TEC Partnership
Training • Education • Careers

CASE STUDY

Proactively protecting one of England's largest providers of further and higher education

The TEC Partnership is reaping the rewards of the Palo Alto Networks portfolio, delivered as an eXtended Managed Detection and Response (XMDR) service powered by KHIPU Networks' Security Operations Centre (SOC). Around-the-clock, proactive threat protection and response enable this leading provider of further and higher education services to operate continually and with confidence—and at a realistic price.

IN BRIEF

Customer
TEC Partnership

Partner
KHIPU
SECURITY OPERATIONS CENTRE

Organisation Size
Almost 20 sites with more than 10,000 students

Industry
Education

Products and Services
Further and higher education services

Country
Grimsby and surrounding areas, UK

Challenges

Safeguarding the education campus spanning almost 20 sites, with more than 10,000 students, 1,200 staff, and over 3,100 endpoints. Lower the total cost of security operations without compromising the quality of security.

Requirements

- Complete, unified cybersecurity across multicampus remote and hybrid learning environments.
- Consolidate visibility and administration across cloud and on-premises.
- 24/7/365 managed security solution in recognition of budget and resource limitations.
- Foundation for Zero Trust strategy.

Solution

KHIPU Networks' XMDR service as part of SOC. Powered by Palo Alto Networks portfolio including ML-Powered NGFWs, Cortex XDR, Cortex XSOAR, Cortex Data Lake, Threat Prevention, URL Filtering, and GlobalProtect.

CHALLENGE

One of England's largest education providers

The TEC Partnership is one of England's largest providers of further and higher education. It comprises the Grimsby Institute, University Centre Grimsby, Scarborough TEC, East Riding College, Skegness TEC, and The Academy Grimsby.

TEC Partnership is on guard against a rising tide of cyberthreats. According to the 2021 National Cyber Security Centre (NCSC) report[1], a rise in ransomware and other attacks has the potential to inflict serious damage on the UK education sector.

The report reveals that institutions would need a substantial amount of recovery time to reinstate critical services—at significant costs too. It comments, 'In recent incidents affecting the education sector, ransomware has led to the loss of student coursework, financial records, as well as data relating to COVID-19 testing.'

It is against this backdrop that the TEC Partnership is transforming the way it defends against ransomware and other cyberthreats. 'Cybersecurity is our number one priority,' explains Harshad Taylor, Group Executive Director of IT, TEC Partnership. 'It can be difficult to predict how a compromise will begin, as cybercriminals adjust their attack strategy depending on the vulnerabilities they find. However, our aim is to stop threats in their tracks before they impact our institution partners.'

The security challenges are immense. The large-scale campus spans almost 20 sites, more than 10,000 students, 1,200 staff, and over 3,100 endpoints. Moreover, a commonplace bring-your-own-device culture can present difficulties in securing the wider network, particularly with IT staff already facing stretched resources.

[1] *Further targeted ransomware attacks in the UK education sector by cyber criminals*, National Cyber Security Centre, 19 March 2021, https://www.ncsc.gov.uk/files/NCSC-Alert-Further-targeted-ransomware-attacks-education-sector-March-2021.pdf

Ensuring policies are adhered to can also be difficult in large institutions like TEC Partnership with a dynamic user population. And of course, there's the ever-present need to 'do more with less,' squeezing more from finite resources.

TEC Partnership has been a long-term, satisfied user of Palo Alto Networks ML-Powered Next-Generation Firewalls (NGFWs) for several years, using the modern, intelligent platform to provide simple, automated network security. However, the education provider recognized the need to go further—to introduce a complete, proactive approach to security and to do it cost-effectively.

> Covid has brought the security threat into sharp focus. The migration to online platforms and personal devices during remote working exposes the Partnership to a heightened risk and underlines the importance of good cybersecurity practices.
>
> **– Harshad Taylor, Group Executive Director of IT, TEC Partnership**

REQUIREMENTS

Cost of prevention less than cost of recovery

The cybersecurity strategy not only needed to protect sensitive data—but also reduce downstream costs. The requirements included:

- Introduce complete, unified cybersecurity across multicampus, remote, and remote and hybrid learning environments.
- Consolidate visibility and administration across both cloud and on-premises.
- Consider a 24/7/365 managed security solution in recognition of budget and resource limitations.
- Move closer to a Zero Trust strategy providing only the necessary level of access privileges.

SOLUTION

Cross-campus monitoring, detection, and response

Taylor was introduced to the KHIPU Networks eXtended Managed Detection and Response (XMDR) service at a security event. He liked what he saw. 'We chose KHIPU owing to their experience within the education sector and ability to monitor, detect, and respond to threats across our entire multicampus estate—not just the endpoint,' he says.

The KHIPU XMDR service comprises a comprehensive, connected Palo Alto Networks portfolio, as ML-Powered NGFWs are embedded within the KHIPU XMDR service to deliver intelligent and proactive network security. Simple to configure and easy to use, they can inspect a file while it's being downloaded and block it instantly if it is malicious without having to access offline tools. This way, the time from visibility to prevention is near zero.

The NGFWs also incorporate Palo Alto Networks Cloud-Delivered Security Services (CDSS):

- **Threat Prevention:** Provides TEC Partnership with comprehensive prevention of known exploits, malware, command and control, and custom rules.
- **URL Filtering:** Prevents access to known and new malicious websites before they can be accessed by users.
- **GlobalProtect™:** Protects the hybrid education staff and students by understanding application use and associating traffic with users and devices.

Cortex® XDR™ is the backbone of endpoint protection, collecting data from more than 3,100 endpoints, the network, cloud, and third-party data resources for extended and comprehensive visibility. Next-generation antivirus blocks malware, ransomware, exploits, and fileless attacks. And as part of the XMDR service, KHIPU can pinpoint attacks with AI-driven analytics and coordinate response.

Cortex XSOAR automates security workflows in the SOC for a more agile response to alerts. And Cortex Data Lake runs AI and ML to continually learn from new data sources to evolve the Partnership's defense.

> Together, Palo Alto Networks and KHIPU give us a holistic approach to threat detection, response, and prevention. The complete solution moves beyond protection for specific areas like servers, PCs, and other endpoints. It extends across the entire network, endpoint estate, third-party and cloud environment. And that security is continually watching for vulnerabilities 24/7/365.
>
> **– Harshad Taylor, Group Executive Director of IT, TEC Partnership**

BENEFITS

Jointly, Palo Alto Networks and KHIPU XMDR are delivering value across multiple dimensions:

One complete, universal view of threat intelligence

TEC Partnership has unified visibility into every type of threat and incident response. If a user who was previously disabled from the system suddenly tries to authenticate against Active Directory®, for instance, or a user downloads game cheats, TEC Partnership is immediately notified as part of the XMDR service with appropriate action being taken.

Out-of-hours and in-hours coverage

24/7/365 managed detection and response ensure first- and second-line SOC response teams are on hand to monitor and respond to incidents both out of hours and in hours. Automated playbooks (through XSOAR) ensure KHIPU's SOC teams instantly investigate high-level/severe alerts, meeting agreed SLAs.

Instant threat response

The proactive threat intelligence ensures TEC Partnership is always one step ahead of threats. Taylor was contacted recently, for example, by a senior Partnership executive concerned they had clicked on a bogus link. The KHIPU SOC team was immediately alerted and investigated the incident, remotely checked the executive's device, and confirmed there were no incidents reported on the system. Prior to the SOC, a person would have had to physically visit the laptop to perform a manual security check.

Reducing the cost of education security

Taylor estimates that the XMDR service delivers a return on investment every year, with the SOC and process automation minimising human interaction. He explains, 'The XMDR service frees up person-hours to the equivalent of one FTE every year. This allows TEC Partnership to use on-site employees when absolutely needed and for confirmed security incidents, freeing them up for other projects.'

Continually learning, always improving

At the start of the curriculum year, approximately 13,000 alerts were received in the SOC. As the AI- and ML-driven insights learned about user profiles, incidents reduced by 30% on average.

Timely, accurate SOC MDR reporting is also used for strategic planning. Network traffic data, for example, can be used to raise concerns that need to be escalated, such as identifying users sending particularly large email attachments.

Simple and intuitive

TEC Partnership is impressed by the ease of use of the portfolio. Taylor added, 'The dashboards are very slick. We have a snapshot of everything we need on the first landing page. We can see any incidents, the sources, and their severity. All of the insights—including those from the firewalls—are there in one simple screen.'

Community-driven insights

Members of the KHIPU XMDR community are automatically and dynamically alerted to the security intelligence generated in the SOC from the TEC Partnership environment, strengthening sector-wide protection.

He closes by acknowledging the value provided by KHIPU. 'The KHIPU team are legends. Nine times out of ten, they immediately answer whatever question we put to them. Their security knowledge, professionalism, and attention to our needs are second to none.'

> “With the growth in ransomware attacks across the education sector, this XMDR solution prevents advanced attacks. It reduces risk, enables our people to work with confidence, and as a managed service, it frees up our staff to focus on strategic tasks.
>
> **–Harshad Taylor, Group Executive Director of IT, TEC Partnership**

Learn more about how KHIPU Networks provides their XMDR service using Palo Alto Networks. Discover the power of industry-leading NGFWs and Cortex on the Palo Alto Networks website.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com