EXECUTIVE GUIDE

Cybersecurity for Fire & Rescue

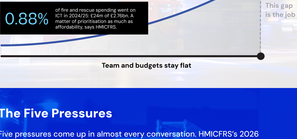
In October 2026 HMICFRS found fire and rescue services are not fully prepared for a growing cyber threat, and set a deadline: baseline CAF standards in every English service by November 2027. Every service knows the bar is rising. Meeting it with the team and budget you have is the hard part.

> **"A major cyberattack isn't a hypothetical scenario."**
>
> HMICFRS, Cybersecurity in police forces and fire and rescue services, October 2026

The Squeeze

- Fire standards
- NFCC
- CAF
- Cyber Essentials Plus

0.88% of fire and rescue spending went on ICT in 2024/25: £24m of £2.76bn. A matter of prioritisation as much as affordability, says HMICFRS.



The Five Pressures

Five pressures come up in almost every conversation. HMICFRS's 2026 inspection found the same five. Each one maps to a stage of the same journey.

01 — A rising standard, static resources

HMICFRS has given English services until November 2027 to reach the baseline CAF standard, with external validation to follow. Monitoring and evidence are expected, without more people or budget.

02 — Small teams cannot cover the clock

Seven of 44 English services had a SOC in 2025. HMICFRS found small teams working beyond capacity, with no surge cover for a prolonged incident. Threats do not keep office hours.

03 — Too many tools, not enough visibility

Security estates grow into a patchwork of overlapping products, adding cost, effort and gaps between tools that nobody owns.

04 — Paying for capability you are not using

Many services hold Microsoft 365 licences that already include protection they are buying again from third parties.

05 — Board accountability, no clear picture

Leaders told HMICFRS that cyber was not part of daily operational decisions. Boards lack a single view of posture, and a case that cyber spend protects operations rather than competing with them.

The good news

Every pressure maps to one of three stages, and the tags show which. The same stages take a service to the November 2027 baseline. Scroll on to walk the journey.

Assess → Protect → Optimise.

Stage 1: Assess

Know where you stand, against the frameworks that matter.

HMICFRS now asks for annual external validation of every service's CAF return. A posture assessment mapped to the CAF and the Digital and Cyber Fire Standard turns a broad set of expectations into a sequence of steps you can plan and fund.

Baseline → **Gaps** → **Roadmap**

Establish current maturity across the estate, mapped to the CAF and the Fire Standard. Independently of your own self-assessment.

Identify the gaps that matter most, ranked by risk to operations. HMICFRS found the common ones: asset management, incident response and assurance.

A prioritised, phased plan to the November 2027 baseline that fits the budget and the team you actually have.

OUTCOME

A baseline for your team and a roadmap for your board: cyber risk becomes something leaders can see, track, govern against and evidence to an external validator.

Stage 2: Protect

Extend your team with a Managed SOC.

HMICFRS wants monitoring and detection available at all times in every English service, and found services relying on supplier alerts could not always confirm anyone was watching. A Managed SOC gives a small Fire & Rescue team what it cannot build alone.

Your small team + **SCC Managed SOC** = **Protect, always**

Context, command and local knowledge.

Specialist monitoring, detection and response.

24/7/365 cover without a night shift you cannot fund or fill.

- **Continuous monitoring** — Your whole estate watched around the clock, including supplier-hosted systems, not just in office hours.
- **Incident response** — Threats contained fast, with surge cover for a prolonged incident and clear escalation into your team.
- **Threat detection** — Alerts triaged by specialists, so your team only handles what matters.
- **Evidence for inspectors** — Proof of active monitoring you can show HMICFRS, external validators and the fire authority.

Stage 3: Optimise

Consolidate onto the Microsoft platform you already own.

HMICFRS found legacy platforms that could not feed a SIEM, run endpoint detection or support modern authentication, alongside patchy MFA. Many services already pay for the fix: consolidating overlapping tools into Defender, Sentinel and Entra cuts cost and complexity at the same time.

Endpoint AV | Email filter | SIEM | Identity / MFA | Web proxy | + more

One Microsoft platform

Defender · Sentinel · Entra

One console · One licence · One view of security

Simpler

Fewer vendors means simpler management, fewer renewals and one coherent view instead of a dozen consoles.

Already included

Microsoft is independently recognised as a leader across endpoint, SIEM, email and identity. Much of it is already in your licence.

Built for the findings

Defender, Sentinel and Entra close the gaps HMICFRS named: endpoint detection, SIEM integration, MFA and access control, on a Zero Trust foundation.

Proof

How this worked for one UK Fire & Rescue Service.

The starting point: a growing Microsoft 365 investment, a set of separate third-party security tools, a small internal team, and no way to provide monitoring outside working hours.

1 — CAF-mapped assessment

Estate assessed against obligations, producing a prioritised roadmap.

2 — Microsoft consolidation

Overlapping tools moved into Defender and Sentinel.

3 — Managed SOC

Round-the-clock monitoring the team could not staff alone.

4 — Ongoing support

Specialist skills throughout, with no disruption to operations.

The Results

Organisations that take our Managed SOC services typically see the following results:

97% of threats automatically eliminated or contained.

60% Savings on average, over multi-vendor security options.

80% Reduction in threat response time.

242% ROI over three years.

SCC Managed SOC Services

Our UK-based Security Operations Centre combines 24/7 monitoring through advanced analytics, expert threat hunting, and rapid incident response. We operate as an extension of your team, detecting threats faster and containing them before they cause damage.

HMICFRS now expects every new or renewed supplier contract to meet Cyber Essentials and Secure by Design standards from May 2027. Our accreditations:

CREST | Microsoft Solutions Partner – Security | Microsoft Solutions Partner | Member of Microsoft Intelligent Security Association

PULSE

SCC's AI-Powered Automation Platform

SCC Pulse is the heartbeat that powers our managed services – ensuring that we deliver services and outcomes that are **faster, smarter and better.**

90% handled through AI and automation, while surfacing the threats that matter.

Start your journey

A cyber posture assessment mapped to the CAF and the Digital and Cyber Fire Standard: a baseline for your team, a roadmap for your board and a clear path to the November 2027 deadline. No commitment beyond the conversation.

Book a conversation



Source: HMICFRS, Cybersecurity in police forces and fire and rescue services, 31 October 2026. Fire and rescue spend figures are 2024/25. SOC coverage figure (2025) is the National Fire Chiefs Council, cited by HMICFRS.