Integrity360
your **security** in mind

CASE STUDY:
CyberFire powers a seamless MDR transition for a leading retail finance organisation

The customer

A market leader in the retail finance industry, an organisation that enables customers to purchase household goods through structured credit offerings. Owned by one of Europe's most prominent banking institutions, they operate in a heavily regulated environment that requires strict compliance with global standards such as the Digital Operational Resilience Act (DORA).

The internal cyber security function, led by a dedicated team under the Group IT Governance, Risk and Compliance Manager, plays a central role in safeguarding the business. This includes not only managing incidents but also developing cyber awareness, governing risk exposure, and aligning operational controls with global mandates.

"I enjoy the problem-solving side of cyber security—connecting people, processes, and technology to reduce risk. That's where CyberFire has helped us stay ahead." – *Risk and Compliance Manager*

Selection criteria

Their RFP process was stringent, evaluating multiple providers based on critical business and technical requirements:

• A local presence that offered direct, real-time support and familiarity with their industry

• Expertise in managing hybrid and strictly on-prem environments

Industry

Retail Financial Services

The challenge

Before partnering with CyberFire MDR, the organisation used another MDR provider but faced significant barriers to operational effectiveness:

- **Alert overload:** The previous MDR service logged virtually everything as an incident, leading to alert fatigue and a lack of prioritisation.
- **On-premise complexity:** As a business that primarily operates on-prem infrastructure, they needed an MDR partner capable of integrating deeply without relying heavily on cloud-based services.
- **Global compliance pressure:** The European parent bank enforced a SOC-aligned detection framework that had to be mapped locally in a meaningful and auditable way.
- **Urgency:** Due to issues with the previous provider, there was no time for delays—full onboarding and transition had to be completed in under two months.

> ***"We had zero room for downtime. The incident management process couldn't stop, not even for a day."***
>
> - Risk and Compliance Manager

Integrity360
your security in mind

CASE STUDY:
CyberFire powers a seamless MDR transition for a leading retail finance organisation

- The ability to map CyberFire MDR's detection capabilities directly to the parent company's global SOC framework
- The willingness and capability to adapt reporting, metrics, and processes to meet specific governance needs
- A cultural fit with a team under pressure and high scrutiny

"CyberFire's ability to respond, pivot and reconfigure to suit new policy updates—even at short notice—has made them an invaluable extension of our team."

– Risk and Compliance Manager

Integrity360's solution

CyberFire MDR deployed a tailored MDR environment that was up and running in just six weeks—complete with compliance sign-offs and internal approvals.

Key areas of support included:

- **Mapped detections:** Aligning CyberFire's native detections with a strict European framework of "use cases," ensuring traceability & compliance
- **Human-centric monitoring:** A true 24/7 SOC with skilled analysts contextualising alerts before escalation
- **Bespoke reporting:** Monthly reports were extended with additional metrics, mapped to KPIs dictated by the client's audit and oversight requirements
- **Ongoing flexibility:** CyberFire MDR continued to adapt rapidly as internal governance policies changed, including backup log requirements and reporting format changes

> **"It's not the quantity of alerts—it's the quality. CyberFire helped us shrink the noise and zero in on what actually matters. Their team knows our people, our processes, and our environment. That context makes all the difference."**
>
> *- Risk and Compliance Manager*

The benefits

- Complete MDR deployment within six weeks, with no disruption to incident management
- Dramatic reduction in false positives, freeing up valuable operational time
- Seamless alignment with both internal & external SOC reporting requirements
- Identification of previously undetected threats through advanced detection tuning
- Regular service reviews and improvement loops, ensuring continual growth and relevance
- A strong partnership built on responsiveness, domain understanding, and trust

> **"We had very strict requirements from our global parent - if you didn't meet the bar, you didn't proceed. CyberFire not only met the bar, they exceeded it."**
>
> *- Risk and Compliance Manager*

Integrity360
your security in mind

CASE STUDY:
CyberFire MDR powers a seamless MDR transition for a leading retail finance organisation

Looking ahead

The client is now collaborating with CyberFire MDR to extend detection and response into business-critical application logs—including custom-developed web platforms and internal transaction systems. This next phase will provide deeper insight into anomalous user behaviour and non-traditional threats that may emerge at the application layer.

"As our environment evolves, so do our risks. CyberFire has shown they can evolve with us."
– Risk and Compliance Manager, Retail Finance Organisation

CyberFire MDR continues to play a vital role in the organisation's cyber security journey—strengthening its people, maturing its governance, and adapting alongside an ever-shifting threat landscape.

About Integrity360

Integrity360 is Europe's leading cyber security and PCI specialist, with offices across Ireland, the UK, Bulgaria, Italy, Sweden, Spain, Lithuania, Ukraine, South Africa, and the Caribbean. The company operates six Security Operations Centres (SOCs) in Dublin, Sofia, Stockholm, and Cape Town.

With an expert team of over 550 dedicated cyber security professionals, Integrity360 offers a full suite of professional, support, and managed security services. These services cover every aspect of cyber risk management, from identification and prevention to detection, response, and recovery.

2500+ Enterprise clients

550+ Cyber professionals

ISO 9001 CERTIFICATION EUROPE™
ISO 27001 CERTIFICATION EUROPE™
ISO 20000-1 CERTIFICATION EUROPE™