PRESIDIO® | CASE STUDY

Munster Technology University Cork

CYBERSECURITY

Secure your organisation & defend from cyber attacks.

MTU Ollscoil Teicneolaíochta na Mumhan Munster Technological University

Many IT departments are challenged by the shortage of skilled security personnel and restricted budgets. And yet, they must still comply with data protection regulations, have full visibility of security posture, rapidly identify threats and respond to thwart these threats.

Overview

Munster Technology University Cork, (formerly Cork Insitute of Technology), partnering with Presidio, deployed Presidio's Managed Security Service platform. It combines Presidio's Managed Security Operations Centre and the toolset powered by IBM QRadar's market-leading technology. This offers the optimum combination of people, process and technology.

Presidio won the tender for MTU's Security Information & Event Management (SIEM) solution with 24/7 Security Operations Centre (SOC) coverage, including solution deployment and configuration and response to high priority alerts.

Now all HEAnet member companies can purchase from this tender - saving time and money. For MTU this service is "less than the cost of one security engineer."

The Challenge

After two non-malicious but important security incidents, MTU needed to upgrade all security systems.

One of the incidents was simply to do with publicly available timetables where a student accessed other student's timetables. But it highlighted a security hole in MTU's security layer which meant the Data Commissioner had to be informed. As a result, MTU had to undertake penetration tests on all systems.

Jonathan McCarthy, Head of ICT at MTU, carried out research to find out how best to secure the organisation. He asked companies in both private and public sector what they felt the best system would be. He was told "in no uncertain terms" that SIEM was what they needed.

The Solution

Jonathan investigated recruiting a cybersecurity expert to run their own SIEM. But he soon realised that it would be hard to recruit and retain this position when there is a shortage of qualified people in the country.

He shopped around for a managed SOC/SIEM service and "Presidio came out on top". MTU purchased Presidio's Managed Security service based on IBM QRadar technology.

Delivered by Presidio's Managed Security services team, analysts focus on the events that matter and act swiftly to defend against them. The service accurately detects and prioritises threats to MTU's IT infrastructure.

What does the SOC/SIEM Service do?

- Central point for monitoring, synthesising and acting on threats
- Prepares for and responds to cyber threats, preventing them from impacting the business
- Provides cyber risk and compliance reporting
- Ensures that groups managing critical infrastructure components are aware of potential threats to enable quick remediation of risks

The Result

The Managed Security service handles at least 1,500 events per second and 50,000 flows per minute. In MTU Cork, it takes just over 6 minutes to process 1 million transactions – no human can deal with that level of activity.

Presidio's Managed Security services offers on-premises, private or hybrid cloud solutions, powered by IBM QRadar

- ✔ detects and responds to threats in real time, keeping data secure
- ✔ increases resilience by learning about the changing threats
- ✔ derives user behaviour intelligence in order to prioritise the deployment of technologies
- ✔ identifies and addresses negligent or criminal behaviour
- ✔ detects risky user behavioural anomalies that could be indicators of insider threat