



ORPHEUS



CASE STUDY

NHS Blood & Transplant

External Attack Surface Management,
Risk-Based Vulnerability Management,
and Third-Party Risk Management

NHS

Blood and Transplant

Summary

NHS Blood and Transplant (NHS BT) operates as a distinct health authority within the NHS, tasked with ensuring the dependable and efficient provision of blood, organs, tissues, and related services to support the healthcare system.

NHS BT faced the challenge of justifying increased cybersecurity investment and demonstrating its value, especially with public funds. Orpheus provided solutions through External Attack Surface Management (EASM) and Third-Party Risk Management (TPRM). EASM introduced a Cyber Risk Score to assess and manage threats and vulnerabilities, making it accessible to non-cybersecurity executives.

It also extended this scoring to third-party organisations, enhancing security posture. Orpheus assisted in prioritising vulnerabilities through Risk-Based Vulnerability Management (RBVM), streamlining patching efforts.

The Orpheus platform's threat intelligence-driven approach ensured adaptability to evolving threats, and its vulnerability prediction capability proved highly accurate. This collaboration strengthened NHS BT's cybersecurity strategy and operational resilience, and was recognised at the Cyber Associates Network awards.

About Orpheus Cyber

Orpheus is a highly accredited cyber threat intelligence company, including by the Financial Conduct Authority and the Bank of England. Our powerful and award-winning technologies collect huge volumes of cyber risk data, which we analyse using Machine Learning and our skilled team to enable you to protect your organisation and your supply chain.



Client Issue

The Problem

NHS BT was grappling with an issue common to all cybersecurity teams - the need for continued, and increased investment in their cybersecurity programmes but with no reliable way to demonstrate a return on investment. While this issue is not unique to NHS organisations, the need to demonstrate that money is being well spent is even more important when it's public money.

There are few good solutions to this problem; it is hard to prove that an attack did not take place because of the actions of the cybersecurity team. Perhaps an attack, thankfully, does not happen, or if an organisation believes its actions and defences prevented or stopped an attack, this itself requires spending money to analyse and prove.

An attack on the UK's critical national infrastructure (CNI), including the NHS does not just have financial ramifications but can also cause the loss of life. An attack on the University Hospital of Dusseldorf resulted in the death of a patient, and the 2017 WannaCry ransomware attack affected various parts of the NHS resulting in thousands of cancelled appointments and treatment delays.

This need to prove a return on investment was coupled with a growing understanding of the risks posed by third-party organisations to NHSBT. Supply chain attacks have been growing in number and severity over recent years with multiple examples of the losses they cause. A future attack on the scale of WannaCry could easily spread between NHS trusts. Should a supplier suffer an attack that halted their operations, NHS BT may also not be able to provide their full critical function.

The Solution

What Orpheus Provided

In response to these cybersecurity problems, External Attack Surface Management (EASM) and Third-Party Risk Management (TPRM) capabilities within the Orpheus platform were identified as being well-positioned to provide necessary solutions.

The attack surface component of the platform scores NHS BT's threats and vulnerabilities, creating an overall Cyber Risk Score that enables effective management of identified critical issues.

This score can be used in executive reporting to demonstrate the success of the cybersecurity strategy the team is pursuing, and operational teams to take the required mitigation actions to reduce or strengthen the attack surface. Constant monitoring regularly provides an updated score which allows the team to demonstrate tangible improvements over time.

Scores are well understood by executive team members who may not yet be proficient in cybersecurity. Cyber risk scoring provided NHS BT with an easy way to communicate value and return on investment, without the need for complex, cybersecurity-specific language.

The attack surface management capability not only provides scoring but also clear indicators of potential technical issues, enabling the NHS BT team to identify and address them on an ongoing and timely basis. They can also further explore and analyse the impact of mitigating the various issues they may be facing with embedded cyber threat intelligence reporting, enabling critical issues to be prioritised and addressed accordingly.

The Cyber Risk Score provided by Orpheus can also be applied to third parties. Through the Orpheus platform, organisations can be viewed in a heat map format, clearly highlighting those with public-facing cybersecurity vulnerabilities and ranking them by likelihood of compromise. This enables NHS BT to quantify and prioritise third-party risk, communicate effectively with key suppliers, and drive measurable risk reduction across its supply chain.

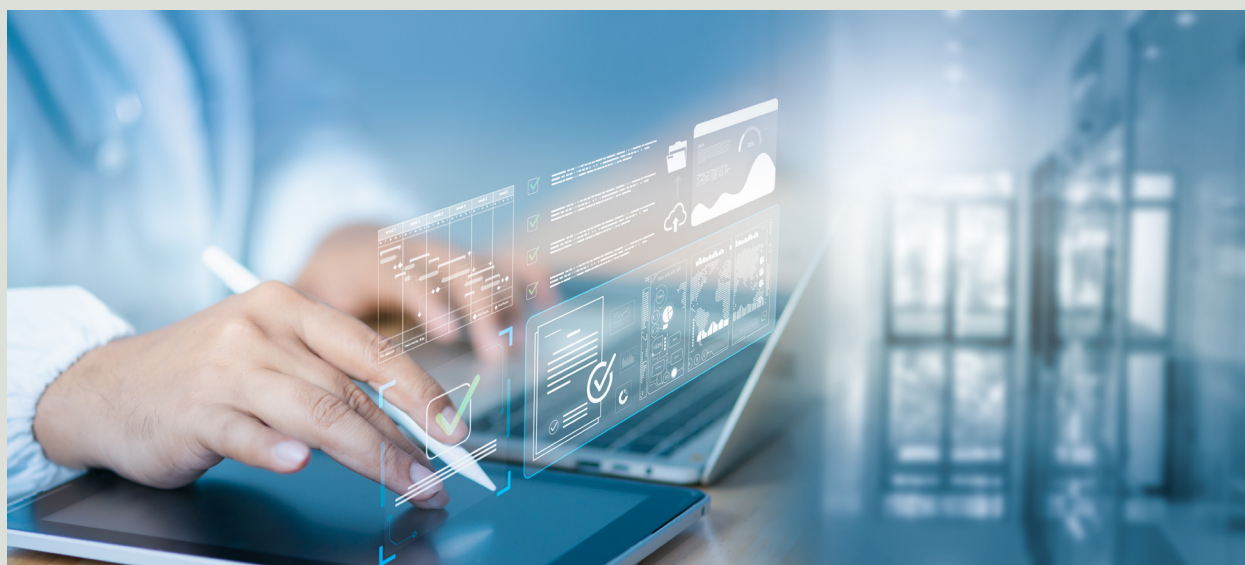
Orpheus' attack surface management functionality provides passive scanning of externally facing infrastructure, requiring no input from third-parties to enable and perform this activity. No additional security risk is introduced because no software or technical relationship is introduced. The scoring enables continuous monitoring so new issues can be dealt with promptly. While many organisations rely on questionnaires to solve this problem, this can be slow, expensive, and inaccurate.

The Next Steps

As NHS BT evolved their cybersecurity program it became apparent that Orpheus could assist with vulnerability prioritisation via Risk-Based Vulnerability Management (RBVM) features of the platform. Thousands of vulnerabilities are discovered each year with very few being exploited. Knowing which ones to prioritise for patching can save an organisation time and money, without compromising security.

It is well known that patching systems can create downtime; something that critical national infrastructure can rarely afford. Reducing the amount of time spent patching - without compromising on security - is a significant win for any cybersecurity team.

NHS BT uploads the results of their internal vulnerability scans to the Orpheus platform. Within minutes, Orpheus highlights any that are being used in ransomware attacks and pinpoints vulnerabilities that are actively being exploited. Additionally, Orpheus predicts which vulnerabilities are likely to be exploited in the future, enabling NHS BT to patch the right vulnerabilities and further control their cyber risk.



The Result

Why Orpheus Is The Right Solution

Everything in the Orpheus platform is led by threat intelligence. This is a key differentiator compared to other services.

As the threat landscape evolves, when threat actors change their tactics or enhance their capabilities, the Orpheus platform and additional services can provide the necessary tools, intelligence, and visibility to react and act proactively to protect against likely attacks or compromise. This means that NHS BT can stay ahead of its cybersecurity risk.

The Orpheus vulnerability exploitation prediction capability has been proven to be over 90% accurate following collaboration with and testing by the Ministry of Defence, enabling the confident prioritisation of identified vulnerabilities impacting NHS BT and its key third-parties.

Results

One exciting result of the work with NHS BT and Orpheus is the team being recognised at the Cyber Associates Network awards (NHS England) where innovation and expertise in cybersecurity across public sector health care are celebrated.

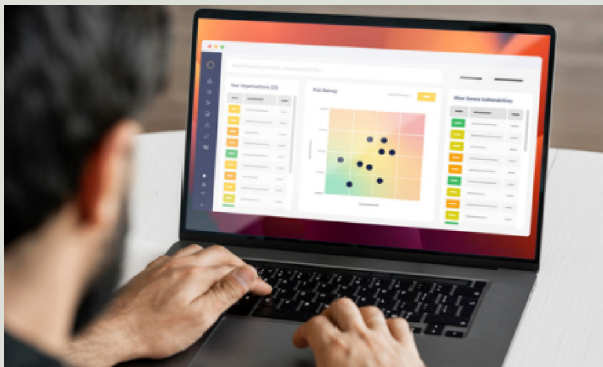
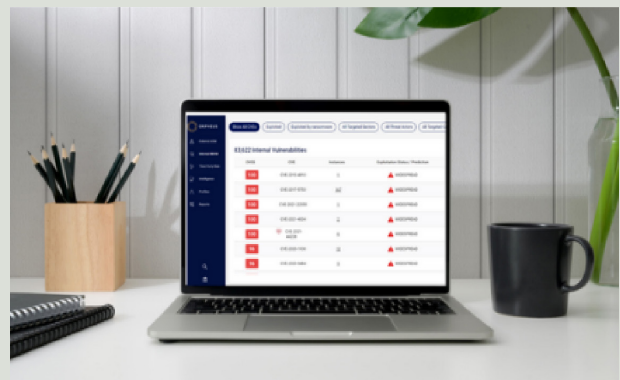
The team won individual awards and a team award, in part because of the way Orpheus has supported its cybersecurity strategy and operations, providing clear targets to remove external threats, reducing the external attack surface, and allowed NHS BT insight into peer scores which is "... unique and not seen in other services and products" - Head of Cyber Security Operations, NHS BT.

Orpheus Platform Modules Deployed for NHS BT

Delivering Results Where It Matters Most

External Attack Surface Management

Orpheus used our cyber risk ratings to monitor the external attack surface of NHS BT. The scores provided the management team with an overview of how the security program was doing and allowed the team to make targeted improvements.

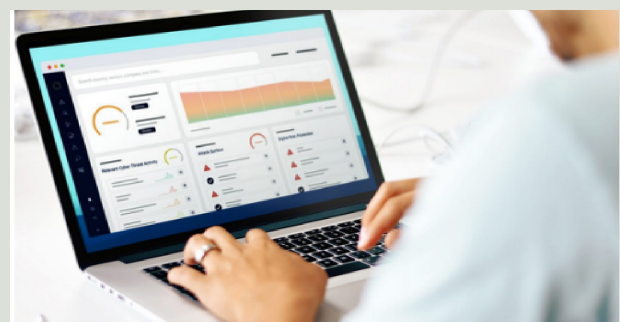


Risk-Based Vulnerability Management

Using the risk-based vulnerability management module has helped NHS BT direct their resources in the most efficient way possible while improving security.

Third-Party Risk Management

The third party risk module in the Orpheus platform was used to monitor the security posture of companies in the supply chain. This has helped limit their exposure to a supply chain attack, keeping the organisation more secure.





ORPHEUS

Orpheus is a UK-government accredited cyber threat intelligence company, delivering independently validated cyber risk ratings and predictive scoring powered by real-world threat intelligence.



CONTACT US:

contact@orpheus-cyber.com

orpheus-cyber.com



Visit our resources page for examples of existing and future content