INDUSTRIAL STRATEGY

UK Research and Innovation

Orpheus Cyber

With funding from the Industrial Strategy Challenge Fund, Orpheus Cyber has developed machine learning which can predict cyber risks with impressive accuracy, helping safeguard companies from attack whether their employees are working from home or the office.

A cyber threat intelligence company that received £140,000 from UK Research and Innovation (UKRI) through the Industrial Strategy Challenge Fund's Next Generation Services challenge to further develop its machine learning capabilities can now predict specific cyber risks to clients with over 90% accuracy.

Orpheus Cyber has more than doubled its revenue each year since being founded in 2016 and provides cyber security for organisations in the public and private sectors. Its technologies help the NHS to protect its supply chain and the company is one of a handful to be accredited by both the Financial Conduct Authority and the Bank of England to deliver cyber resilience testing to critical infrastructure organisations.

Less than three months after the company completed its project under the Next Generation Services challenge, the COVID-19 pandemic arrived, prompting a rush to remote working across the public and private sector.

This resulted in a significant increase in opportunities for hackers to break into companies. The remote access technologies many organisations put in place so that staff could reach critical systems and information were poorly secured and opened up new weaknesses.

The holes in companies' defences are often due to the many thousands of common vulnerabilities and exposures (CVEs) discovered in software every year. These are ripe for exploitation unless patched or remediated, but the problem is knowing which ones to prioritise as it is impossible to focus on them all.

CEO and founder Oliver Church said: "In addition to using threat intelligence to know which attack methods are already being exploited by hackers, so that those can be prevented, organisations also need to understand which vulnerabilities will be exploited in the near future. That means they can move faster than the adversaries they face and stop cyber risks before they happen.

"What we've developed, in part through our involvement with UKRI, is machine learning which will predict with 90% accuracy which CVEs will be exploited by hackers in the future"

Orpheus Cyber has also benefited from Innovate UK's Innovation Continuity Loan, allowing the company to enhance its existing capabilities and combine them into a full-spectrum, cyber risk management platform.

Orpheus Cyber's approach is sophisticated. Its machine learning algorithms learn from large datasets taken from the dark web, criminal forums and marketplaces, and hacker chatrooms to find references to vulnerabilities and other attack methods being discussed by criminals. It also looks at a variety of other features to assess the risk of a vulnerability being exploited and its attractiveness to hackers.

Extensive testing, including using its machine learning to risk-score historic vulnerabilities and then cross-referencing its predictions against those that were eventually used by adversaries, showed it could deliver a 90% match. This predictive percentage is improving as the system gets better.

Oliver added: "We look at an organisation from a hacker's perspective. By providing clients with a detailed understanding of both their 'attack surface' and the threats they face depending on their individual characteristics as an organisation, they can act to prioritise their defences on what really matters to them."