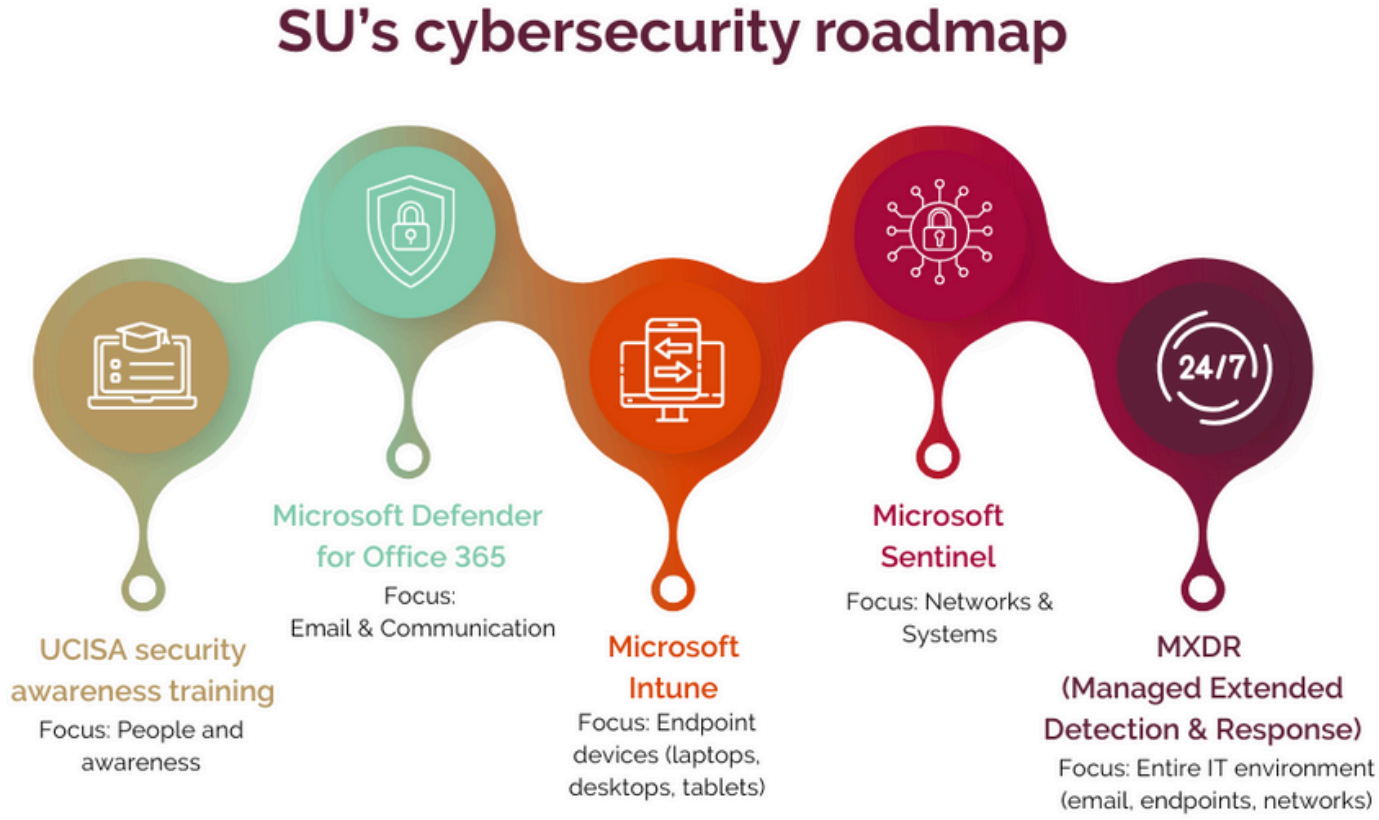
Stellenbosch UNIVERSITY IYUNIVESITHI UNIVERSITEIT

SU Information Technology
ICandelo lezobuChwepheshe laseSU
US Informasietegnologie

Protecting SU – Enhancing the cybersecurity landscape

At Stellenbosch University (SU), keeping our campus community, data and resources safe is a top priority for the IT Division. Over the past few years, we have been building stronger layers of security to protect you and the University from the growing threats in the digital world. From cybersecurity awareness training to advanced threat protection, secure device management and real-time monitoring, each step has been part of a broader effort to strengthen the protection of our information and communication landscape. This timeline reflects our commitment to enhancing the cybersecurity landscape at SU without disrupting the daily work of SU staff and students or invading their privacy.



This simplified overview illustrates how the various tools in SU's cybersecurity strategy work together to protect people, devices, communication and systems. Please note: this is a high-level representation intended for general understanding and does not reflect all technical functions or integrations.

Building cybersecurity awareness with UCISA training

As part of our ongoing efforts to protect SU from cyber threats, the UCISA Information Security Awareness training for staff and students was introduced. UCISA (Universities and Colleges Information Systems Association) is a UK-based organisation that develops cybersecurity training tailored for higher education institutions. The course covers essential topics such as an introduction to cybersecurity, recognising phishing and scams, safe information management, password and access control, protecting devices and responsible use of privileged access. This training complements our technical defences by building human awareness.

If you have not already completed the training, we encourage you to do so – it is quick, informative and helps keep the University safer. You will find it on SUNLearn under My courses via this link: https://learn.sun.ac.za/course/view.php?id=32398

Stopping threats before they reach your inbox with Defender

We also began addressing the most common way threats reach us - through email. By introducing advanced anti-spam, anti-malware and anti-phishing measures, we significantly reduced the number of malicious messages reaching inboxes. Some of the most powerful protections were made possible through Microsoft Defender for Office 365, which allows us to apply enhanced anti-phishing policies that go beyond standard email filtering.

Managing and protecting SU devices with Microsoft Intune

Next, we rolled out Microsoft Intune, a cloud-based endpoint management solution that securely manages University-owned identities, apps and devices such as laptops, desktops and tablets. It ensures that only trusted, compliant devices can access tools like Outlook and OneDrive. Intune plays a key role in strengthening cybersecurity without disrupting daily digital activities. Nearly 7200 university-owned devices are managed and protected with Microsoft Intune, reducing risks from outdated software and unsecure devices.

Ongoing protection with Sentinel

Microsoft Sentinel was deployed for continuous monitoring of SU's networks and systems. Sentinel helps the IT team respond to thousands of security alerts every month, ensuring threats are detected and contained quickly to protect our campus. Just in April and May alone this year, almost 12 000 incidents were reported.

Continuous security with MXDR

We have recently advanced our security measures with the implementation of Managed Extended Detection and Response (MXDR). MXDR is a proactive cybersecurity service that helps detect, investigate and respond to potential threats across our IT systems. Furthermore, advanced technology experts monitor to identify and stop cyber threats before they can cause harm to protect your data and the University's information systems. If malware, ransomware or other suspicious activity are detected, MXDR acts to limit impact and protect our systems and data.

What MXDR does:

- Monitor for signs of cyber threats
- Detect, analyse and contain attacks before the user is aware or system is impacted
- Helps to maintain a safe and secure digital environment for all
- Minimise the downtime and data loss if a cyber-attack takes place

What MXDR does not do:

- Access personal communication or content
- Collect or share personal information beyond what is necessary as a security measure
- Monitor privately owned devices (except where explicit permission was provided by the user for SU IT to onboard the device)

The IT Division will continue to share more updates on developments as we continue to protect SU's digital landscape.

Article published in July 2025