auditors

Peter Hannay is a security researcher currently working within the School of Science at Edith Cowan University and is also involved in network vulnerability, malware and OT research projects under the banner of the Security Research Institute. His research focus is network security and digital forensics, specifically relating to small and embedded devices. Peter has been working within this role for near to ten years. In addition to teaching and research work, Peter has undertaken consulting work within the private and public sector, performing vulnerability assessments, source code review, for critical infrastructure providers and other high security environments. Peter is currently enrolled as a post-graduate at Edith Cowan University. Peter's Doctoral thesis topic is focused on determining effective methods for reliably extracting locational information from generic embedded devices. Additionally, Peter holds Bachelor's and Honours degrees in Computer Science, where his thesis focused on the extraction of locational history from small and embedded devices. As a result of his extensive experience and knowledge of locational forensics, Peter has engaged with law enforcement on several occasions to provide investigative assistance. In addition to his professional work, Peter is an active member of the international cyber security community. Peter is a regular speaker at industry events including those run by IEEE, Interpol, ACSC, and ISACA. Peter is an organiser of Perth's largest annual security conference and has spoken at numerous security conferences including Defcon, BlackHat, Kiwicon, Unrestcon and BSides Canberra.

Clinton Carpene is a senior security consultant and security researcher. As a security consultant, Clinton has participated in numerous security testing engagements ranging from vulnerability assessments and penetration tests, to application source code review. Clinton focuses his research on the security issues surrounding IPv6 and the Internet of Things. Prior to his work as a penetration tester he worked for five years at Edith Cowan University under the Security Research Institute. During this time Clinton undertook postgraduate research, with his position funded by Cisco. During this period, Clinton published numerous papers on the topics of IoT and IPv6 security. Clinton holds a PhD in Computer Science. Clinton's doctoral thesis topic of IPv6 host enumeration search methods assessed the efficacy of various search algorithms for enumerating unknown devices in IPv6 networks. Clinton also holds the industry recognised OSCP certification, that demonstrates practical security competency. In addition, Clinton holds an Honours degree in computer science, for which he audited endpoint smart grid devices from a network security perspective. Clinton is an active member of the security community. Clinton is an organiser of Perth's largest annual security conference, organises monthly cyber security talks and is a member of national security organisations. Clinton has spoken at numerous national and international conferences. Peter and Clinton are both respected members of the information security community and recognised experts within their fields. They have demonstrated their skills academically, professionally and are actively involved in the local community, working to build new talent and foster the future of cybersecurity within Western Australia.

The 2020 Review Team

Kenneth Tan is an undergraduate cybersecurity student at Edith Cowan University (ECU) in Western Australia. Kenneth is also a cybersecurity student ambassador at ECU, who conducted multiple cyber awareness workshops and presentations in local high schools. Some of his previous roles includes ICT intern, system administrator, and information security analyst. Additionally, Kenneth also works in an advisory role within the digital law enforcement agency. He is also an active team member in creating specialised forensics Capture the Flag (CTF) challenges that is known to be used in the 2019 Perth vs Canberra CTF Challenge. Additionally, Kenneth holds a part time position as a cybersecurity consultant for AustCyber' Cyber Check Me programs. Kenneth is also actively involved in numerous CaptureTheFlag (CTF) competitions and Cyber Security Conferences including WACTF, BlackHat, AISA Australian Cyber Conference and BSides Perth and Canberra.

Meidi van der Lee is a post-graduate cybersecurity student at Edith Cowan University in Western Australia. Meidi also hold degrees in information system management and accounting, with many years of career in accounting, finance and company management. Meidi is a member at Australian Computer Society (ACS), Australian Information Security Association (AISA), Australian Women in Security Network (AWSN), Women in IT Western Australia (WiTWA), and Information System Audit and Control Association (ISACA). Meidi is also a volunteer tutor and mentor for Cisco Cybersecurity Learning, Girls Programming Network (GPN), National Computer Science School (NCSS) Challenge and cybersecurity consultant for AustCyber' Cyber Check Me programs. Meidi is an active member at the global organisation Trace Labs that does Open Source Intelligence (OSINT) to find missing persons, as a contender and a judge. Meidi is also actively contending in various CaptureTheFlag (CTF), competitions for penetration testing and she a member of challenge creator team at ECU CTF programs.

Rossa Risdiana is a post-graduate cybersecurity student at Edith Cowan University in Western Australia. Rossa also holds a degree in International Relations, with several years of experience in Retail Company as deputy manager store of INDITEX group, intern in the Ministry of Foreign Affairs in Indonesia, Directorate General for Asia Pacific and African Affairs, and International Non-Government Organization (INGO) named East Asia-Australasian Flyway Partnership (EAAFP). Rossa was involved in Asia Africa Conference Commemoration (AACC) event in 2015. Rossa also did a social project in Shanghai with *Association Internationale des Étudiants en Sciences Économiques et Commerciales* (AIESEC), an international non-governmental organization that provides young people with leadership development, cross cultural internships, and global volunteer exchange experiences. Rossa is a member of the Australian Information Security Association (AISA).

3. Scope of The Review

The review evaluates the functionality of Crystal Eye platform which has evolved to include more technologies since its first review in 2017. With the advanced and comprehensive cybersecurity protection, the platform is now called Extended Detection and Response system (XDR). The latest software version under review is version 4 or CE XDR v.4. Evaluation was performed on an appliance instance provided with online access and the product user manual, against claims made by RP.

The functionality review investigates the integration of the various controls, application, and systems that CE XDR put together to provide multilayered cybersecurity protection. They include the Identity and Access Management (IAM), Extended Detection and Response (XDR), Security Orchestration and Automated Response (SOAR) and Secure Access Service Edge (SASE), and all controls that specify the functionalities. The review also investigates how the platform helps manage cybersecurity risk management and compliance.

The review process was undertaken from 31 July 2020 until 16 October 2020.

While precautions have been taken in the preparation of this deliverable, the information contained in this document may contain errors and omissions and the authors assume no responsibility or liability for them. Nor the authors guarantee its completeness, accuracy, usefulness and timeliness. Any third party reviewing the content of this document for a basis of making decision needs to make their own assessment on the appropriateness of the information contained.

4. Crystal Eye Extended Detection and Response Platform

Crystal Eye XDR is a cybersecurity product that offers a comprehensive, multilayered defence against cyberattacks by combining various security technology products and integrating them together into an overall defence system that allows seamless monitoring and management. It differs from conventional approaches where companies combine various security products from various vendors and manually integrate them together into an overall defence system, resulting clients have to manage multiple product platforms from competing vendors which has the potential of overwhelming besides of the overhead costs. Crystal eye platform aims to reduce such burdens by unifying the services, protection, and consolidating the alerts.

Crystal Eye XDR converges amongst others, anti-malware, content filtering, firewall, intrusion detection and prevention systems, data loss prevention, vulnerability scanner, and so on which are orchestrated to work together to provide comprehensive threat detection, attack prevention and quick responses to incidents. The CE XDR has the advanced capabilities to defend against cyberattacks that target different segments of a network. The protection processes continue to feed into RP threat intelligence network, forensics logging and compliance processes if required. Clients who require compliance to certain standards, best practices or industry regulation will find the required features in the XDR.

Every XDR appliance is made to order, assembled from the latest generation components available at the time of order allowing cutting-edge hardware performance. This is one of the strategies to overcome the fast rate of technology obsolescence.

Clients can choose the level of network protection and services that are suitable to their business needs and can easily scale up and down whenever needed with the convenience of the Marketplace function, within which the platform provides automatic generation of Service Level Agreements (SLA).

All configuration and management of the system from initial set up to daily running is performed through a user-friendly web Graphical User Interface (GUI). The modules are categorised into Dashboard, System Configuration, Network Control, Security Configuration, Compliance Controls, Reports, Marketplace, and Support. All menus are designed to be no more than two levels with more breakdown and description laid flat on the panel display and each module selected comes with description at the top of the window to assist novice users.

CE XDR allows users to monitor cyber events on dashboards and manage cyber protection of systems through a single console.

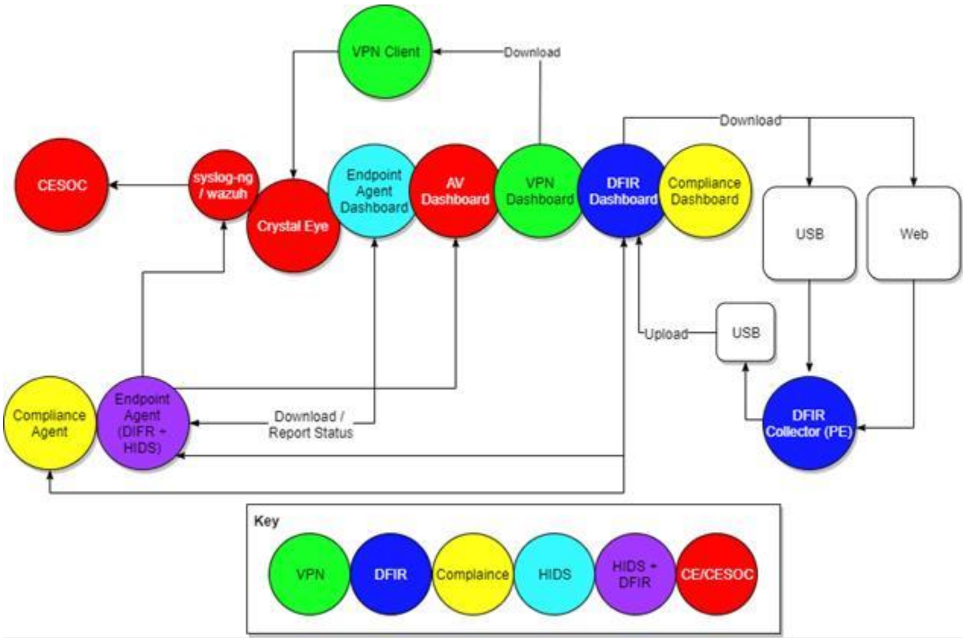


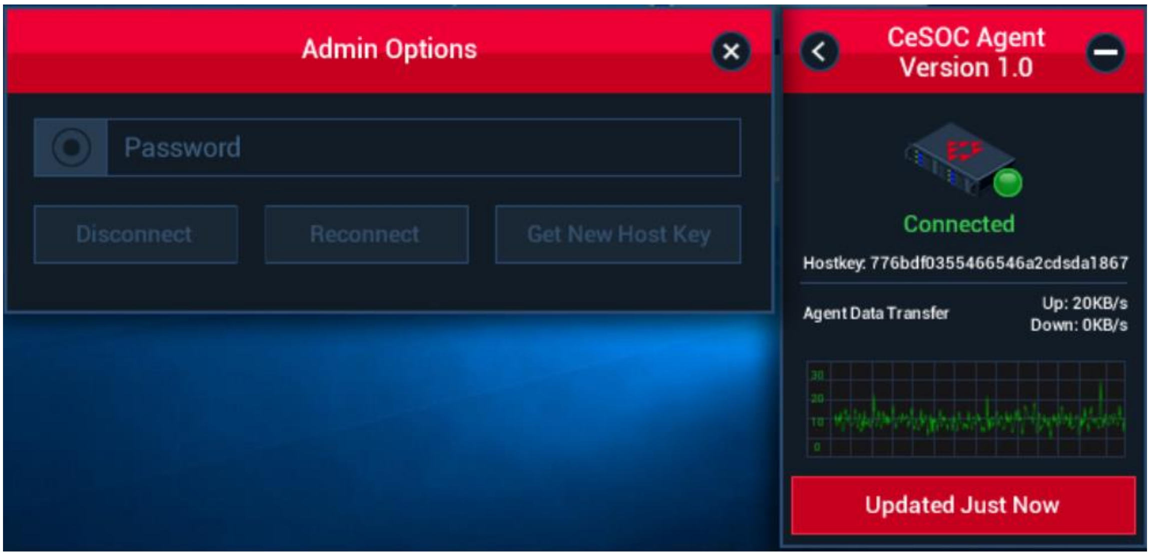
Figure 1: Topology of Crystal Eye XDR System

4.1 Deployment Options

CE XDR typical installation is at the perimeter as a gateway. It can be deployed by implementing the device on a network in various configuration that suits different networks and application needs. The appliance can be deployed on existing hardware infrastructure, virtual infrastructure, or hybrid cloud infrastructure. Several options include deployment at large networks, active or passive high availability, and multi-Wide Area Network (WAN). To secure a large network, the CE XDR is capable of segmenting it into smaller sub networks, such as enterprise network, branch office network, and remote users. Network deployment on active or passive high availability scenario provides uninterrupted access to systems during a failure event. When deployed at multi-site or multi-WAN structure, multiple CE XDR appliances are used to create IPSec VPN tunnels between offices with an appliance at each site.

CE XDR can be installed on both *greenfield* and *brownfield* infrastructures. When deployed in a *greenfield*, it manages the routing, DHCP, DNS and other key functions as well as the advanced firewall and IDPS with content filtering and other security and compliance functions. When deployed in a *brownfield*, it can be configured to match existing network configuration either as a gateway or as a device behind an existing router or firewall.

CE XDR is built to accommodate multi tenanted clients as in the case of Managed Service Provider (MSP) type of clients, which are the majority. All security related information from the XDR appliance deployed at an end client are continuously pushed to a protected, load balanced and redundant server at Crystal Eye Security Operation Centre (CESOC), the RP's centralised monitoring system, using an agent app. All the connection to the CESOC is via secure encrypted connection using TLS 1.2/1.3.



Admin Options

Password

Disconnect

Reconnect

Get New Host Key

CeSOC Agent
Version 1.0

Connected

Hostkey: 776bdf0355466546a2cdsda1867

Agent Data Transfer

Up: 20KB/s
Down: 0KB/s

Updated Just Now

Figure 2: CESOC Agent

Red Piranha brings the deployment through cloud mechanisms particularly on Azure, AWS, TPG cloud and hybrid networks. Hybrid network is an option of deployment that offers flexibility and security control but still requires a hosting infrastructure.

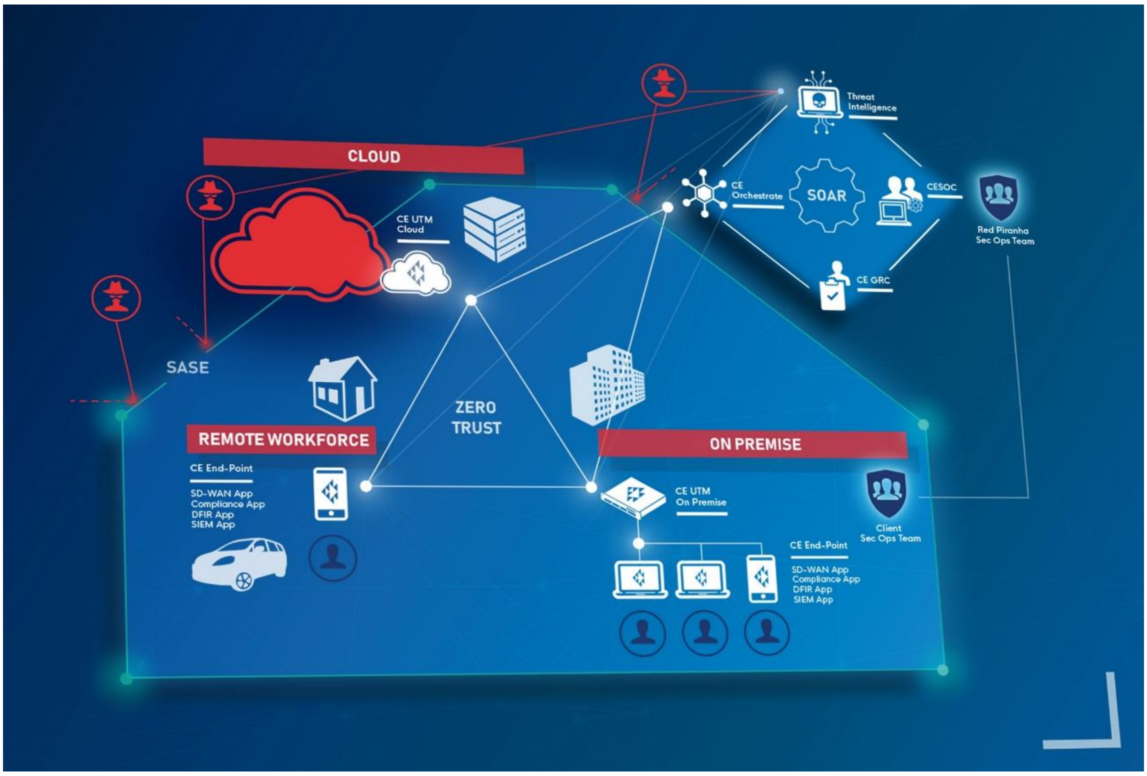


Figure 3: Crystal Eye XDR Deployment

4.2 Features Integration and Live Monitoring

It is critically important for an XDR product to be able to quickly identify network breaches or if a protective mechanism must be adjusted. As the CE XDR unifies multiple security functionalities, it is possible for the platform to alert if incompatible configuration options are set between different modules. For example, if a VPN endpoint is configured but a firewall rule prevents it from operating, it is possible for the product to detect and provide an alert to the administrator. This capability is a significant reduction in the complexity of troubleshooting exercises as the administrator does not need to examine and cross reference multiple debug logs from multiple platforms to identify the issue.

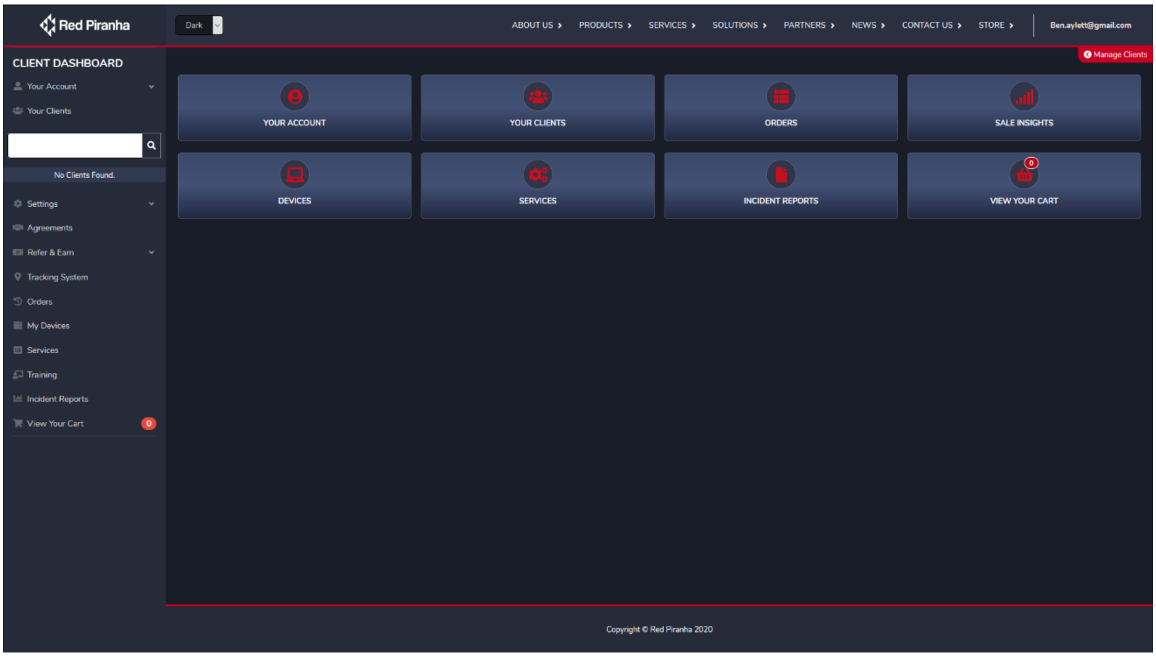
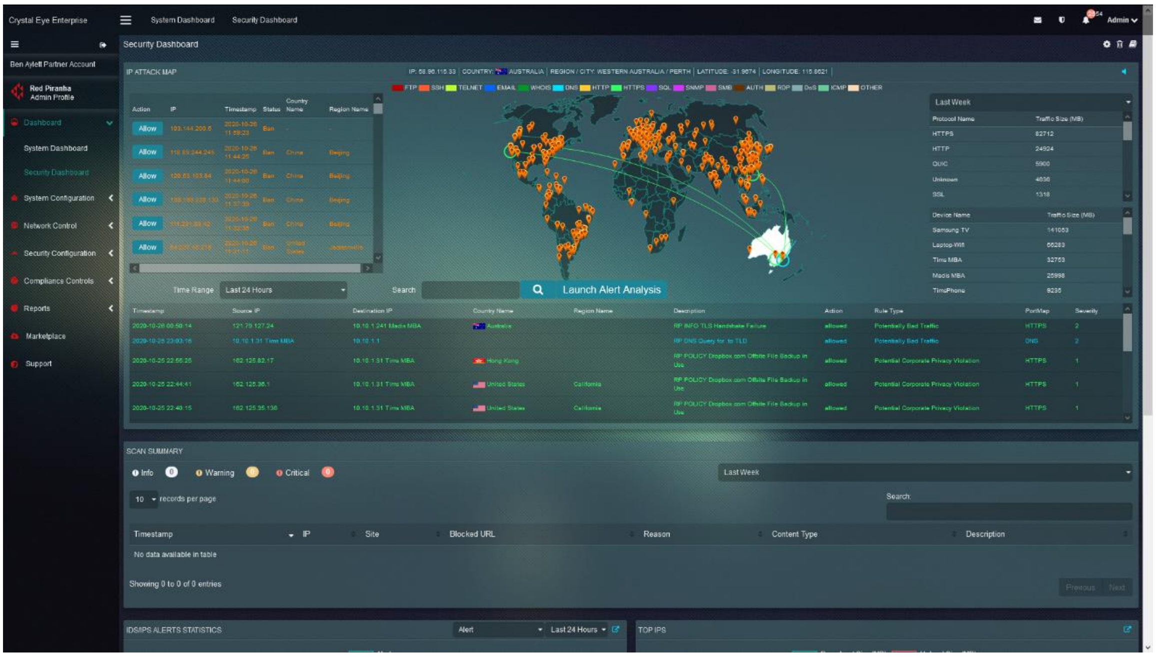


Figure 4: Client Dashboard

The CE XDR live monitoring system displays real time information in two dashboards System Dashboard and Security Dashboard which is user customisable.

The system dashboard provides a quick glimpse into information on CPU and memory usages, LAN and WAN interfaces, applications statuses, event logs and recent software activities, disk usage, and quick widgets to create users and group, and to shut down or restart.

The CE security dashboard provides a single view of all Crystal Eye devices and endpoints and a comprehensive view of all security events and alerts like IP attack map, scan summary, IDPS alert statistics, top IP by activities, network map and top protocol by traffic size graph. Within the dashboard, users could further investigate the alerts, reconfigure the settings or escalate to RP’s managed service.



Crystal Eye Enterprise — System Dashboard — Security Dashboard — Admin

Ben Aylett Partner Account

Red Piranha Admin Profile

Security Dashboard

IP ATTACK MAP

IP: 58.96.115.33 | COUNTRY: AUSTRALIA | REGION / CITY: WESTERN AUSTRALIA / PERTH | LATITUDE: -31.9674 | LONGITUDE: 115.8621 |

Action	IP	Timestamp	Status	Country Name	Region Name
Allow	103.144.200.6	2020-10-26 11:59:23	Ban	-	-
Allow	118.89.244.245	2020-10-26 11:44:25	Ban	China	Beijing
Allow	120.53.103.84	2020-10-26 11:44:00	Ban	China	Beijing
Allow	139.196.228.130	2020-10-26 11:37:39	Ban	China	Beijing
Allow	111.231.89.42	2020-10-26 11:32:35	Ban	China	Beijing
Allow	54.207.46.218	2020-10-26 11:21:11	Ban	United States	Jacksonville

Time Range: Last 24 Hours — Search — Launch Alert Analysis

Last Week

Protocol Name	Traffic Size (MB)
HTTPS	82712
HTTP	24924
QUIC	5900
Unknown	4836
SSL	1318

Device Name	Traffic Size (MB)
Samsung TV	141053
Laptop-Wifi	66283
Tims MBA	32753
Madis MBA	25998
TimsPhone	9236

Timestamp	Source IP	Destination IP	Country Name	Region Name	Description	Action	Rule Type	PortMap	Severity
2020-10-26 00:50:14	121.79.127.24	10.10.1.241 Madis MBA	Australia		RP INFO TLS Handshake Failure	allowed	Potentially Bad Traffic	HTTPS	2
2020-10-25 23:03:16	10.10.1.31 Tims MBA	10.10.1.1			RP DNS Query for .to TLD	allowed	Potentially Bad Traffic	DNS	2
2020-10-25 22:56:25	162.125.82.17	10.10.1.31 Tims MBA	Hong Kong		RP POLICY Dropbox.com Offsite File Backup in Use	allowed	Potential Corporate Privacy Violation	HTTPS	1
2020-10-25 22:44:41	162.125.36.1	10.10.1.31 Tims MBA	United States	California	RP POLICY Dropbox.com Offsite File Backup in Use	allowed	Potential Corporate Privacy Violation	HTTPS	1
2020-10-25 22:40:15	162.125.35.136	10.10.1.31 Tims MBA	United States	California	RP POLICY Dropbox.com Offsite File Backup in Use	allowed	Potential Corporate Privacy Violation	HTTPS	1

SCAN SUMMARY

Info 0 Warning 0 Critical 0

Last Week

10 records per page

Search:

Timestamp	IP	Site	Blocked URL	Reason	Content Type	Description
No data available in table						

Showing 0 to 0 of 0 entries

IDS/IPS ALERTS STATISTICS — Alert — Last 24 Hours

TOP IPS

Figure 5: Security Dashboard

4.3 Protect, Detect and Respond

The following explains various multilayer protection concepts and how CE XDR employs them.

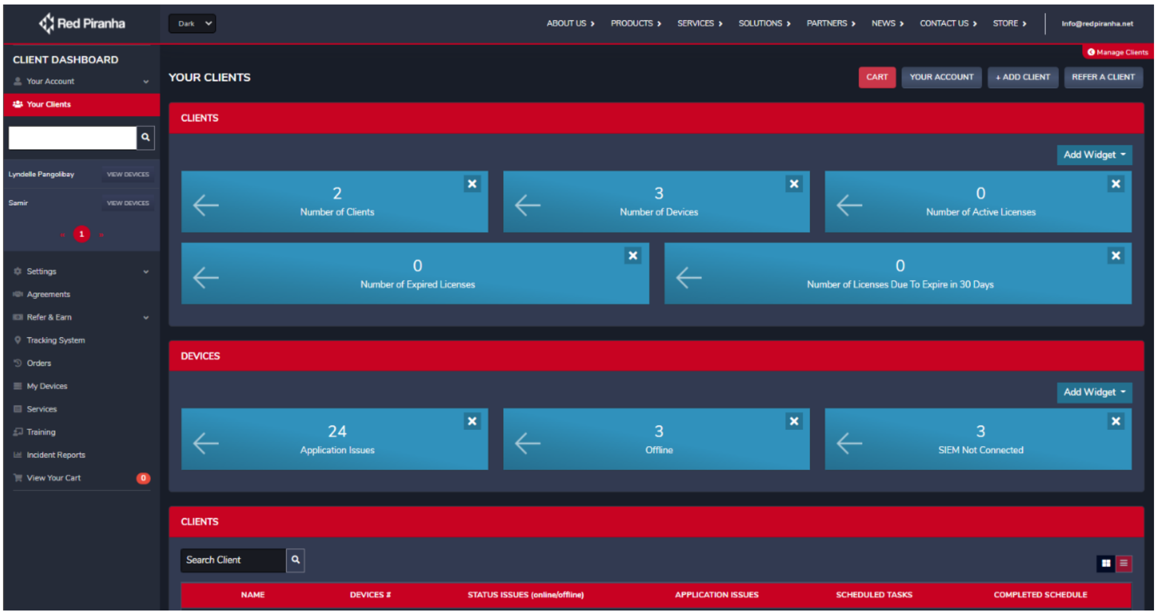
4.3.1 Security Orchestration, Automation and Response (SOAR)

The CE XDR platform enables the delivery of Security Orchestration, Automation and Response (SOAR) across various environments to ensure that the confidentiality, integrity and availability of client’s information and systems are kept at the highest standards.

The three primary SOAR capabilities are:

- **Orchestration** - threat triaging and vulnerability management
  Proactively provides protective measures to system and network, such as pre-scheduled vulnerability scanning, virtual patching, automatic detection and multitask coordination and management.
- **Automation** - security operations automation
  This enables the automation and orchestration of threat intelligence, threat analysis, threat hunting, compliance controls and reporting.
- **Response** - security incident response
  The ability to seamlessly integrate threat detection alerts to provide instant automated response while allowing user to escalate incidents into RP’s managed service.

Through SOAR, the CE XDR platform can prioritise security operations activities, and orchestrate, automate, coordinate, and manage real time threat intelligence. This is to provide instant incident response processes through the orchestration of all capabilities and features that forms a Crystal Eye total security platform.



YOUR CLIENTS

CLIENTS

2 Number of Clients

3 Number of Devices

0 Number of Active Licenses

0 Number of Expired Licenses

0 Number of Licenses Due To Expire in 30 Days

DEVICES

24 Application Issues

3 Offline

3 SIEM Not Connected

CLIENTS

NAME	DEVICES #	STATUS ISSUES (online/offline)	APPLICATION ISSUES	SCHEDULED TASKS	COMPLETED SCHEDULE

Figure 6: Crystal Eye Orchestrate

The following graphic depicts the applications that converge in the SOAR model.

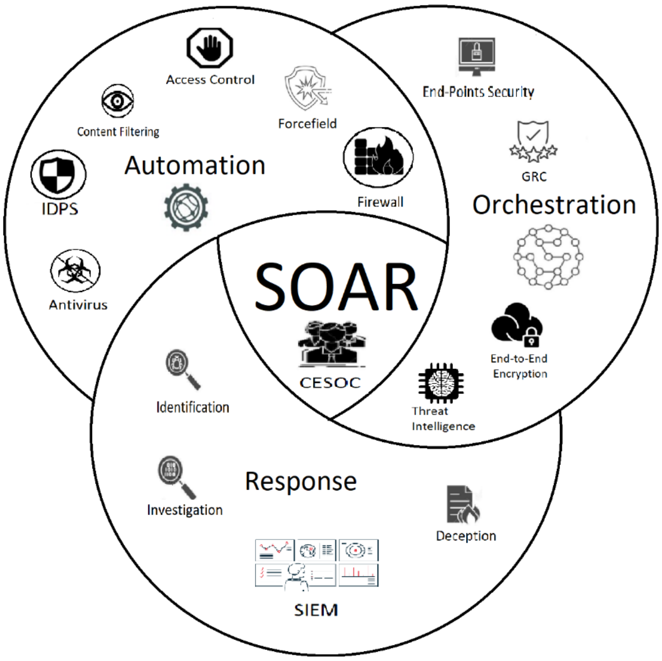


Figure 7: SOAR Depiction

4.3.1.1 Firewall (FW)

Firewall monitors incoming and outgoing network traffic, permits and blocks data packets based on a set of security rules. Its purpose is to block malicious traffic.

The Crystal Eye firewall does advanced application protection as well as traditional stateful packet inspection (SPI) capability at the network and application layers and integrates with other key security controls like IDPS to achieve defence-in-depth capability.

It is fast and advanced with up to 4 different firewall engines with multi-threaded capabilities to handle over 3,000 different protocols.

The Crystal Eye firewall engine is based on *IPtables* and can be used to implement both simple and advanced firewall protection. In its simplest form, the firewall can either allow or block data packets based on the port, host, protocol, or state of the connection. Through the implementation of more advanced rulesets, the platform supports port forwarding, load balancing and packet mangling among other things. The ***Application Filters*** module that is applied on the firewall enables for traffic to be allowed or denied based on the application protocol detected by the platform, by identifying and classifying over 160 network protocols across a broad range of application protocols, for example:

- File sharing application: *Microsoft OneDrive, Dropbox, Apple iCloud, etc*
- Online gaming: *Armagetron, StarCraft, Warcraft III, World of Kung Fu, etc*
- Instant messaging: *WhatsApp, Weibo, WebEx, Snapchat, etc*
- Media: *PPLive, PP Stream, QQLive, Spotify, TVUPlayer, etc*
- Remote desktop: *Remote Desktop Protocol, TeamViewer, VNC, PCAnywhere, etc*

4.3.1.2 Intrusion Detection and Prevention System (IDPS)

CE XDR’s IDPS engine supports signature-based, anomaly-based, and policy-based rules. The engine uses Suricata framework which is fully owned by Open Information Security Foundation (OISF) which in turn is supported by RP’s threat intelligence expert team. The framework has more than 43,000 rules. The threat signature database is updated many times in a day to keep up with the most recent known threats. Since the signature based IDPS supports both exploit-facing and vulnerability-facing, it is possible that the IDPS could deliver a zero-day protection.

The IDPS examines incoming data traffic with deep packet inspection technique which inspects the detail of each data packet including encrypted packet streams and acts on this analysis before passing the streams through other modules, thereby saving on processing power. The packet capture module (***PCAP Snap***) allows CE XDR to capture network traffic and transmits them to Red Piranha servers for automatic analysis.

Utilising the decryption engine, the IDPS scans both attack signatures and behaviours in both plaintext and encrypted communication. The functionalities of the platform apply on both inbound and outbound traffic.

The CE XDR has achieved 60 Gbps of IDPS throughput in the lab, verified by IEEE test results in August 2019. This ability to process gigabit traffic enables the platform to process encrypted traffic more effectively compared to its competitors in the market. The underlying ability to achieve that high throughput is the multithreading capability and CPU affinity in the appliance’s operating system, as explained below.

4.3.1.3 Multithreading

Multithreading is the ability to scale up a CPU (a core in a multi-core processor) capability by adding threads for running multiple applications concurrently if supported by the operating system. CE XDR uses multi-core system that enable multithreading to run its IDPS engine. It allows users to increase the number of threads allocated to the IDPS tasks and it can be configured to use anywhere from a single thread up to dozens of threads.

The Multithreading configuration allows CE XDR to scale both vertically and horizontally and ensure that the resources of the system are used optimally.

4.3.1.4 CPU Affinity

In addition to the configurable number of threads allocated to IDPS tasks, CE XDR also supports the Suricata CPU affinity feature which allows the user to specify CPU cores allocation, and the distribution of the workload amongst them. Distributing the processing between resources ensures that the IDPS engine does not overload resources on the CE XDR system. Additionally, this feature ensures that surplus CPU cores do not go underutilized.

4.3.1.5 Firewall Integration with IDPS

With its Unified Communication Management (UCM) integration system, CE XDR integrates the firewall capabilities with other components of the XDR. For example, when the IDPS identifies nefarious MAC addresses, it can map that across to the firewall to automatically create a firewall rule which blocks those addresses and stops the threat in its tracks.

Because they are unified under one management interface, they can work together flexibly to be used across different configurations of an enterprise network. In other words, the platform can position the IDPS module outside the firewall to repel attacks and reject the traffic before it is processed any further or to work with an existing firewall infrastructure at a headquarter network.

TCP/IP engines	Detection Engine	HTTP Engine
• Scalable flow engine • Full IPv6 support • Tunnel decoding ○ Teredo ○ IP-IP ○ IP6-IP4 ○ IP4-IP6 ○ GRE ○ VXLAN • TCP stream engine ○ tracking sessions ○ stream reassembly ○ target based stream reassembly • IP Defrag engine ○ target based reassembly	• Protocol keywords • Multi-tenancy per vLAN or capture device • xbits – flowbits extension • PCRE support ○ substring capture for logging in EVE • Fast pattern and prefilter support • Rule profiling • File matching ○ file magic ○ file size ○ file name and extension ○ file MD5/SHA1/SHA256 checksum — scales up to millions of checksums • Multiple pattern matcher algorithms that can be selected • Extensive tuning options • Live rule reloads — use new rules w/o restarting • Delayed rules initialization • Lua scripting for custom detection logic • Hyperscan integration	• Stateful HTTP parser built on libhtp • HTTP transaction logger • File identification, extraction and logging • Per server settings — limits, personality, etc • Keywords to match on (normalized) buffers: ○ uri and raw uri ○ headers and raw headers ○ cookie ○ user-agent ○ request body and response body ○ method, status and status code ○ host ○ request and response lines ○ decompress flash files ○ and many more
Protocol Parsers		**Packet Acquisition**
Support for packet decoding: • IPv4 • IPv6 • TCP • UDP • SCTP • ICMPv4 • ICMPv6 • GRE • Ethernet • PPP • PPPoE • Raw • SLL • VLAN • QINQ • MPLS • ERSPAN • VXLAN	App layer decoding: • HTTP • SSL • TLS • SMB • DCERPC • SMTP • FTP • SSH • DNS • Modbus • ENIP/CIP • DNP3 • NFS • NTP • DHCP • TFTP • KRB5 • IKEv2 • SIP • SNMP • RDP • New protocols developed in Rust language, for safe and fast decoding	• High performance capture ○ AF_PACKET ▪ experimental eBPF and XDP modes available ○ PF_RING ○ NETMAP • Standard capture ○ PCAP ○ NFLOG (netfilter integration) • IPS mode ○ Netfilter based on Linux (nfqueue) ▪ fail open support ○ ipfw based on FreeBSD and NetBSD ○ AF_PACKET based on Linux ○ NETMAP • Capture cards and specialized devices ○ Endace ○ Napatech ○ Tilera

Table 1: List of Engines and Capabilities Deployed by Crystal Eye XDR

4.3.2 Managed Detection and Response (MDR)

The CE Managed Detection and Response (MDR) platform provides services such as 24/7 monitoring and detection, rapid investigation and mitigation and advance threat hunting and intelligence. This service encompasses the extent capabilities of Extended Detection and Response (XDR) by integrating ***DFIR, SIEM***, and ***IDPS*** modules to enable CESOC with the immediate assist in delivering a comprehensive view on real time threat intelligence and the overall security posture of the system.

The Crystal Eye XDR enables unified security incident and response that automatically collects and correlates data from multiple CE endpoints. XDR provides high visibility of all endpoints, while processing threat information originating from the IDPS. Additionally, the XDR capability also enables rapid response to allow the IR team to minimise threats that may impact the availability of client systems or networks. The XDR solution offered by RP encompasses centralised management and the on-demand integration with networks, cloud-based, and host-based detection.

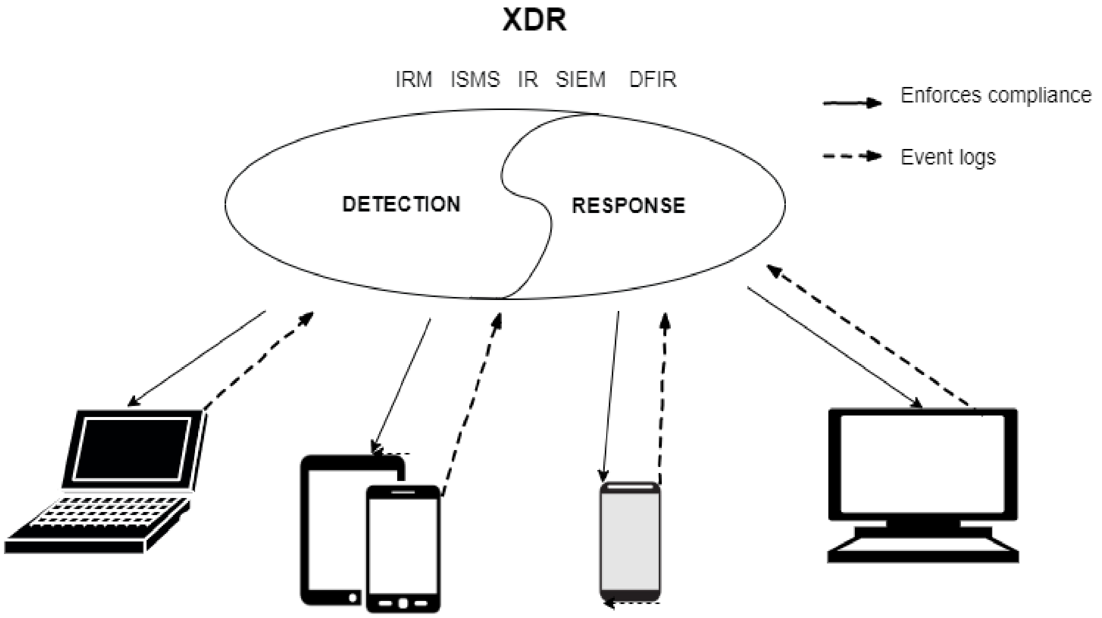
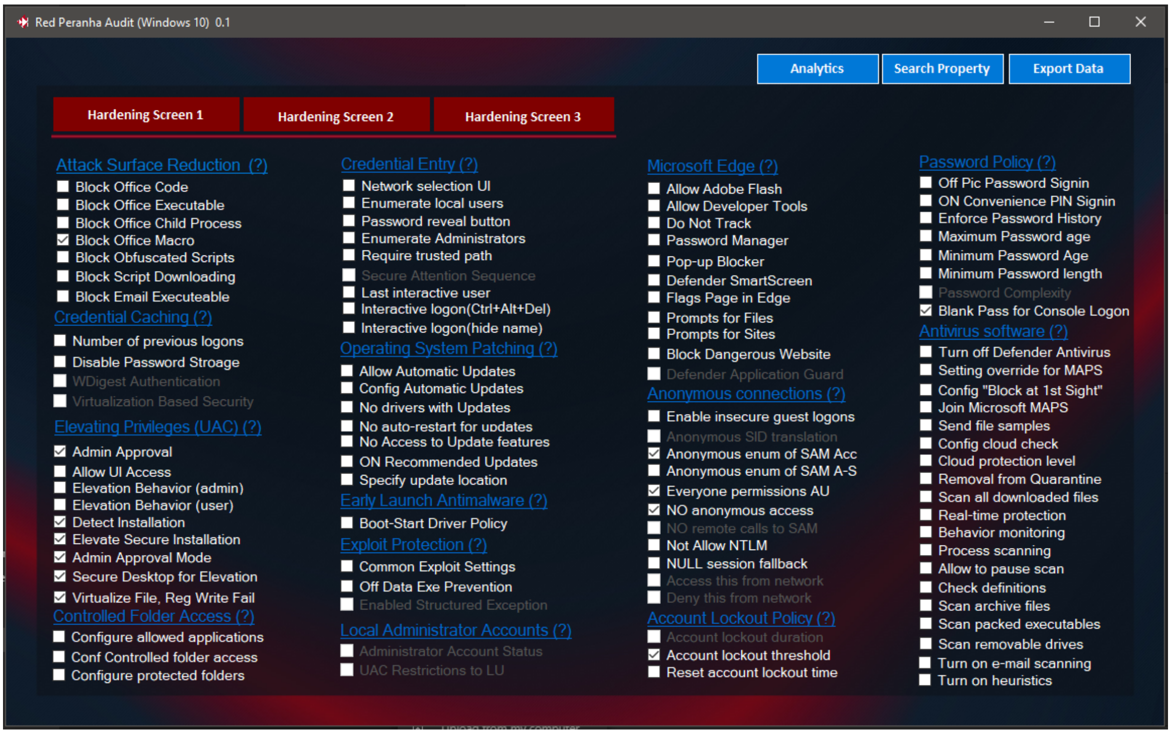


Figure 8: XDR Depiction

Extended Detection and Response (XDR) improves security by centralizing and correlating security information from multiple sources. It increases the overall detection capabilities when it comes to endpoint detection and response (EDR). Activities such as root cause analysis, impact assessment, threat hunting and automated detection and response will run with the aim to respond to new threats and generate a report. XDR utilises MDR to allow integration with CESOC to enable immediate assistance in delivering a comprehensive view of the overall security posture by sending captured data back to the CE centralised data processor.

Applications offered by MDR that integrate into XDR capabilities include:

Compliance Application – This application ensures that all endpoints connected to the CE networks fulfil a set policies and standards. The **Windows hardening** feature is part of the compliance application that enforces technical configurations to all vulnerable endpoints in a timely manner. An example of Windows hardening is the administrator enforcing strong password policy through this application across all devices connected to the CE network.



Attack Surface Reduction (?)
- □ Block Office Code
- □ Block Office Executable
- □ Block Office Child Process
- ☑ Block Office Macro
- □ Block Obfuscated Scripts
- □ Block Script Downloading
- □ Block Email Executeable

Credential Caching (?)
- □ Number of previous logons
- □ Disable Password Stroage
- □ WDigest Authentication
- □ Virtualization Based Security

Elevating Privileges (UAC) (?)
- ☑ Admin Approval
- □ Allow UI Access
- □ Elevation Behavior (admin)
- □ Elevation Behavior (user)
- ☑ Detect Installation
- ☑ Elevate Secure Installation
- ☑ Admin Approval Mode
- ☑ Secure Desktop for Elevation
- ☑ Virtualize File, Reg Write Fail

Controlled Folder Access (?)
- □ Configure allowed applications
- □ Conf Controlled folder access
- □ Configure protected folders

Credential Entry (?)
- □ Network selection UI
- □ Enumerate local users
- □ Password reveal button
- □ Enumerate Administrators
- □ Require trusted path
- □ Secure Attention Sequence
- □ Last interactive user
- □ Interactive logon(Ctrl+Alt+Del)
- □ Interactive logon(hide name)

Operating System Patching (?)
- □ Allow Automatic Updates
- □ Config Automatic Updates
- □ No drivers with Updates
- □ No auto-restart for updates
- □ No Access to Update features
- □ ON Recommended Updates
- □ Specify update location

Early Launch Antimalware (?)
- □ Boot-Start Driver Policy

Exploit Protection (?)
- □ Common Exploit Settings
- □ Off Data Exe Prevention
- □ Enabled Structured Exception

Local Administrator Accounts (?)
- □ Administrator Account Status
- □ UAC Restrictions to LU

Microsoft Edge (?)
- □ Allow Adobe Flash
- □ Allow Developer Tools
- □ Do Not Track
- □ Password Manager
- □ Pop-up Blocker
- □ Defender SmartScreen
- □ Flags Page in Edge
- □ Prompts for Files
- □ Prompts for Sites
- □ Block Dangerous Website
- □ Defender Application Guard

Anonymous connections (?)
- □ Enable insecure guest logons
- □ Anonymous SID translation
- ☑ Anonymous enum of SAM Acc
- □ Anonymous enum of SAM A-S
- ☑ Everyone permissions AU
- ☑ NO anonymous access
- □ NO remote calls to SAM
- □ Not Allow NTLM
- □ NULL session fallback
- □ Access this from network
- □ Deny this from network

Account Lockout Policy (?)
- □ Account lockout duration
- ☑ Account lockout threshold
- □ Reset account lockout time

Password Policy (?)
- □ Off Pic Password Signin
- □ ON Convenience PIN Signin
- □ Enforce Password History
- □ Maximum Password age
- □ Minimum Password Age
- □ Minimum Password length
- □ Password Complexity
- ☑ Blank Pass for Console Logon

Antivirus software (?)
- □ Turn off Defender Antivirus
- □ Setting override for MAPS
- □ Config "Block at 1st Sight"
- □ Join Microsoft MAPS
- □ Send file samples
- □ Config cloud check
- □ Cloud protection level
- □ Removal from Quarantine
- □ Scan all downloaded files
- □ Real-time protection
- □ Behavior monitoring
- □ Process scanning
- □ Allow to pause scan
- □ Check definitions
- □ Scan archive files
- □ Scan packed executables
- □ Scan removable drives
- □ Turn on e-mail scanning
- □ Turn on heuristics

Figure 9: Compliance App (Windows hardening)

DFIR Application – The Digital Forensics and Incident Response module is capable of collecting, analysing, and reporting evidence in a timely manner. The agent module that is deployed remotely on a specific network or sets of endpoints collects specific logs that are needed for the investigation. For example, the module can be scheduled to rapidly collect windows registry and RDP session logs in an event of a remote access breach for immediate investigation.

Furthermore, the application extends its coverage to the incident response (IR) team. The network based DFIR capability available in the on-premises firewall provides host-based data collection. As a result, it allows incident responders to rapidly address any incidents with a comprehensive set of data.

4.3.3 Identity and Access Management (IAM)

IAM is a fundamental in cybersecurity control, and it forms a critical part of Zero Trust Network Access (ZTNA) and Cloud Access Security Broker (CASB) protection for Secure Access Service Edge (SASE). The platform manages users' permission based on individual roles and group policies and each policy is module specific. Users and administrators can be allocated the minimum privileges needed to perform their duties.

The latest CE XDR allows IAM to be managed from a standalone Active Directory (AD) instance within Crystal Eye or by integrating with clients' existing AD. CE XDR uses Lightweight Directory Access Protocol (LDAP), an open, vendor-neutral, industry standard application protocol to manage the sharing of information about users, systems, networks, services, and applications throughout the network via AD. LDAP allows many different applications and services to validate users centrally.

Forcefield technique is applied as an additional protection layer on the IAM. It detects and blocks multiple failed logins that may be advanced persistent attack or botnet, allowing only legitimate users or traffic.

Account manage*r, *account role, and their sub-modules under System Configuration group and ***forcefield*** module under Security Configuration group work together to achieve IAM.

4.3.4 Secure Access Service Edge (SASE)

Secure Access Service Edge (SASE) is an emerging technology that combines Wide Area Network (WAN) capabilities with cloud-native security functions such as secure web gateways, cloud native security, firewalls, and zero trust network access. The CE SASE is mainly a cloud-based approach to secure WAN with ZTNA and CASB for its key cloud native security technologies.

ZTNA is a modern approach to securing remote access with endpoint-initiated and service-initiated architectures. It can be established in CE XDR by integrating network protection with the endpoint modules to provide stronger protection from on-premises out to remote devices. Network Control, System Configuration and Security Configuration module groups in CE XDR works together to support the establishment of ZTNA.

CASB or cloud access security brokers are either on-premise or cloud-based security policy enforcement points which are placed between cloud service consumers and cloud service providers that combine and implement enterprise security policies when the cloud-based resources are accessed. CASB consolidates multiple types of security policy enforcement. In CE XDR application, the examples of security policies include the users, user groups and group policies, device profiling, encryption, tokenization, logging, alerting, malware detection/prevention and so on.

Modules under Network Control group that allows CE XDR to deliver a SASE solution are described below:

Certificate Manager - This module allows users to generate self-signed certificates and upload external certificates, including those of the certificate authority. Certificate Manager helps to limit access that enforces the principle of least privilege in ZTNA.

***Border Gateway Protocol* –** Also known as BGP, is designed to enable optimization of internet connections by allowing exchange of routing information between gateway hosts in a network of autonomous systems. BGP establishes least possible latency and stable connection by ensuring the addresses in routing table has quality of pathing to each router. BGP could determine the best routes. It is a highly configurable routing protocol that allows the options of altering BGP attributes, creating prefix list and possibly change the cost of different available routes.

Device Management – This module makes use of the *network map* to identify various devices connected to the network. This module increases visibility of the enterprise network while also allows the administrator to map devices to users by referencing the related MAC Addresses. The Device Management provides a proper network segmentation as a basis of ZTNA architecture.

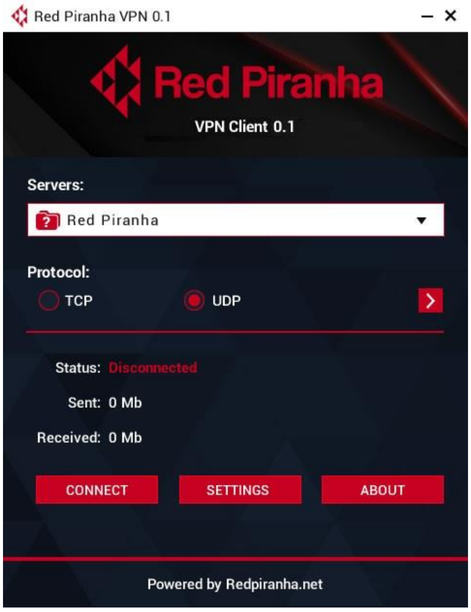
Infrastructure – The infrastructure module allows users to deploy various network configurations of the network. Infrastructure components of the CE XDR platform include, *DHCP server*, *DNS server, IP settings* and *SSH server*.

Quality of Service (QoS) – This module allows administrators to prioritize certain types of internet traffic. QoS can also be used to create downstream and upstream priority class rules. The main function of QoS is to facilitate bandwidth management. SASE contains QoS in the cloud and dynamically shapes traffic based on the policies that prioritise critical application requirement.

Web Proxy Server – This module acts as an intermediary for web requests originating from a network. This allows the CE XDR to act as a gateway and coordinate with the source server to start caching or storing its resources. This improves the security by preventing users from accessing any known malicious websites. Additionally, web proxy servers also provide better privacy, as it allows configurations to be made to encrypt web requests.

***Wireless Access Point* –** this module helps to configure and manage the wireless network interface on the CE XDR system. It supports the segmentation of guest access by generating a different Wi-Fi network that has no access to the internal network.

***SD-WAN App* –** This module provides remote users with secure connection from devices back to the corporate network as well as to cloud-based apps, data, and internet access. SD-WAN components of the CE XDR include *IPsec VPN* and *SSL VPN*. The *IPsec VPN* provides site-to-site tunnels to connect two sites through secure protocols. *SSL VPN* provides secure remote access to the CE XDR system, local network, and remote users. SD-WAN is the key foundation of SASE that provides endpoint protection for remote users.



Servers: Red Piranha

Protocol: ○ TCP ● UDP

Status: Disconnected

Sent: 0 Mb

Received: 0 Mb

Figure 10: VPN Application

Modules under Security Configuration group that allow CE XDR to perform SASE solution are described below:

***Agentless Application Whitelisting (AWL)* -** Crystal Eye's patented AWL technology allows the gateway appliance to control applications running on endpoint devices without the need to install and manage endpoint agents as well as extending protection on BYOD, IOT and SCADA devices.

***Content Filter* –** this module comes with default settings as an internet filter, but the administrator can customise the filtering policies based on parameters such as blacklists, phrase lists, mime type, file extensions, banned sites, gray sites and exception sites. Each parameter has granular breakdown allowing total control of what is allowed what is not for web browsing.

***DNS Insure* –** this module is a DNS filtering system that blocks websites and email services that point to domain names that are known to be malicious. Users can also build and continue to maintain users blacklist, listing all web addresses that clients' policy prohibits.

DNS Insure works in tandem with content filter which blocks web access based on its content.

***DMZ Firewall*–** this module allows an administrator to create a separate untrusted network, providing accessibility from untrusted network to the internet while maintaining isolation from the Local Area Network (LAN). The connection between DMZ and private network is blocked by default, but the administrator can open a pinhole for cases where special permission may be granted.

Forcefield – this module scans the system for authentication failures across all services installed. If the failure threshold is exceeded, the app assumes there is a brute force attack and thus bans the attacking IP address. Forcefield comes with default setting while allowing the administrator to adjust the criteria, like for example the maximum retry or failure threshold and friendly IP addresses to be excepted when listed in the whitelist.

It is an additional layer of protection that works with the convergence of IAM, a part of the SASE solution. It obstructs bots and unwanted traffic from entering the system, allowing only legitimate users or traffic.

***Gateway Security* -** CE XDR managed gateway security with *antimalware*, *anti-phishing* and *antivirus*. The *antimalware* works by scanning the server's file system for malware and instantly quarantines any infected file. The *anti-phishing* application blocks users from visiting malicious sites unintentionally. The platform makes use of signature-based and heuristic mechanisms to identify malicious websites even when a weblink is cloaked for deception. The *antivirus* application uses a central antivirus engine to scan web, FTP, mail, and others to examine files as they transit in real time through CE XDR before they reach the clients' systems. The application blocks encrypted files and compressed files of which size is suspicious to have contained malware. It also blocks files that are sent recursively, preventing Distributed Denial of Service (DDoS) attacks coming from file transfer.

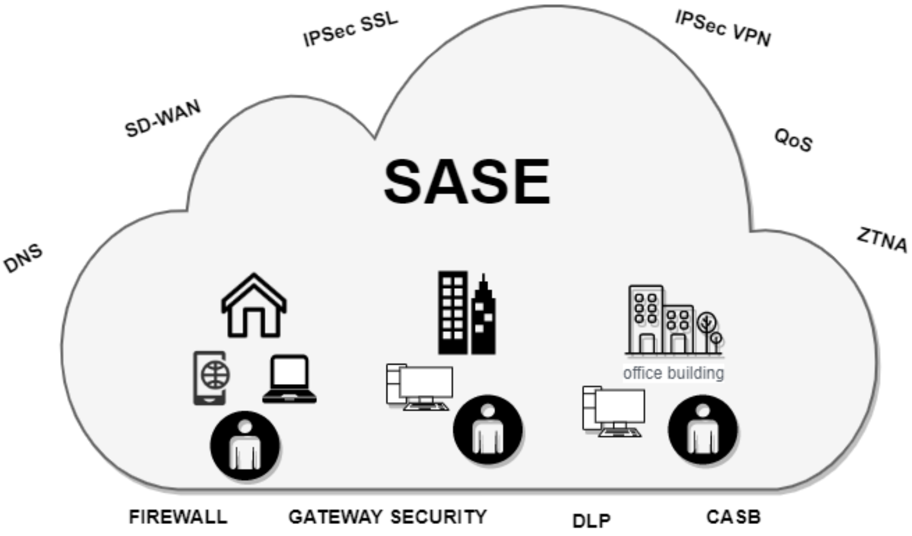


Figure 11: SASE Depiction

4.3.5 Threat Intelligence Platform (TIP)

CE XDR is a Threat Intelligence Platform (TIP) that aggregates, correlates, and analyses internal and external threat information in real-time for better defence. TIP provides solutions to reduce detection time, assist investigation, and enable a fast response to cyber threats. CE XDR has advanced IDPS that works with OISF framework to perform security scanning at the network level in real-time. OISF processes over 20 million Indicator of Compromises (IoCs) every day. In the context of the Threat Intelligence Platform, the function of IoCs investigation is to determine the characteristics, motives, and tactics of the future attack. The effectiveness of security defence can be increased with the TIP features which include:

4.3.5.1 Threat Analysis and Threat Hunting

CE XDR Threat hunting utilises several aspects such as machine learning and UEBA to analyse potential risks. Threat hunting helps to stop the cyberattacks by using the IoCs to identify the threats and to respond before they cause any disruption. Threat analysis and threat hunting can be achieved with the integration of modules within the CE XDR, like *vulnerability management,* the *risk report*, and other methods explained below.

Vulnerability management covers vulnerability scanning and reporting as well as proactive measures such as virtual patching to provide zero-day protection and reduce operational burden on IT staff.

Vulnerability scanning is designed to detect and flag any potential security weaknesses in servers and users' devices that exist in the CE XDR network. The three main types of vulnerability scanning include, *Deep – Non-Destructive Full and Slow Scan*, *Default – Non-Destructive*, *Full and Fast Scan* and lastly the *Ultimate – Full and Fast Scanning including Destructive*. All the vulnerability scan results are catalogued and can be included in a report for compliance auditing and risk management purposes.

Virtual patching is a quick fix done on the system or network environment as opposed to the source code of an app to overcome a security flaw so that it prevents an exploit from occurring as a result of a newly discovered vulnerability.

CE XDR coodrinates vulnerability management with its overarching SDN for update, upgrade and patching, ***application whitelisting***, ***content filter and proxy***, ***DNS insure***, ***firewall***, ***gateway security***, and ***protocol filtering*** modules under Security Configuration, and ***vulnerability scanning*** module under Compliance Control.

Threat hunting is employed to protect the system from current and future attack. Moreover, the automation of threat hunting performs a critical role in the XDR. It will enable the XDR to learn and use the information to detect similar events within the CE XDR system.

4.3.5.2 Deception

Deception techniques are misdirection methods used to deflect malicious users away from legitimate target and at the same time monitor unauthorised attempts for threat intelligence and analysis purposes. The Crystal Eye XDR platform can deploy deception technologies using the ***Network File Share*** (NFS) module which is under *Network Backup* in Compliance Control menu.

NFS can be configured to be intentionally accessible on the local network with intent to deceive attackers. The network share is populated with honey files, which if accessed, will send alert to the Crystal Eye XDR monitoring system.

Deception technology leverages ***Data Loss Prevention*** (DLP), that allows tagging of documents according to document classification policies set by the administrator. With the tags, documents are tracked when they are copied, moved or exfiltrated from a protected system. The CE XDR platform can also be configured to send alerts when a tagged file is moved.

DLP is a powerful tool that provides additional protection against a data breach of confidential and sensitive information including but not limited to Personally Identifiable Information (PII), company financial information or trade secrets.

On the Crystal Eye XDR Platform, the ***Data Loss Protection*** module is accessed under Compliance Control, with the main purpose to provide an additional layer of industry-standard protection of data stored within the Crystal Eye XDR's network against unauthorised access and exfiltration.

4.3.5.3 UEBA and Machine Learning (ML)

UEBA or User and Entity Behaviour Analysis is a technology that uses normal behaviour of users and computing environment as a baseline to detect anomalies or deviations from the normal patterns.

ML or Machine Learning is a subset of Artificial Intelligence (AI) that uses computer algorithms and statistics in a way that it gives the machine the ability to automatically learn and improve from experience without being explicitly programmed

CE XDR adopts UEBA technology to analyse input from various sources including the firewall, IDPS, databases as well as file management servers and alert when anomalies are detected to prevent attack. At the same time the anomalies detected are also used for threat analysis.

4.3.6. Compliance

The CE XDR compliance service also offers on-going custom policy management derived from the integration of eCISO and vCISO services that allows clients to keep track of their baseline compliance in real time. The compliance application often comes in handy during an audit as it supports a series of automated features.

The key compliance areas addressed include:

- Security Policy Management
- Awareness and Education
- Identity and Access Management
- Vulnerability Management
- Incident response
- Business Continuity Management / Disaster Recovery Planning (BCM / DRP)

Below are functionalities that are embedded within the compliance application:

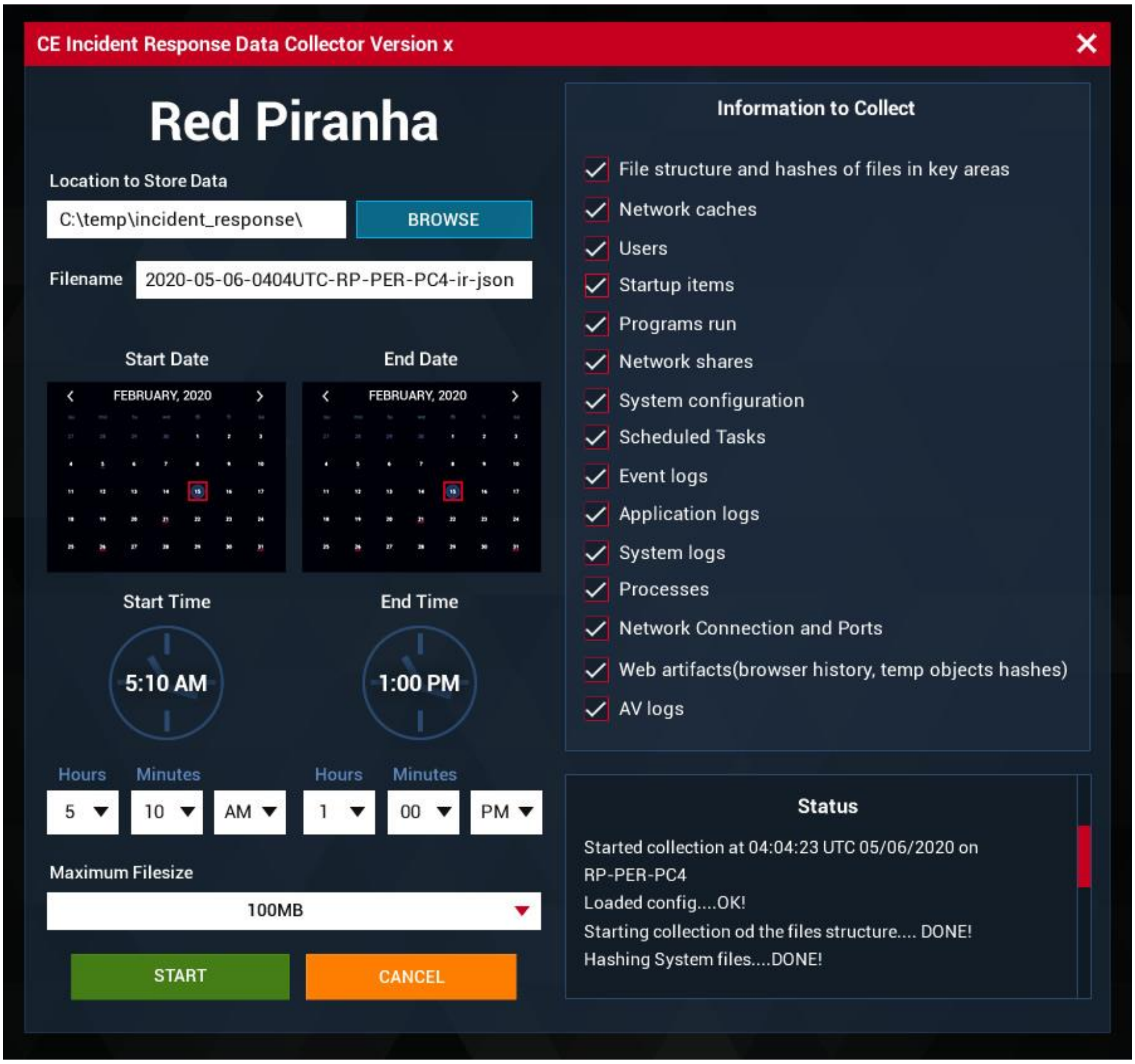
- **Integrated Risk Management (IRM)**, a set of practices and processes in risk-aware organizations, enabled by the technology, improves decision making and performance through an integrated view of how well an organization manages its unique set of risks.

  The Crystal Eye IRM provides an automated and integrated approach to meeting compliance obligation by pulling together relevant compliance information and controls from multiple points across the network into a central dashboard for easy visibility and drill down buttons for faster response. It allows clients to manage and report on the information to ensure compliance to a range of standards and provides a snapshot of compliance posture at a point in time.

  Modules that work together to form the IRM functionality are: ***IDPS*** and ***log processing and reporting*** found in Security Configuration group, and ***PCAP snap***, ***risk auditing****,* and ***security plan wizard*** modules found under Compliance Control group.

- **Information Security Management System (ISMS)** provide support to the risk management system, to aid with better accuracy during the generation of risk scores in the ***risk auditing*** module. This functionality aims to govern the policies, procedures, processes, and workflow that was chosen to protect the organisation.

- **Incident Response**, the platform seamlessly integrates alerts into RP's managed services in CESOC to provide rapid response to security incidents that occur across the clients' network in real-time. Incident response is orchestrated by the ***IDPS*** and ***SIEM*** modules.



Location to Store Data: C:\temp\incident_response\

Filename: 2020-05-06-0404UTC-RP-PER-PC4-ir-json

Start Time: Hours 5, Minutes 10, AM

End Time: Hours 1, Minutes 00, PM

Maximum Filesize: 100MB

Information to Collect

- ☑ File structure and hashes of files in key areas
- ☑ Network caches
- ☑ Users
- ☑ Startup items
- ☑ Programs run
- ☑ Network shares
- ☑ System configuration
- ☑ Scheduled Tasks
- ☑ Event logs
- ☑ Application logs
- ☑ System logs
- ☑ Processes
- ☑ Network Connection and Ports
- ☑ Web artifacts(browser history, temp objects hashes)
- ☑ AV logs

Status

```
Started collection at 04:04:23 UTC 05/06/2020 on
RP-PER-PC4
Loaded config....OK!
Starting collection od the files structure.... DONE!
Hashing System files....DONE!
```

Figure 12: Crystal Eye Incident Response Data Collector

- ***Incident and Event Services SIEM*** module, helps users to manage various settings that define various levels of security analysis carried out by RP's Security Operation Team, also enables transmission of incident and event data to the Red Piranha SIEM Server. Under the compliance control module CE XDR has ***incident response service*** that tracks and has the feature to escalate alerts and logs for detailed analysis.

4.3.7 Service Delivery Network (SDN)

CE XDR is backed by Red Piranha's SDN and supports all the applications that come with the appliance and their subsequent upgrades, updates, patches, and databases. It ensures that only the latest version of application is available for clients to install from the Marketplace module. A team of experts test and verify all upgrades, updates, and patches before pushing them to the cloud for clients' systems to apply, which include the malware signature, URL blacklist, DNS sinkhole, rule sets, etc. The SDN processes give users security assurance on the applications and the references used.

Clients can schedule an update check as frequently as daily, twice a day, every two hour or hourly basis.

4.3.8 Backup

Backup is a very important hedge against eventualities like hardware damage, system misconfiguration, cyberattacks, and various other events regardless of the cause, that require data restore from backup.

CE XDR manages backup and restore of configuration settings, users' documents, databases and log files with several modules or menu as described below.

Baremetal backup and Restore – backs up all configuration settings and home directory, found under System Configuration menu.

Configuration Backup and Restore – backs up configuration settings, including all application configuration if they are managed within CE XDR. There are options of storing the backup files locally, at Red Piranha Cloud, at clients' own server, at Azure, and in USB device, all of which could be done concurrently if desired. There are options for full, incremental, or differential backup. The backups are immediately compressed while encryption is optional. Encryption algorithm used is the Advanced Encryption Standard (AES) which is also used by the U.S. government to protect classified information. This module is found under System Configuration menu.

Backup PC - manages the backup of users' documents, databases, and log files. This module is found under Compliance Control menu.

All backup processes in CE XDR can be done manually or automatically by schedule.

4.4 List of Modules

Modules that build up the functionalities of multilayer protection are categorised into: System Configuration, Network Control, Security Configuration, Compliance Control and Report. The following is the list of all available modules, broken down into categories. They include modules that are available by default and additional modules that can be installed from the Marketplace as and when required to add further layers of protection.

System Configuration	
Level 1	***Level 2***
Account Manager	Accounts
	Active Directory Authentication
	Directory Server
Account Roles	Administrators
	Groups
	Users
Backup	Baremetal Backup and Restore
	Configuration Backup and Restore
	Storage Manager
Date and Time	
Factory Reset	
General Settings	
High Availability	
Mail Settings	
Software Updates	
System Registration	
More from Marketplace	
Email Scanner	
Network Control	
Level 1	***Level 2***
Certificate Manager	
Border Gateway Protocol	
Device Management	Network Map
Email Scanning Gateway	
Infrastructure	DHCP Server
	DNS Server
	IP Settings
	SSH Server
Network Diagnostic Tool	
Quality of Service (QoS)	
Routing	Multi-WAN
	NAT Firewall
	Port Forwarding
Web Access Control	
Web Proxy Server	
Wireless Access Point	
SD-WAN	IPSec VPN
	SSL VPN
More from Marketplace	
1 to 1 NAT	
DMZ	

Table 2a. CE XDR modules and functionality, broken down by categories

Security Configuration	
Level 1	***Level 2***
Application Whitelisting	
Content Filter and Proxy	Deep Packet Inspection
DNS Insure	
Firewall	Custom Firewall
	DMZ Firewall
	Egress Firewall
	Firewall
Forcefield	
Gateway Security	Anti-Malware File Scanner
	Antiphishing
	Antivirus
Intrusion Protection and Detection System	
Log Processing and Reporting	
Protocol Filtering	Application Filter
	Protocol Filter
More from Marketplace	
Compliance Control	
Level 1	***Level 2***
Data Loss Protection	
Incident Response Service	
Incident and Event Services (SIEM)	
Network Backup	Backup PC
	Database Backup
	Forensic Logging
	Network File Share
PCAP SNAP	
Risk Auditing	
Security Plan Wizard	
Vulnerability Scanning	
More from Marketplace	
Software RAID Manager	

Table 2b. CE XDR modules and functionality, broken down by categories (continued)

Reports	
Level 1	***Level 2***
Executive Report App Status Disk Usage Events and Notification Gateway Scan Report IP Attack Map IDPS Alerts Log Viewer Network Detail Report Network Interfaces System Report System Resource Report VoIP Monitor Filter and Proxy Report	
Linux Monitoring Sensors	
More from Marketplace	
Network Visualizer	

Table 2c. CE XDR modules and functionality, broken down by categories (continued)

4.4.1 The Marketplace

The Marketplace is a menu in CE XDR where clients can get additional optional functionalities. The main purpose of the Marketplace is to simplify management of the CE XDR system. There are many default modules that are already included in the platform when first installed, which provide the functionalities to protect, detect, and respond for clients' systems. Users can add more modules for additional layers of protection as and when needed from the Marketplace. If a module needs additional billing, licensing, or service level agreement (SLA), they are all managed automatically and instantaneously within the Marketplace.

4.5 Report

The CE XDR provides reporting functionality that assists with diagnostic, monitoring and network maintenance tasks. The reporting functionality contains several modules as described below:

Executive Report - generates reports that combine multiple reports from other modules as listed below in a single report, to help company executives get a quick look into some or all of the system and security incident reporting metrics. Users can configure what reports to include. The reporting frequency can be automatically scheduled, and the report can be sent to designated email addresses.

App Status - provides a report of all application and service statuses installed on the CE XDR platform. Within the module there is a start-stop service function for each the content filter, web proxy server, antivirus, intrusion protection and reporting, log processing and reporting, forcefield, and security incident and event management

(SIEM). The start-stop service function potentially helps expediting responses when an event report requires action.

Disk Usage - the Disk Usage module displays a visual representation of the current disk usage and the remaining disk space on the platform. The application helps analysis of disk usage for each directory of the CE XDR.

Events and Notification - provides log reports on various events that occur in the CE XDR appliance on a real time basis. The events can be categorized as informational, warning, and critical events. The module can be configured to send email notification to multiple email addresses.

Gateway Scan Report - provides the virus scan result and the detail of malicious files. The report displays the scan summary in detail, that includes timestamp, IP address, site, blocked URL, reason, content type and description. The report can be generated based on hours, days, weeks, and months.

IP Attack Map - the IP Attack Map displays the world map showing real-time attacks to CE XDR network systems. It also displays banned IPs table, real-time attack tracker, protocol traffic size indicator, device traffic size indicator, alert report, and alert analysis.

IDPS Alerts - generates a list of reports regarding alerts, flows, DNS, and SSH/TLS on a real-time basis. The alert report shows a 360-degree view of the alerts that have been recorded by CE XDR and they can be filtered by time range.

The IDPS alerts app helps administrators in classifying and analysing alerts generated by the CE XDR, and this helps the threat intelligence platform. The app also elaborates the attack information in detail, including the source IP, destination IP, country of origin, region name, description of the attack in the IDPS Alert Report.

Log Viewer - generates the report of the system log files in the CE XDR system transparently. The logs display the Timestamp, Level, Subsystem, and Message. The log viewer app helps in investigating a security incident and performing troubleshooting tasks.

Network Detail Report - provides a report on network information, including the bandwidth consumed, the utilisation of network devices, and active IP addresses. The Network Detail Report helps in analysing factors that impact network performance.

Network Interfaces - provides network throughput information of all network interfaces. The report displays the data transmitted and received (in Mbps) in graphical and tabular representation.

Network Visualizer - provides a graphical view record of network utilization with various parameters within the Crystal Eye XDR. The Network Visualizer report helps in troubleshooting, optimizing the network, and detecting network performance issues. The administrator can easily understand the configuration of the appliance’s network and identify the network bandwidth used by the individual with this report.

Protocol and Application Detail Report – generates a report that provides an insight into network traffic within the CE XDR including size and packet information of the protocol as well as the application data details. The reports are divided into three sub-reports which are Top Protocols, Top Devices, and Top Protocol classification reports.

Risk Report – generates a report that supports the IRM. It includes Risk Overview, Status, Risk Review Status, Management Risk Review Log, and so on. The overall report supports risk analysis and mitigation planning.

System Report - provides operating system information of the CE XDR. The report is divided into two main sections, System Details and File System Summary. The System Details provides important information related to CE XDR appliances such as the CE XDR firmware, the kernel version, system time and date, CPU model, memory size, uptime, and load. The File System Summary generates a summary of disk related information in detail including the total size of internal disk space, available space and the percentage of the space used.

VoIP Monitor - provides insight of a broad range of attack on Voice Over IP (VoIP) protocol based on the attack patterns, in the form of alerts. The timestamp of the attack, the source IP address of the attacker, the destination IP address of the affected machine, the country of origin, attack description, and the rule that generate the alert (attack type), can be analysed from the data. The statistics of the data can be presented in the form of line chart, pie chart and tables.

CE XDR protection extends to VoIP systems if they are integrated into clients' protected network. VoIP systems are subject to different kinds of intrusions, some of which are specific to VoIP, and some of which follow a general pattern of attacks against an IP infrastructure. Nevertheless, all are within the umbrella of Crystal Eye XDR protection. CE XDR logs and reports attacks against the VoIP system separately for better monitoring and risk management.

The VoIP monitoring system can also implement Session Initiation Protocol (SIP) monitoring, by correlating the network statistics of the VoIP connections.

Linux Monitoring Sensors – provides real-time statistics from the Linux environment sensors that are deployed at CE XDR appliances. The report delivers data such as CPU temperature, case temperature, fan speed, NIC temperature, etc. The generated report is useful for availability and integrity monitoring. Furthermore, the function can also generate alerts when it detects anomalies.

5. Product Security

The reviewers undertook a technical security review on the CE XDR version 4.0 which has evolved since the initial technical review in 2017 in response to changing landscape of cyber threats.

The reviewers found that the CE XDR platform offers a myriad of cyber protection functions that are comprehensive and when deployed together they provide not only multilayered protection against cyberattacks but also a platform for threat intelligence and compliance control. The comprehensiveness of the available functions is convincing that the platform is adequate for cybersecurity assurance for small and medium businesses and possibly beyond.

The product secures systems at the perimeter or the borders with outside internet, all the way to each individual endpoint and that includes computers, laptops, tablets, smartphones, etc. The managed and orchestrated services gives multiple coverage on system vulnerabilities against threats and help with risk management while at the same time logs events extensively without compromising network and computing capacity.

The reviewers found no pre-authentication vulnerabilities and thus merely provided several recommendations to improve the user experience of the CE XDR at the Graphical User Interface (GUI). These changes have been taken into consideration and are being implemented through the constant CE XDR improvement program.

Nevertheless, the technology and standards keep evolving and they may undermine the current functionality of this product in the future. However, the reviewer team is confident that Red Piranha team will address any issues discovered with the product in a timely manner as they emerge and continuously evolve with the technology advancement.

6. Conclusion

The review was performed with the intention of verifying and validating the functionalities of the latest evolution of the CE XDR platform, which is currently version 4.0, against the claims by Red Piranha. The review is an expansion from technology report by auditors which was done in 2017. Since then the platform has evolved to include more functionalities and latest technology in cyber protection. It is now more than a next generation firewall, it is a comprehensive extended detection and response system also known as XDR.

The review found that the strength of the product is the features integration that allows multilayered security protection which is very much in line with recommendation by all cybersecurity standards. It includes features that allow users to reach cybersecurity maturity with the inclusion of events documentation within the comprehensive Report and the Compliance control modules.

The system allows easy vertical and horizontal scaling to accommodate various clients' needs. We continue to agree with the initial auditors that the platform is a sophisticated yet flexible cybersecurity solution suitable and even beyond for their current target market which is small and medium businesses.

CE XDR deploys multiple modules that work together to build the cybersecurity features like XDR, SOAR, AIM and SASE even with the default installation. The level of protection can be scaled according to client's changing needs and risk profile.

CE XDR does not only offer cybersecurity protection, but it is also a threat intelligence platform as it collects and analysis security incident and events and actively exchanges information on indication of compromise or as known as IoC with Open Information Source Foundation (OISF). The Red Piranha Security Operation (SecOps) team is an active contributor to OISF.

Although compliance is often overlooked within small and medium businesses despite the oversight could translate into risks to business operation, Red Piranha has anticipated the need of compliance for its clients. The compliance control module prompts clients for recommended actions like vulnerability scanning, risk management, data loss protection, and overall business continuity management and disaster recovery planning.

The platform also provides the ease of monitoring activity with the use of dashboards that displays all significant device information and network security landscape in user-friendly graphical maps, charts, and clean tables. The dashboards also provide ability to perform common tasks without the need to leave the view and drill down the menu pane. This feature allows faster response to an event.

The SDN which checks and verifies all updates, upgrades, and patches before they are pushed to the cloud for client adds security assurance to the protection system.

At the bottom line, the reviewers concluded that the CE XDR platform is a very good product and ahead of its competitors in the industry. The platform continuously improves to cover evolving threats and puts the platform in a good position for the business going forward.

Glossary

AES: Advance Encryption System, which is a symmetric block cipher that uses a block length of 128 bits and key lengths of 128, 192 or 256 bits. AES relies on the same key for both encryption and decryption.

Authentication: The process or action of verifying the identity of a user or process.

AWS: Amazon Web Service, a remote computing service that provides cloud computing infrastructure provided by Amazon.com Inc.

Azure: A cloud services platform provided by Microsoft.

BGP: Border Gateway Protocol is the postal service of the internet and it is also the protocol that makes internet work. It does it by enabling data routing on the internet.

Blacklist: The opposite of Whitelist, a list of items, including but not limited to email addresses, passwords, URLs, IP addresses, domain names, file hashes, etc, that are denied access.

Brownfield: An environment where development or deployment of a new system is within the immediate presence of existing (legacy) system.

BYOD: Bring Your Own Device(s), refers to being allowed to use one's personally owned device, rather than being required to use an officially provided device.

Certificate: Security certificate, a digital file containing information of a public / private key-pair, used to establish the authenticity of one or more parties involved in digital communication.

Cyberattack: Any attempt to expose, alter, disable, destroy, steal, or gain unauthorised access to or make unauthorised use of an asset by digital based connection.

Cybersecurity: The protection of computer systems and networks from the theft of or damage to their hardware, software or electronic data, as well as from the disruption or misdirection of the of the services they provide.

Data Loss Prevention: A system that detects and prevent potential data breaches / data leakage / data exfiltration by monitoring sensitive data while *in use* (endpoint action), *in motion* (network traffic) and *at rest* (data storage).

DHCP: Dynamic Host Configuration Protocol, a network management protocol used on Internet Protocol (IP) networks, whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on the network, so that they can communicate with other IP networks.

DMZ: Demilitarized Zone, is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted, usually larger, network such as the Internet.

DNS: Domain Name System, part of internet communication system that associates IP addresses with domain names.

eCISO: Electronic CISO (Chief Information Security Officer), a Red Piranha product that is an automated service that integrates CE XDR with remote consulting services to produce in-depth compliance reports and help clients develop a detailed information security plan.

Endpoint: Any device, laptop, desktop, tablet, phone, etc that are on the ‘edge’ (or periphery) of the network system.

Exfiltration / exfiltrating: Unauthorised copy, transfer or retrieval of data from a computer or network system to outside of the network.

Exploit-facing: a signature-based malicious activity detection that detects based on common attack patterns.

Firewall: A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules, which basically comprise of the network address, protocol and port number.

FTP: File Transfer Protocol, a standard network protocol used for the transfer of computer files between one system to another.

Greenfield: An environment where development or deployment of a new system is started from scratch or fresh page without any legacy constraint.

IDPS: Intrusion Detection and Prevention System, a system that could be a device or software that monitors a network or system for malicious activity or policy violations. Any activity or violation is typically reported to an administrator or collected centrally using a security information and event management system or SIEM. IDPS can drop communication should a threat or policy violation be detected.

IoCs: Indicator of Compromises, are pieces of forensic data that identify potentially malicious activity on a system or network.

IoT: Internet of Things, is a system of interrelated computing devices, mechanical and digital machines provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction

IP address: Internet Protocol address, is a numerical label assigned to each device connected to a computer network that uses the internet protocol for communication. IP address is also referred to as logical address as oppose to MAC address which is a physical address.

IRM: Integrated Risk Management, is a set of practices and processes in risk-aware organizations that are enabled by the technology that improves decision making and performance through an integrated view of how well an organization manages its unique set of risks.

ISMS: Information Security Management System is established to governs the policies, procedures, processes and workflow that are chosen to help protect organisation data security.

LAN: Local Area Network, is a network that covers small geographical area such as homes, offices and groups of building.

LDAP: Lightweight Directory Access Protocol, is an application protocol for querying and modifying items in directory service providers like Active Directory, which supports a form of LDAP.

MAC / MAC address: NAC stands for Media Access Control. It is a unique identifier assigned to a network interface controller or also known as network card, for use as a network address in communications within a network segment. This use is common in most IEEE 802 networking technologies, including Ethernet, Wi-Fi, and Bluetooth. MAC address is also referred to as physical address, as oppose to IP address which is a logical address.

NGFW: Also known as Next-generation Firewall, it is part of the third-generation firewall technology that combines the capability of traditional firewall with other network device filtering functions including deep packet inspection and intrusion prevention system.

PCAP: Packet Capture, is an application that captures live network packet data for analysing or further processing.

Phishing: A cybercrime in which target or targets are deceived by the perpetrator disguising as a trustworthy entity in an electronic communication. The disguise can come in email, phone call or text message, luring potential victim to do something, for example to visit fraudulent website which will download malware into the victim's system. **Anti-phishing** is security measures that counter the phishing attack that includes awareness training, suspicious email blocking, web link blocking, etc.

PII: Personal Identifiable Information, is any data that can be used to identify a specific individual. For example: name, date of birth, occupational details, medical records, etc.

SCADA: Supervisory Control and Data Acquisition is a control system architecture comprising computers, networked data communications and graphical user interfaces (GUI) for high-level process supervisory management, while also comprising other peripheral devices like programmable logic controllers (PLC) and discrete proportional-integral-derivative (PID) controllers to interface with process plant or machinery.

SDN: System Delivery Network, a software update delivery system that uses a dedicated team of engineers and developers to verify integrity and fixed errors and bugs in software updates and upgrades before they are pushed to clients.

SD-WAN: Software-defined Wide Area Network, is a technology that distributes network traffic across wide area network (WAN) that uses software-defined networking (SDN) concept.

SIEM: Security Information an Event Management, a system that manages security event logs and use rules and statistical correlations to turn the logs into actionable information. The information produced helps cybersecurity team to detect threats in real time, manages incident response and perform forensic investigation and prepare audits for compliance purposes.

SIP: Session Initiation Protocol, is a group of rules to set up the internet telephone calls, video conferencing and other multimedia connections.

SSH: Secure Shell, is a connection protocol using encryption to secure the connection between two endpoints in a network system.

SSL: Secure Socket Layer, is a standard technology for establishing an encrypted link between two endpoints in a network system.

TCP/IP: Transmission Control Protocol / Internet Protocol, is a suite of communication protocols used to interconnect network devices on the internet. All modern internet connection run on this protocol.

TIP: Threat Intelligence Platform, is an emerging technology discipline that helps organizations aggregate, correlate, and analyse threat data from multiple sources in real time to support defensive actions.

TLS: Transport Layer Security, is a security protocol designed to facilitate privacy and data security for communications over the internet. Conceptually, TLS and SSH have a very strong similarity that offers data encryption, server authentication, client authentication, and data integrity mechanism. Although, SSH is not the strongest encryption method, it's feasible protocol to secure communication. TLS most used as a security layer for HTTP, SMTP, and FTP traffic.

UEBA: User and Entity Behaviour Analytics, a machine learning model that helps to prevent cyberattack by detecting security anomalies.

vCISO: virtual CISO (Chief Information Security Officer), a Red Piranha product that offers on-site and remote access to their pool of highly experienced security experts to develop client’s cybersecurity plan and meet client’s reporting requirements. It can be utilised by clients who use the CE XDR as well as those who do not.

VPN: Virtual Private Network, is a network communication protocol that add encryption into packet data to create a kind of tunnelling for safe communication between a personal computer to the VPN server.

Vulnerability-facing: a signature-based malicious activity detection that detects by the identification of specific network vulnerabilities.

WAN: Wide Area Network, is a network of computing resources that covers larger geographical areas.

Whitelist: The opposite of Blacklist, a list of items, including but not limited to email addresses, passwords, URLs, IP addresses, domain names, file hashes, etc, that are allowed access.

XDR: Extended Detection and Response, is a platform that collects and automatically correlates data across multiple security layers: email, endpoint, server, cloud workloads and network, so that threats can be detected and responded faster.

Zero Trust Network Access (ZTNA): is a set of network access technologies deployed at the perimeter of a network that operates on an adaptive trust model that starts with no one is trusted and access is granted on a *need-to-know* or least privilege basis, defined by granular policies.

Zero-day Exploits: is a cyberattack that occurs on the same day a weakness is discovered in software. At that point, it's exploited before a fix becomes available from its creator.

Zero-day Protection: is the ability to provide protection against *zero-day* exploits. Since *zero-day* attacks are generally unknown to the public it is often difficult to defend against them.

References

Australia's cyber security strategy 2020. (2020). Retrieved 17 August 2020 from: https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

Australia's cyber security strategy. (2016). Retrieved 17 August 2020 from: https://www.homeaffairs.gov.au/cyber-security-subsite/files/PMC-Cyber-Strategy.pdf

Brozek, M. (2020). XDR Listed as a Top Security and Risk Management Trend by Gartner. Retrieved 27 August 2020, from https://blog.paloaltonetworks.com/2020/04/cortex-security-and-risk-management/

Firstbrook, P., & Lawson, C. (2020). Innovation insight for extended detection and response. Retrieved 27 August 2020, from https://www.gartner.com/en/documents/3982247

Force field security the next generation, proactive approach to cyber security. (2020). Retrieved 10 August 2020 from: https://www.forcefieldsec.com/

Goldman, J. (2018). Cisco vs Palo Alto networks: top ngfws compared. Esecurityplanet.com. Retrieved 14 August 2020 from: https://www.esecurityplanet.com/products/cisco-vs-palo-alto-networks-ngfw-comparison.html.

Johnson, R., Vienot, A., & Johnson, R. (2020). Understanding ueba: what it does and how it works - the tech report. The Tech Report. Retrieved 27 August 2020, from https://techreport.com/blog/3468988/understanding-ueba-what-it-does-and-how-it-works/.

Lerner, A. (2019). Say hello to SASE (Secure Access Service Edge). Gartner Blog Network. Retrieved 24 August 2020, from https://blogs.gartner.com/andrew-lerner/2019/12/23/say-hello-sase-secure-access-service-edge/.

Malmgren, A., & Persson, S. (2016). A comparative study of Palo Alto networks and juniper networks next-generation firewalls for a small enterprise network. Retrieved 14 August 2020 from: https://www.diva-portal.org/smash/get/diva2:934269/FULLTEXT01.pdf

Mardisalu, R. (2017). What is Advanced Encryption Standard (AES): beginner's guide. Retrieved 17 August 2020 from: https://thebestvpn.com/advanced-encryption-standard-aes/

Morgan, S. (2019). Global cybersecurity spending predicted to exceed $1 trillion from 2017-2021. Retrieved 17 August 2020 from: https://cybersecurityventures.com/cybersecurity-market-report/#:~:text=Worldwide%20spending%20on%20information%20security,and%20%24170.4%20billion%20in%202022.

What is a threat intelligence platform? (2019). Retrieved 13 August 2020 from: https://www.scmagazine.com/home/advertise/what-is-a-threat-intelligence-platform/