XM Cyber

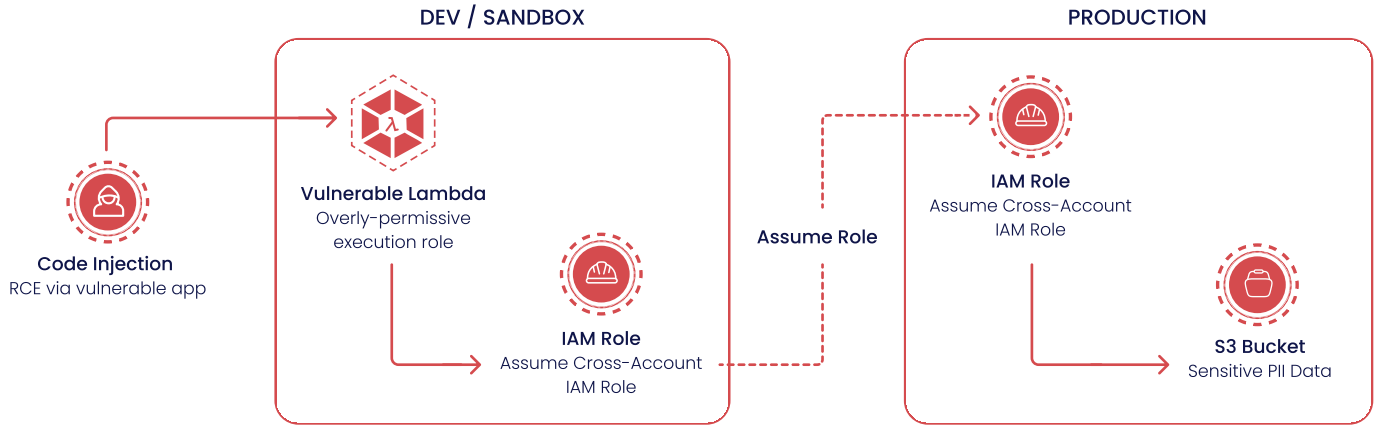
The Path to FinServ Resilience

3 Real-Life Attack Paths Identified By XM Cyber

In the financial sector, the prevailing thought is that a layered defense (defense-in-depth) equals security. But in truth, the perimeter is no longer a wall, but a filter. Despite significant investment in hybrid-cloud architecture, critical assets remain accessible through interconnected exposures. Here we'll look at three examples when XM Cyber identified these logical failures, how we broke the attack paths and cut off risk.

The Offshore Sandbox Failure

Hardening a "Sandbox" environment for a year is a futile exercise if the logical boundary between Dev and Production is permeable at the IAM layer.

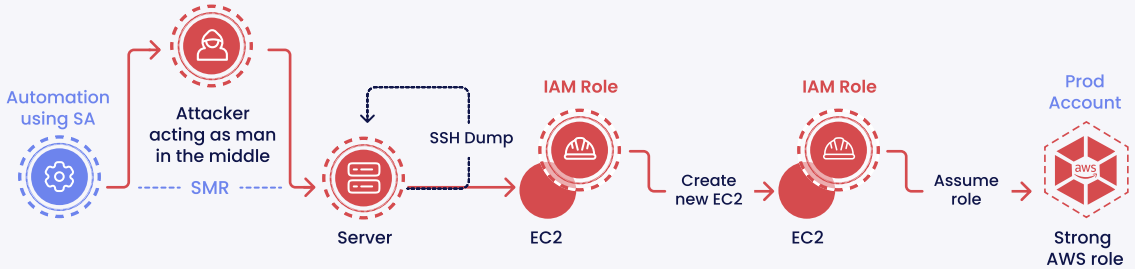


The Attack Path Breakdown:
An attacker identified an AWS Lambda function within a "hardened" sandbox environment configured with an overly permissive execution role. By abusing this role, the attacker "assumed" a cross-account IAM role. This role provided a direct bridge into the live production environment.

The XM Cyber Difference:
While traditional cloud posture tools flag individual misconfigurations, they often fail to visualize the interconnections that allow an attacker to move laterally between accounts. XM Cyber identified the trust relationship failure that linked the sandbox to the core, exposing a path that segmentation alone could not sever.

The Service Account "Domino Effect"

Automation increases efficiency but simultaneously expands the attack surface. In many banks, a single service account can be a single point of failure that can jeopardize the entire software supply chain.

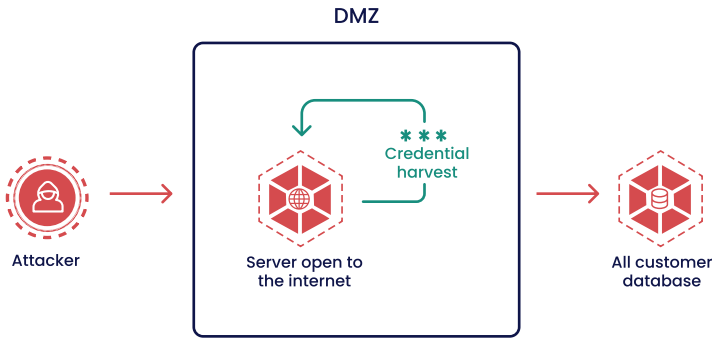


The Attack Path Breakdown:
The attacker identified an automated process and executed a Man-in-the-Middle (MitM) attack to capture a service account's authentication token and access a workstation containing unprotected private SSH keys. These keys allowed the attacker to spin up a Shadow EC2 instance to evade monitoring.

The XM Cyber Difference:
The logical gap here is the assumption that service accounts are "low risk" because they are non-human. We mapped the sequence from an on-prem port to a cloud-based supply chain compromise, demonstrating how a minor oversight in local permissions leads to a systemic breach.

The "DMZ-to-Domain" Express

A DMZ (Demilitarized Zone) can provide a false sense of security if the assets within it are joined to the primary domain.



The Attack Path Breakdown:
An attacker identified a Windows server in the DMZ with an internet-facing vulnerability. A Domain Admin had recently logged in to troubleshoot an issue, leaving high-privilege credentials cached in the system's memory. The attacker compromised the server and utilized LSASS memory dumping to extract those credentials.

The XM Cyber Difference:
Compliance checklists mandate a DMZ, but they rarely account for the corner-cutting administrative login that leaves behind the keys to the kingdom. XM Cyber identified the presence of these credentials on an exposed asset, closing a path that no patch-management tool would have flagged.