CASE STUDY:

Job Centre
AUSTRALIA

Job Centre Australia Limited (JCAL)

Red Piranha

Background

Job Centre Australia Limited (JCAL) is a not-for-profit community-based organisation that has provided employment services to people with disabilities, through State and Federal Government funding for over 27 years. JCAL manages 32 sites across NSW and Queensland, with over 200 staff and servicing a client base of more than 2,500 people living with a disability. JCAL specialises in empowering people with disabilities, illness or health conditions to improve their daily lives and individual circumstances delivered through a range of training, support and employment opportunities.

Challenge

Targeting of the health sector by malicious actors has the potential to interfere with the supply of critical products and services to those in need, cause reputational and financial damage to health organisations, and threaten the wellbeing of patient's daily lives.

The health sector remains a valuable and vulnerable target for malicious cyber activity due to:

- highly sensitive personal data holdings
- carefully designed scams, fraud, and phishing attacks targeting disadvantaged individuals and the carers who support them
- valuable intellectual property on technology and research, such as those relating to COVID19 vaccine research and development
- the criticality of services delivered by the health sector
- pressure on health sector organisations to maintain and, if disrupted, rapidly restore business continuity public trust in health sector organisations, particularly those linked to Government services.

Understanding the extremely pervasive threat of cybercriminals targeting the health industries, JCAL sought to protect their assets and gain a better understanding of any potential corporate network vulnerabilities that may be visible from the internet.

JCAL began an ongoing engagement with Managed Service Provider, DigitalKit, to perform comprehensive reviews of the existing environment where it was determined that the infrastructure of JCAL required vulnerability assessment and penetration testing. This testing was to ensure its IT infrastructure and business applications were secure, and conformed to CIS v7.1 and ACSC ISM standards and to Australian Government regulations for privacy and compliance requirements like the HIRP Act, HPIP Act, Privacy Act and more.

Project Brief

JCAL identified the need for a capable and knowledgeable Managed Service Provider (MSP) to provide day-to-day upkeep for their complex environment. The team sought the assistance of DigitalKit Solutions, who are a trusted and valued partner of Red Piranha. Despite being a partner, DigitalKit conducted a review of multiple cybersecurity firms to provide Vulnerability Assessment and Penetration Testing services, along with their review of multiple technology solutions and selected Red Piranha and the Crystal Eye XDR over other alternatives due to its ability to implement multiple layers of defence that created greater visibility and security awareness across the entire organisation. This also meant that future vulnerability scans could be automatically scheduled and performed from within the network environment, without the requirement of outsourcing the process.

Crystal Eye offered comprehensive reporting and features as part of the built-in GRC controls that meant JCAL and the board could:

- Quickly understand their organisation's security maturity from a centralised platform
- Establish which areas demand immediate improvements
- Keep business-critical documents and information safe by monitoring the activity of all devices accessing the corporate environment via VPN and SD-WAN connections
- Restrict the use of unapproved applications on corporate networks with Application Whitelisting (AWL), one of the Governments 'Essential 8' mitigation strategies
- Respond and remediate for any future attacks against, or breaches of the organisation

Red Piranha being an Australian organisation with the ability to manage and support the deployment from the local Security Operations Centres (SOCs) was also a critical factor in JCAL's decision.

For JCAL, it was also encouraging that Red Piranha's fully integrated Extended Detection and Response security programs are a standard inclusion with the licence subscription, as well as full network, device, and configuration management from the central Orchestrate dashboard. This provides proactive monitoring and response from the highly advanced global threat intelligence coupled with human expertise from the Australian based 24/7 SOC teams.

Technology

- Vulnerability Assessment & Penetration Testing External Testing: (duration 3 months)
- CE Appliances:
  - 4 x Crystal Eye XDR Series 40
  - 2 x Crystal Eye XDR Series 50
  - 3 years Standard License

Deployment

The coordinated approach from DigitalKit and Red Piranha entailed site surveys, technology reviews and detailed reconnaissance of connections to and from the main data centre, to JCAL headquarters, and to remote sites. The critical sites were identified for the centralised solution and Crystal Eye hardware was subsequently deployed to provide the full ecosystem with a secure and stable environment in which to operate.

In order to maintain critical business operations, Red Piranha worked with JCAL to replace existing infrastructure at 4 sites and implement the Crystal Eye XDR hardware with additional back up appliances in High Availability configuration at all sites to provide device and system redundancy.

Due to the complexity of the network, the Red Piranha team were required to integrate a considerable number of configurations, including secure connections via SD-WAN between 25 sites into the closed Data Centre environment, to ensure each of their assets were able to communicate in line with the enhanced security policy.

Solution

JCAL and DigitalKit engaged Red Piranha for a complete Vulnerability Assessment and Penetration Testing service which led to identification and remediation of the gaps and vulnerabilities found.

JCAL deployed the Crystal Eye XDR solution at their sites across Australia giving them full network coverage, visibility, and security across all their branches and remote employees.

Through regular communication between the two companies, JCAL have achieved a higher degree of cybersecurity maturity, are better protected from malicious attacks, and are also poised to immediately detect, respond to, and remediate any future attempts to breach their network.

Red Piranha have also provided to tools and resources necessary for JCAL to build their roadmap towards ISO 27001 and Right Fit For Risk certification, which is a Department of Education Skills and Employment mandate for all providers of employment skills training and disability employment services.

Future

Deploying the Crystal Eye XDR solution has already helped JCAL in achieving heightened security outcomes, and furthermore, can greatly simplify the journey to certification by utilising Red Piranha's integrated security resourcing and service packages. When JCAL are looking to harness the full potential of Red Piranha's capability, we recommend the Electronic Chief Information Security Officer (eCISO) service, which is designed to automate compliance processes through delivery of integrated risk management, active and regular reporting, as well as professional remote consultation which adheres to strict regulatory requirements.