Case Study

eSENTIRE

Aston Villa Football Club

How Aston Villa Football Club partnered with eSentire to consolidate their cybersecurity strategy, achieve NIST framework alignment, and gain 24/7 threat detection and response capabilities to protect their ambitious growth in the Premier League.

ORGANISATION

Aston Villa Football Club is a Premier League club in the English Premier League, established in 1874. As one of the Premier League's historic clubs with significant success over the years, Aston Villa is currently enjoying strong performance both in the league and in the Europa League.

- Relatively small IT and security team managing rapid organisational growth
- Extensive infrastructure including a historic stadium with complex technology requirements
- Microsoft technology stack requiring enterprise-level cybersecurity capabilities
- Subjected to UK/EMEA compliance regulations, including GDPR
- Participating in Premier League's Section K technology standards and security baseline requirements

Solutions and Results

Aston Villa Football Club partnered with eSentire to strengthen the maturity of their security operations, increase visibility across their entire attack surface, harden their security defences, and reduce gaps in their threat detection and response capabilities through:

- **24/7 MDR for Microsoft** to provide comprehensive threat detection and response across Microsoft environments with seamless integration into Aston Villa's existing Microsoft technology stack
- **MDR for Log** to deliver 24/7 active log monitoring, critical multi-signal visibility, ensure compliance across their multi-cloud environment
- **NIST Cybersecurity Framework Assessment through Cyber Threat Exposure Management (CTEM)** to establish a baseline security maturity score and an implementation roadmap aligned with the club's strategic objectives

Business and Security Outcomes

- 24/7 threat detection, investigation, and response capabilities by eSentire's global SOC team, providing coverage that was previously impossible with Aston Villa's small in-house team
- Alignment with NIST Cybersecurity Framework with a structured 3-year implementation roadmap to continuously improve security maturity
- Achievement of 100% scores in endpoint hardening and email security on the Premier League's security baseline platform
- Seamless integration with existing Microsoft E5 technology stack, eliminating fragmented security solutions and enabling rapid deployment
- Enterprise-level cybersecurity expertise and guidance without the cost of hiring specialised in-house cybersecurity staff
- Enhanced ability to detect and respond to threats such as business email compromise, leading to the development of internal security playbooks
- Compliance with UK/EMEA regulations including GDPR requirements
- Partnership approach that provides appropriate technical expertise while allowing Aston Villa's small IT team to focus on strategic initiatives and day-to-day operations

The Challenge

Football clubs have long been considered high-value targets for threat actors given the type of confidential data they hold, such as athlete transfer news and contract details, sensitive information about athletes and coaching staff, and Personally Identifiable Information (PII) about their employees and fans. The Aston Villa Football Club is no different.

Unlike traditional businesses with linear growth trajectories, football clubs experience rapid, compressed timelines with constant change. The club's rapid expansion brought an influx of new staff, additional infrastructure, and evolving business operations, all without a dedicated cybersecurity function in place.

So, as Aston Villa experienced significant growth on and off the pitch, their cybersecurity challenges also increased.

"The challenge isn't just trying to keep up with making sure that systems and accounts are secure. We also need to make sure the technology that we're implementing is also fit for purpose. But things move so quickly, it's incredibly difficult to keep up with that," Carl Maycock, Head of IT at Aston Villa, explains.

After conducting an initial NIST Cybersecurity Framework assessment, Aston Villa identified significant gaps in their security posture. While they had various technical tools in place, it became clear that they needed additional guidance and support for:

- 24/7 security monitoring and threat detection capabilities
- Specialised technical understanding of the cyber threat landscape
- A cohesive cybersecurity strategy aligned with industry frameworks
- The ability to respond quickly to emerging threats
- Expert-level guidance to implement and maintain comprehensive security controls

In addition, the threat landscape was particularly concerning for a high-profile organisation like Aston Villa for two primary reasons.

First, data breaches are always of concern since any leaked data can compromise business operations as well as football matches. However, there is an added layer of complexity with football clubs; the leaked data contains confidential information about the athletes, which may offer a competitive advantage to anyone who can access it.

Second, threat actors are creating increasingly sophisticated malware and ransomware that targets the club's employees, so having 24/7 threat detection and response capabilities that stop attackers in their tracks is critical—especially for an organisation who doesn't have the resources to run an internal Security Operations Centre (SOC).

"Even though we are a Premier League club, the reality is that we just don't have the resources to be able to run an internal SOC. So, our ability to monitor and react to cyber threats 24/7 is limited," Carl says. "We need that ability and the only way to do that is to engage a third-party provider so we can actively monitor and respond to the various different threats."

With match-day operations being time-critical, with a stadium full of fans and live broadcasters, any security incident could have devastating consequences for the club's reputation and operations.

"If you've lost all your data or the data has been leaked, you can never bring it back in again," Carl states. "And the same thing with your people's accounts or data that they've been locked out of at that point, the business can't operate. Those are the two big things I think really scare me in terms of my day-to-day and the things that I always try to keep as a focal point moving forward."

As part of their compliance with the Premier League's Section K technology standards, Aston Villa also needed to provide extensive connectivity for media, broadcasters, and other third parties on match days, creating hundreds of potential entry points that required careful, comprehensive monitoring and security controls.

"We have lots of third-parties that come in and plug unknown random equipment into the network, which you don't have a lot of control over a lot of the time. We've seen rogue access points that are advertising fake wireless networks and we've seen them wander around the ground because you can pick them up from our wireless environment."

However, the club's small IT team was stretched thin, managing everything from networking and servers to cloud services and match-day operations. So, when it came time to address cybersecurity gaps, Aston Villa faced a critical decision: hire expensive cybersecurity specialists or find a trusted partner who could provide enterprise-level security expertise.

Given these challenges, Aston Villa needed a strategic partner who provided 24/7 threat detection and response capabilities with round-the-clock security monitoring and offered enterprise-level cybersecurity expertise at a fraction of the cost of building an in-house security operations team.

Why Aston Villa Chose eSentire As Their Proven MDR Partner

When Aston Villa began their search for a Managed Detection and Response (MDR) provider, they conducted a thorough evaluation of multiple vendors. The selection process revealed varying experiences with different providers; some overwhelmed them with information overload, while others were frustratingly vague about their capabilities and approach.

From an initial field of providers, Aston Villa narrowed their selection down to four finalists and ultimately chose eSentire. Several key factors differentiated eSentire from the competition:

Enterprise-Level Expertise and Partnership Approach:

Aston Villa needed a true partner who could provide enterprise-level expertise while understanding the unique constraints and requirements of a Premier League football club.

Unlike other providers, eSentire approached the engagement as a partnership, taking time to understand Aston Villa's specific challenges, goals, and constraints rather than simply pushing a one-size-fits-all solution.

Seamless Integration with Microsoft Technology Stack:

Aston Villa had made significant investments in Microsoft technologies, including Microsoft E5 licensing. Finding an MDR provider who could leverage these existing investments while providing comprehensive security coverage was critical.

eSentire's MDR for Microsoft offering provided the perfect solution, delivering comprehensive 24/7 threat detection and response capabilities while maximising Aston Villa's existing Microsoft investments and eliminating the need for additional, disparate security tools.

Structured Approach to NIST Framework Alignment:

One of Aston Villa's key objectives was aligning with the NIST Cybersecurity Framework. eSentire not only conducted the initial maturity assessment but also provided a clear, structured 3-year roadmap for implementation.

24/7 SOC Capabilities Without the Overhead:

Building and staffing an in-house SOC was financially and operationally impossible for Aston Villa's small team and limited budget. eSentire's 24/7 SOC-as-a-Service provided world-class monitoring, detection, and response capabilities without the overhead of hiring, training, and retaining specialised cybersecurity staff.

"We ingest data from all of our logs, our Microsoft environments, our firewalls into eSentire's SOC, giving us the ability to not only monitor everything 24/7 but also respond very quickly," Carl explains. "When we have some sort of alert that comes through, eSentire's SOC Analysts very quickly alert us to that. Plus, with the Atlas User Experience, we can see everything in real-time. And if it's really critical, the SOC team will immediately contact us so we can try and remediate it."

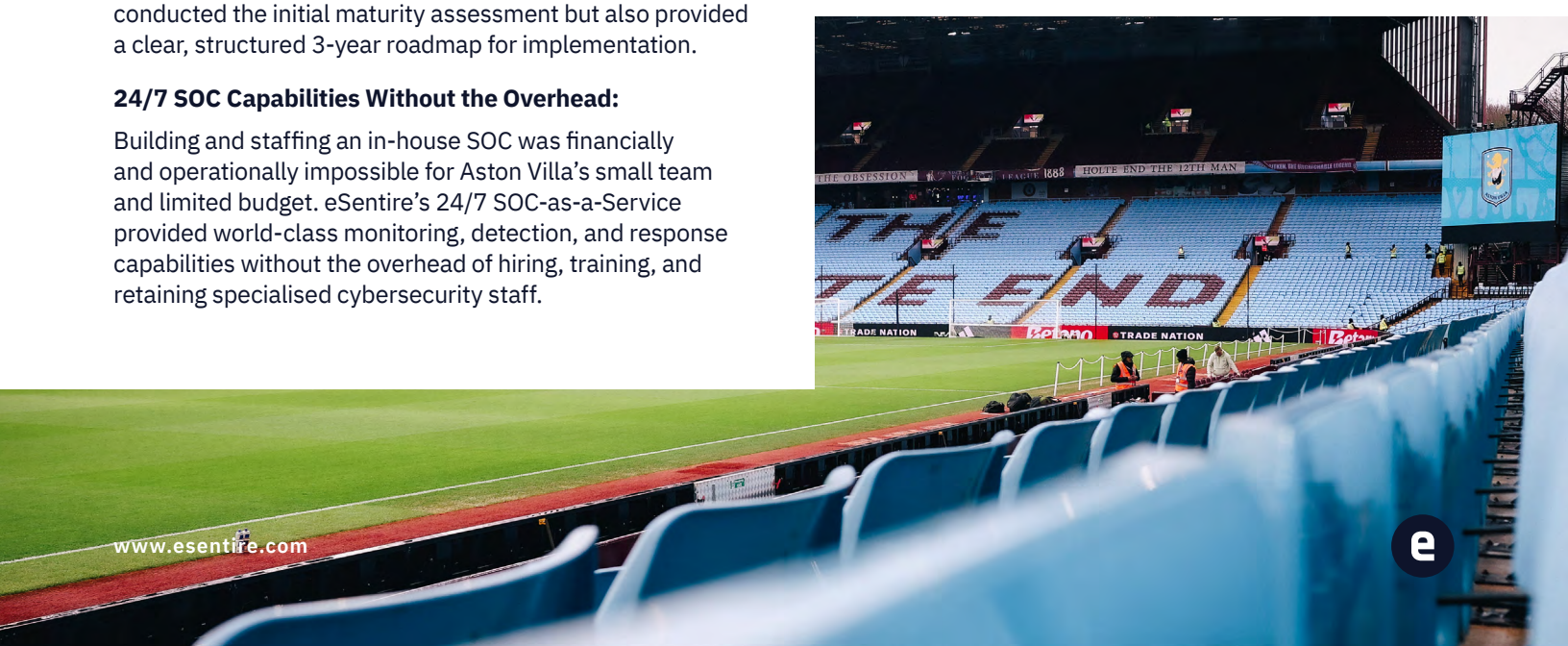
Rapid Deployment and Time to Value:

Once the decision was made, eSentire's onboarding process was straightforward and efficient. The partnership officially began in January 2025, with services deployed rapidly to provide immediate protection.

Throughout the evaluation and onboarding process, eSentire demonstrated responsiveness, expertise, and a deep understanding of the threat landscape. The team's ability to communicate clearly, provide actionable recommendations, and respond quickly to questions gave Aston Villa confidence in their choice.

The results spoke for themselves. Following deployment, Aston Villa experienced:

- Significant improvement in their NIST maturity score from the initial baseline of 45%
- Achievement of 100% scores in endpoint hardening and email security on the Premier League's security baseline platform
- Detection and response to security threats such as business email compromise attempts, with three employees clicking on a phishing email that eSentire quickly identified and contained
- Development of internal security playbooks based on real-world incidents detected by eSentire



Conclusion

For high-profile organisations like Premier League football clubs, the stakes of cybersecurity are exceptionally high. A breach doesn't just mean lost data or operational disruption; it can mean competitive disadvantage, reputational damage, and loss of fan trust.

Aston Villa Football Club's partnership with eSentire demonstrates how organisations with limited resources and small teams can achieve enterprise-level cybersecurity through strategic partnerships. By outsourcing 24/7 security monitoring, threat detection, and response to eSentire's global SOC, Aston Villa gained capabilities that would have been impossible to build and maintain in-house.

The structured approach to NIST Cybersecurity Framework alignment has provided Aston Villa with a clear roadmap for continuous improvement, while the seamless integration with their Microsoft technology stack eliminated the complexity and fragmentation of managing multiple security vendors.

As Aston Villa continues its journey of growth and success both on and off the pitch, eSentire remains a trusted partner by providing the expertise, technology, and 24/7 vigilance needed to protect the club's sensitive data, maintain operational resilience, and ensure that Carl and his team can focus on enabling the club's ambitious goals.

Carl's advice to other security leaders is simple: "Anything you do to make your environment secure is progress. Don't assume that you're going to do it all overnight. We are still in a long programme to deliver all the things we need to, and even when we've done that we will come back again and start again."

Ready to Get Started?

To learn how eSentire MDR can help your organisation reduce your cyber risks and build a resilient security operation, connect with an eSentire cybersecurity specialist today.

CONTACT US →

IF YOU'RE EXPERIENCING A SECURITY INCIDENT OR BREACH CONTACT US (0)8000-443242

eSENTIRE