UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

Wits University protects 41,000 students with modern, AI-based security operations

RESULTS

Continuous learning

Supports continuous and uninterrupted learning experience

Reduced alerts

Volume of alerts has dramatically reduced

24/7/365

Advanced cyber defence proactively identifying and blocking malware, ransomware, and file-based and fileless attacks

paloalto NETWORKS

The University of the Witwatersrand in South Africa is using a modern, AI-driven security operations strategy from Palo Alto Networks to stop threats in their tracks –wherever they might attack. A holistic, integrated Cortex XDR and XSOAR platform delivers extended protection, detection, and response across the University's entire attack chain through attack surface reduction, attack prevention, breach prevention, and response.

Threat actors are watching the University of the Witwatersrand's ('Wits') cybersecurity like hawks. Cybercriminals are continually trolling higher education providers such as Wits, and hacktivists never stop trying to exploit weaknesses to target identity-based data.

The attack surface is vast: 41,000 students across five faculties, 30+ service departments, and more than 3,000 courses. Prior to the Palo Alto Networks partnership, alert noise was high, and Wits' security team struggled to monitor and respond to every threat.

A modern Palo Alto Networks security operations platform, managed by KHIPU Networks, drives continuous and uninterrupted learning and research. Integrated Cortex XDR and XSOAR pinpoint threats in the early phases of the cybersecurity lifecycle, detect anomalies indicative of an attack, and automatically route remediation activities. By protecting the integrity of Wits' network, Palo Alto Networks is mitigating risk, improving the student and staff experience, and ensuring data privacy.

IN BRIEF

Customer

University of the Witwatersrand

Industry

Higher Education

Country

South Africa

Organisation Size

47,000 students and staff across five faculties and 3,000+ courses

Web

www.wits.ac.za

Partner

KHIPU CYBER SECURITY

Challenges

+ Sophisticated, multistage threats and exposures are increasing rapidly in higher education. Existing endpoint security tools surfaced a mass of alerts, which was overwhelming for the SecOps team to manage.

Solution

Palo Alto Networks® AI-Driven Security Operations Platform including:

+ Cortex XDR®
+ Cortex XSOAR®

Results

+ Supports continuous and uninterrupted learning experience.
+ Eliminates zero-day malware, ransomware, and fileless attacks.
+ Frees SecOps staff to concentrate on strategic, value-add tasks.
+ Reduces the volume of alerts dramatically.
+ Discovers and investigates threats faster.

CHALLENGE

Balancing students, processes, and tools

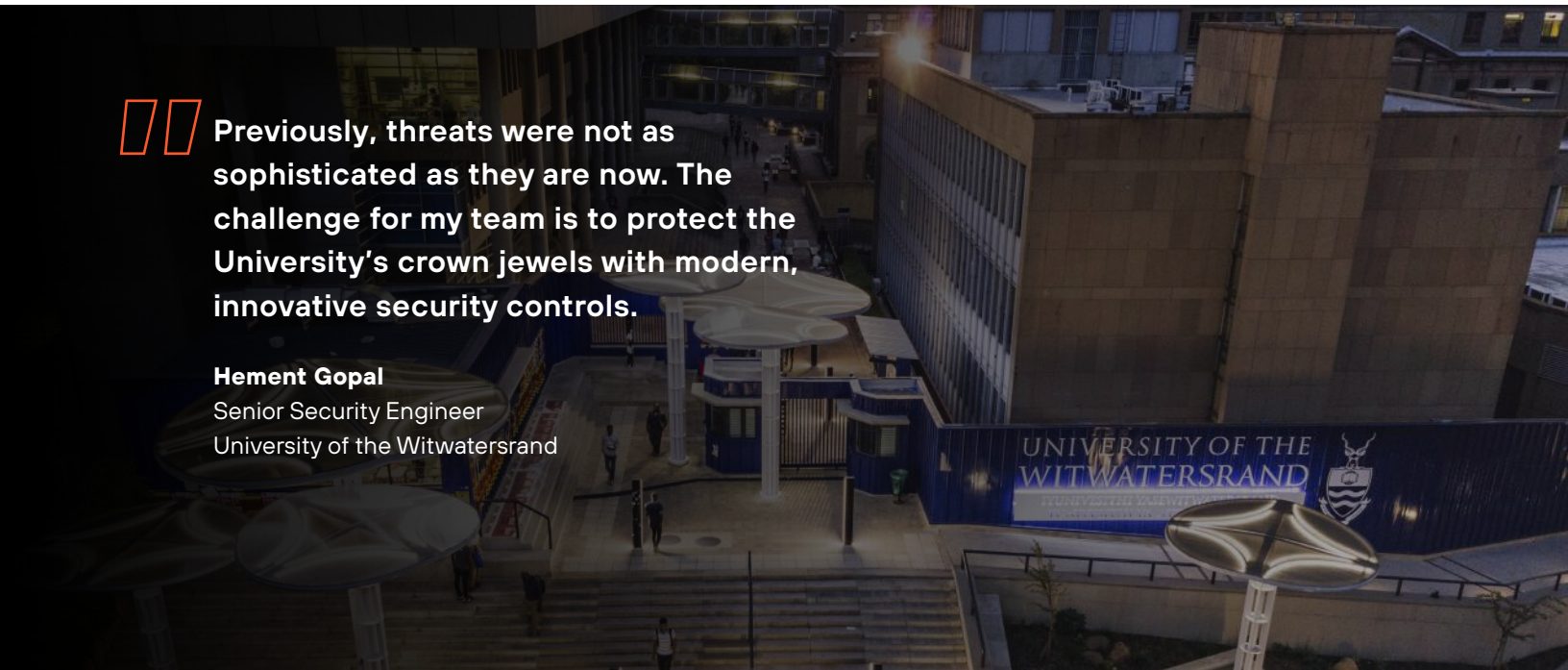
Wits is a multicampus South African university located in Johannesburg. It is internationally acclaimed for its research, high academic standards, and commitment to social justice. The University is home to 41,000 students; almost 1,700 academics; and 6,000 employees.

Just like any education institution, Wits is at daily risk from cyberattacks. Vast volumes of sensitive research and academic data, students connecting from a multiplicity of devices, and the evolving threat landscape make it a prime target for threat actors. Open access to resources needs to be balanced against the need to safeguard data.

Funding and resources compound these challenges. Hement Gopal, Senior Security Engineer at Wits, explains: "Previously, threats were not as sophisticated as they are now. The challenge for my team is to protect the University's crown jewels with modern, innovative security controls."

Prior to engaging with Palo Alto Networks and its leading cybersecurity partner KHIPU Networks, Wits' endpoint security was based on a basic SIEM monitoring tool. "We still had many alerts," says Hement. "Without automation, our security team was almost overwhelmed responding to them."

In response, Wits turned to KHIPU Networks' managed detection and response SOC service. Hement explains: "Higher education needs are very diverse compared to the more controlled private sector. KHIPU Networks has specialist knowledge of the demanding security pressures facing higher education. Security insights are also shared across the KHIPU community, reinforcing collective protection."



> **Previously, threats were not as sophisticated as they are now. The challenge for my team is to protect the University's crown jewels with modern, innovative security controls.**

Hement Gopal
Senior Security Engineer
University of the Witwatersrand

SOLUTION

Complete picture of each incident

Wits chose Palo Alto Networks Cortex XDR to underpin its security operations. The modern extended detection and response (XDR) platform protects 300+ servers across the University's estate. Application-based behavioural analytics pinpoints evasive threats, and machine learning profiles the behaviour to detect anomalies indicative of attack.

Cortex XDR ingests data from multiple University and external sources, including antivirus software, the firewalls, Cisco IPS, and mail gateways. Hement elaborates: "Cortex stitches separate data, alerts, and insights together, giving us a single, consolidated root cause view of incidents and user behaviour."

300+

Cortex XDR is protecting 300+ servers across the university's estate

The alerts are fed into the KHIPU Networks' SOC for investigation and follow-up. "The out of hours cyberthreat monitoring doesn't just alert, it protects against and prevents threats impacting the University's operations," says Hement.

The SOC includes Cortex XSOAR to orchestrate incident detection, investigation, and remediation. Playbooks automate routine alert management, route tickets, and support the escalation of more serious risks.

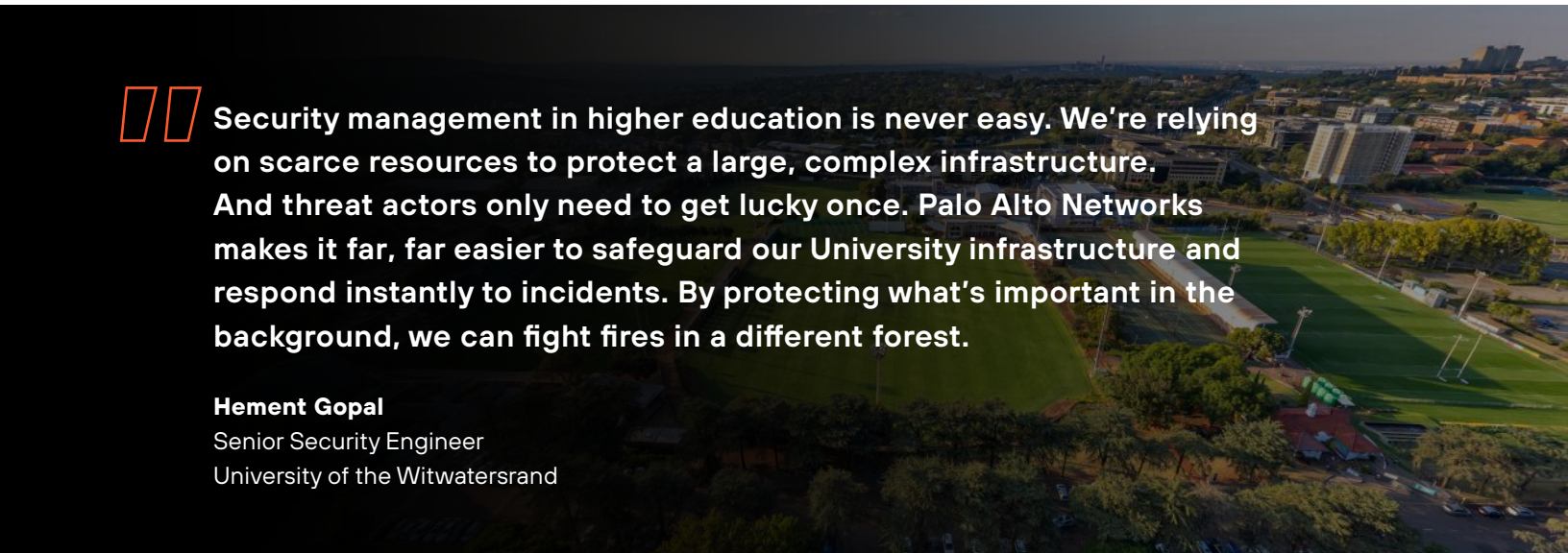
"We receive automated emails with a comprehensive snapshot of an incident," explains Hement. "It includes everything we need to act. Together, Cortex XDR and XSOAR give us eyes across the entire University estate in one standalone solution."

RESULTS

Trusted endpoint security reduces risk

Wits' security-first approach delivers holistic protection across the network, clouds, endpoints, and applications. The benefits include that it:

+ **Underpins continuous, uninterrupted learning:** 41,000 students and 6,000 higher education staff can teach, learn, and administrate anytime and anywhere, confident that data and devices are securely protected from threats.
+ **Eliminates zero-day malware, ransomware, and fileless attacks:** The behaviour-based platform – with KHIPU Networks' SOC – provides 24/7/365 advanced cyber defence across Wits' servers, proactively identifying and blocking malware, ransomware, and file-based and fileless attacks.
+ **Enables the University to do more with less:** With resources already squeezed, the Cortex platform automates many routine tasks, liberating security staff to concentrate on strategic, value-added tasks.
+ **Reduces volume of alerts:** According to Hement, "With the original SIEM tool, we gave up counting how many alerts were coming in – there was so much noise. Using Cortex, we are seeing just a fraction of these alerts. The vast majority are managed silently in the background."
+ **Delivers trusted security:** The University recently engaged with a forensics business partner to examine an incident in parallel with an examination by KHIPU Networks' SOC team. Both parties reported similar outcomes, validating the reliability of the strategy.
+ **Discovers and investigates threats faster:** Cortex XDR proactively blocks attacks and collects rich endpoint data across all data sources. Unified interface facilitates management of alerts and incidents for detection and response as well as Cortex XDR policies.



> **Security management in higher education is never easy. We're relying on scarce resources to protect a large, complex infrastructure. And threat actors only need to get lucky once. Palo Alto Networks makes it far, far easier to safeguard our University infrastructure and respond instantly to incidents. By protecting what's important in the background, we can fight fires in a different forest.**

Hement Gopal
Senior Security Engineer
University of the Witwatersrand

© 2024 Palo Alto Networks, Inc. Palo Alto Networks and the Palo Alto Networks logo are registered trademarks of Palo Alto Networks, Inc.