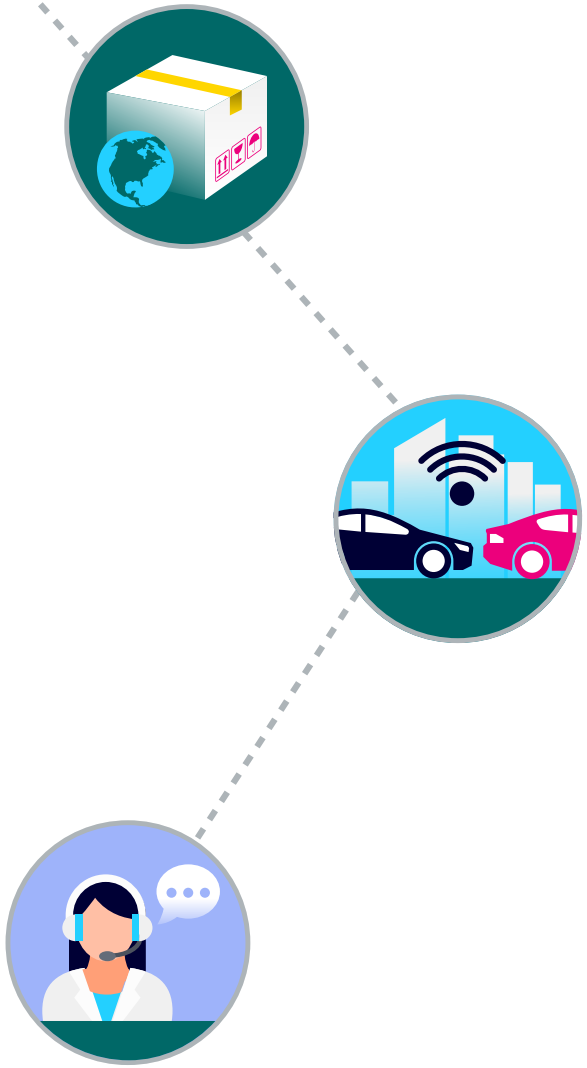
XM Cyber

Guide

Breaking Attack Paths to Legacy and OT Systems



Legacy & OT Systems Hit Different

The convergence of IT, Operational Technology (OT), and legacy systems introduces complexities and risk. IT networks, designed for scalability and accessibility, are increasingly connected to OT systems, which prioritize reliability and uptime. Legacy systems, designed without modern cybersecurity controls or even a consideration for internet connectivity, compound the challenge by exposing outdated protocols and unpatched vulnerabilities.

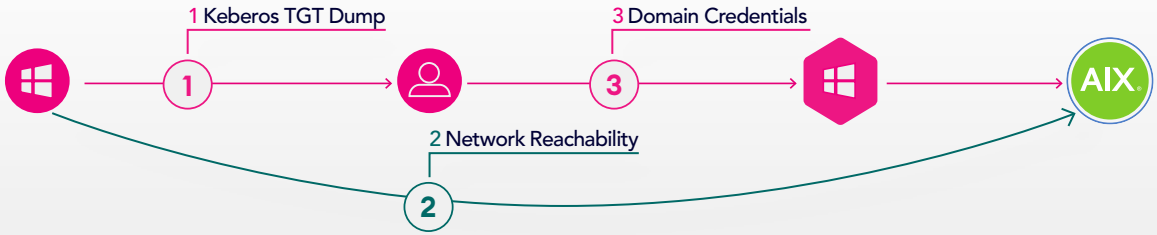
These factors create exploitable paths for attackers, who can pivot from modern IT environments into legacy systems or OT networks, potentially causing operational disruptions, financial losses, and even risks to physical safety.

Breaking these attack paths is critical to safeguarding hybrid ecosystems. This document, the companion to the How Attackers (Really) Advance: Unveiling 11 Real-Life Stories, focuses on attacks targeting OT and legacy systems. By proactively securing the pathways between these networks, organizations can reduce the likelihood of compromise, protect critical assets, and maintain operational continuity. Understanding and mitigating the unique cyber risk at the IT/OT/legacy system intersection is an integral piece of your enterprise-wide cybersecurity strategy.

Read on for more about Legacy and OT Risks to business operations.

Applying Modern Cybersecurity Approaches to Old Time Platforms

Yaara Shichman, Platform Product Director



Who was the customer?

A provider of administrative support, document management, payroll, and customer service solutions.

What was the scenario?

The customer relies on AIX machines to host databases and applications that interface with their more modern infrastructure. Due to the cost, complexity, and potential for service disruptions, the customer has maintained these legacy systems despite the operational and security challenges.

What was the attack path?

While there was no compelling event that forced the project, they knew the system's age and connectivity required meant elevated risk. There were no patches for vulnerabilities, nor could they deploy an EDR agent. Their current plan included manual security workarounds and processes that added complexity, reduced open access to data, and slowed operations.

What was the impact?

The AIX machines contain sensitive customer data including insurance details and payroll information protected by multiple compliance regulations. Any downtime would have a significant impact to business operations, directly impact thousands of customers, and subject the organization to fines or sanctions.

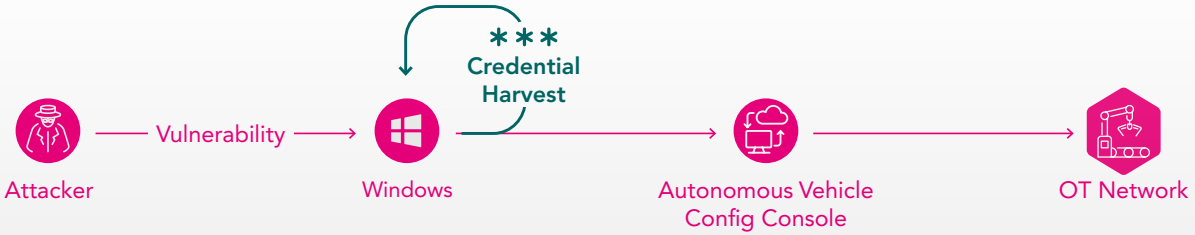
How was it remediated?

Working together with XM Cyber, the customer identified legacy machines and built attack scenarios that showed how an attacker could access the AIX environment. By prioritizing and remediating the exposures and chokepoints (where multiple attack paths converged) that led to the AIX machines, the organization broke the attack path.

"Any downtime would directly impact thousands of customers..."

Bridging From a Digital Credential Theft to Physical Goods Theft

Bill Bradley, Sr Director Product Marketing



Who was the customer?

A consumer packaged goods company that manufactures and distributes household and personal care products.

What was the scenario?

As part of their digitization, automation, and plant safety initiatives, autonomous pallet trucks moved raw materials and finished goods throughout the plant. These vehicles connected to the traditional IT network for routing instructions.

What was the attack path?

Through an Active Directory misconfiguration, a regular employee account could laterally move through Active Directory and escalate his or her privileges to become an Account Operator. This privilege allowed the employee to take over devices in the organization by running a Resource-Based Constrained Delegation Attack on a Secured Zone Server. On that Server, strong Service Account Credentials were cached and not secured, allowing access to the OT Jump Host. From that OT Jump Host, the employee could exploit a vulnerability on an HMI device, which led to the impact on delivery of the finished goods.

What was the impact?

The compromised truck brought the finished goods to a remote plant location where a vehicle was waiting to offload them. The employee then sold the goods on the black market.

"The employee then sold the goods on the black market."

How was it remediated?

XM Cyber showed the attack path to the critical asset in the digital twin. The employee linked AD misconfigurations, identity issues, and unpatched vulnerabilities to compromise the OT device. With this detailed attack path SecOps could mobilize the needed resources to resolve the immediate risk and break the path for future attacks.

Driverless (and Dangerous) Vehicles are Coming!

Tobi Traebing, Director of Sales Engineering & Field CTO, EMEA

Who was the customer?
A large manufacturer in EMEA.

What was the scenario?
They had a vulnerability management solution in place, some hardening done, but were overwhelmed by the sheer amount of work. As in any industrial setting, heavy goods were being transported from place to place and they used unmanned vehicles to transfer the goods. We were having a POC with them.

What was the attack path?
This deployment included a server responsible for controlling uncrewed/unmanned vehicles that were transporting goods in the factory.

We located an attack path that would allow an attacker to gain control of the vehicles using a software vulnerability that could be exploited from asset #1 to asset #2. Then the attacker would be able to harvest credentials to compromise User A. Lastly, the compromised user could be used to login on to the critical asset.

What was the impact?
If an attacker got access, they'd be able to gain control of the vehicles and cause physical harm and damage – that means IT Security could have a direct impact on the safety of personnel.

How was it remediated?
They quickly realized that they needed to get a deeper understanding of their networks and created plans to onboard attack path modeling tools.

"If an attacker got access, they'd be able to gain control of the vehicles and cause physical harm and damage."

Getting Along with Legacy and OT Systems

Legacy and OT systems are a part of your organization today and for the foreseeable future. As a security or IT leader your teams need to adopt modern and proactive approaches to reduce the risk of these platforms to your enterprise. Understanding the attack paths that lead to these systems is the first step in breaking the chain.

XM Cyber, the leader in Continuous Threat Exposure Management (CTEM), lets you visualize how exposures can lead to critical assets and systems like OT and legacy systems. By prioritizing these you're able to better defend your business from attacks.

Want to read more about attacks targeting IT systems?
Click here to read more: How Attackers (Really) Advance: Unveiling 11 Real-Life Stories

XM Cyber

XM Cyber is a leading Continuous Exposure Management company that transforms the way organizations approach cyber risk, enabling security teams to prevent more attacks with 75% less remediation effort. Its XM Attack Graph Analysis™ capability discovers CVEs, misconfigurations, and identity issues across on-premise and all major cloud environments. It analyzes how attackers can chain exposures together to reach critical assets, identifies key "choke points", and provides remediation guidance. Founded by top executives from the Israeli cyber intelligence community, XM Cyber has offices in North America, Europe, APAC-Japan, and Israel.