



NOT-FOR-PROFIT **VULNERABILITY MANAGEMENT CASE STUDY**

Business Size
50+ employees

Service
vSOC RECON

Customer Since
2022

THE HIGHLIGHTS



Challenge

As a prerequisite of successful Cyber Essentials Plus accreditation, the client's overarching challenge was to find a way to stay abreast of emerging cyber threats and to correlate and remedy them. However, it isn't a huge organisation and, as such, has limited in-house resources, so the client was often overwhelmed with the volume and frequency of vulnerabilities it needed to stay on top of.



Solution

With our vSOC Recon service, together with Vulnerability Threat Briefings (VTBs), we've helped this client to maximise its ROI from vulnerability management technology and validate internal and outsourced patching procedures.



Results

With the support provided by the VTBs, the client has been able to do this:

- Successfully measure and evidence progress and risk-remediation efficiency.
- Gain a clear picture of its risk posture across all devices and servers.
- Garner valuable performance metrics for the organisation.
- Achieve Cyber Essentials Plus accreditation.

THE BACKGROUND

The client's organisation is committed to supporting commissioners and frontline restorative practitioners by creating and managing innovative programmes and delivering leading-edge training and restorative-justice services. It aims to provide an opportunity for a crime victim to meet or communicate with the perpetrator, discuss the impact of the crime and, ultimately, provide a sense of closure and understanding for the victim.

It's developed over 15 restorative-justice services, and its team of 46 employed staff and 20 sessional staff – supported by around 100 volunteers – works nationally and locally with organisations to make restorative-justice approaches accessible to all.



61K

Charities, by estimate, experienced a cyber attack or data breach in the last 12 months.

How working with Data Connect has provided the client and its IT support provider with **an enhanced level of cyber security expertise and guidance during Cyber Essentials Plus accreditation and beyond.**

When our client, an SME, first engaged with Data Connect, its in-house IT capabilities were limited and heavily relied on an outsourced IT services provider. However, when it came to improving the cyber security posture across all the devices on its network and meeting the requirements of Cyber Essentials Plus accreditation, it needed the help of a specialist external partner to take its awareness, visibility and vulnerability remediation capabilities to the next level – which is where Data Connect came in.

The client's director of corporate services expanded by telling us this:

"It's been a real process over the last four years; we've gone from absolutely nothing and having little understanding of what situation the devices used across the organisation were in to getting into the habit of looking at the dashboard every day. There was lots of stuff about which I had no idea what it meant. I introduced our engineer at our IT provider to Chris at Data Connect, and they spent an awful lot of time communicating with each other.

Chris was hugely helpful – there was stuff that even our engineer wasn't sure about. Without the experienced human expertise provided by Data Connect, we wouldn't have got as far as we got. It's important to say, right from the start, they were incredibly helpful to me personally, as someone that doesn't 'speak the language'. When I asked questions, never once was there a raised eyebrow or a patronising response. The Data Connect team would send screenshots and links to help us get to the solution. No question was ever a problem; they were always quick to respond."

THE CHALLENGE

With a Cyber Essentials Plus audit looming, our client needed to ensure its security posture was fully compliant with the Cyber Essentials Plus requirements. The client told us this:

“We’d met all the requirements to get through the audit first time around, and I’d assumed we’d get through it a second time. What I hadn’t realised is that, since our initial accreditation, software providers were issuing updates regularly, and I needed to make sure we were keeping step across all of the devices on our network.”



#1

Challenge for organisations pursuing Cyber Essentials certification is patch management.

THE SOLUTION

Our vSOC Recon service has helped the client to reduce its cyber security risk dramatically and prioritise software and configuration vulnerabilities across its network and devices, with visibility and control provided through Data Connect's vSOC Connect Console.

The vSOC Connect Console identified 731 issues that needed to be resolved before the audit date, and it became a trusted monitoring agent for the client. It identified issues and informed the client's remedial strategy; this included commissioning its IT solutions provider to carry out equipment updates as required, and it also highlighted the need to recruit an in-house ICT manager.

“vSOC Recon, together with the Vulnerability Threat Briefings (VTBs), allows us to see what we’re actually doing and clearly shows us what the gap is between where we are and where we need to be. We rely heavily on the vSOC Connect Console, specifically because we have a decentralised IT infrastructure. That means we don’t have on-premises hardware to monitor our users – everything goes through the cloud; we don’t have inbuilt Microsoft monitoring tools to tell us the health and status of individual devices. However, with the vSOC Connect Console, I can check and monitor everything and access the information that I need quickly, at any time. I have the vSOC Connect Console open all day, every day.”

VULNERABILITY THREAT BRIEFINGS (VTBs):

These periodic strategic sessions have afforded the client insight into emerging vulnerabilities, including both a summary of why each has been flagged as a vulnerability and an explanation of its priority. After the session, the client was able to access on the vSOC Connect Console a synopsis of how to remediate the vulnerability. This synopsis includes links to relevant resources provided by Microsoft / third-party developer solutions or to security councils' forums, which impart a better understanding of what that issue is and how to expedite its resolution.



37%

Year-over-year growth was seen in critical software vulnerabilities in 2024.

The client's ICT manager told us about his experience of the VTBs:

"Whilst I've personally only had two of the quarterly Vulnerability Threat Briefings (VTBs) so far, they've been invaluable. Chris and the team at Data Connect were very knowledgeable about our threat landscape and the challenges that were pertinent to us. The information presented to us was very focused, and he made sure we weren't overloaded with data that wasn't actually relevant to us. During the sessions, Chris had all the information laid out simply and concisely. And whenever I had a question, he was happy to move away from the slide show and the data he'd prepared and drill down into his view of the console, explaining where the information had come from and how the graph shown had tracked over time."

THE RESULTS

vSOC Connect Console: With a new ICT manager in place who was focused on fully utilising the vSOC Connect Console and ensuring best practice was observed by all members of the team, Data Connect became a partner, not just a provider.

The client's director of corporate services explained:

“Our ICT manager was interfacing with the vSOC Connect Console on a daily basis, but we still had lots of contact with the team at Data Connect. In the lead up to the second audit, we had a dedicated engineer at our IT provider. I introduced him to Chris and the team at Data Connect. They were all hugely helpful. There were things highlighted on the vSOC Connect Console that even our IT provider's engineer wasn't sure about. The team provided real human expertise that perfectly complemented the effectiveness of the vSOC Connect Console.”

Director of Corporate Services

Vulnerability Threat Briefings (VTBs): Data Connect provided periodic strategic sessions to give tailored information. The briefings have helped the client to stay abreast of specific emerging threats and access remediation solutions and guidance from several sources.

The client's ICT manager said this:

"The way that information was presented to me in the briefings allowed me to immediately see when there were spikes in vulnerabilities that had to be addressed, and this enabled me to be able to forward plan. For example, if I know on a 'Microsoft Patch Tuesday' there's going to be a large spike when new updates are released and new threats are discussed and identified, then I can prepare for that. The result is simply that I have insight at my fingertips that keeps me ahead of the game. For example, I've now got a graph of the last two weeks, and I can see that our vulnerabilities are dropping at a steady rate, which means we're in a very secure position."

The client's director of corporate services added this view:

"The Vulnerability Threat Briefings (VTBs) are driving cyber security best practice at our organisation. They're providing a reassuring 'sense check', helping us to be sure things are going in the right direction and bringing to our attention anything we need to know about."

Cyber Essentials Plus accreditation achieved, supporting the client's contract acquisition strategy:

Several years ago, His Majesty's Prison and Probation Service (HMPPS) launched what's known as the 'Dynamic Framework'; this is a central portal through which all organisations that want to deliver services commissioned by HMPPS need to register themselves. Within this portal, the minimum requirement for one of the first contracts the client wanted to bid for (in terms of cyber security) was Cyber Essentials Plus.

In addition, Police and Crime Commissioners and Regional Mayors, who commission many of the restorative justice services delivered by the client, increasingly require providers to have Cyber Essentials Plus accreditation in place before commencing delivery.

The client's director of corporate services told us:

"In order for us to bid, it was made clear that having Cyber Essentials Plus in place – from day one of delivery – was a mandatory requirement. Not knowing where to start, I contacted the IASME (Information Assurance for Small and Medium Enterprises) network and was signposted to a shortlist of potential providers, one of which was Data Connect. The fact that Data Connect was locally based made them the obvious choice to contact for initial advice, especially if I were ever to be required to meet them in person."

They added:

“As director of corporate services, IT is one of the areas that sits in my portfolio, and I felt it was important for us to have a look at what we were doing and make sure we were doing it well. I knew that Data Connect’s vSOC Recon service, with Vulnerability Threat Briefings (VTBs), would be instrumental in supporting this objective.”

To conclude, we asked the ICT manager to describe his personal experience of the Data Connect team. This is his reply:


“As people, the team at Data Connect are very helpful and open. Nothing seems to be too much trouble. If I ever have a query, no matter how simple it sounds, they treat it as a valuable question, and they do what they can to answer it. Team members are never too busy to help; they take ownership of any issues we have. My experience of working with them has been great. I really can’t fault them.”





Get in touch with our dedicated team to discuss your needs.

Talk to an expert

The Owlery, Spa Bottom Farm,
Haggs Road, Follifoot, Harrogate,
North Yorkshire, HG3 1EQ

 01423 425 498

 moreinfo@dataconnect.co.uk

 dataconnect.co.uk