Crystal Eye Passive Encryption Control Application

Securing IoT & Critical Infrastructure

Red Piranha

INTRODUCTION

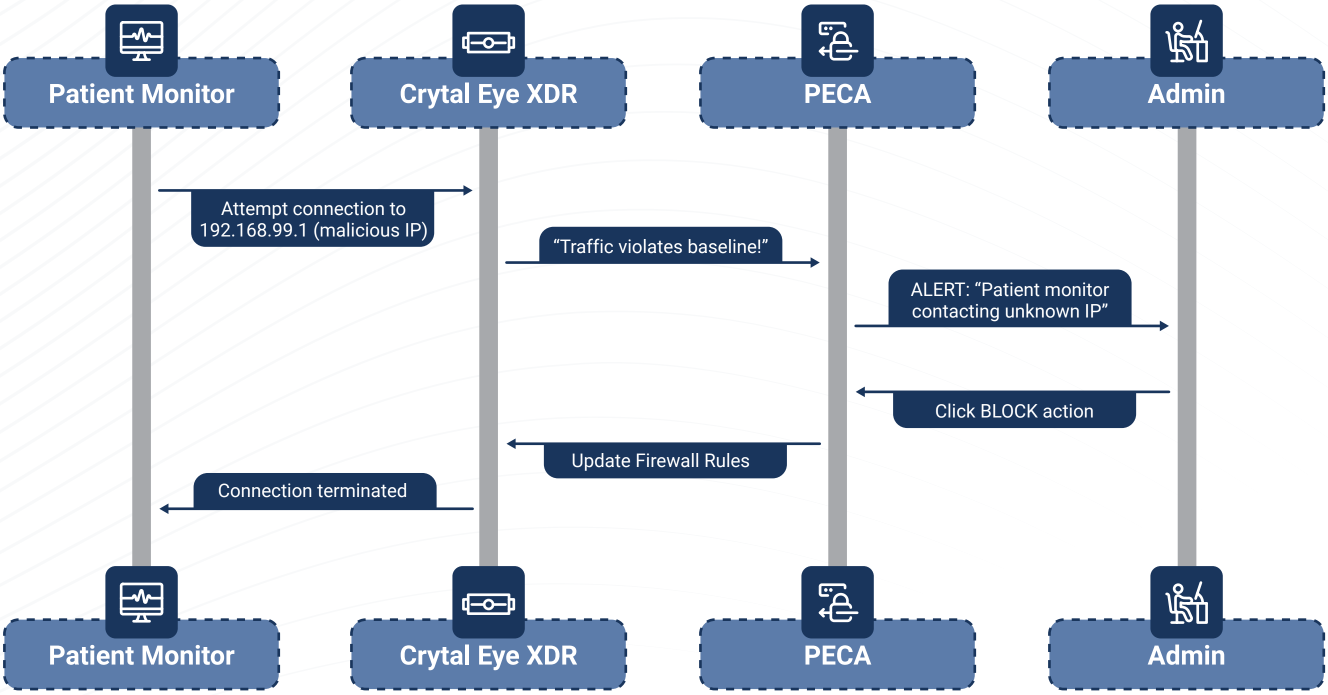
Cyber threats are evolving, and today's attackers exploit encrypted channels to bypass traditional defences. Red Piranha's Passive Encryption Control Application (PECA) within the Crystal Eye unified security platform closes this gap. It monitors encrypted traffic without decryption, identifies behavioural baselines, and alerts on anomalies in real-time, making it ideal for protecting IoT, Operational Technology (OT), and Industrial Control Systems (ICS) in sectors like healthcare, mining, and energy.

CORE FUNCTIONALITY OVERVIEW

Feature	Description
Passive Monitoring	Profiles benign encrypted traffic without requiring decryption or agents
Behavioural Baseline Detection	Learns normal traffic patterns for IoT/OT devices; flags anomalies
Encrypted C2 Detection	Detects covert Command & Control attempts over SSL/TLS channels
Granular Device Isolation	Allows blocking by device, server, protocol, or application
Integration with Firewall & DLP	Works with Advanced Firewall and DLP for layered Zero Trust enforcement
IEC 62443 Alignment	Supports zone-based segmentation and security level assignment for IACS

USE CASE SNAPSHOT: HEALTHCARE

A patient monitor should only talk to hospital servers. If it attempts to connect to an unknown IP, PECA detects and blocks it instantly protecting sensitive data and patient safety.

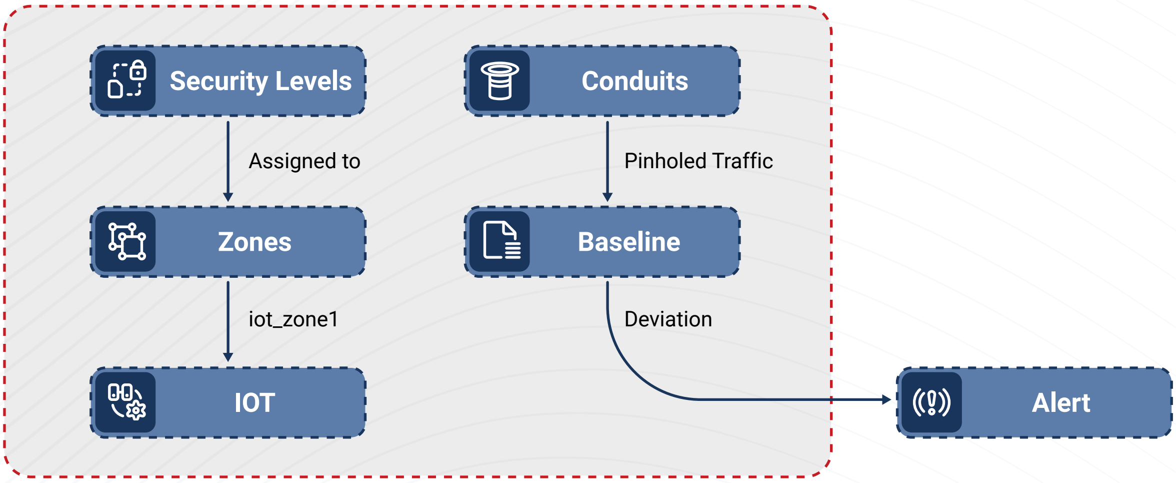


IEC 62443 ZONE-BASED SECURITY MODEL

Crystal Eye enables compliance with IEC 62443 by enabling segmentation into Zones and Conduits. PECA enforces encrypted traffic policies within and between zones:

IEC 62443 Concept	Crystal Eye Implementation
Zone	Firewall-defined segment for IoT/OT devices
Conduit	Pin-holed network path between zones with controlled encrypted flow
Security Level	Enforced using DLP, Firewall rules, and PECA behavioural baselines

IEC 62443 Framework



TECHNICAL STACK SYNERGY

The Crystal Eye Platform integrates the following for a defence-in-depth Zero Trust posture:

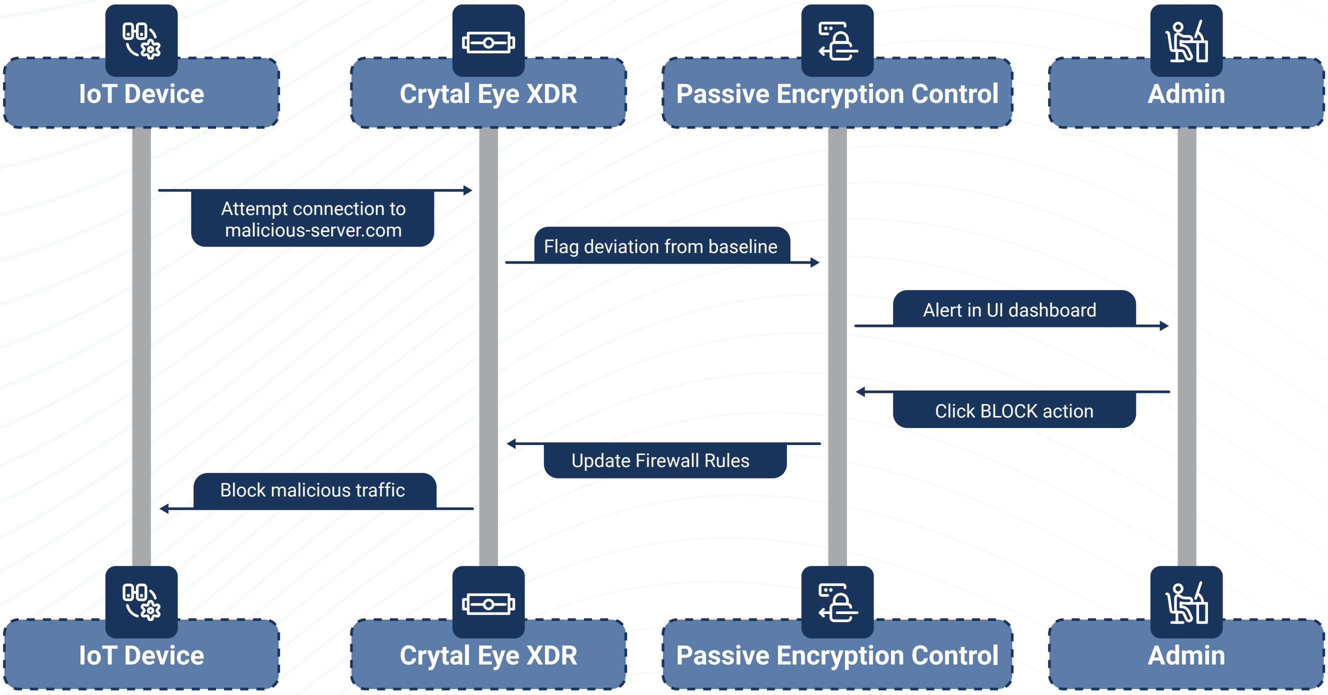
- Passive Encryption Control – Monitors encrypted traffic behaviour
- Advanced NGFW – Segments network, enforces policy, manages zones
- Declarative Authorisation Service (DAS) – Application-layer policy enforcement
- Data Loss Prevention (DLP) – Content-aware inspection, blocks data exfiltration

COMPLIANCE OUTCOMES

- Supports IEC 62443, ISO 27001, and Essential Eight alignment
- Detects unauthorised encrypted flows without deep packet inspection
- Enables policy-based isolation, control and visibility across IoT & OT assets

CRITICAL INFRASTRUCTURE USE CASES

Industry	Threat Vector	Crystal Eye Outcome
Healthcare	IoT device calling external server	PECA blocks connection, logs alert, device quarantined
Mining	ICS sensor exfiltrating data over SSL	Firewall isolates device; PECA terminates abnormal flow
Energy	SCADA RTU accessing rogue domain	Traffic blocked; DAS confirms policy violation; forensic alert triggered



WHY RED PIRANHA?

- Built and supported in Australia with sovereign cyber capabilities
- Designed for full visibility and control of encrypted IoT traffic
- Complements your existing infrastructure with zero friction integration

TAKE ACTION

Ready to secure your IoT, OT and ICS systems with encryption-aware intelligence?

Contact Red Piranha today to arrange a demonstration of Crystal Eye with Passive Encryption Control Application.

Red Piranha
unified threat management

CYBER THREAT ALLIANCE · Australian Government Department of Defence · Australia · Defence Industry Security Program · OISF · CRYSTAL EYE XDR · AUSTRALIAN MADE

NEXT STEPS

1. Get in touch
2. Get a proposal
3. Get started

✉ info@redpiranha.net

☎ +61 8 6365 0450
+61 2 8089 1219

redpiranha.net