EXECUTIVE GUIDE

# Cybersecurity for Fire & Rescue

The Digital and Cyber Fire Standard, NFCC guidance and the Cyber Assessment Framework are raising the bar for every service. The challenge is not awareness. It is meeting a rising standard with the team you have.

## The Squeeze

- Fire standards
- NFCC
- CAF
- Cyber Essentials Plus




## The Five Pressures

Five pressures come up in almost every conversation, and each one maps to a stage of the same journey.

**1 — A rising standard, static resources**
Structured risk management, monitoring and demonstrable resilience are now expected, without a matching rise in people or budget.

**2 — Small teams cannot cover the clock**
Threats do not keep office hours. A team of a few people cannot provide 24/7/365 monitoring and response alone, however skilled.

**3 — 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.

**3 — Paying for capability you are not using**
Many services hold Microsoft 365 licences that already include protection they are buying again from third parties.

**1 — Board accountability, no clear picture**
Cyber risk now sits at board level, but leaders lack a single view of posture and a roadmap they can govern against.

**The good news**
Every pressure maps to one of three stages, and the numbered tags show which. Continue scrolling to walk the journey:

**Assess → Protect → Optimise.**

## Stage 1: Assess

**Know where you stand, against the frameworks that matter.**
A posture assessment mapped to the Cyber Assessment Framework and the Digital and Cyber Fire Standard turns abroad set of expectations into a sequence of manageable steps.

**Baseline**
Establish current maturity across the estate, mapped to the CAF and the Fire Standard.

→

**Gaps**
Identify the gaps that matter most, ranked by risk to operations, not by checklist order.

→

**Roadmap**
A prioritised, phased plan 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 and govern against.

## Stage 2: Protect

**Extend your team with a Managed SOC.**
A Managed Security Operations Centre gives a small Fire & Rescue team what it cannot build alone. Your people keep context and decisions; the SOC provides the cover.

**Your small team**
Context, command and local knowledge.

+

**SCC Managed SOC**
Specialist monitoring, detection and response.

=

**Protect, always**
24/7/365 cover without a night shift you cannot fund or fill.

24/7

**Continuous monitoring**
Your whole estate watched around the clock, not just in office hours.

**Incident response**
Threats contained fast, with clear escalation into your team.

**Threat detection**
Alerts triaged by specialists, so your team only handles what matters.

**Evidence for auditors**
Proof of active monitoring you can show inspectorates and the board.

## Stage 3: Optimise

**Consolidate onto the Microsoft platform you already own.**
Most services already pay for much of the protection they need. Consolidating overlapping tools into the Microsoft platform 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, streamlined renewals and one coherent view instead ofa 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 future**
Defender, Sentinel and Entra align to Zero Trust on a foundation that grows with the service.

## Proof

**How this worked for one UK Fire & Rescue Service.**
Most 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 who take our Managed SOC services typically see the following results:

| 97% | 60% | 80% | 242% |
|---|---|---|---|
| of threats automatically eliminated or contained. | Savings on average, over multi-vendor security options. | Reduction in threat response time. | 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.

PULSE

**SCCs 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, no commitment beyond the conversation.

**Book a conversation**

