CASE STUDY

Implementing a world-class SOC at the University of Derby

The University of Derby has standardised on a proven Palo Alto Networks security solution, delivered as part of an eXtended Managed Detection and Response (XMDR) service powered by KHIPU Networks Security Operations Centre (SOC). The institution is benefiting from AI-powered security and behavioural analytics with dedicated cybersecurity experts available 24/7/365. All of this is also being achieved at "one-third the cost" of other vendor solutions, according to the customer.

IN BRIEF

Customer

The University of Derby

Partner

KHIPU | SECURITY OPERATIONS CENTRE

Industry

Higher Education

Organisation Size

34,000 students studying in full-time, part-time, online and on-campus.

Location

Derby, United Kingdom

Challenges

The university faced a widening attack surface and an audit that had identified vulnerable threat vectors for endpoint and network security improvements. The institution required a smart, powerful, and proactive way to protect its infrastructure, including 7,500 endpoints, with fewer resources.

Requirements

+ Cost-effectively safeguard the university's critical infrastructure against continual cyberthreats.
+ Enable students, staff, researchers, and other stakeholders to work securely without interruption.
+ Continuously adapt to rapidly changing threats and outpace adversaries.

Solution

The University of Derby increases cybersecurity visibility and lowers cost of ownership to secure the university's researchers and scientists, some of the most highly cited in the world. They use KHIPU Networks eXtended Managed Detection and Response (XMDR) service built upon Palo Alto Networks Cortex XDR, Cortex XSOAR, Cortex Data Lake, and WildFire.

CHALLENGES

Higher education institute of the year

The University of Derby provides industry-relevant, expert teaching, from undergraduate degrees to postgraduate study and research. The university's academics were recently ranked among the most highly cited scientists in the world by Stanford University, and the university was 'Higher Education Institution of the Year' at the 2020 NEON Awards.

The university and the wider UK higher education community are at a tipping point. According to the Jisc cyber impact report,[1] it is no longer a case of 'if' a security incident will hit institutions—it's 'when'. Jisc's computer security incident response team (Janet Network CSIRT), for example, is recording up to 6,000 incidents every year, including more than 1,000 denial-of-service attacks on the Janet network, targeting 236 members.

Higher education institutions are struggling to keep up, Jisc reveals. IT staff are being diverted from everyday tasks to resolve data breaches, and incident recovery costs are spiralling. Another Jisc finding[2] is that "recovery is challenging, time consuming and expensive." A lengthy rebuild of a digital estate could easily consume several million pounds, according to Jisc.

The University of Derby is not standing still. Following a recent security audit that identified shortcomings in security, including endpoints and areas of the network, the institution is taking decisive action to reimagine and bolster its cybersecurity ecosystem.

[1] *Cyber impact*, Jisc, 9 November 2020, https://www.jisc.ac.uk/reports/cyber-impact.

[2] Henry Hughes, "Ransomware: what's the impact and how can we stop it?" Jisc, 2 July 2021, https://www.jisc.ac.uk/blog/ransomware-whats-the-impact-and-how-can-we-stop-it-02-jul-2021.

> The breadth of study here is remarkable. We have people conducting aquariums analysis, medical research, links with internationally recognised manufacturers, and we own Derby Theatre. Thousands of unique devices are attached to the network, sometimes using vast volumes of data—right across the world. It’s our job to prevent successful cyberattacks while maintaining academic freedom.

–James Eaglesfield, Head of IT Governance and Portfolio, University of Derby

REQUIREMENTS

Protection against widening attack objectives

Striving to protect its endpoints, infrastructure, and cloud environment, the university’s requirements and objectives included:

- Cost-effectively protecting mission-critical servers and devices against increasing attack objectives, including scamming individuals for money, accessing systems to defraud payroll, ransom payments, and stealing research intellectual property.
- Enabling students, staff, researchers, and other stakeholders to work securely without interruption.
- Continuously adapting to rapidly changing threats and outpacing adversaries.

SOLUTION

AI-Based continuous security delivered by a 24/7/365 SOC

Working in partnership with its technology partner KHIPU Networks, the university has implemented the Palo Alto Networks Cortex® XDR™ platform, incorporated within KHIPU’s XMDR service. The service includes 24/7/365 access to KHIPU’s comprehensive security operations center (SOC).

The SOC alerts the university to incidents, analyses the root cause, mitigates attacks, and works with the university to continuously improve operations and stay in front of threats. Eaglesfield comments, “The implementation was remarkably quick, owing to the collaborative skills and professionalism of the Palo Alto Networks and KHIPU teams. We went live in just four months, working as one to achieve an on-time, on-budget deployment.”

The university has subsequently added 15 terabytes of Cortex Data Lake to collect, integrate, and normalise network traffic, including the firewall logs. Cortex XDR runs AI and machine learning to protect data, continually learning from new data sources to evolve the university’s defence. Integration with Palo Alto Networks WildFire® adds close inspection of unknown files, with intelligence automatically shared across the endpoints.

Eaglesfield says: “If the KHIPU SOC identifies a threat, we can cross-check it to ensure everything is working as it should. One of the key benefits of KHIPU’s service is that it doesn’t just collect logs and alert us; it protects against cyberthreats with a team of cybersecurity experts available to us 24/7/365.”

Recently, for example, Cortex XDR's behaviour analytics alerted the SOC to a university endpoint transferring excessive data to an external site. The destination was not a popular upload site for endpoints, and the endpoint had not previously downloaded a large amount of data from the site. Automated investigation and mitigation identified the transfer not as malicious data exfiltration but as legitimate cross-border sharing of large volumes of research data. Given that the university's resources are not available 24/7/365, it is very important to have visibility over activity of this sort.

> The XMDR service gives us the granular visibility we've never had before. We can't be certain what comes in through an endpoint. Cortex XDR, as part of the KHIPU XMDR, ensures the university has a trusted endpoint and network protection strategy proven to identify, stop, and prevent attacks.
>
> **–James Eaglesfield, Head of IT Governance and Portfolio, University of Derby**

BENEFITS

Continuous, 360-degree visibility

The university benefits from advanced, 360-degree cyber defence across its infrastructure, proactively identifying and blocking malware, ransomware, file, and file-less attacks. Indeed, during the first two months of operation, Cortex XDR generated more than 220 incidents (10 high severity and 65 medium severity). More than 95% of all alerts were generated by the Cortex analytics component of the SOC service. All alerts are analysed and investigated by the KHIPU SOC before the university is alerted. This ensures the university isn't overwhelmed by false-positive and low-fidelity alerts and extraneous information.

Low total cost of ownership

When the university issued this tender, it received proposals more than three times the cost of the Palo Alto Networks and KHIPU outcome. For a relatively small investment, the university benefits from world-class protection across its infrastructure, a 24/7/365 SOC which is fully staffed and available, incident response, and a service that continually improves. The pre-built XMDR model also frees up investments with a predictable opex model. "We are achieving all this for the equivalent cost of two FTE security staff. The KHIPU SOC team is effectively an extension of my team," says Eaglesfield.

Deployed rapidly and with minimal risk

By standardising on the KHIPU SOC, the university benefits from a proven, pre-packaged 24/7/365 SOC. The implementation was completed within four months, with more than 400 incidents identified and resolved within the first two months of operation.

Always learning, always improving

The solution enables continual improvement of the university's security posture, including coordinated prevention from zero-day attacks. If suspected malware is deemed malicious, for example, new protection is automatically distributed to all endpoint agents and other areas being protected, such as the firewall environment.

The KHIPU SOC also monitors other higher and further educational environments, using a ‘community-wide rapid response’ approach to share new security insights across the sector and reinforce collective protection. The more institutions that join the community, the better protected the education sector will become.

Delivers closed-loop prevention, detection, and response

Behavioural analytics and a single, connected view of security enable the university to quickly find hidden threats. Incident scoring allows the university to focus on the threats that matter and conduct internal investigations, even if endpoints are not connected to the network.

“The Palo Alto Networks and KHIPU XMDR service gets better as every day passes. It’s a great relationship and one that establishes a firm security footing for the future. The service enables us to meet our strategy of delivering a world-class SOC designed for our university and the sector,” Eaglesfield concludes.

Discover for yourself the power of Cortex and read how KHIPU Networks provides their XMDR service using Palo Alto Networks.

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