

■ Case study ■ Historic England

Securing England's history with 24/7 threat detection and response

Historic England is the public body that helps people care for, enjoy and celebrate England's spectacular historic environment. Managing its digital estate – and providing shared IT services to other government bodies – requires robust security round the clock.

Partnering with Socura for [Managed Detection and Response \(MDR\)](#) has helped reduce Historic England's cyber risk by decreasing the time taken to identify and respond to threats and enhancing the protection of specialist systems, data and users.



The security challenge

Historic England is an Arms-Length Body part of the Department for Culture, Media and Sport (DCMS). The organisation's responsibilities include managing, protecting and championing national heritage and historic places.

As a public organisation with a broad remit, Historic England has a responsibility to safeguard various specialist systems and applications. The organisation was acutely aware of the potential impact a cyber attack could have on its ability to maintain the integrity and availability of historical records and artefacts, provide essential public services and uphold its reputation as a trusted authority.

Responsible for the IT and cyber security needs of not only its own estate but a small number of other public bodies, maintaining round-the-clock threat monitoring was not feasible for Historic England's in-house technical governance and infrastructure operations teams. They needed an MDR partner with the expertise required to not only proactively monitor its systems but also respond swiftly to attacks, regardless of when they occur.

Main security concerns

- Strengthening the protection of specialist systems and data, incl. other bodies it provides services to
- Achieving round-the-clock monitoring without overburdening its internal teams
- Minimising the risk of phishing attacks against a fluctuating workforce of over 4,000 users
- Protecting its reputation and relationships with other public bodies and partner networks
- Ensuring compliance with the latest government security standards

The solution

Following a competitive tender procurement process that involved the evaluation of several managed security services providers, Historic England selected Socura as its Managed Detection and Response (MDR) partner.

Socura's UK-based Security Operations Centre (SOC) now provides round-the-clock proactive security monitoring across Historic England's environments, which includes triaging, investigating and responding to alerts generated by its network and endpoint security controls. To uncover novel or unknown threats, Socura uses aggregated threat intelligence to perform regular threat hunts and continually optimise coverage and visibility. Unlimited detection engineering is included as a core feature of the service at no additional charge.

Key benefits

01

Greater peace of mind

With Socura responsible for round-the-clock monitoring, Historic England's internal teams no longer have to worry about out-of-hours threats. They have the reassurance that experts are watching their systems and will quickly investigate and respond to issues at any time of day.

02

Broad threat visibility

By deploying and optimising the security controls required to identify and disrupt threats, Socura has enabled Historic England to enhance threat visibility and bolster coverage against the latest attack techniques.

03

Proactive response

Socura MDR improves outcomes and alleviates the daily operational burden on Historic England's infrastructure and governance teams by not only identifying threats but also containing and disrupting them before they can spread.

04

Suspicious email triage

Because security controls can't block every threat, Socura MDR provides an extra layer of protection by allowing Historic England users to report suspicious emails for forensic analysis. If phishing or other threats are confirmed, Socura can immediately block malicious links and reset compromised accounts.



Moving to a 24/7 MDR service has been like 'turning the lights on' across our environments.

Nick Seal, Head of Operations, Historic England