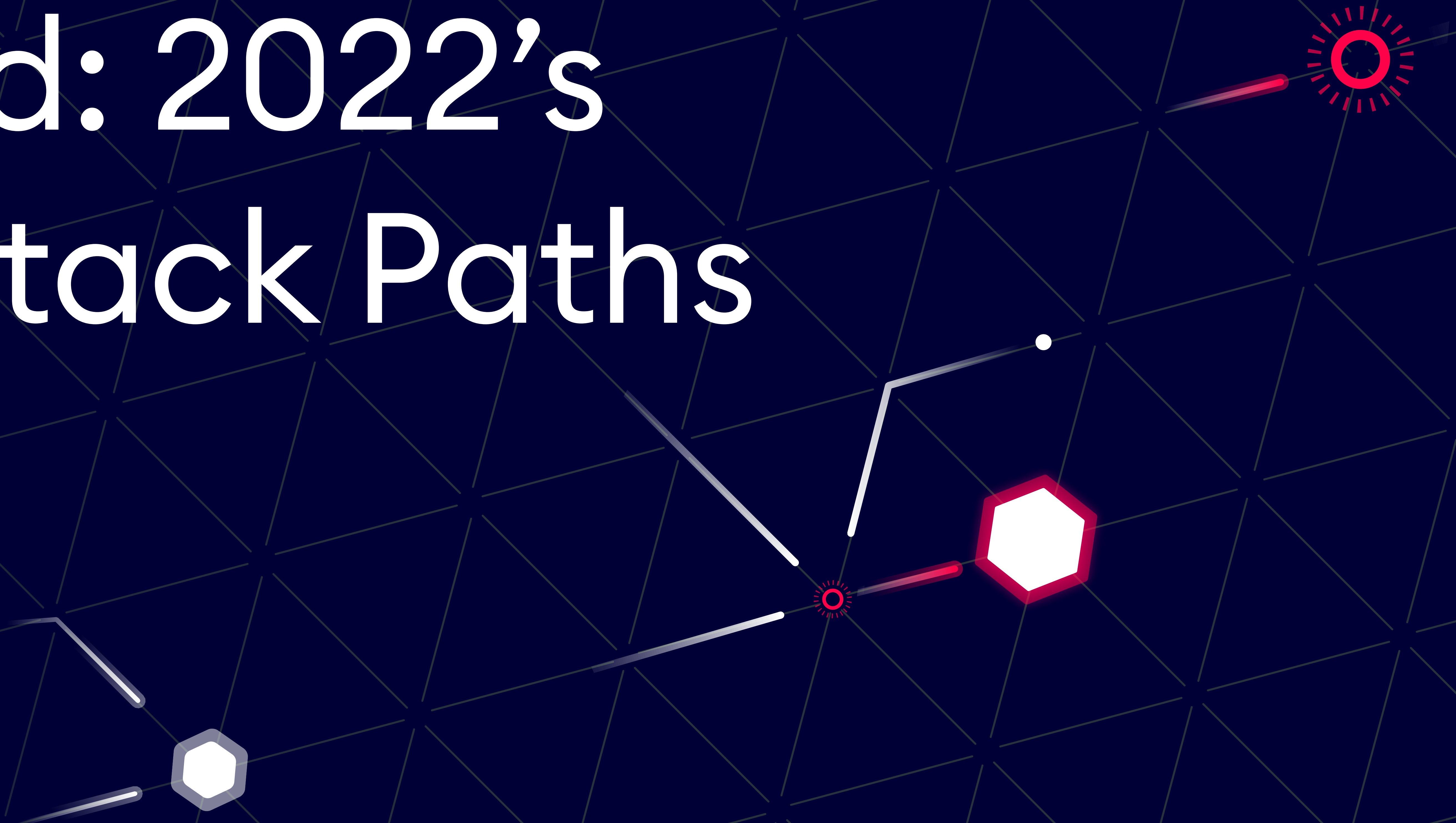
XM Cyber | See All Ways™

What We Found: 2022's Most Potent Attack Paths



Contents

Introduction

Attackers don't think like you do.

They're looking for ways to bypass your security controls and take advantage of various exposures that exist in your environment. They're not just looking for vulnerabilities, they're on the hunt for a combination of exposures and attack techniques that could help them reach their target.

But what happens once they get their initial foothold?

Well, that depends on the exploitable attack paths available to them. An attack path is a visual representation of the string of vulnerabilities, CVEs, misconfigurations, overly permissive roles, behaviors, and more, that when combined, can be used to exploit security gaps within systems and networks.

Identities	Vulnerabilities	Misconfigurations	Compliance and security controls	Active Directory
Member of the wrong group	ZeroLogon CVE-2020-1472	Public S3 bucket	CIS controls	Member of group
Excessive permissions	PrintNightmare CVE-2021-34527	Access control	ISO 27001	Add Logon Script
Cached credentials	Log4j CVE-2021-44228	Public storage account	NIST Framework	DC sync

Organizations typically have lots of security tools in use, but these tools overwhelm teams for two important reasons: they don't enable any level of prioritization, leaving security professionals in the dark when it comes to discerning which issues should be dealt with first and which can wait. Moreover, they are lacking context – they fail to provide an understanding of how issues combine with others and how they can lead an attacker to a critical business asset.

This lack of knowing what matters most can lead organizations to try to fix it all – or more likely, fix nothing at all.

In this ebook, we will take you through the 11 most potent real-life attack path scenarios our in-house experts found in customers' hybrid environments using XM Cyber's Exposure Management Platform over the course of 2022.

Some of the attack paths are complex, with critical assets only being reached via many complicated hops; some are scarily simple, wherein critical assets are reachable in two to three steps. In fact, our in house research shows that 75% of an organization's critical assets can be compromised in their current security state. And of those, 94% of critical assets can be compromised in four hops or less from the initial breach point. This variation demonstrates the unique and dynamic nature of attack paths, and how hard it can be to anticipate them and head them off without the right tool set.

So now, without further ado, let's allow the experts and their stories to speak for themselves.

The Shipping M&A vs The ZeroLogon Patch That Didn't Update

Rinat Villeval, Manager of Technical Enablement

Who was the customer?

A large shipping company that had just bought three different companies; one in the USA, one in Asia, and one in South Africa.

What was the scenario?

Routine customer call.

What was the attack path?

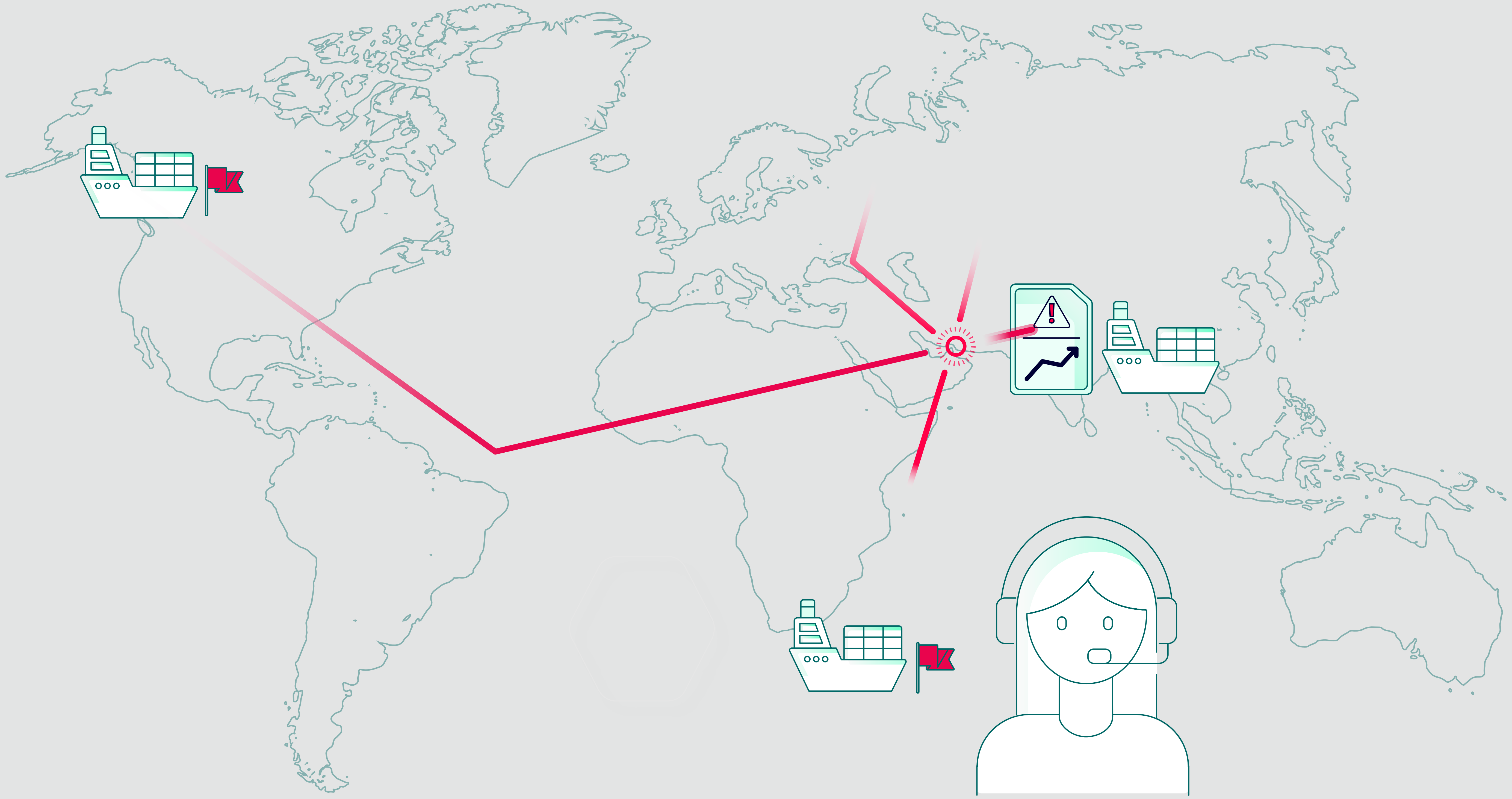
We showed them the Active Directory located in Asia had a high risk score, and could be **compromised in just two steps.** It turned out that the **ZeroLogon patch was missing** because though they had patched it, it did not reboot. In fact, their vulnerability scanner said it was safe but **it hadn't been applied and the DLL version was still the previous one.** The outbound attack path from that remote active directory was compromising all the other active directories in the organization, as trust had already been established as part of the M&A process.

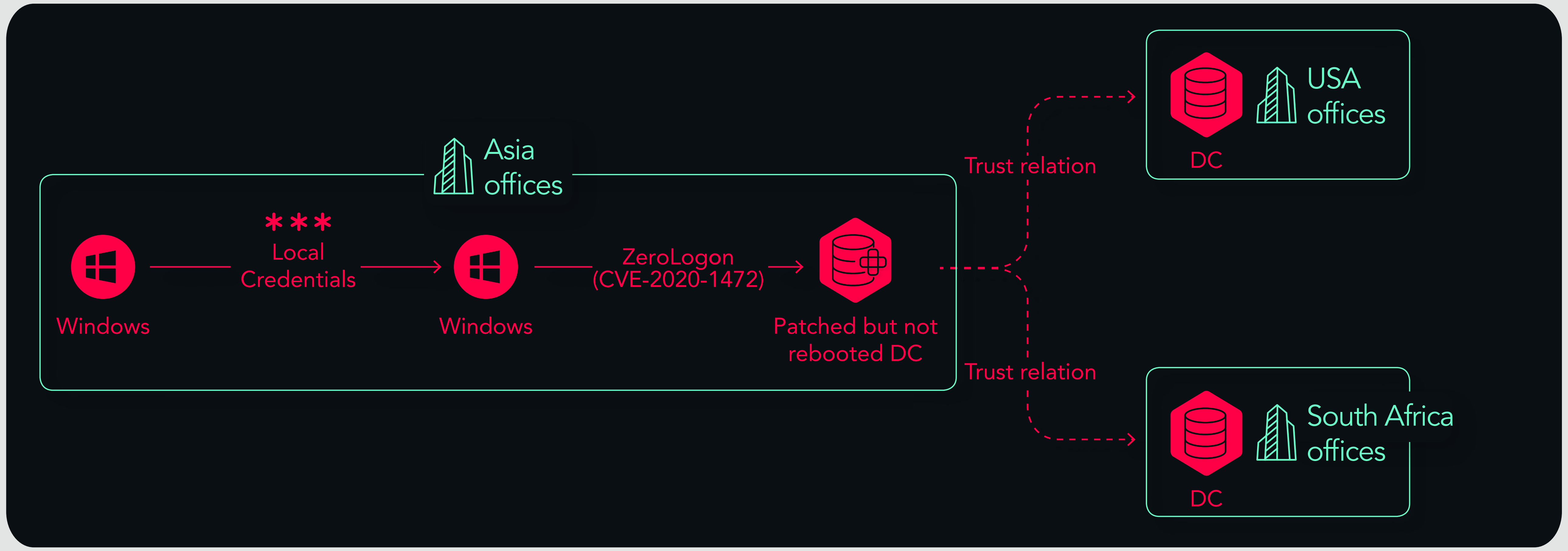
What was the impact?

Any attacker could have easily compromised the entire Active Directory Forest, leading from one company to all others.

How was it remediated?

Amazingly, a small fix was able to reduce a big exposure. All they had to do was reboot the active directory and then the DLL version was updated.





Asia offices

Windows

***
Local Credentials

Windows

ZeroLogon (CVE-2020-1472)

Patched but not rebooted DC

Trust relation

USA offices

DC

Trust relation

South Africa offices

DC

The Man-in-the Middle at The Financial Company

Paul Giorgi, Director of Sales Engineering

Who was the customer?

A large **financial service**.

What was the scenario?

Routine customer call.

What was the attack path?

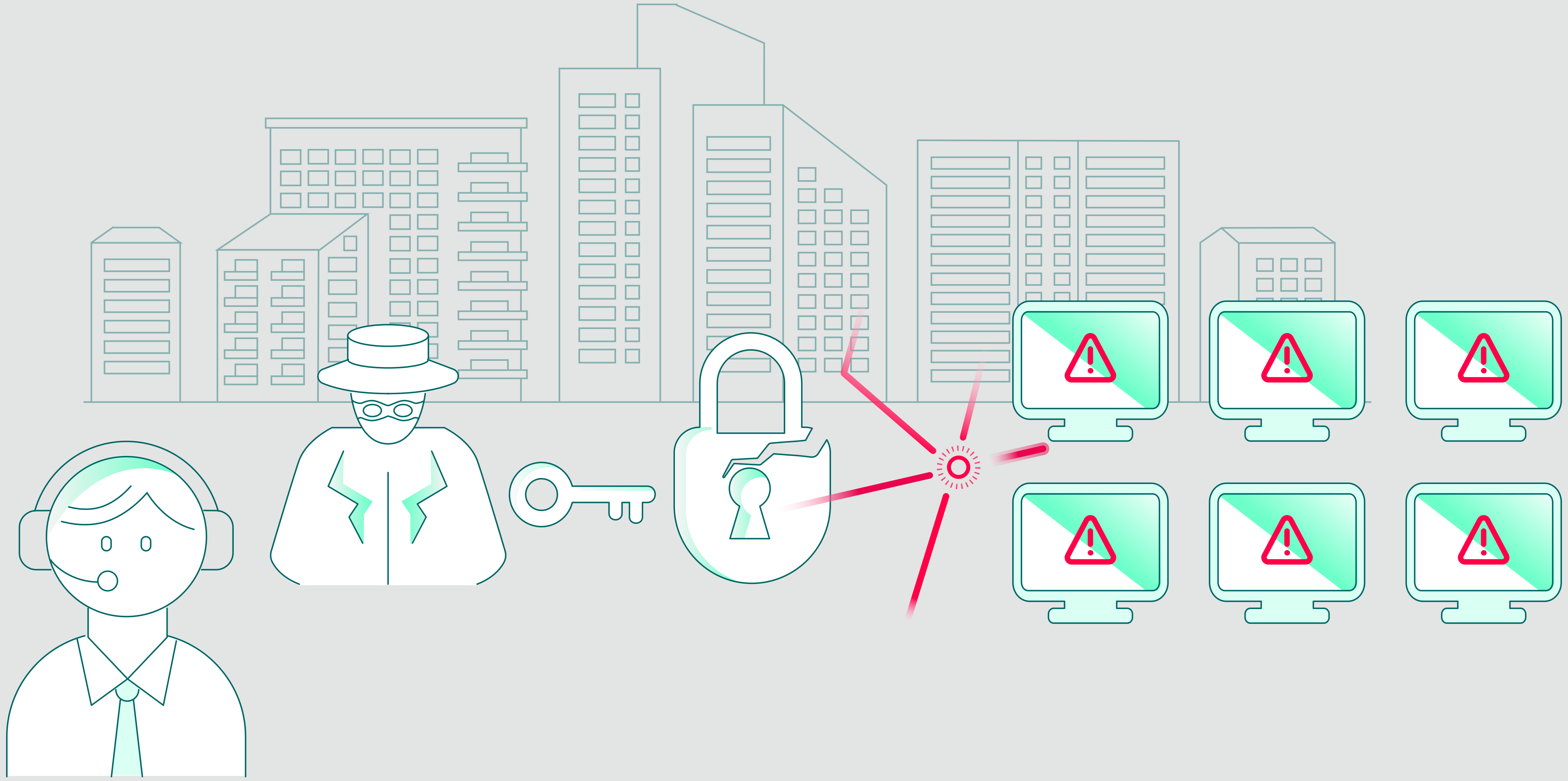
A small subset of machines was sending out **DHCP v6 broadcasts**, enabling an attacker to position themselves as a **Man-in-the-Middle** to exploit a Windows update vulnerability on that system. One of those systems was a developer's machine with **several private SSH keys unprotected in their downloads folders.** Using those SSH keys, **an attacker would've been able to easily compromise around 200 Linux systems** within their on-premise datacenter and in their cloud environment.

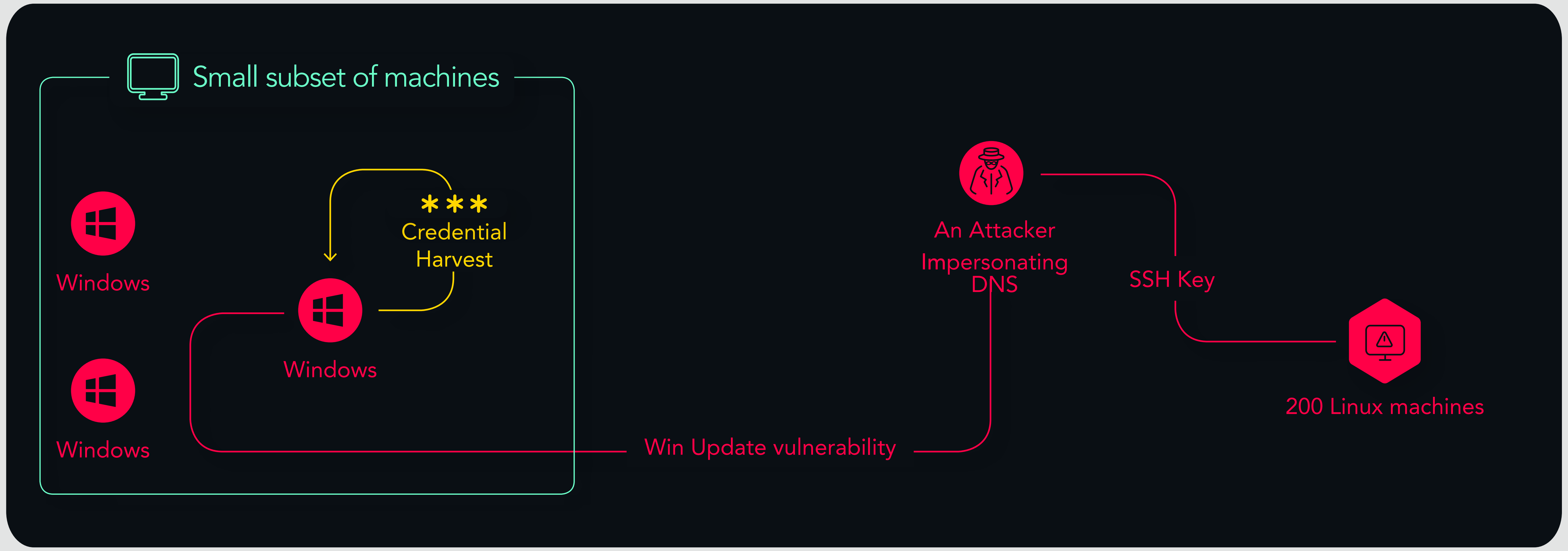
What was the impact?

This could have allowed a large majority of their Linux servers to be compromised. From those systems, the attacker could have carried out additional attacks, encrypted systems/data for ransom, or exfiltrated data.

How was it remediated?

By disabling DHCPv6 and patching the developer's machine, both the vulnerability and misconfiguration were addressed. It was also a good time to review best practices with the developers to make them aware of the SSH keys putting their Linux systems at risk, to limit future risk.





Small subset of machines

Windows

Windows

Windows

***

Credential Harvest

Win Update vulnerability

An Attacker Impersonating DNS

SSH Key

200 Linux machines

The PrintNightmare Nightmare

Matt Quinn, Technical Director

Who was the customer?

A large travel company.

What was the scenario?

They had just merged with another company in the same industry and brought their infrastructure across.

What was the attack path?

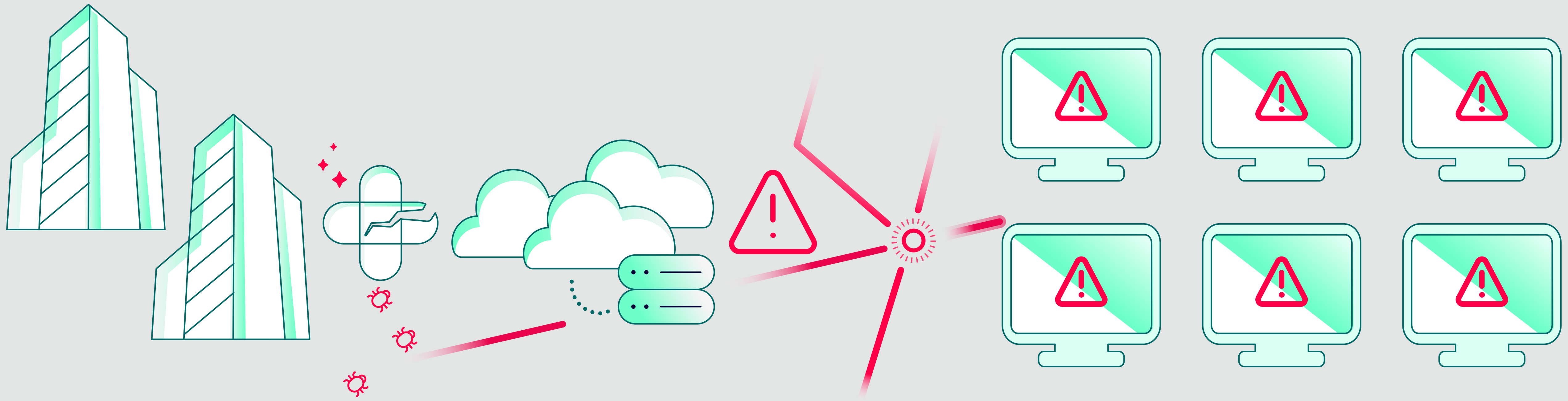
They had a server for product testing which was always running and wasn't particularly important. They thought they were patching, but in reality, **patches had not been applied correctly** since 2017! So they had a huge list of vulnerabilities on the server, including PrintNightmare and EternalBlue. And while an attack could compromise this unimportant server, it would have provided a path to move on to MUCH more important ones.

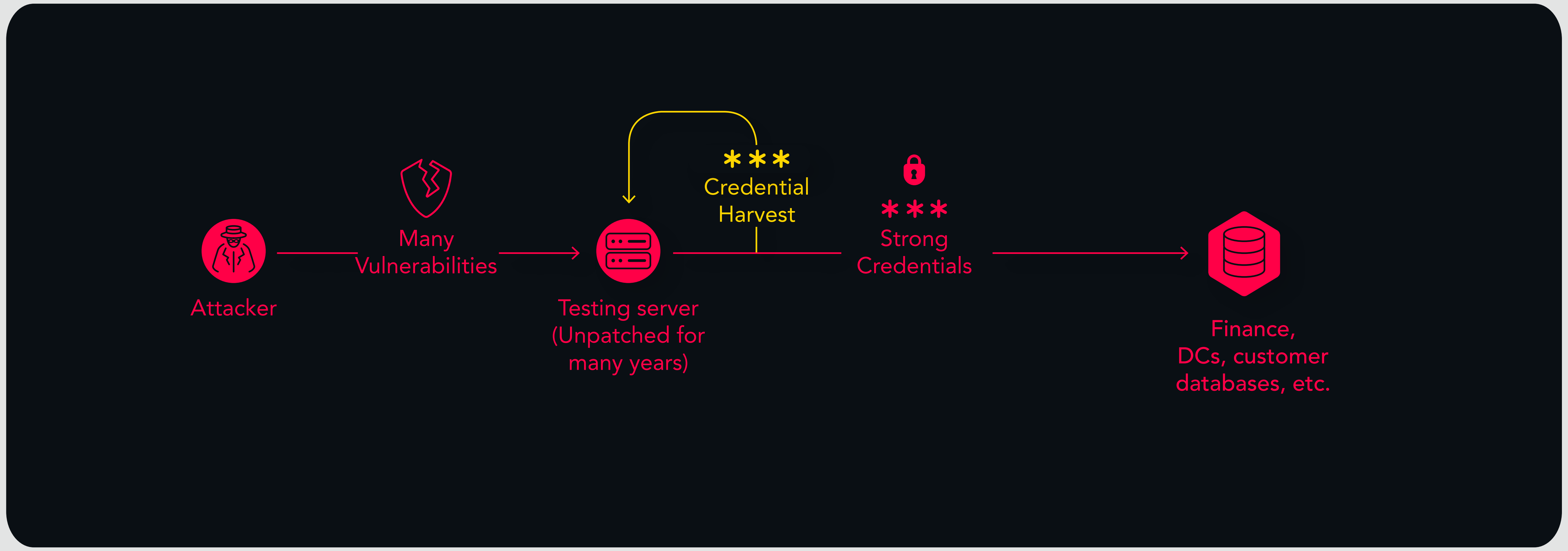
What was the impact?

When they actually looked at the server, they realized they didn't even need it – so they just turned it off!

How was it remediated?

Simply turning it off had a huge impact on reducing risk to the rest of the environment.





Attacker

Many Vulnerabilities

Testing server (Unpatched for many years)

*** Credential Harvest

*** Strong Credentials

Finance, DCs, customer databases, etc.

The Bank and The Complicated – Yet Plausible and Potent – Attack Path

Shahar Solomon, Customer Success Team Leader

Who was the customer?

A global financial institution.

What was the scenario?

Routine customer call.

What was the attack path?

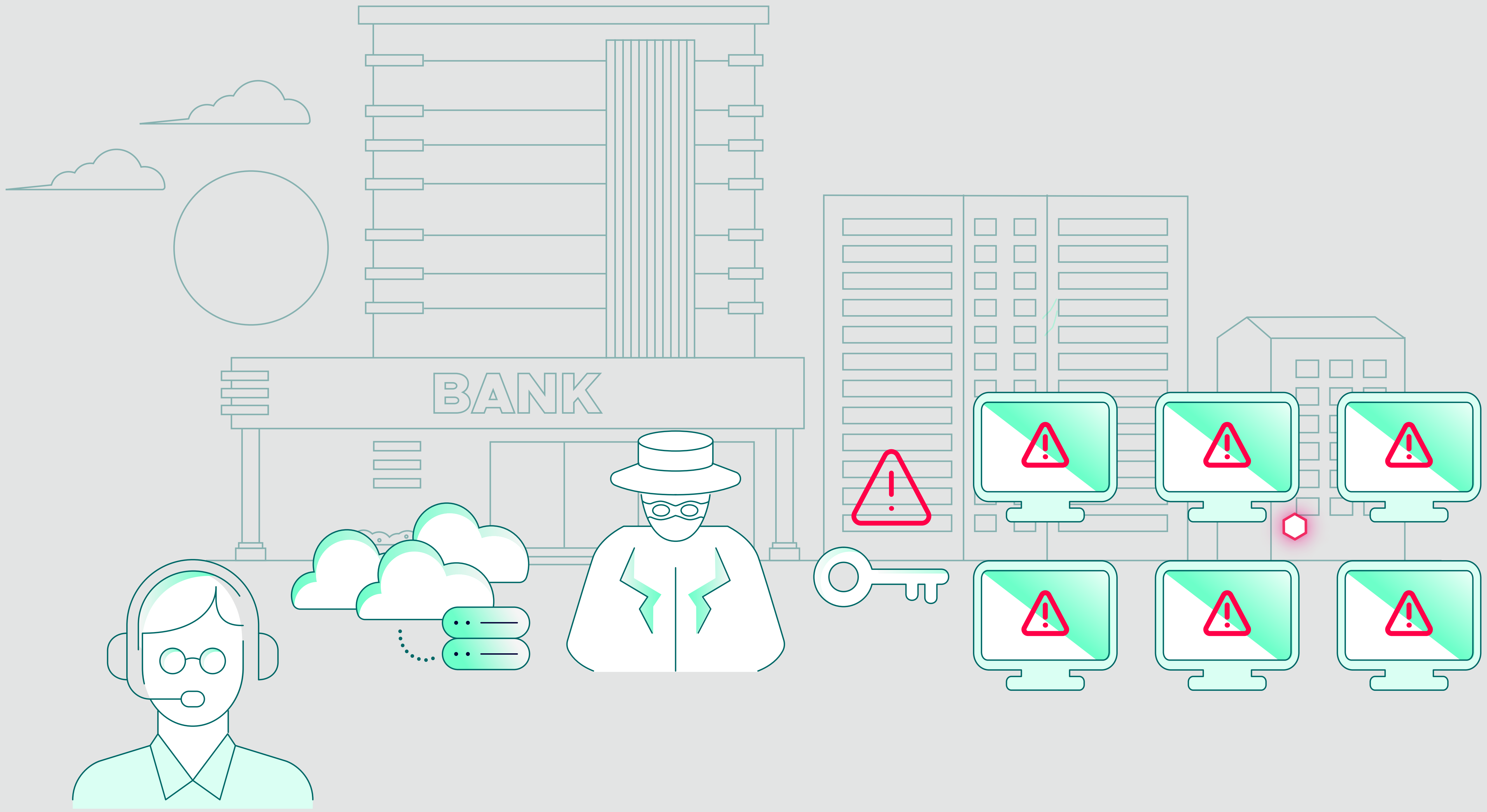
We identified an **automation using a service account** which had initiated an action based on SMB port. This could **risk credentials** from this service account to be used for a **Man-in-the-Middle** attack inside **the network, which would allow an attacker to laterally move to another device/ workstation** in the network. Next, we found **SSH private keys to a server running on an EC2 instance (AWS).** Attached to this EC2 was an IAM role, and using its permissions it was possible to **spin up a new EC2**. Finally, this could be used to compromise one of **their most critical assets**, used for deployment in the customer environment.

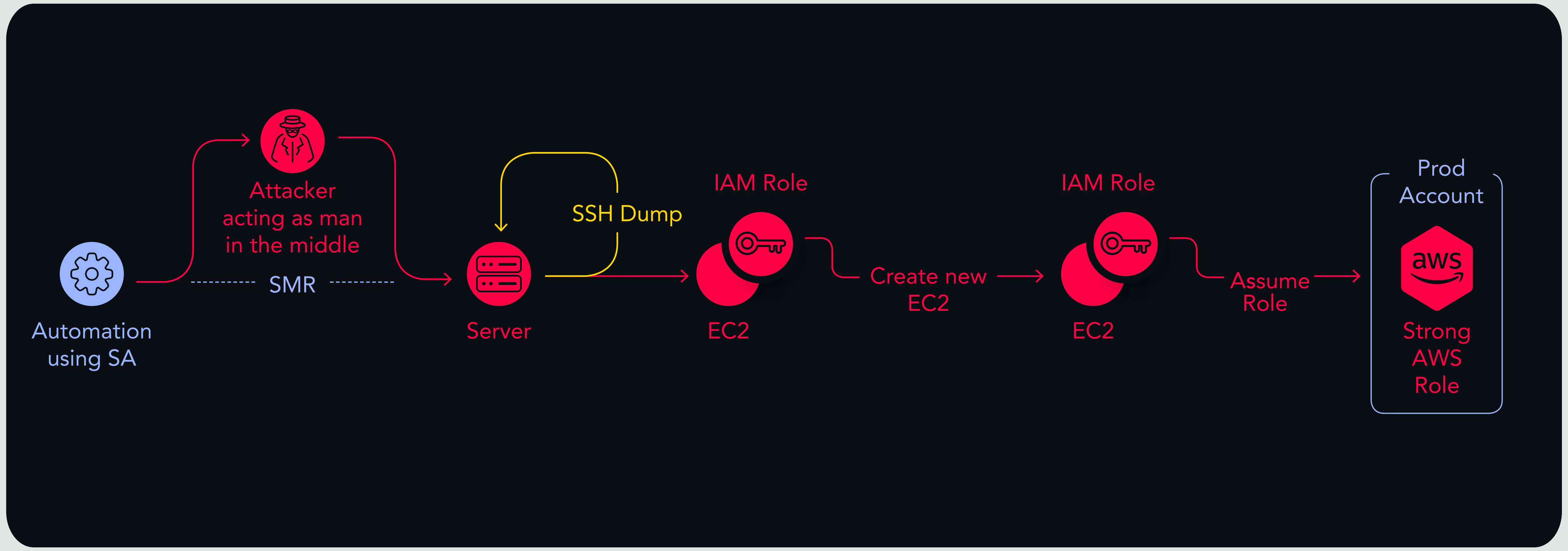
What was the impact?

Although it's a bit of a complex path, it's very potent – and if the wrong entities were to locate it, it could be a disaster.

How was it remediated?

They immediately remediated each part of the attack path by removing private SSH keys, resetting IAM role permissions, and removing specific users.





This is Why Nobody Takes the Bus Anymore

Konrad Haag, Customer Success Manager

Who was the customer?

A public transportation company.

What was the scenario?

They had recently onboarded to the system and we were having a meeting to get them set up.

What was the attack path?

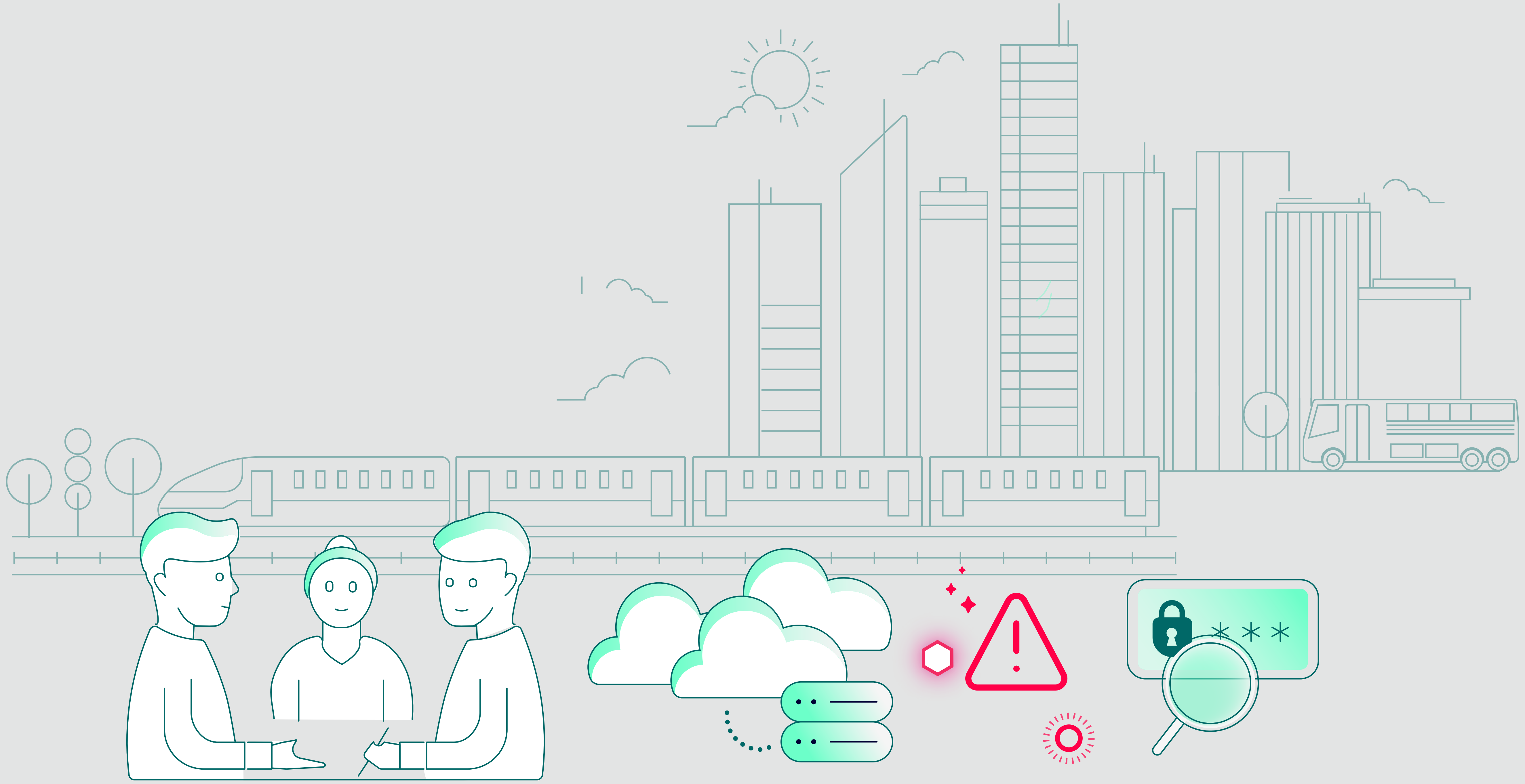
We uncovered an **open path from a DMZ server** (directly reachable over the internet), that could directly lead to the domain compromise. The DMZ server is a Windows server, which **was joined to the customer's Windows domain** and administered with a domain admin account.

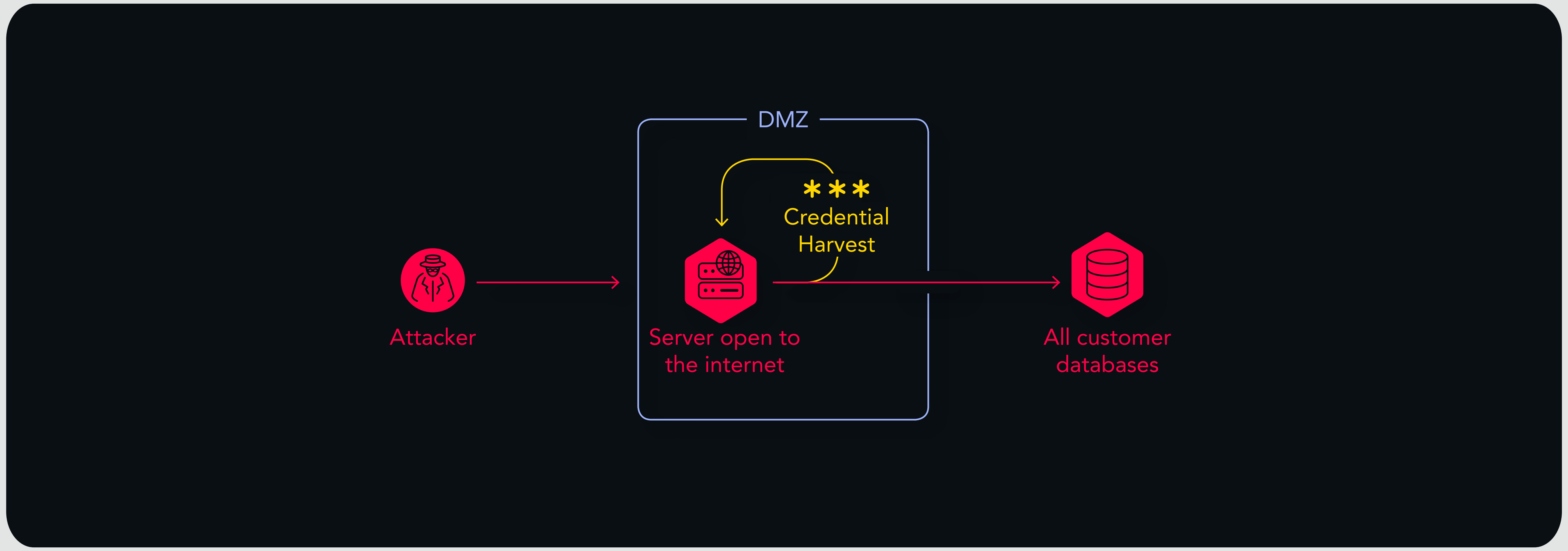
What was the impact?

If the DMZ server were to be compromised, the attacker could directly harvest domain admin credentials and connect to the domain controller with all permissions.

How was it remediated?

They fixed the issue by restricting permissions and removing users.





The Hospital Where Active Directory Was Making it Sick

Shira Bendkowski, Director of Product Management

Who was the customer?

A hospital that has very good security hygiene and cares deeply about ensuring best practices.

What was the scenario?

Routine customer call.

What was the attack path?

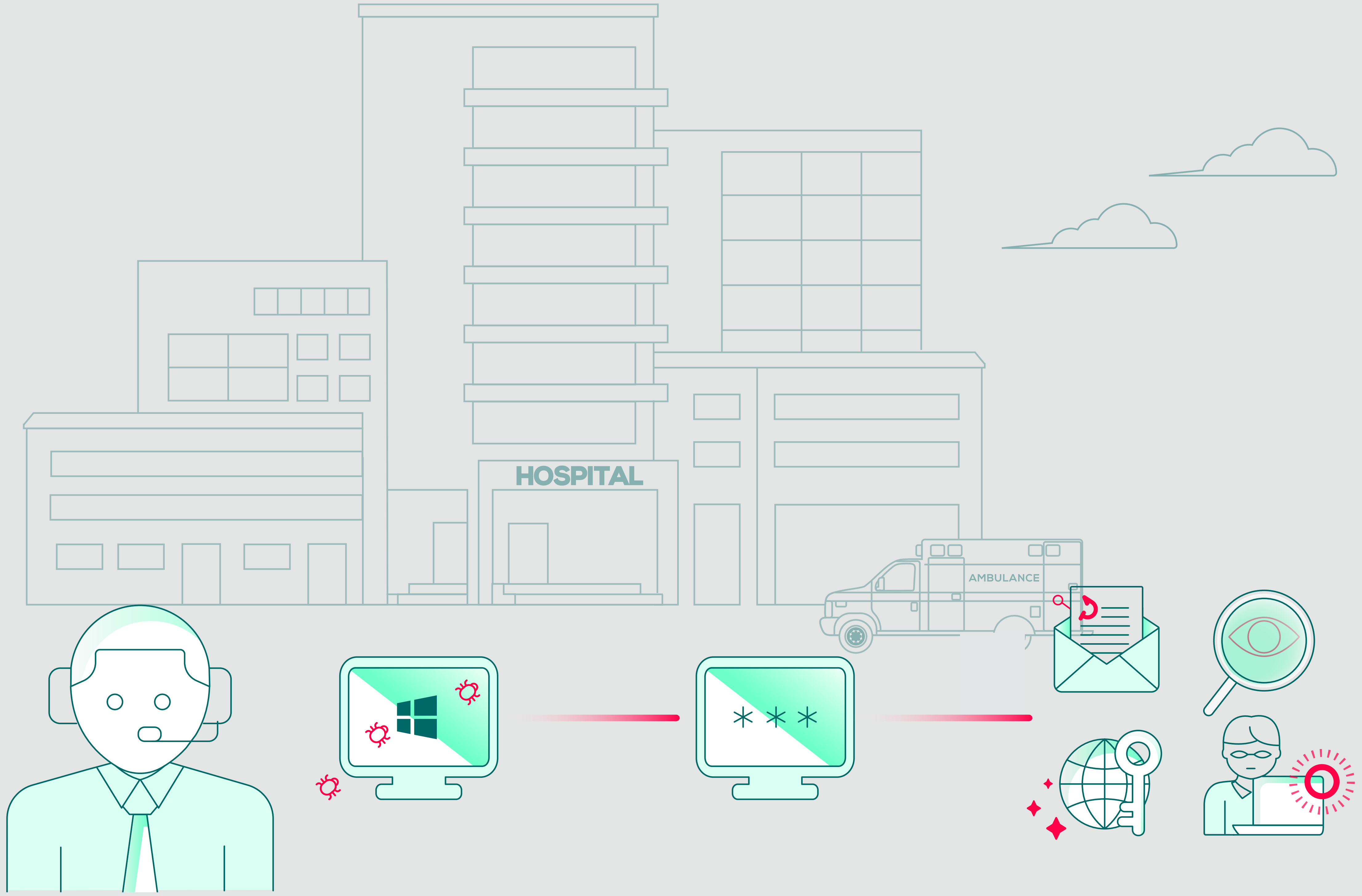
Despite the fact that security really is of prime importance, their active directory was another story. Inside their active directory, **all authenticated users (basically any user) in the domain had been erroneously granted the right to reset passwords!**

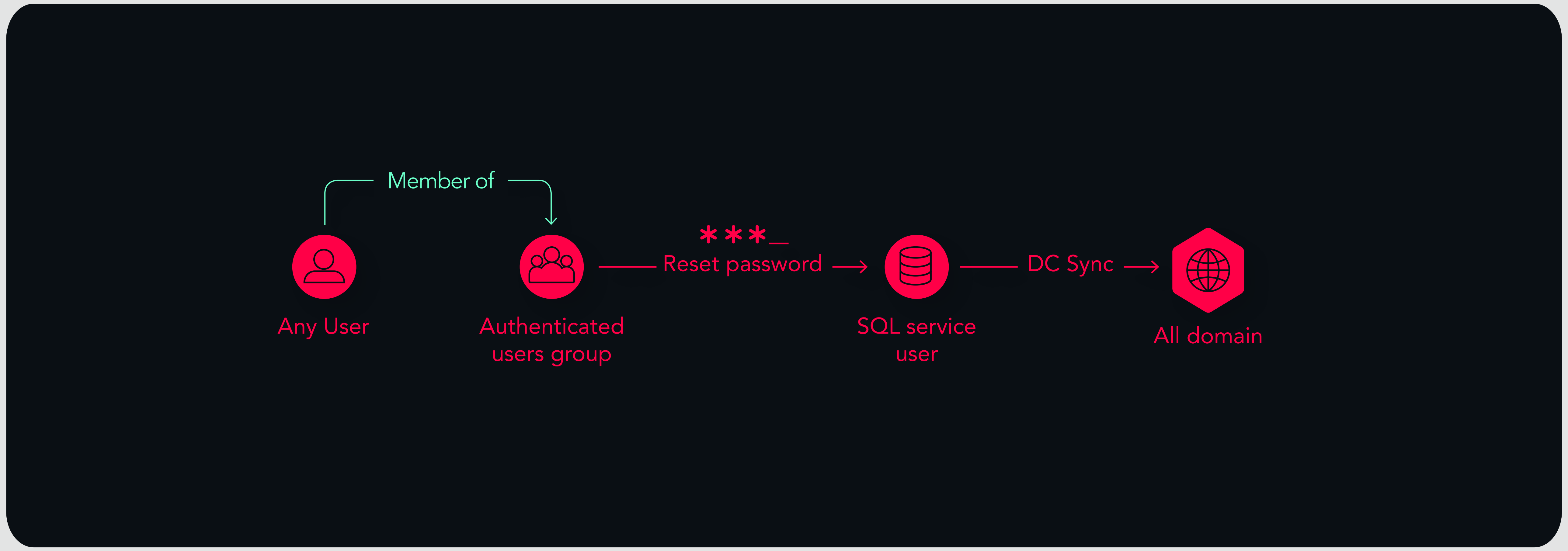
What was the impact?

So if an attacker took over one active directory user via phishing or other social engineering techniques, they could then reset any passwords for other users and take over any account in the domain.

How was it remediated?

They locked down and hardened their active directory security practices and put a remediation plan into place which covers analysis of critical assets at risk, their choke points, and the attack techniques that could be leveraged.





That Time the Financial Giant Thought the Patch was Deployed, But ...

Boaz Gorodissky, CTO & Co-Founder

Who was the customer?

A major player in the financial services industry.

What was the scenario?

Routine customer call.

What was the attack path?

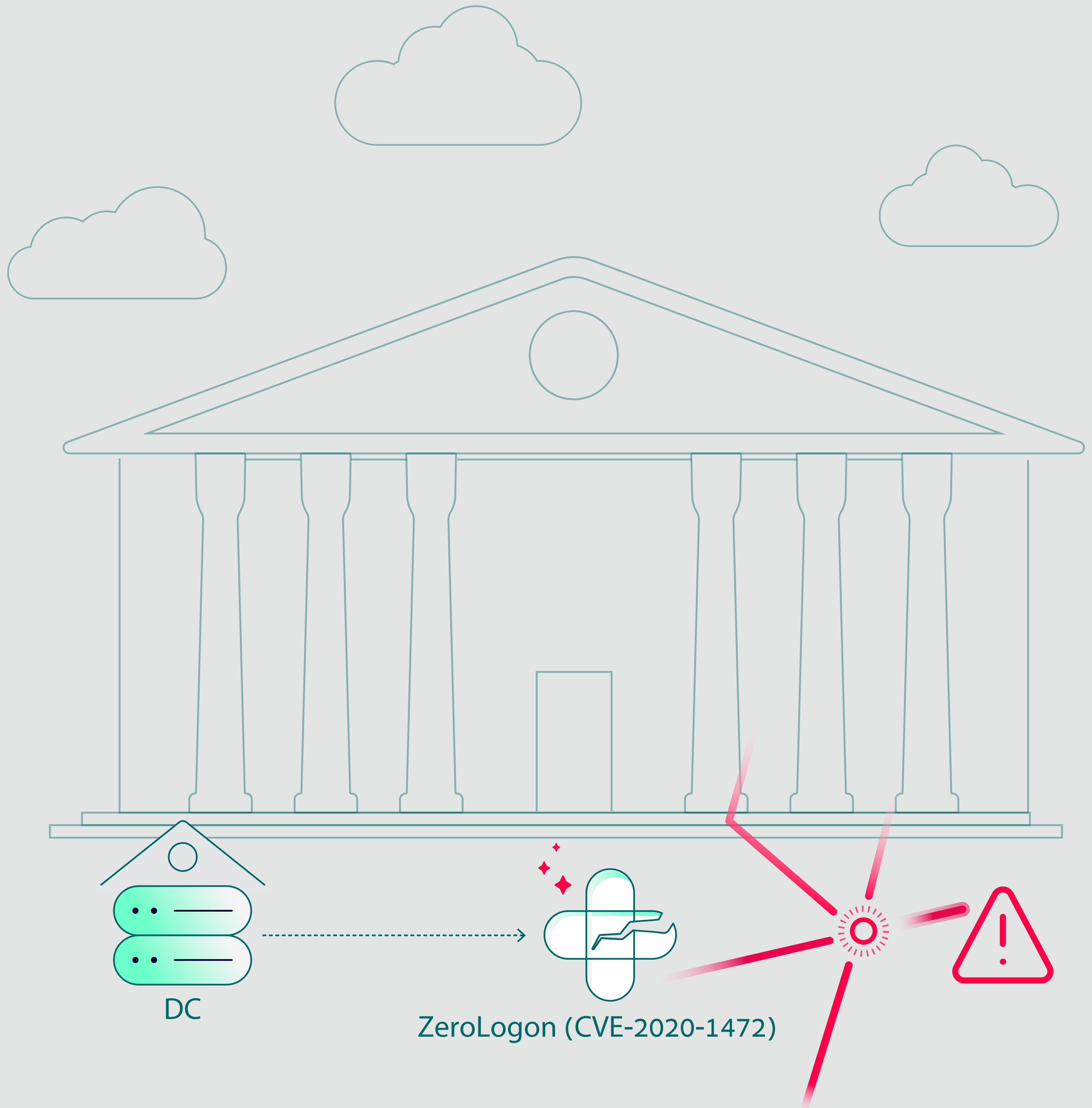
As part of Patch Tuesday, they had **tried to patch all servers using SCCM.** This included the patch for the **ZeroLogon (CVE-2020-1472)** vulnerability on the domain controllers. The domain controllers are very sensitive and mission critical, so **not all were rebooted after the patch update**.

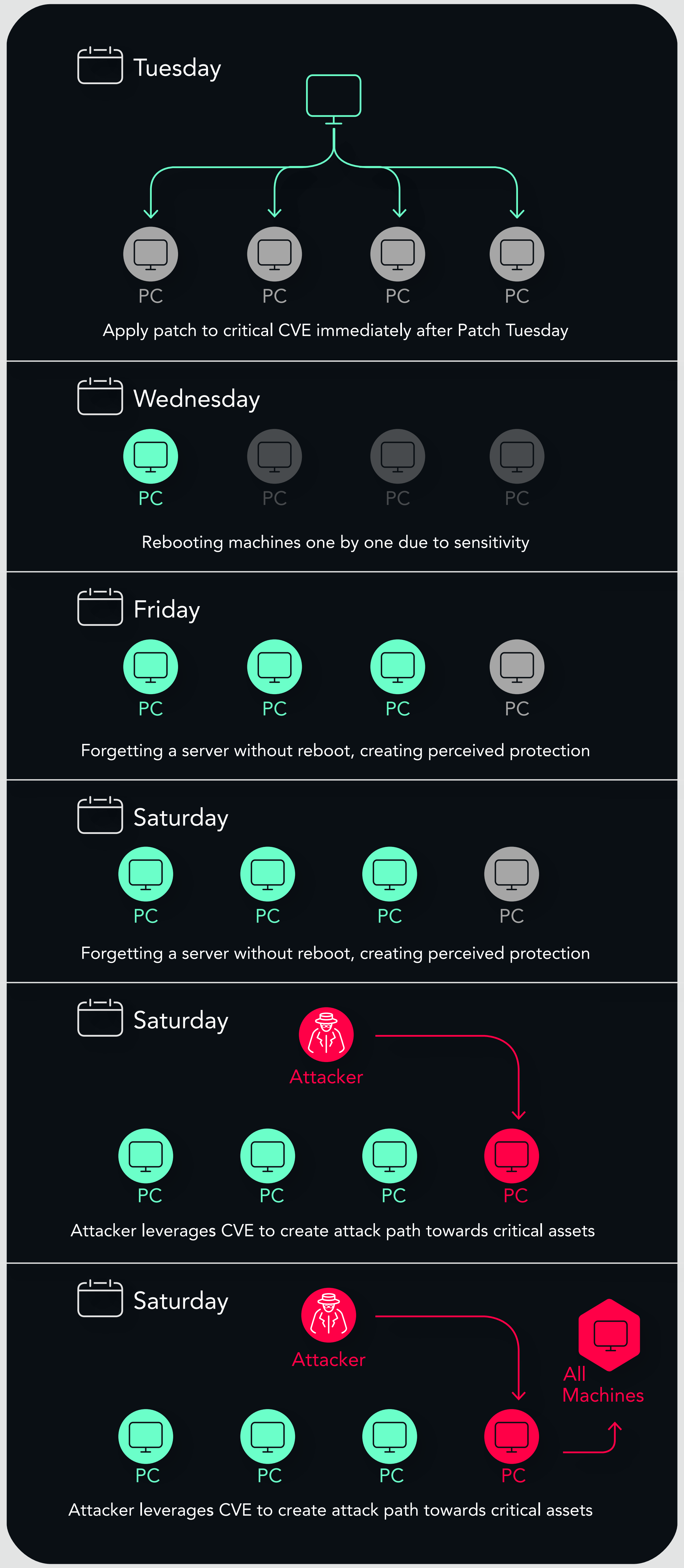
What was the impact?

Essentially, the patch was deployed but not installed, leaving an open avenue that attackers could use to compromise the domain controllers.

How was it remediated?

As soon as we showed them the issue, they changed their procedures to ensure that in the future, they'll never forget to reboot after patching.





Apply patch to critical CVE immediately after Patch Tuesday

Rebooting machines one by one due to sensitivity

Forgetting a server without reboot, creating perceived protection

Forgetting a server without reboot, creating perceived protection

Attacker leverages CVE to create attack path towards critical assets

Attacker leverages CVE to create attack path towards critical assets

The Healthcare Provider Where Anyone Could be a Domain Admin

Gali Rahamim, Customer Success Manager

Who was the customer?

A large healthcare provider.

What was the scenario?

Routine customer call.

What was the attack path?

The Authenticated Users group is a built-in (predefined) Windows group that **includes all users whose identities were authenticated when they logged on.** We found an attack path using the authenticated users group with permissions to **change the GPO policy's gPCFileSysPath to a path with malicious policies.**

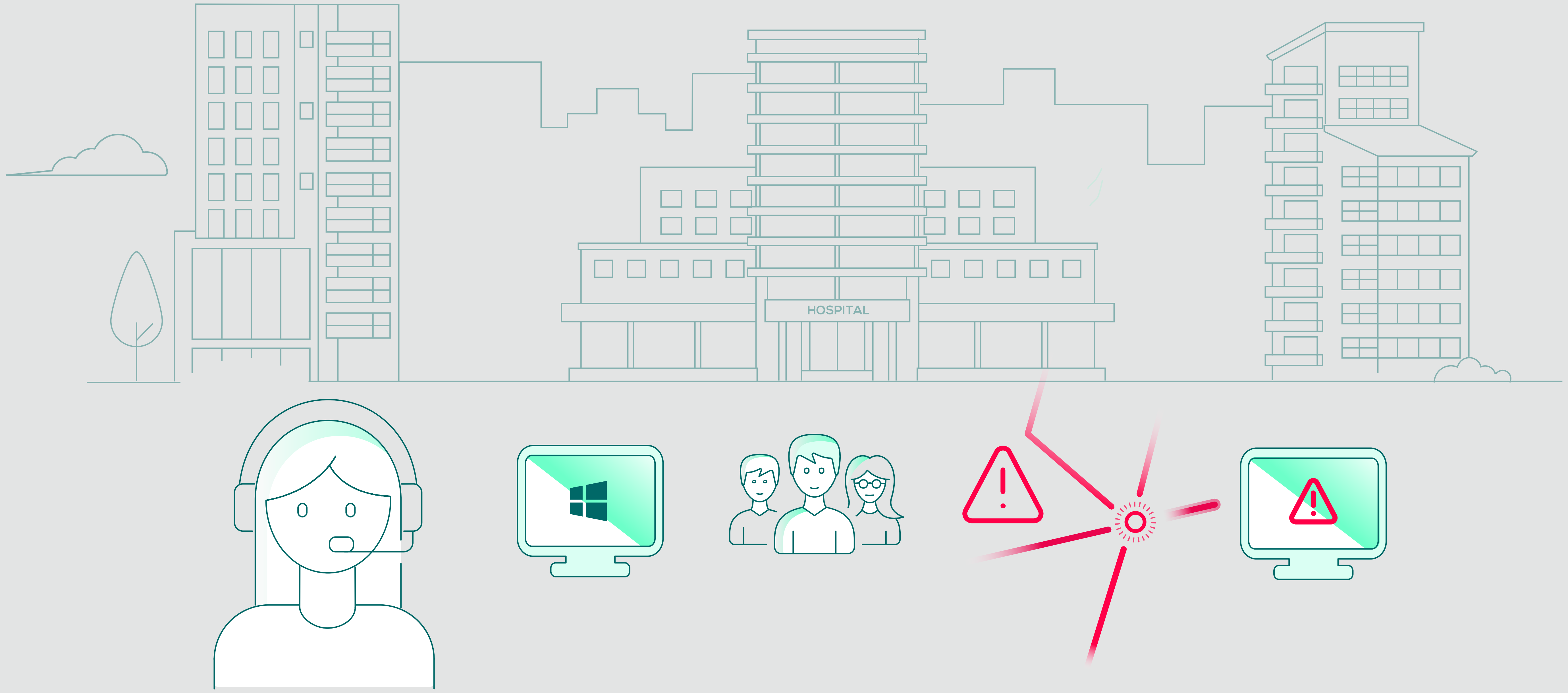
One of the affected objects was the **AD Users Container**, with a child object that's a user who's part of the Domain Admin group. So any user in the domain could gain Domain Admin permissions -- all an **attacker needed was one non-privileged user to click on a phishing campaign to compromise the entire domain**.

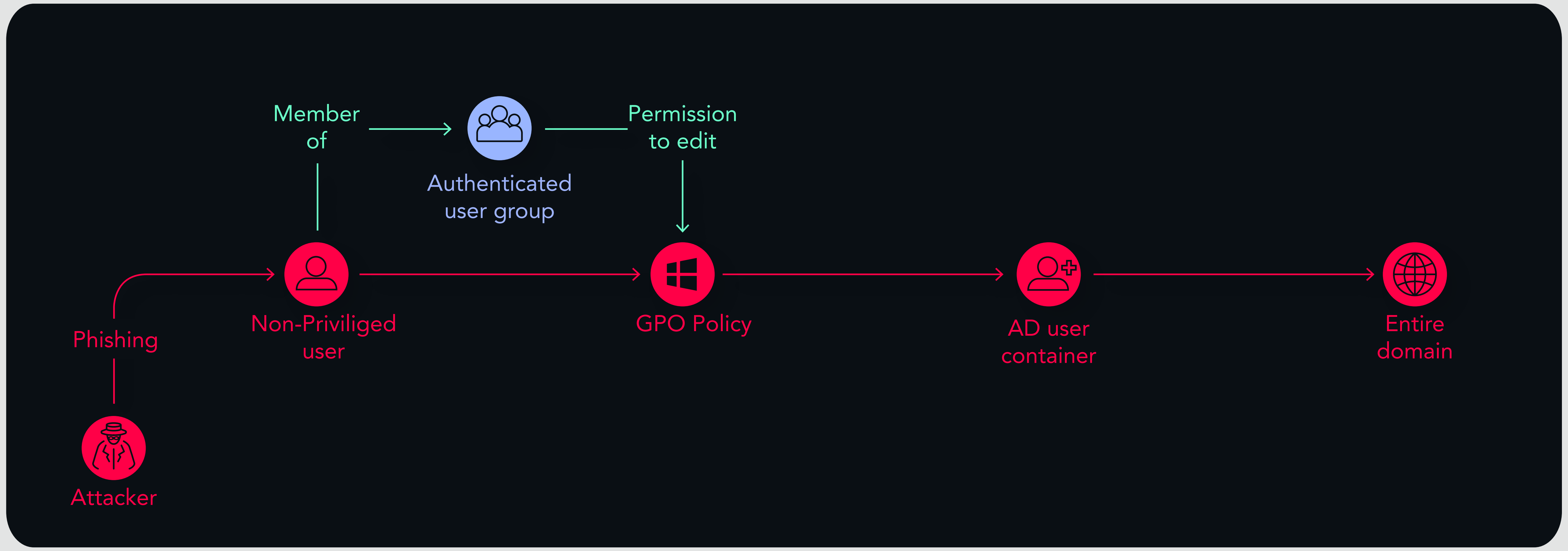
What was the impact?

The impact could have been a complete compromise of their domain.

How was it remediated?

Luckily, we were able to have it remediated by removing permissions to modify the path before any damage was done.





Driverless (and Dangerous!) Vehicles are Coming!

Tobi Trabing, Technical Director

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?

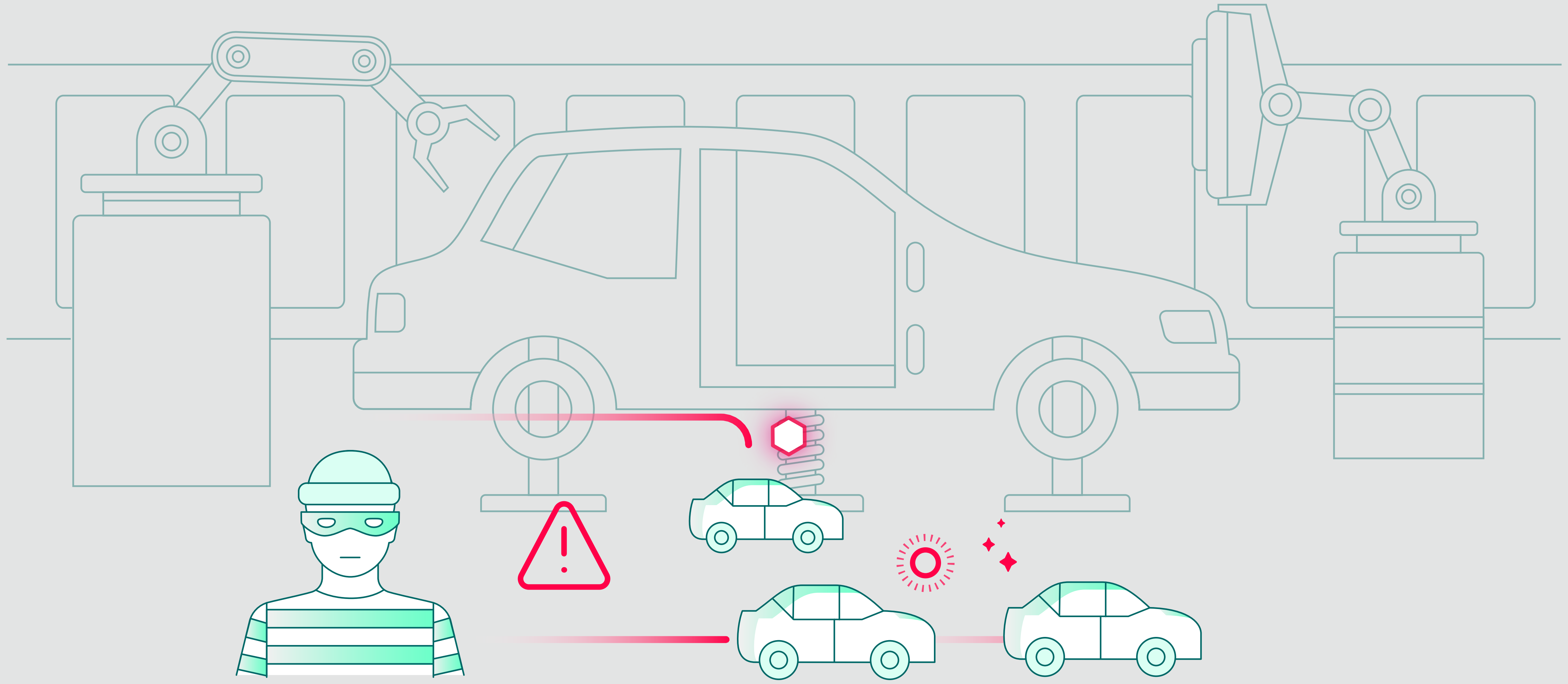
This deployment included a **server responsible for controlling uncrewed/unmanned vehicles** that were transporting goods in the factory. We located an attack path that would **allow an attacker to gain control of the vehicles** using a software vulnerability that could be exploited from asset #1 to 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.**

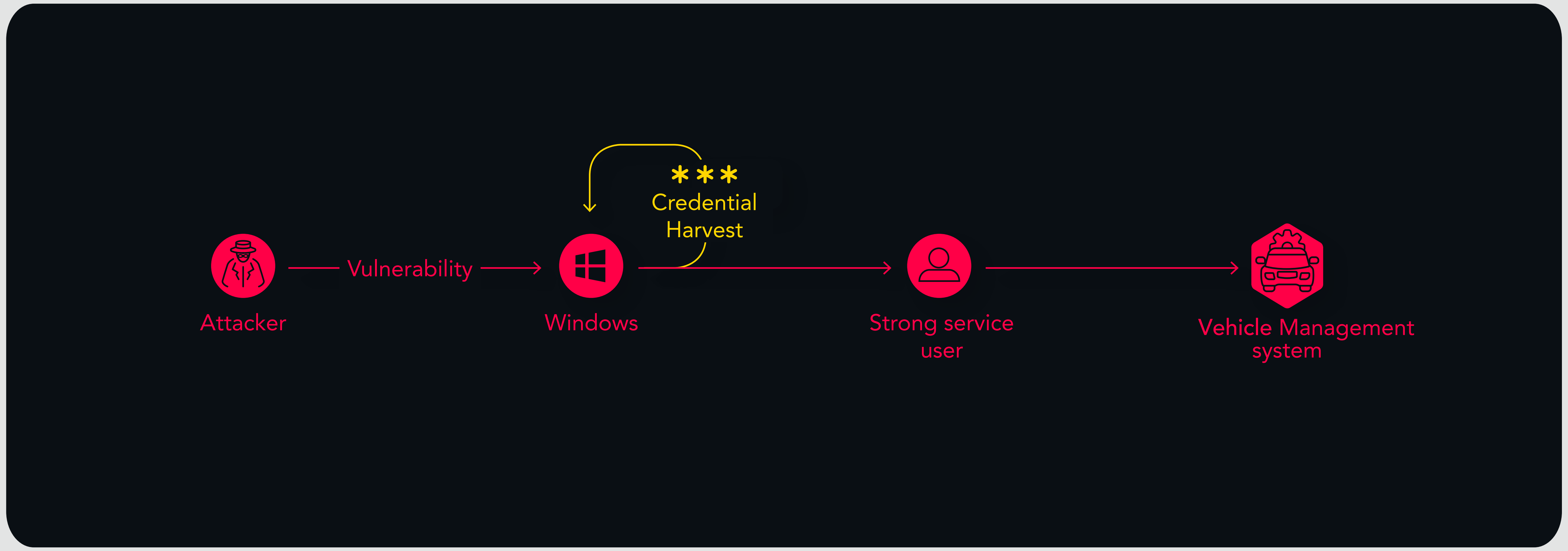
What was the impact?

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.





The Telecom Giant and the Credential Dump that Should have Never Been

Sascha Merberg, Technical Director

Who was the customer?

An enterprise with many subsidiaries in the telecom industry.

What was the scenario?

Routine customer call.

What was the attack path?

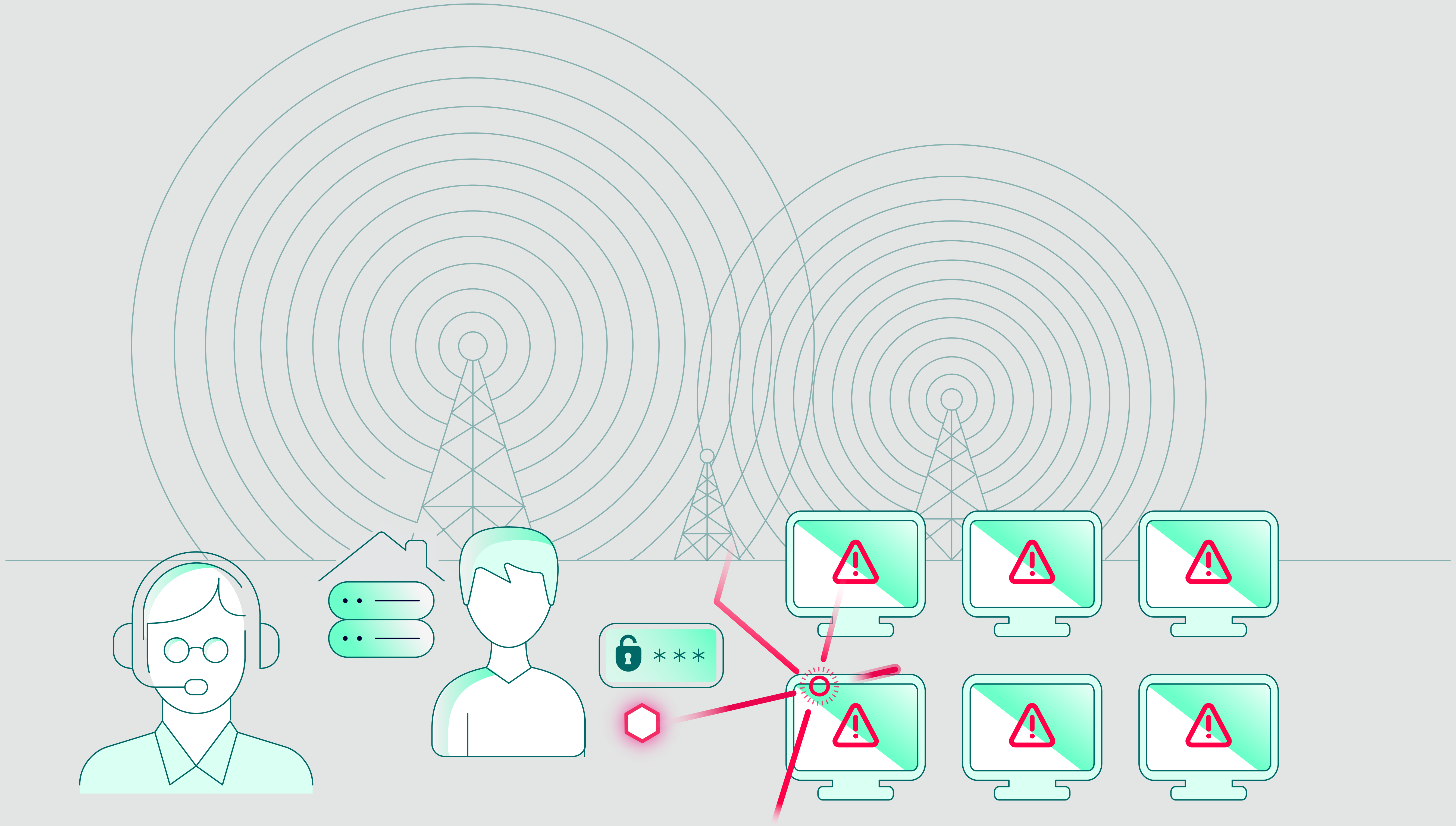
They had **one admin account** for an elite group of systems that **was using one account per admin**, which they used for everything - domain admin, installing software, administering databases – truly everything. From any client machine that had been logged into, and used by the admin, we were able to **dump credentials** and move quickly laterally through the domain controller and **show how the whole domain could be compromised.**

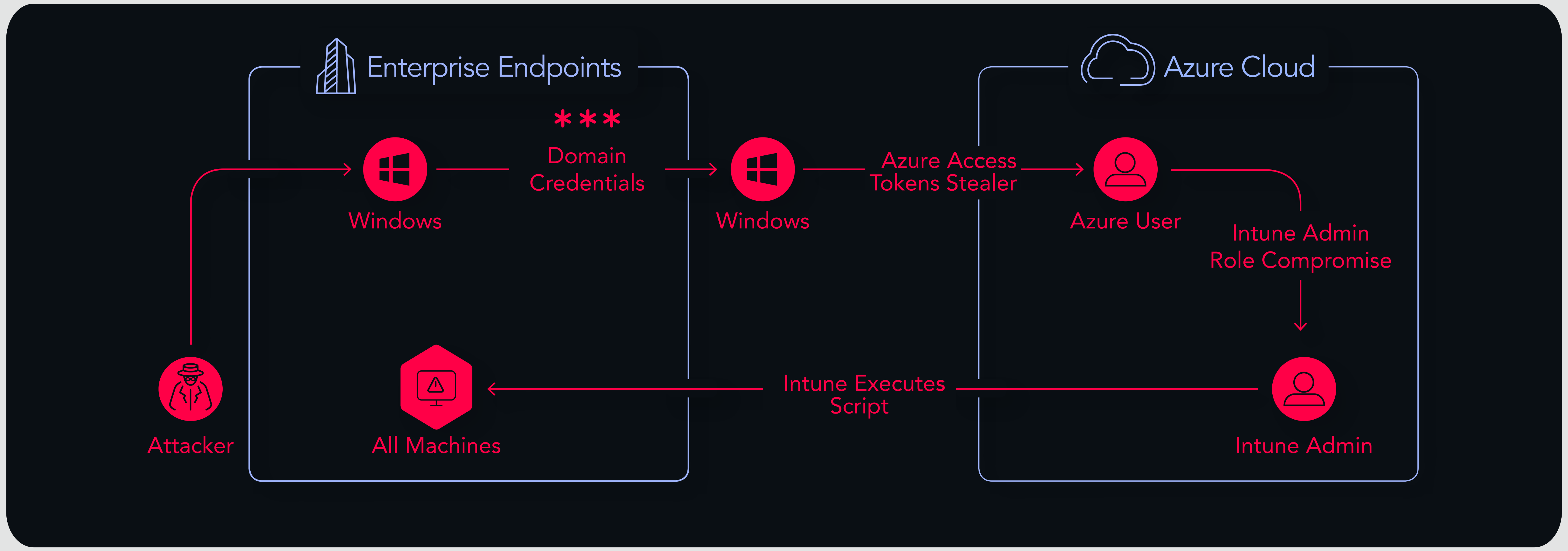
What was the impact?

Interestingly, they already had an initiative to change this – they wanted to introduce new accounts for admins and hardware tokens for authentication to prevent cached credentials – but the project got put on the back burner. This enabled them to go to management and show the urgency, helping it to be prioritized.

How was it remediated?

They removed risky credentials, and re-established best practices for implementing best practices when creating roles and permissions.





Now You Know Why Your Package Never Made its Way to You

Zur Ulianitzky, VP of Research

Who was the customer?

A major shipping and logistics company.

What was the scenario?

Routine customer call.

What was the attack path?

The attack path started from a random workstation machine **in the on-prem environment.** After exploiting some credentials issues in the enterprise environment, **we were able to pivot into the cloud** (Azure environment) by **harvesting valid Azure access tokens** (claimed with MFA).

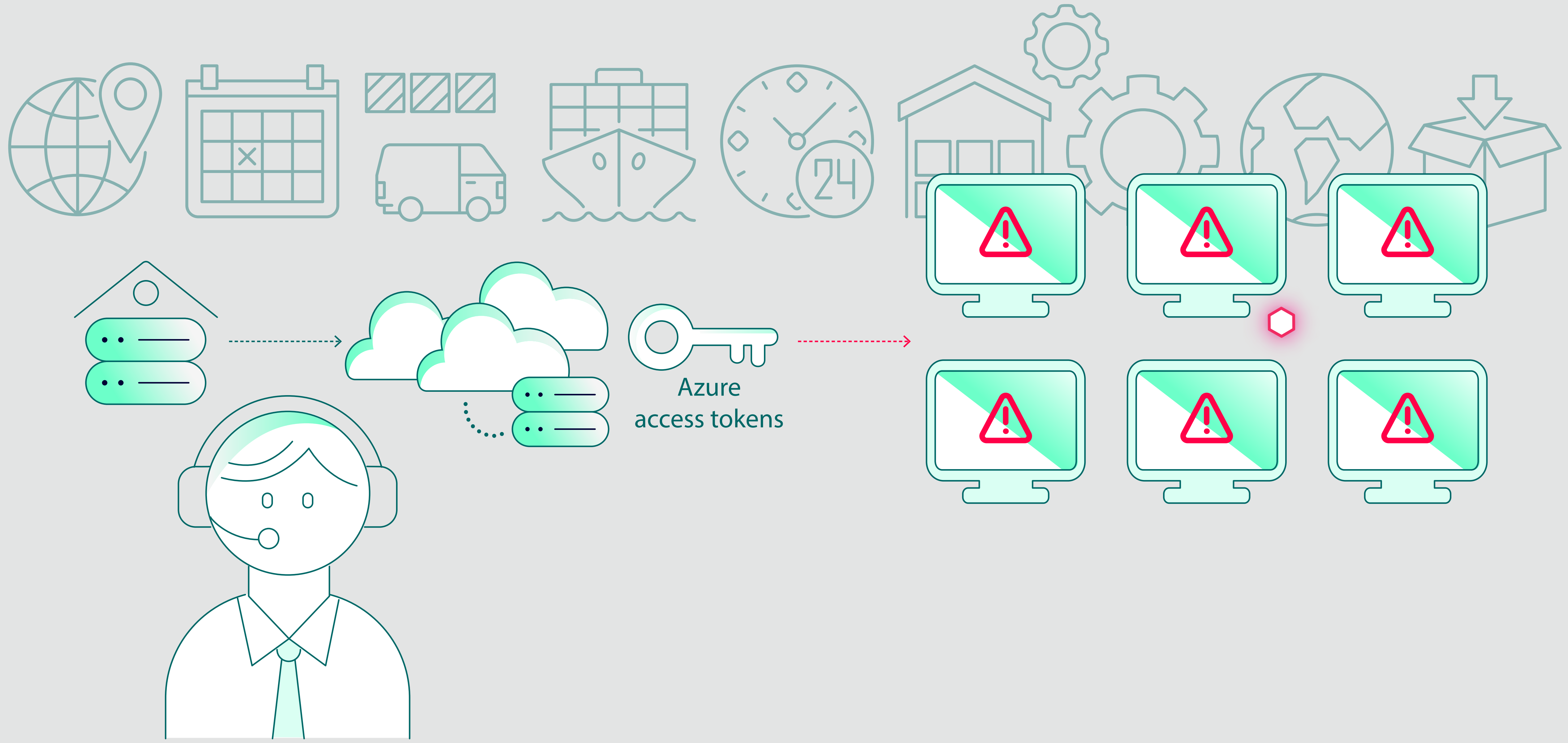
Once the Azure recon phase was completed, we were able to **escalate our privileges**, and finally compromise an Intune (Azure MDM solution for managing devices) Administrator User. By abusing the permissions of that user, we could **execute code back on enterprise machines** which he managed.

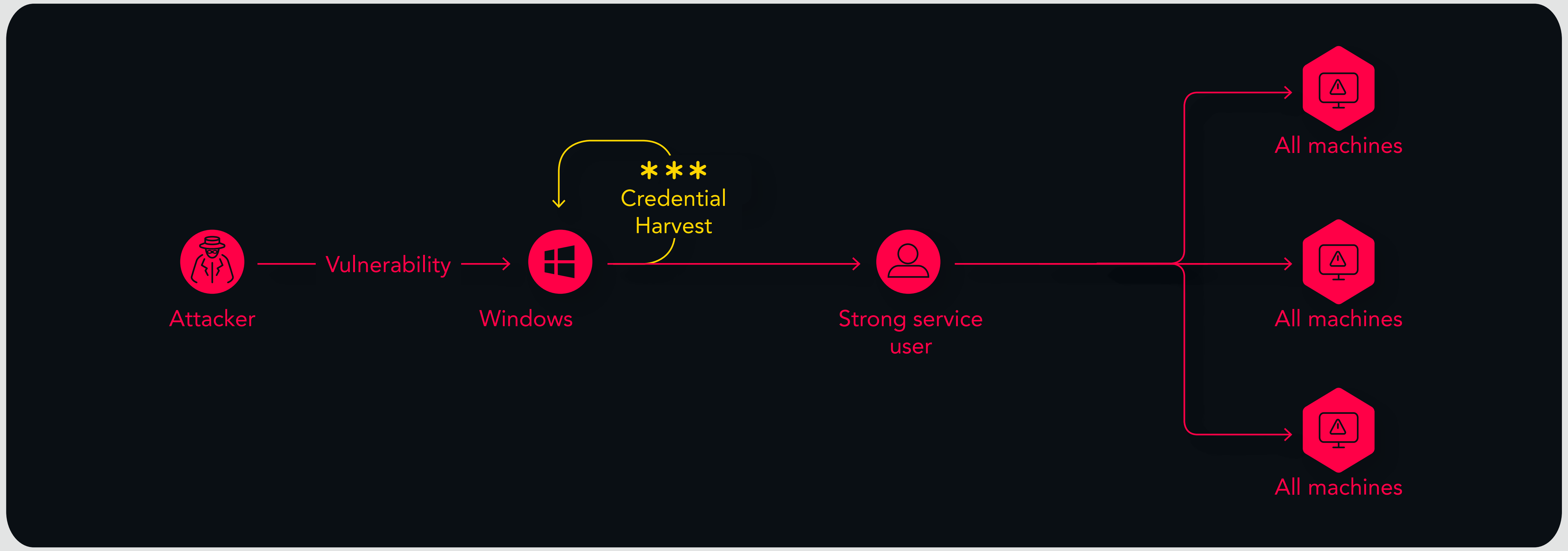
What was the impact?

Continued lateral movement would have led to the compromise of the entire enterprise environment.

How was it remediated?

There were more users than expected with the Intune Administrator role so we removed all irrelevant users and remediated the problem. If it had not been remediated, this could have allowed any attacker to get control over their entire environment.





The Big Takeaway

The one recurring theme here is that all of these organizations had proper security measures in place. They were all using best practices and felt they had an adequate understanding of their risks. But they failed to see their exposures through a holistic lens, viewing issues in siloes, which provided a false sense of security.

With XM Cyber's Exposure Management Platform, they were able to gain a context-based understanding of their environment and see how issues in their environment combined together to which they had previously been blind. They were able to prioritize what really needed fixing and harden their environment to prevent these weaknesses from being leveraged in real life.

About XM Cyber

XM Cyber, a Schwarz Group company, is a leading hybrid cloud security company that's changing the way innovative organizations approach cyber risk. By continuously uncovering hidden attack paths to businesses' critical assets and security controls gaps across cloud and on-prem environments, it enables security teams to remediate exposures at key junctures and eradicate risk with a fraction of the effort. Many of the world's largest, most complex organizations choose XM Cyber to help eradicate risk. Founded by top executives from the Israeli cyber intelligence community, XM Cyber has offices in North America, Europe, and Israel. XM Cyber was acquired by the fourth largest retailer in the world, Schwarz Group in November 2021.

Tel-Aviv:	+972-3-978-6668
New-York:	+1-866-598-6170
London:	+44-203-322-3031
Neckarsulm:	+49-7132-30485600
Paris:	+33-1-70-61-32-76

xmcyber.com