Guide

# **Implementing FxDR** in your banking security systems

## Your go-to-guide for a smarter approach to fraud prevention

FxDR builds on the foundational principles of Extended Detection and Response (XDR), employing specialised threat intelligence to identify and counteract fraud schemes.

It offers adaptable and minimally disruptive protection against ATO, ATS, and APP fraud. Unlike traditional methods that react to known attacks, FxDR proactively identifies and counters emerging fraud tactics, providing a more precise and dynamic defence against evolving threats.

**Here is our guidance on establishing an internal process to seamlessly integrate FxDR into your fraud management framework.**

## 1. Laying the groundwork: Assessing your fraud prevention strategy

Before integrating FxDR, institutions must conduct a thorough evaluation of their current fraud prevention systems. This step provides the foundation for a successful transition by identifying gaps and areas for improvement.
**Consider the following:**

**Customer journey gaps:** Are there points in the customer journey where fraud might go undetected?

**Advanced threat detection:** Can current tools identify multi-vector fraud tactics, such as those involving social engineering and account takeovers?

**Reactive vs. proactive approaches:** Traditional systems often detect fraud only at the point of transaction, by which time the damage is already done. Can you proactively identify attack patterns earlier to prevent them from scaling into larger campaigns?

**Cross-departmental insights:** Are current processes capable of correlating data across departments or operational silos?

**Proactivity vs. reactivity:** Do existing tools offer actionable insights in real-time, or do they primarily react to fraud after it occurs?

**Visibility and understanding:** 'You can't manage what you can't see.' Many institutions focus exclusively on transactions, ignoring the pre-transaction signals left by attackers during reconnaissance or testing phases. Can you detect and understand indicators like bot attacks, unusual credential usage, or malware traces, which are critical early warning signs?

A thorough gap analysis sets the stage for a phased, goal-oriented FxDR implementation.

## 2. Breaking down silos: Unifying cybersecurity and fraud teams

FxDR facilitates the collaboration between fraud and cybersecurity teams, increasing the level of efficiency of fraud prevention activities. **This is why financial institutions should:**

**Set shared goals:** Define unified objectives for fraud prevention and cybersecurity, focusing on mutual success metrics.

**Cross-team data sharing:** Fraud and cybersecurity teams should schedule periodic discussions to align strategies, review emerging threats, and share data to maximise efficiency.

**Create unified dashboards:** Leverage integrated platforms where both teams can access shared data and insights.

**Develop coordinated incident response plans:** Ensure both teams work together seamlessly during fraud incidents with predefined roles and workflows.

**These steps** will enable smoother collaboration, more effective threat detection, and a holistic approach to fraud prevention.


**A cyber-fraud approach empowers institutions to proactively identify, analyse, and mitigate risks** through advanced tools like machine learning, behavioural analytics, and contextual threat intelligence. It also evaluates the broader context, including account logins, device interactions, API calls, and external threat feeds.

## 3. Selecting the right FxDR platform: Features that matter

To combat the varied and sophisticated fraud tactics employed today, an effective FxDR platform must go beyond one-dimensional detection methods.

**When choosing an FxDR platform, prioritise solutions with:**

- **Comprehensive visibility:** End-to-end monitoring of the customer journey.
- **Multiple detection models tailored to different attack types:** For example, behavioural analytics for unusual patterns, transaction monitoring for anomalies, and malware detection for system compromise.
- **Advanced data correlation:** Integration of diverse data sources, including transaction records and external threat feeds.
- **Real-time detection and response:** Dynamic interventions tailored to evolving threats.
- **Scalable:** Adaptability to increasing data volumes and fraud complexities.
- **User-friendly:** Simplified adoption and training for teams.

GRUPPO BCC ICCREA

## How BCC Iccrea Group got ahead of fraud before it struck

With over 5 million members and nearly 2,500 branches, **BCC Iccrea Group knows trust is everything**. But as digital transactions surged to 85% of their activity, fraudsters weren't far behind, targeting instant transfers, launching phishing attacks, and slipping through traditional defences.

Fraud tools that worked yesterday were struggling to keep up. Cyber and fraud teams operated in silos, leading to false positives, unnecessary friction for customers, and gaps for attackers to exploit.

With Cleafy's FxDR platform's real-time behavioural intelligence, advanced threat detection, and a unified approach, BCC Iccrea Group didn't just react to fraud, it saw it coming.

- Fraud rates **dropped by 80%.**
- The bank now **saves over €0.5 million** each month in fraud-related costs.
- Unecessary account friction **plummeted**.
- Customer experience **improved**.

> We've gone from chasing fraud to staying ahead of it. Cleafy gives us exactly what we need, when we need it."
>
> - **Giuseppe Scampone, Fraud Manager, BCC Iccrea Group**

Read the case study

## 4. Practical steps forward: Training teams and redefining processes

FxDR adoption requires both technological and cultural shifts. **Steps to maximise its potential should include:**

1 **Training programs**
Equip your teams with the knowledge and skills to leverage FxDR tools effectively.
Training should cover:

- Understanding analytics outputs and how to act on them.
- Configuring automated responses and tailoring interventions to specific scenarios.
- Staying informed about the latest fraud tactics and how FxDR tools address them.

2 **Fostering a culture of continuous learning**
Fraud tactics evolve rapidly, and so should your institution's defences.
Provide ongoing education for fraud and cybersecurity teams, including:

- Regular updates on emerging threats.
- Periodic training sessions on new FxDR features and capabilities.
- Encouragement for teams to share insights and lessons learned from specific incidents.

3 **Aligning and reengineering processes**
Integrating FxDR principles often requires rethinking workflows and protocols.
Focus on:

- Updating escalation protocols to prioritise real-time responses.
- Redefining team roles to align with FxDR's proactive approach.
- Ensuring continuous feedback loops between teams to refine strategies over time.

## 5. Moving forward with confidence

Integrating FxDR into your institution's fraud prevention strategy is a **journey**—one that requires commitment, collaboration, and adaptability.

By assessing your current systems, fostering cross-departmental alignment, selecting the right technology, and empowering teams with knowledge and resources, you can build a robust framework that not only addresses today's fraud challenges but also anticipates tomorrow's threats.