

XM Cyber Helps Leading Financial Services Provider Gain Real-Time Exposure Visibility



The Challenge

Red Team Limits and Privilege Leakage

A leading financial market infrastructure provider, responsible for completing trades, safeguarding assets, and other essential financial services across global capital markets, needed a clearer picture of its exposures.

"We realised that even though we spend a considerable amount of resources on security, Red Teams are still limited in time and scope," said Jo M., head of the organization's Offensive Security Center.

"We had limited knowledge of how privileges could leak in our environments," he added. This gap made it difficult to see how unnecessary or excessive access rights could be abused and how attackers might use them to move toward critical assets.

The Solution

Continuous Coverage and Actionable Findings

"XM enabled us to see how users are really interacting with our assets and how critical assets are linked to the rest of our network," Jo M. explained.

The real lightbulb moment was when the organization understood how XM Cyber connects isolated weaknesses into full attack paths, giving continuous visibility into how critical assets could be exposed. This eliminated guesswork. "It has removed the 'false positive?' question. You might see a weakness — an old account, a leaked password, an open port, a CVE — and be left guessing what it really means," Jo M. said. "XM Cyber takes that uncertainty away by showing how exposures interconnect across environments, giving you the full picture: user logins, network reachability, and privileges in a single pane of glass."

Collaboration improved as well. "We set up monthly technical boards where we gather people from IT and Operations and discuss the new findings. They can immediately see what is a real problem and what can wait."

Organization:

Financial Services

Number of Employees:

6000

Region:

Europe

One of the world's largest providers of domestic and cross-border settlement and related services for bonds, equities, derivatives and funds. This EU-based financial institution provides a wide range of services – from banking to insurance to settlements – and so much more.



"XM enabled us to see how users are really interacting with our assets and how critical assets are linked to the rest of our network."

"XM enabled us to see how users are really interacting with our assets and how critical assets are linked to the rest of our network."

Benefits and Outcomes

Zero False Positives and Effective Prioritization

XM Cyber delivered immediate value:

- **Real-time attack paths** – “After the tuning and distilling the data, we could find attack paths used by a Red Team in almost real time. This would typically take multiple days if this was done manually.”
- **Critical asset focus** – “With the Domain Accounts screen you can quickly identify which exposures are critical to fix based on the built-in prioritization mechanism.”
- **Support for incident response** – “It is invaluable for CIRT because when they get an alert they can know in a few seconds if they should panic or not.”
- **Peace of mind** – “The one key benefit is: Effective prioritization that still lets you sleep at night.”

Recommendation and Future Outlook

Focus on What Matters

Jo M. explained that defining critical assets makes XM Cyber even more effective. “If you identify your critical assets well, you can gain a real-time perspective on how an Advanced Persistent Threat (APT) may navigate through your network,” he said. That perspective helps the team direct resources to the exposures that matter most.

Summing up his experience, Jo M. added: “XM Cyber helps you focus on what matters and reduces the volume of exposures that need attention. It filters out the noise of low impact risk.”



“The real lightbulb moment was understanding how XM Cyber connects isolated weaknesses into full attack paths, giving continuous visibility into how critical assets could be exposed.”



“XM Cyber takes uncertainty away by showing how exposures interconnect across environments, giving you the full picture: user logins, network reachability, and privileges in a single pane of glass.”



“The one key benefit is: Effective prioritization that still lets you sleep at night.”



“It is invaluable for CIRT because when they get an alert they can know in a few seconds if they should panic or not.”



**Real-Time
Exposure Visibility**



**Zero False
Positives**



**Critical Asset
Prioritization**



**Incident
Response Insight**