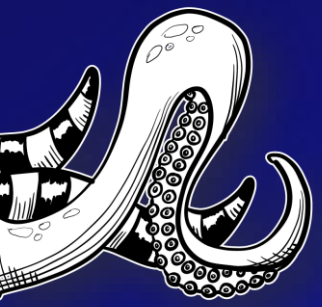
DYNAMICS MINDS

Microsoft Dynamics 365 and Power Platform Conference

Pre-Day: MAY 26, 2024

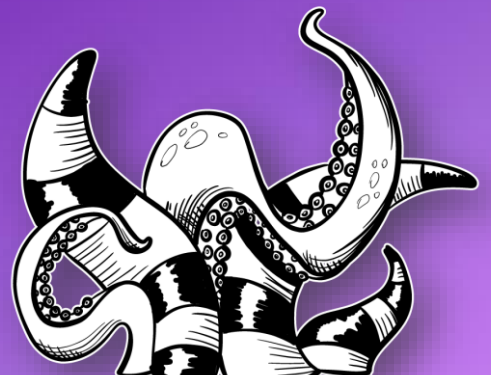
MAY 27 - 29, 2024

Portorož, Slovenia, Europe



Exploring Zero Trust Security for Power Platform

Raphael Pothin - Druid
Lead Power Platform Reliability Engineer @Manulife



Who am I?

Microsoft Bizapps MVP

Power Platform & DevOps Enthusiast

Raphaël Pothin

@RaphaelPothin

Raphael POTHIN

Raphaël Pothin

rpothin

Why bother with security for Power Platform?

Introduction

Understand the risks

Why Zero Trust?

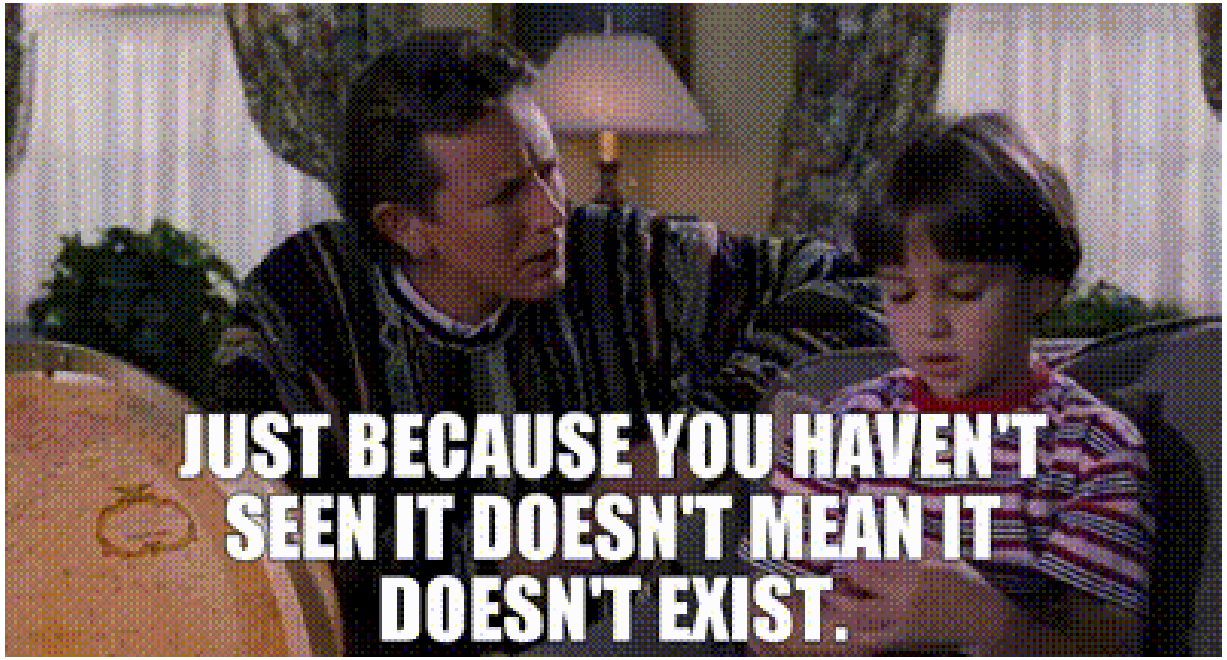
Generation 1:
Castle & Moat

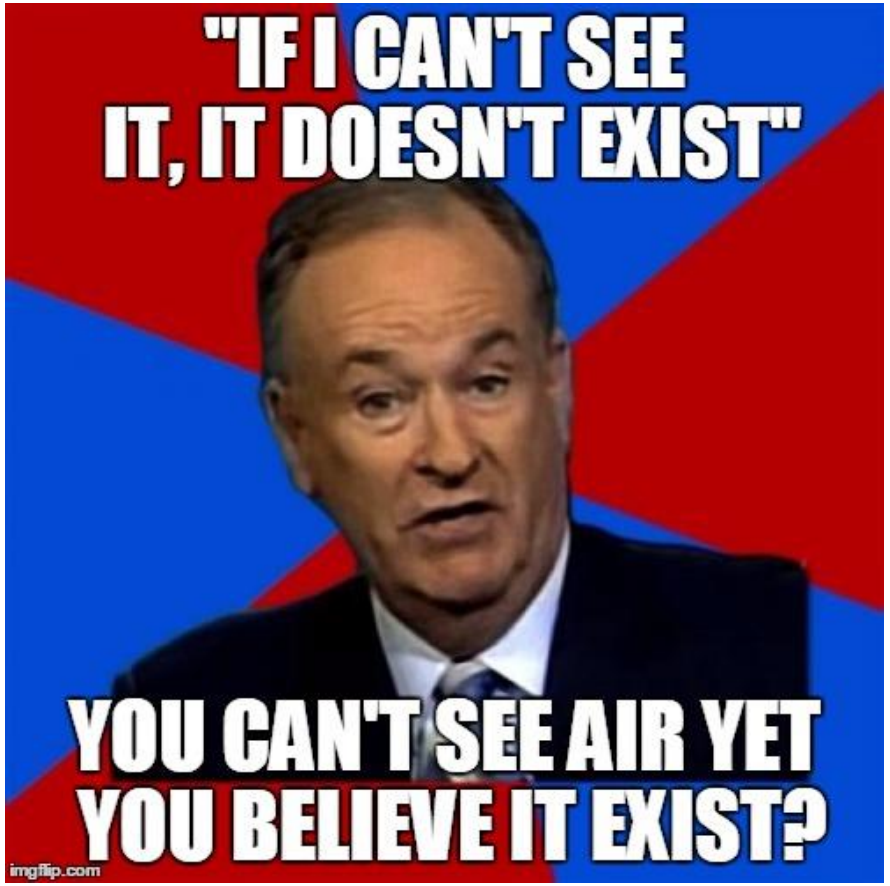
Generation 2:
Virtualized Functions

Generation 3:
Zero Trust Network

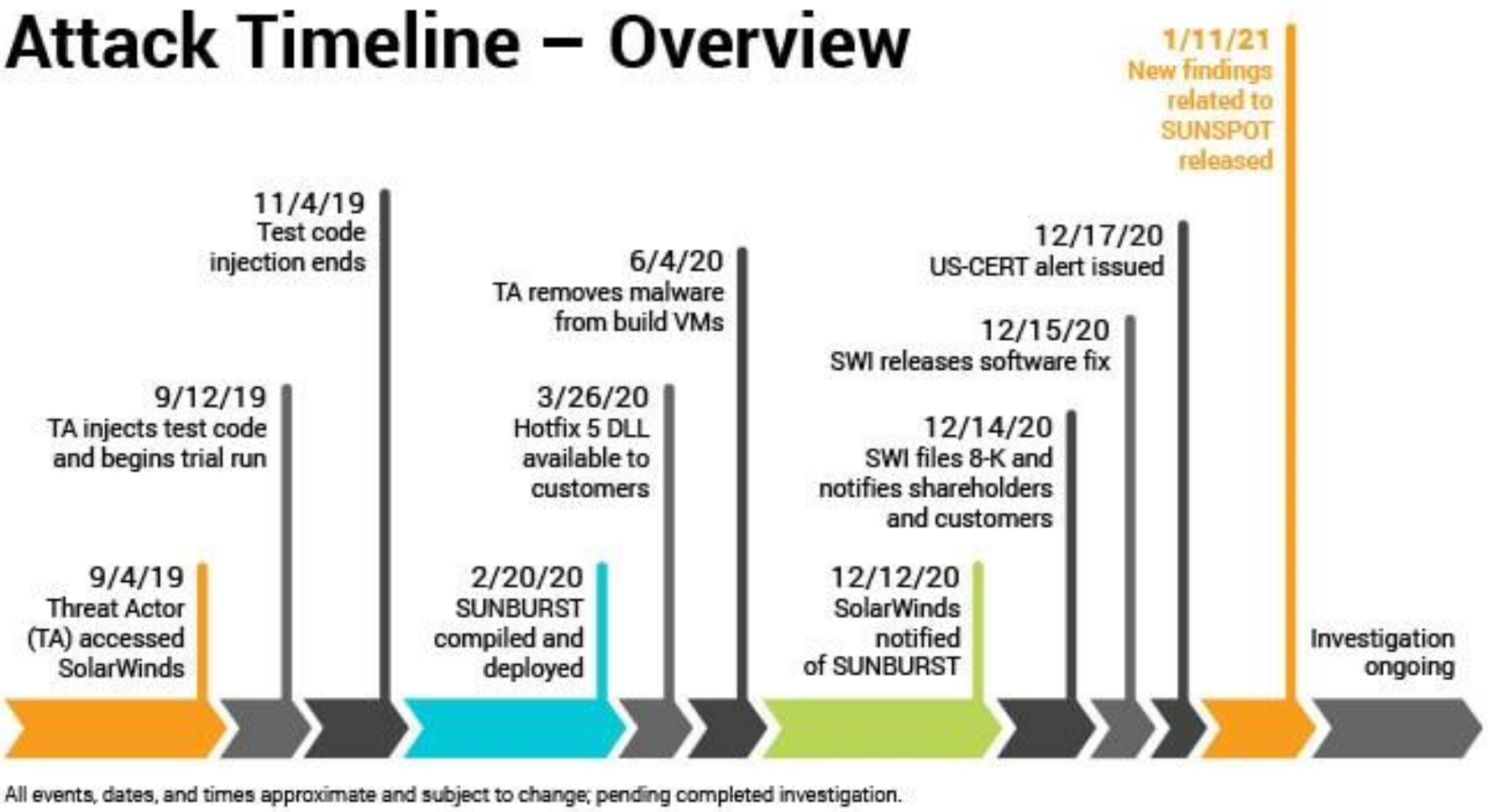
What are the Zero Trust principles?

Assume breach!

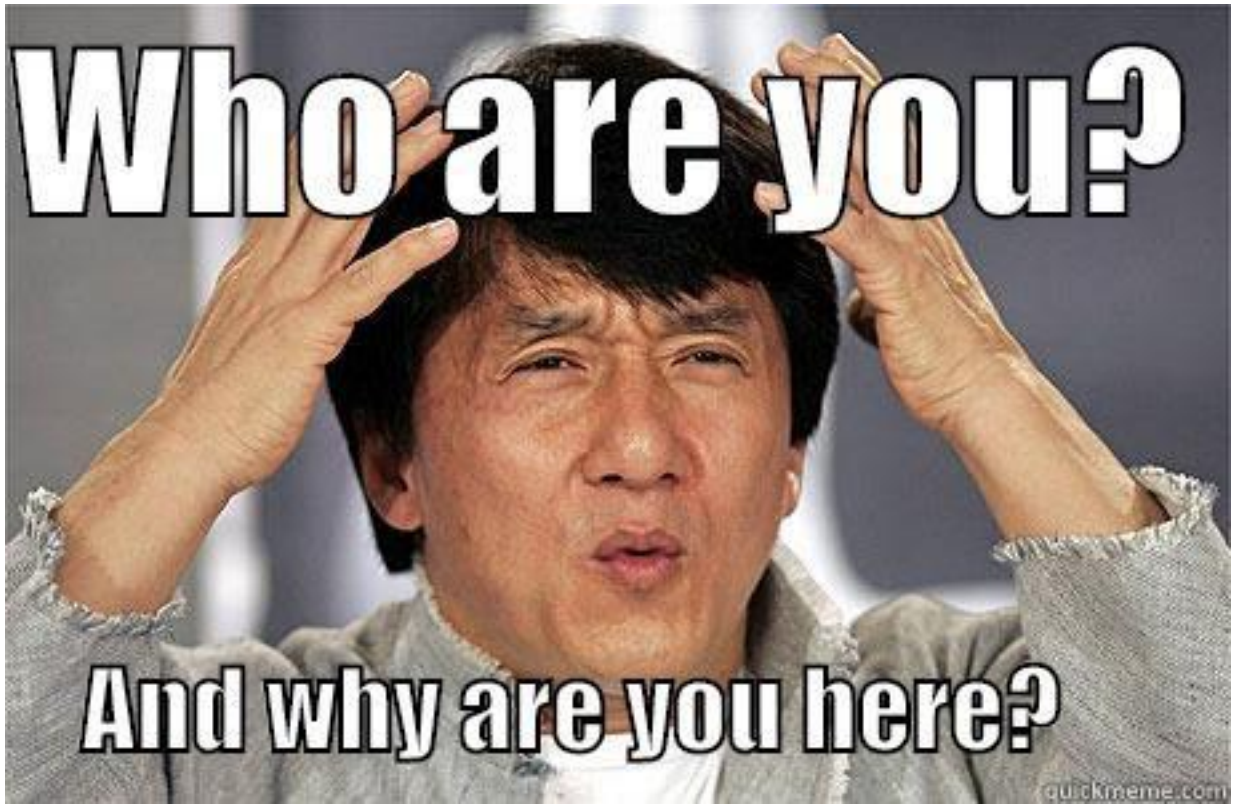




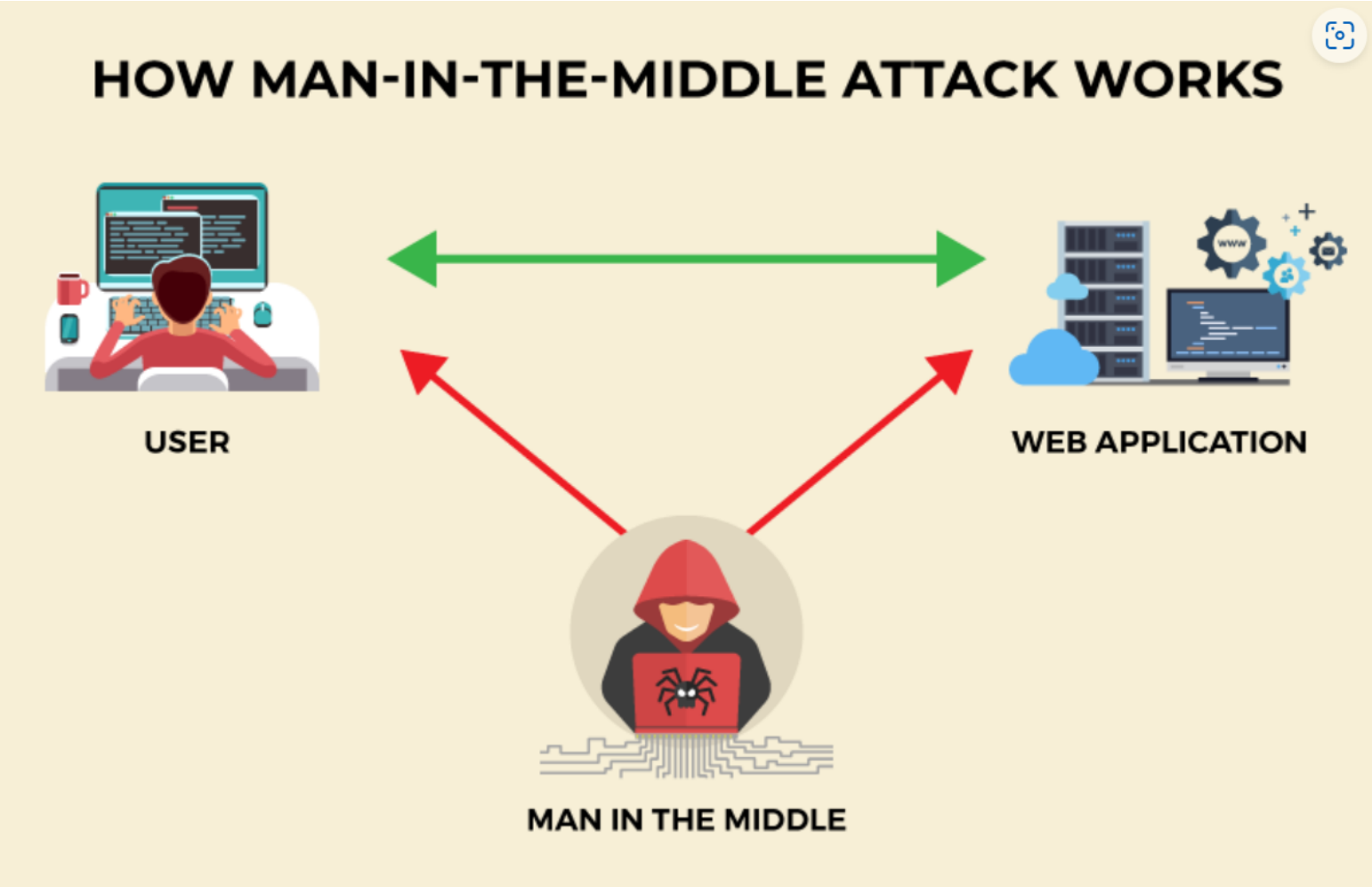
Assume breach!



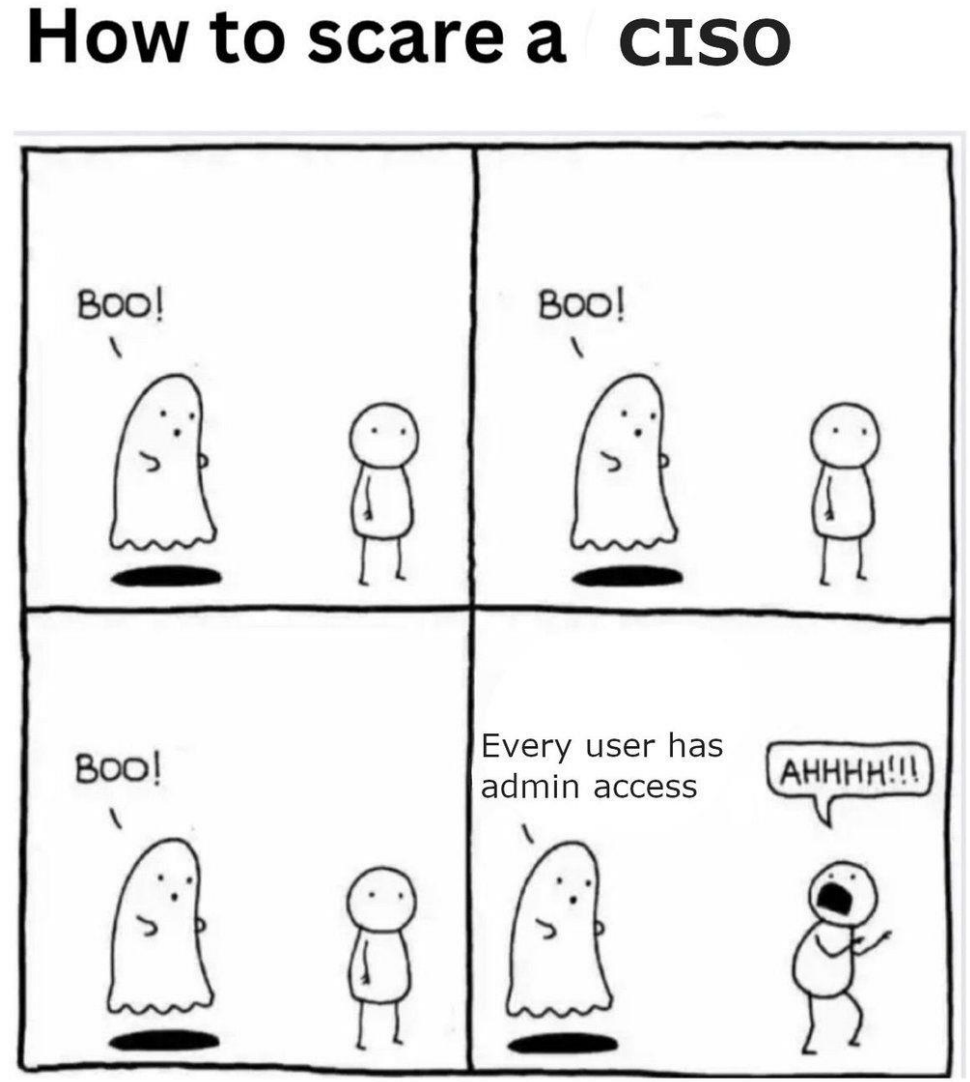
Verify explicitly!



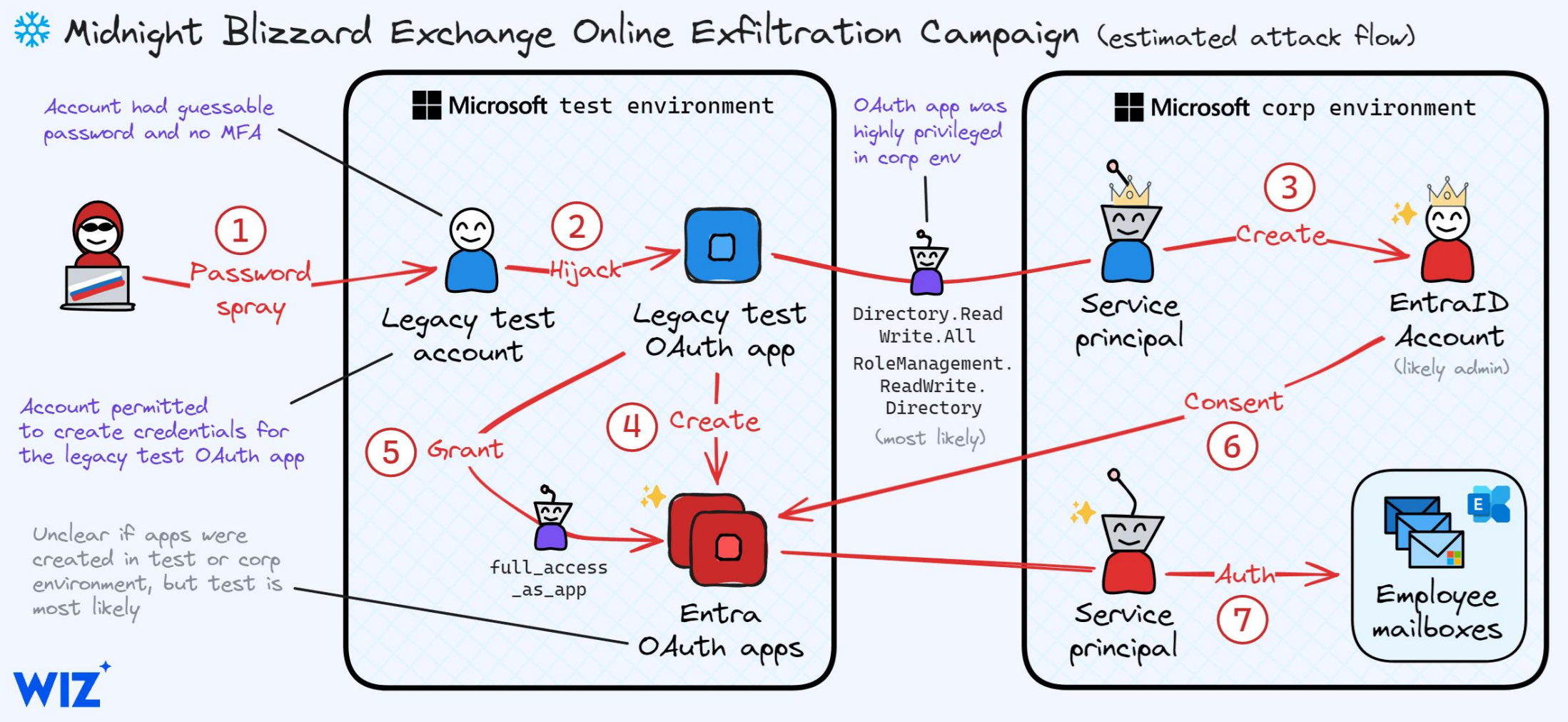
Verify explicitly!



Use least privileged access!



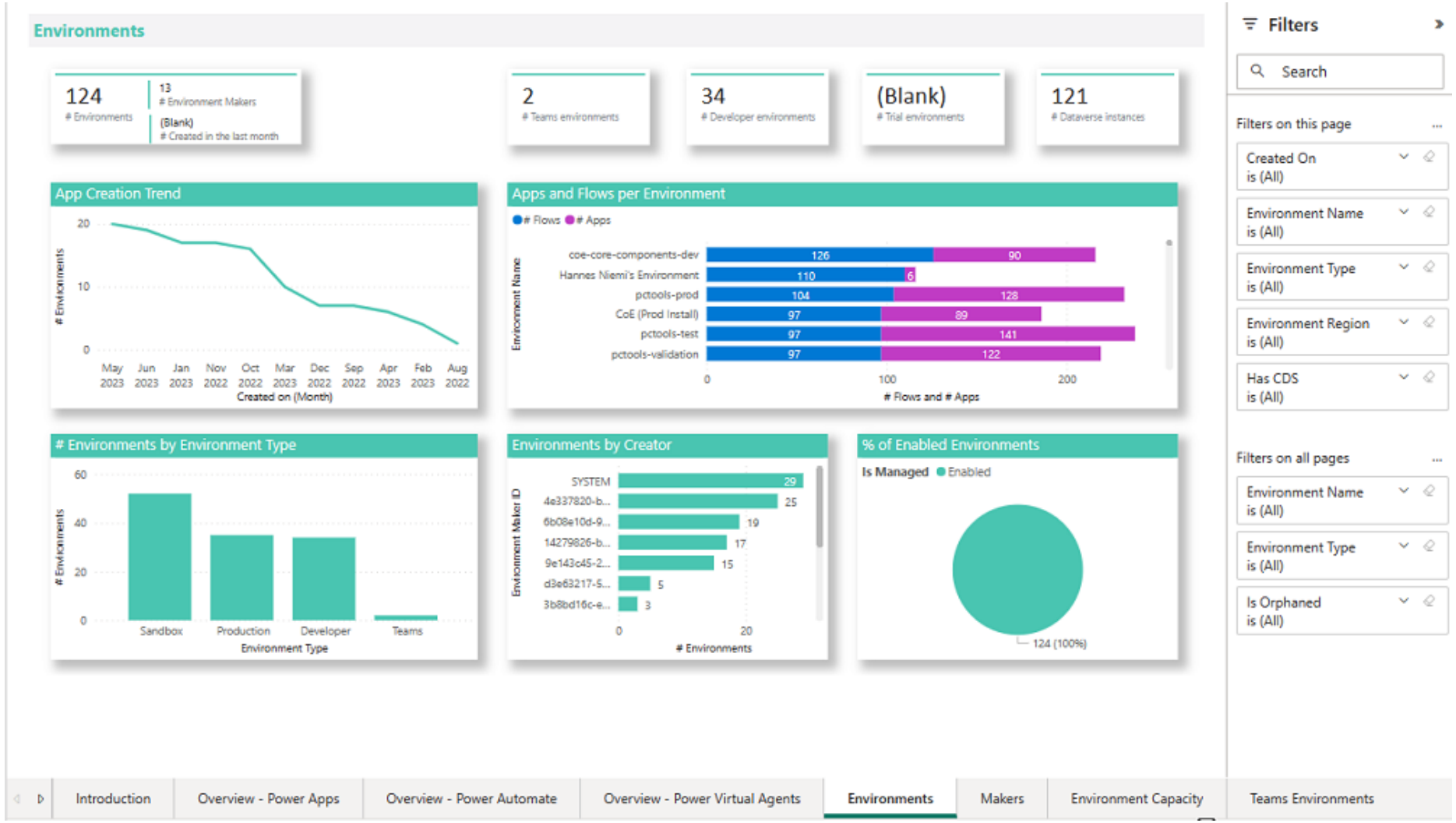
Use least privileged access!



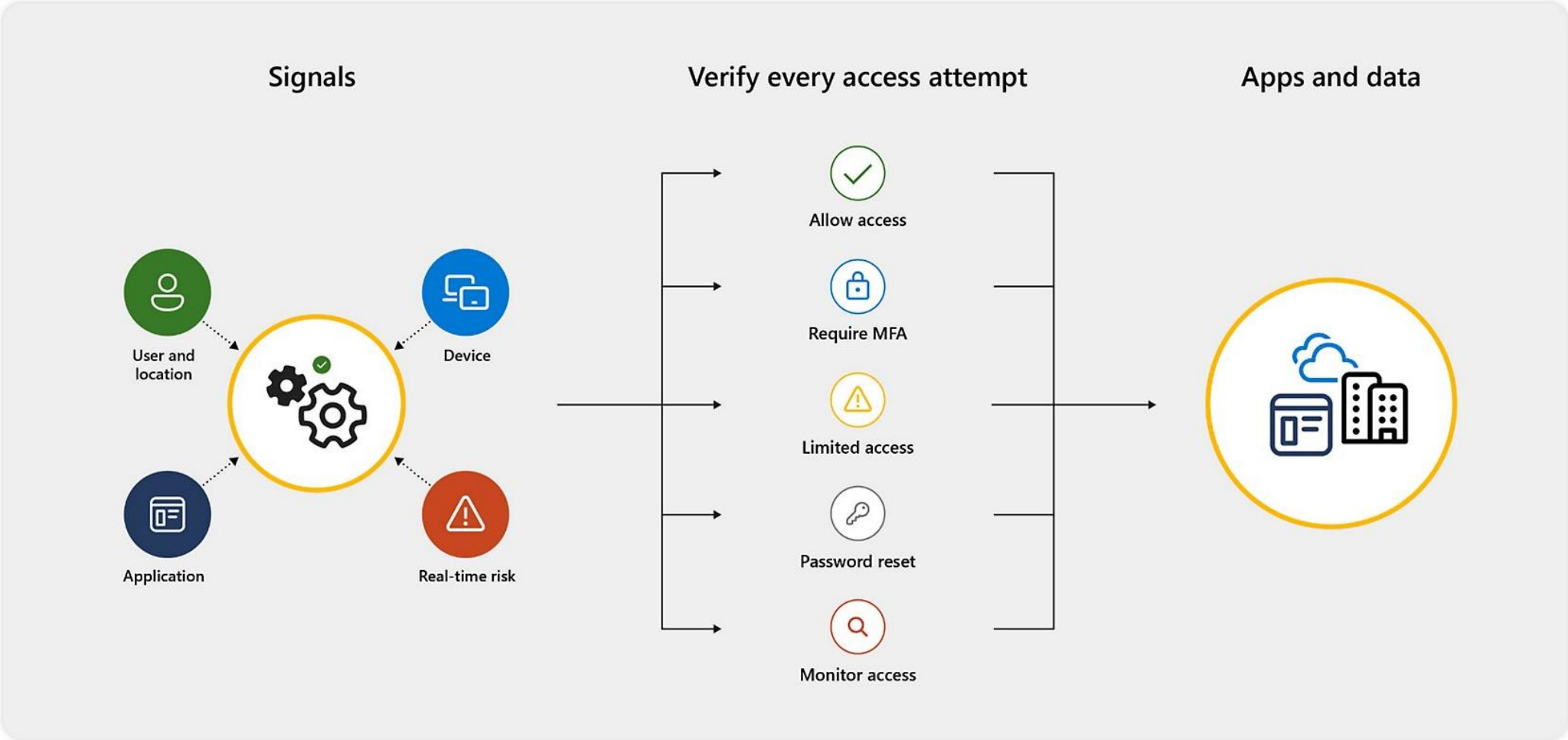
What can you do?

DYNAMICS MINDS

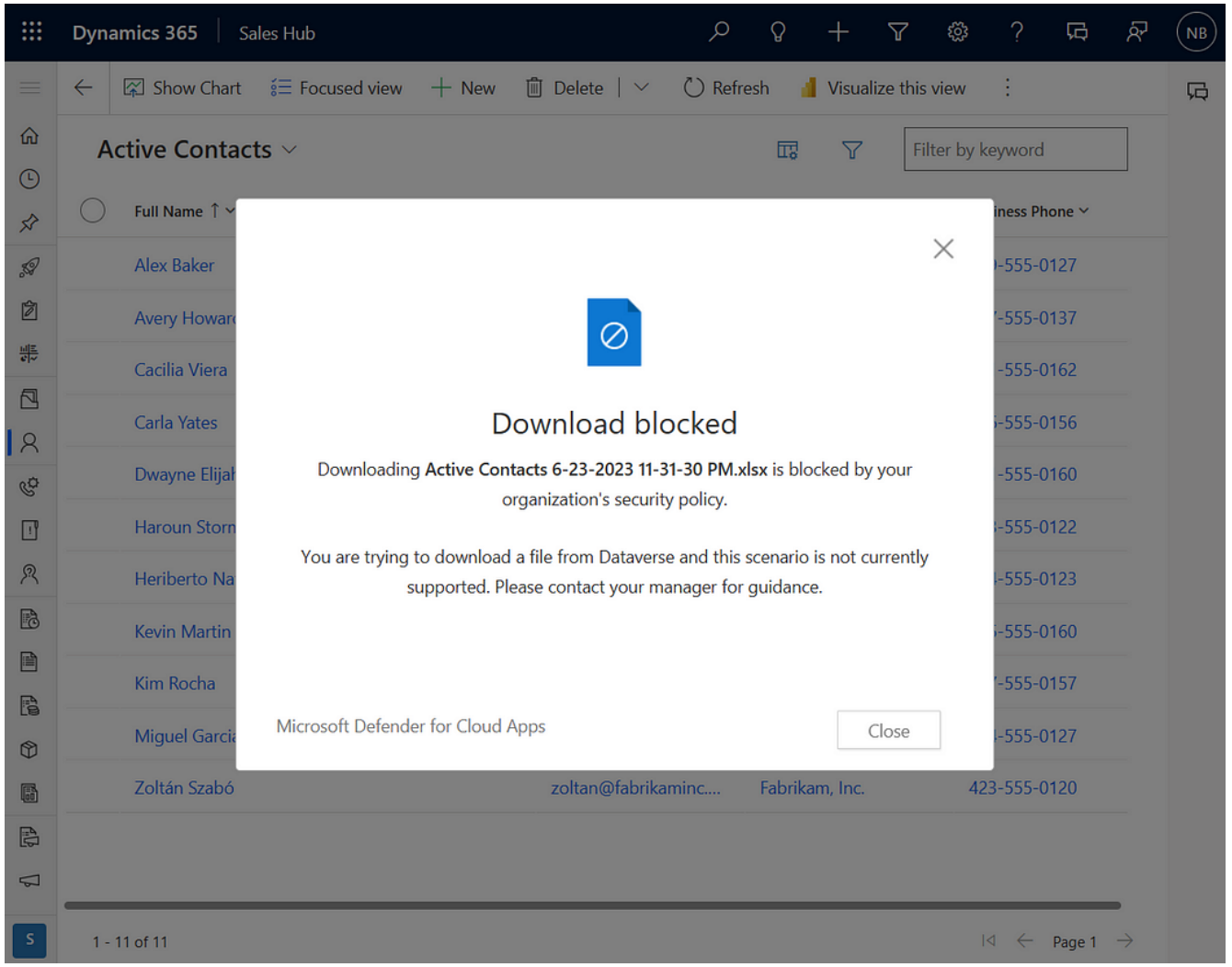
Risk analysis – Monitor with the CoE Starter Kit



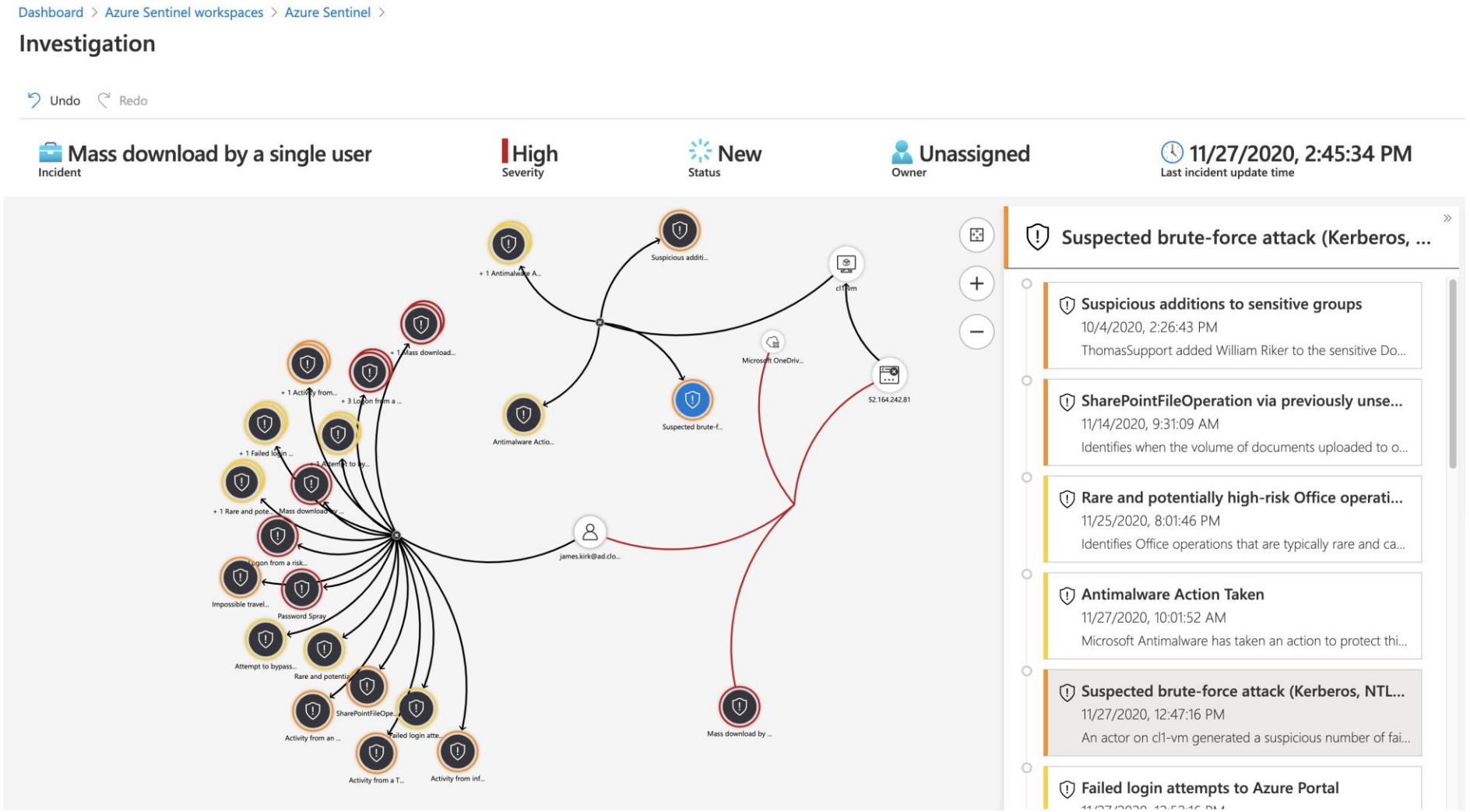
Verify explicitly - From authentication...



Verify explicitly - ... to authorization ...



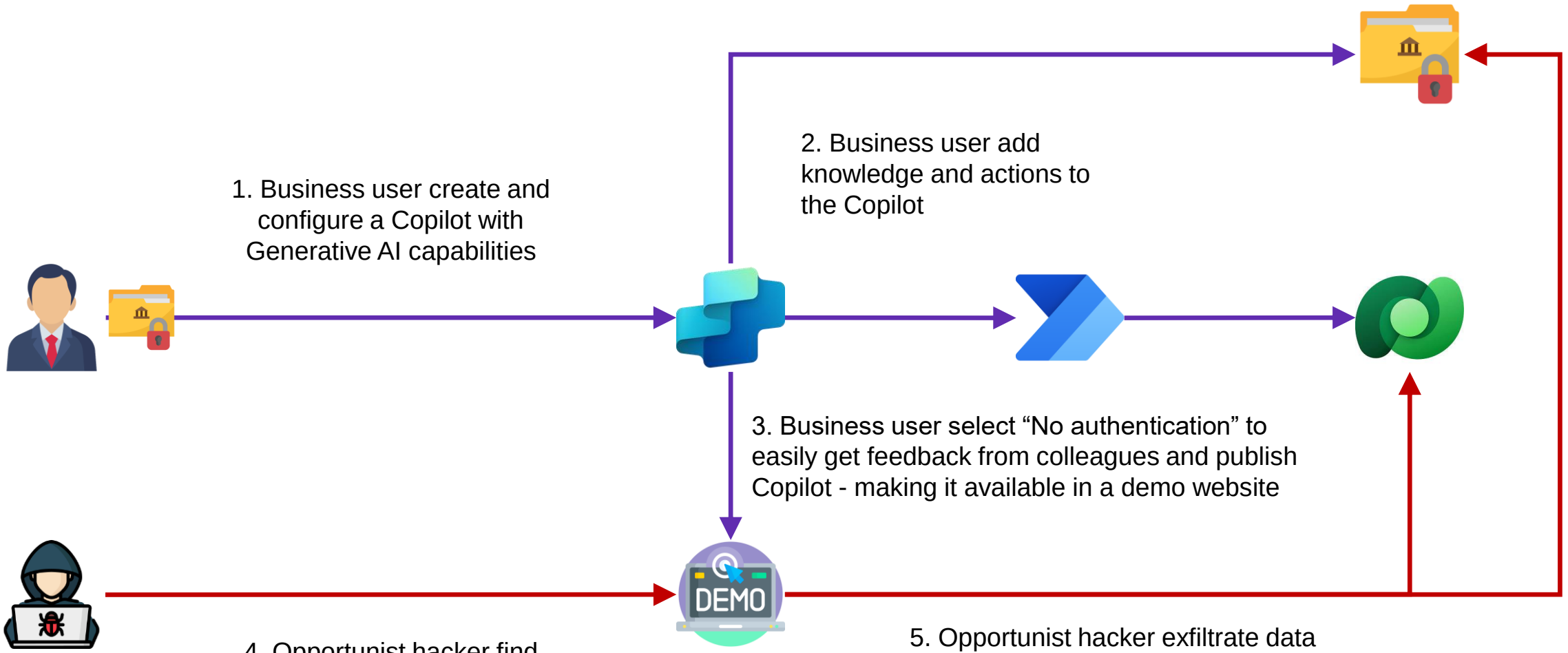
Verify explicitly - ... and beyond



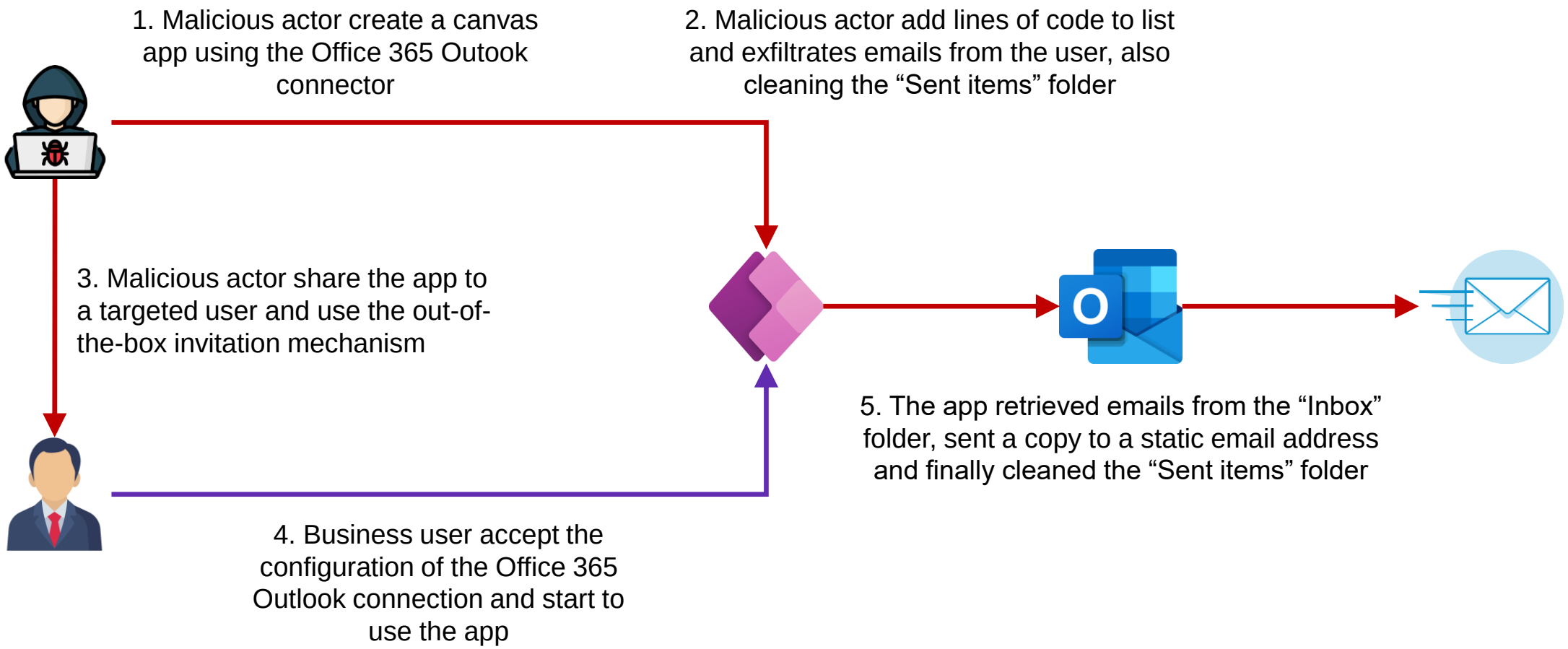
Scenarios

That could potentially happen in real life…
(most likely in tenant not well configured)

Data leak from a misconfigured Copilot



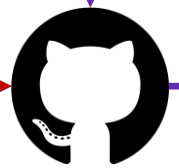
Phishing attack through a canvas app



Repository hijack for Dataverse data exfiltration

1. Developer configure a GitHub repository with secrets for the management of solutions*

* To be able to deploy solutions, the considered application user (*application registration in Entra ID*) will need to have full privileges in the considered Dataverse environments (*"System Administrator" security role*)

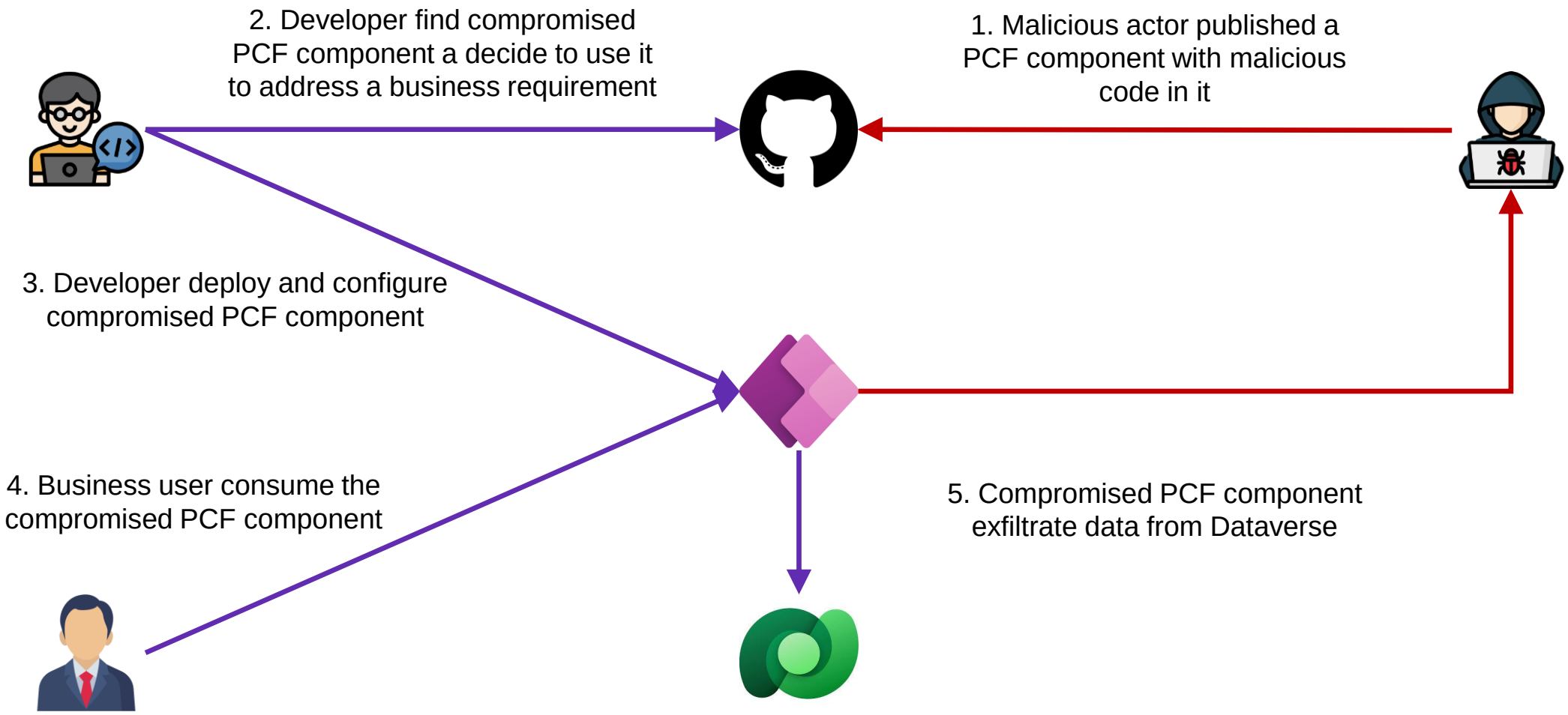


2. GitHub workflows can successfully interact with related Dataverse environments (*like Production*)

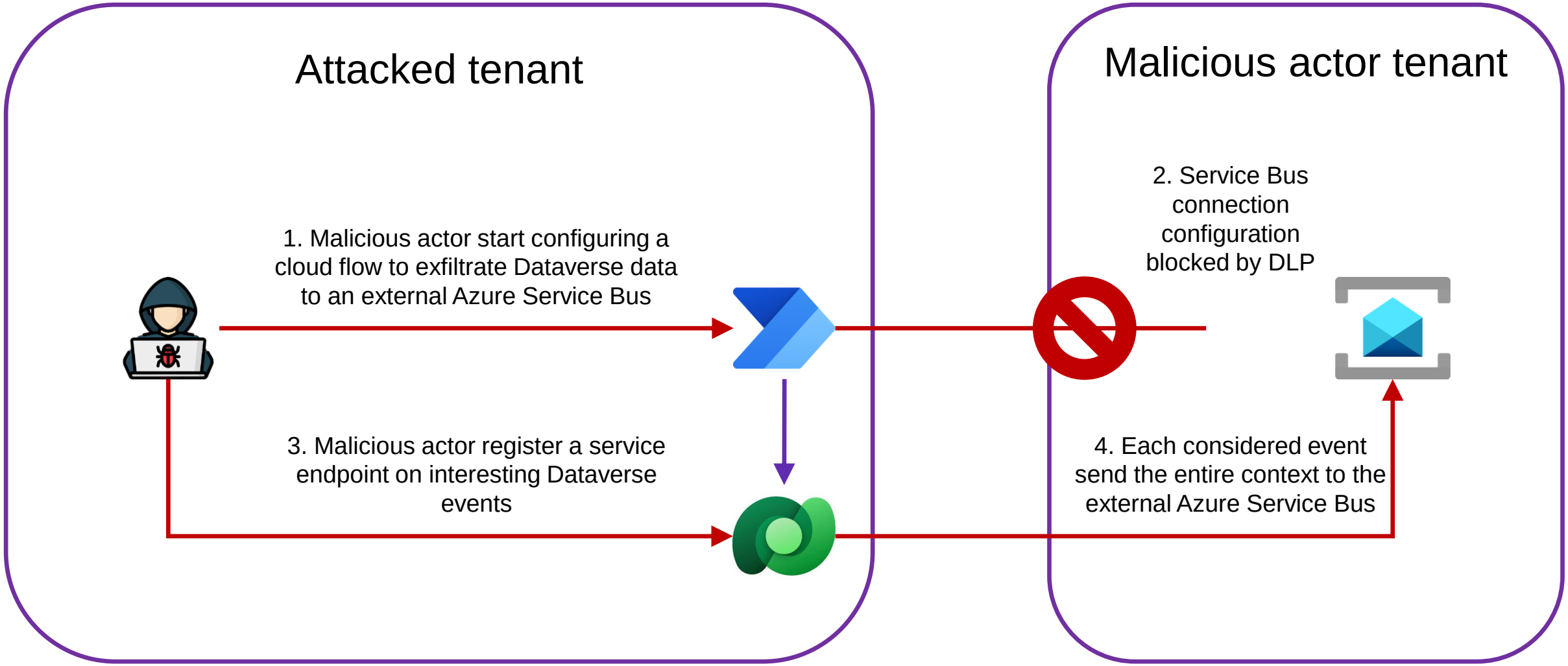
3. Malicious actor gain access to a user account with contribution permissions to the GitHub repository

4. Malicious actor used the compromised user account to configure a branch with code and automation to exfiltrate data

Supply chain attack



If you can't block it, monitor it!



Let’s wrap up!

A few recommendations before the end

Identity Management

- Enable MFA for all your users if possible
- Use Privileged Identity Management (PIM) for just-in-time high privilege elevation for specific administration tasks
- Use Conditional Access Policies to take user's context into consideration during the authentication phase

A few recommendations before the end

Power Platform

- Disable the “Share with everyone” tenant setting
- Use Tenant isolation to control the traffic with other tenants
- DLP policies are not foolproof, but well configured there could limit the attack surface and lateral movements
- Managed Environments capabilities, like IP address-based cookie binding or IP firewall, should be considered in your cyber defense arsenal
- Upcoming network capabilities, like VNet integration, will help avoiding to put at risk resources in your network

A few recommendations before the end

Monitoring

- Purview Compliance provide a great visibility regarding what is going on in Power Platform, but to protect the data in Dataverse you will need to conscientiously configure the audit
- Microsoft Sentinel is a great tool to consider, it combines multiple signals from your entire information system to add another layer of protection for Power Platform
- The governance of the data in Dataverse can be achieve using the Microsoft Purview integration and it can help you identify your most critical environments

Other Resources

- OWASP Low-Code/No-Code Top 10 | OWASP Foundation
- "Protect and Manage Your Enterprise Data Effectively at Scale" with Mihaela Blendea and Jocelyn Panchal (*from Microsoft*)
- Power Platform security FAQs - Power Platform | Microsoft Learn (*including sections related to "OWASP top 10"*)
- Microsoft Power Platform security and governance documentation - Power Platform | Microsoft Learn
- Enterprise security with Power Platform - Power Platform | Microsoft Learn (*white paper*)
- Power Pwn - An offensive and defensive security toolset for Microsoft 365 Power Platform

Thank you very much for your participation!