SECURE YOUR ORGANISATION

Trust Arkphire to defend your organisation from cyber attacks

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.

So how do you overcome these restrictions?

Cork Insitute of Technology (CIT), partnering with Arkphire, deployed Arkphire's Managed Security Service platform. It combines Arkphire'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.

Arkphire won the tender for CIT'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 CIT, this service is "*less than the cost of one security engineer*."

(Tender details: CIT Cyber Security Managed Services RFT2017/01213/10407)

Key Features

- Powered by IBM QRadar
- 24x7 security event, log monitoring and analysis
- Real-time security event response to known and emerging threats
- Collect and parse logs from 450+ device types
- Agent and agentless collection options available
- IBM X-Force Threat Intelligence feeds

Arkphire's Managed Security Service

Arkphire's Managed Security service offers on-premises, private or hybrid cloud solutions and is powered by IBM QRadar's market-leading security intelligence technology. It also:

- 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 shape and prioritise the deployment of technologies
- finds weaknesses before they are exploited
- identifies and addresses negligent or criminal behaviour
- detects risky user behavioural anomalies that could be indicators of insider threat or fraud

CIT Case Study

After two non-malicious but important security incidents, Cork Institute of Technology needed to upgrade all security systems.

CORK INSTITUTE OF TECHNOLOGY
INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

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 CIT's security layer which meant the Data Commissioner had to be informed. As a result, CIT had to undertake penetration tests on all systems.

Jonathan McCarthy, Head of ICT at Cork IT, 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.

To DIY or not to DIY

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 "Arkphire came out on top". CIT purchased Arkphire's Managed Security service based on IBM QRadar technology.

Delivered by Arkphire'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 CIT's IT infrastructure. Jonathan McCarthy says in his presentation at HEAnet 2018 that Cork IT's SOC/SIEM solution is "less than the cost of one security engineer."

WHY DID CIT NEED SIEM?

- Wanted to be secure in the knowledge that data is fully protected
- Wished to prevent cyber threats impacting the business
- Hackers are getting younger and hacking is getting easier!

WHAT DOES SIEM DO FOR CIT?

- Figures out normal behaviour
- Follows an incident management process when abnormal behaviour is detected
- Provides a Red, Amber, Green alert process to tell CIT what happens and when

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

Result

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