VECTRA®

DISSECTING THE MIDNIGHT BLIZZARD ATTACK AGAINST MICROSOFT

Sophisticated attack against Entra ID & M365

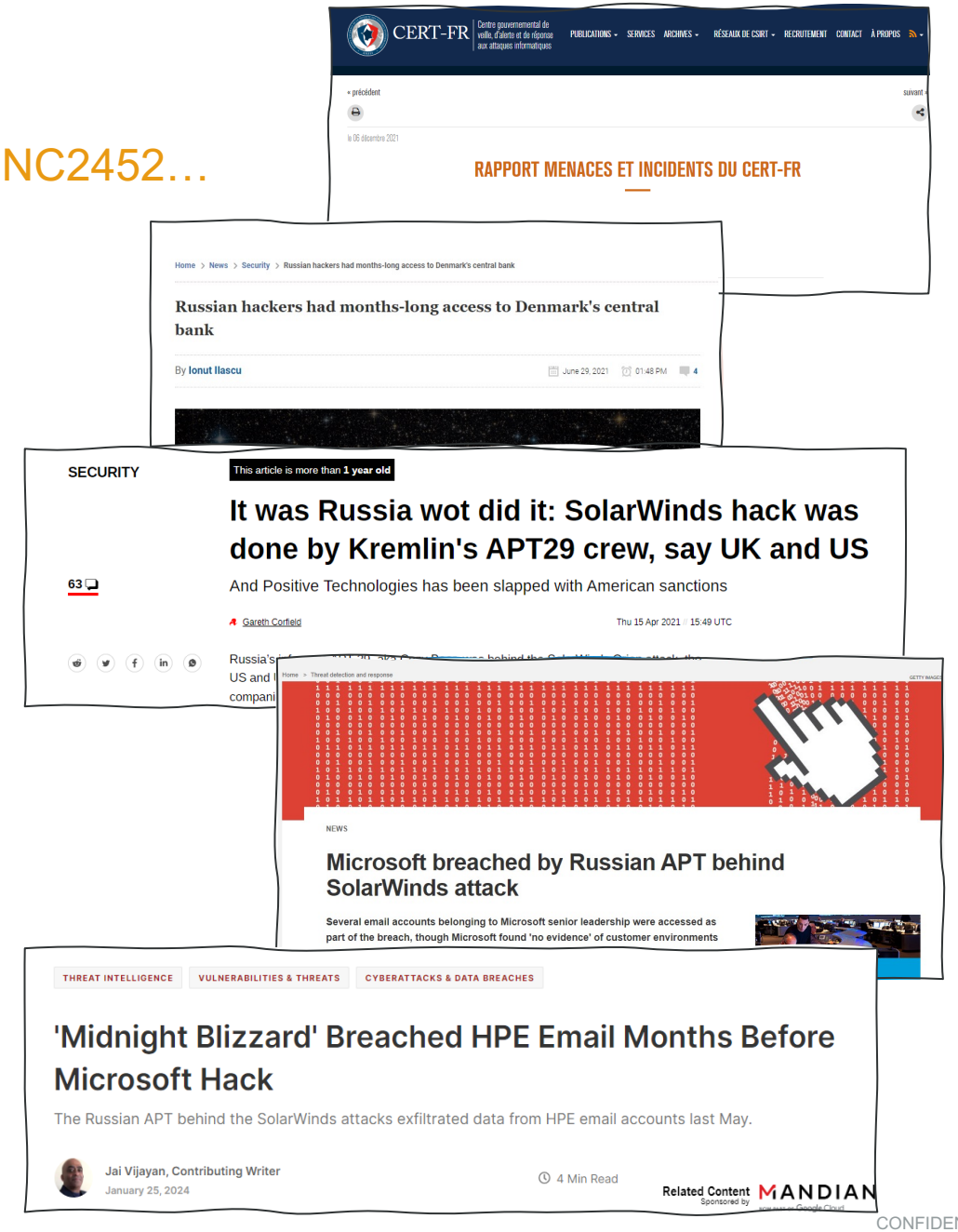
Stijn Rommens

Sr. SE Director EMEAn

MIDNIGHT BLIZZARD

Aka APT29, Cozy Bear. NOBELIUM, The Dukes, Dark Halo, UNC2452…

1. Russia's Foreign Intelligence Service
   - > Most known for SolarWinds
2. Strategic targets
   - > Governments
   - > Technology and research
   - > Supply chain conduits
3. Highly Sophisticated
   - > High Opsec
   - > Evolving attacker methods
   - > Identity focused attacks



VECTRA

RECENTLY OBSERVED ACTIVITY OF MIDNIGHT BLIZZARD

1. **Microsoft breached**
   - > Detected on Jan 12th
   - > Successfully exfiltrated data including source code data

2. **HPE was**
   - > Breached in Jan 2024
   - > Successfully exfiltrated emails and other data

https://www.microsoft.com/en-us/security/blog/2024/01/25/midnight-blizzard-guidance-for-responders-on-nation-state-attack/
https://www.bnnbloomberg.ca/hpe-says-it-was-hacked-by-group-believed-to-be-midnight-blizzard-1.2026168

KEY OBSERVATIONS ON MIDNIGHT BLIZZARD

No 0days, Malware or exploits

MFA still **is not enforced** in the majority of MAU (60%+)

No endpoint interactions - everything was API based over cloud

"The attack was not the result of a vulnerability in Microsoft products or services."

The attack was executed
using Microsoft products as
they are **designed**

VECTRA®

DISSECTING MIDNIGHT BLIZZARD TACTICS

MICROSOFT VS MIDNIGHT BLIZZARD

Introduction & context on the real-world attack

- Microsoft communicated on Jan 19 about the breach
  - Happened in late November 2023
  - Detected on Jan 12th
  - Detected by reviewing Exchange Web Services (EWS) activity logs
  - Exploiting exclusively M365/Entra ID (features)
  - Further details communicated on Jan 25
  - Attributed to Russian state-sponsored actor

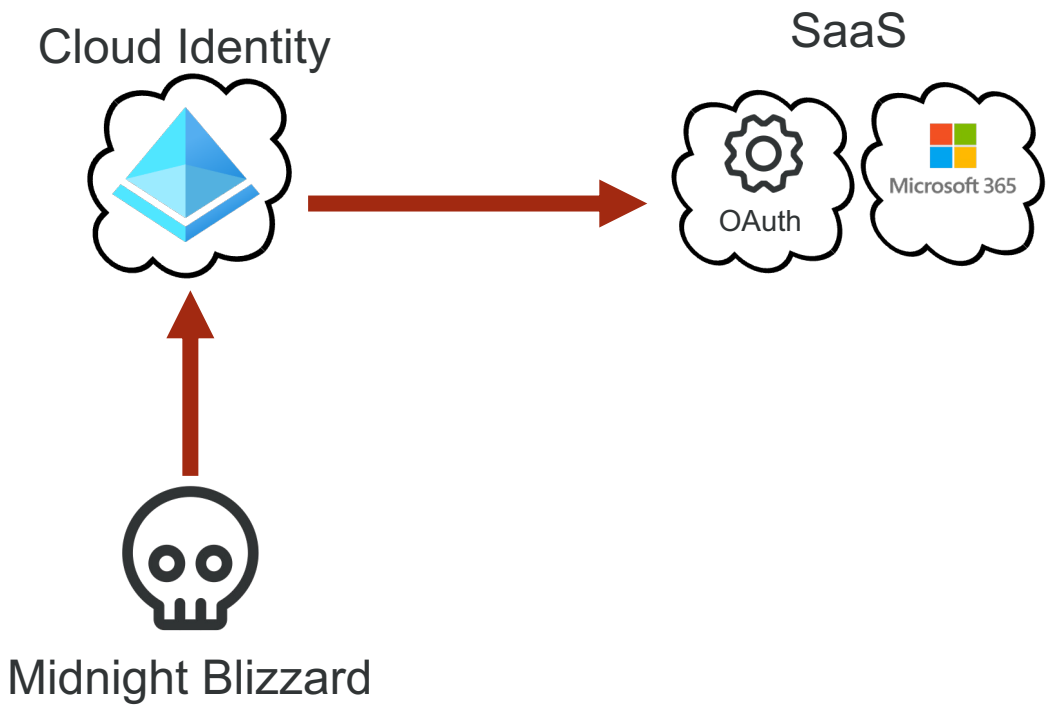
Microsoft

Microsoft Entra ID

Time to Detection = **1.5 months**!

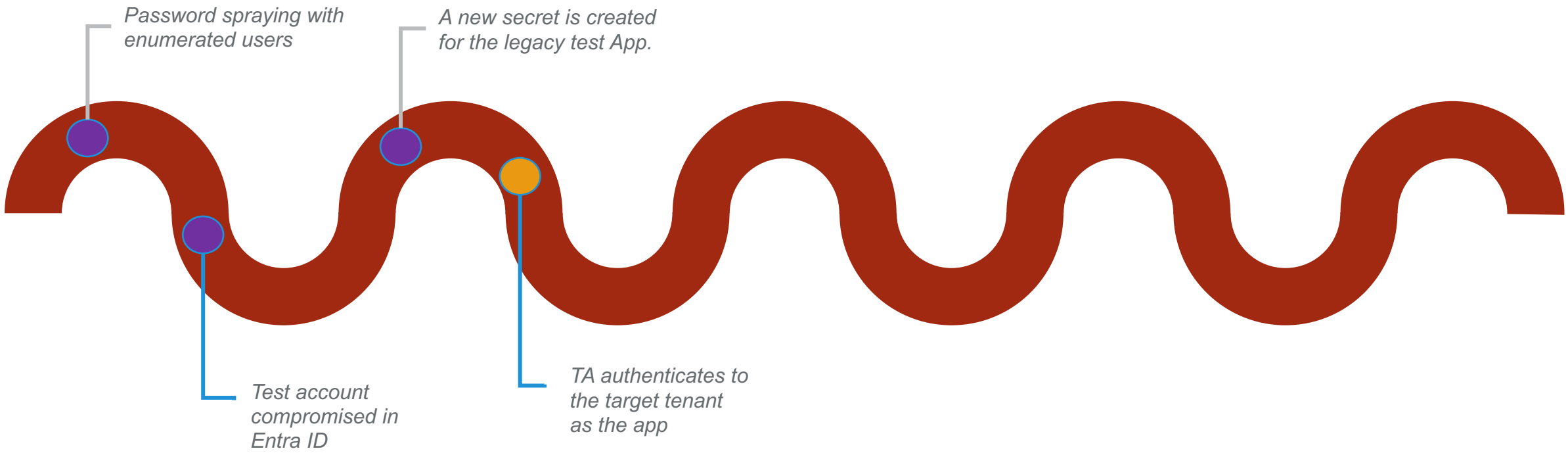
https://www.microsoft.com/en-us/security/blog/2024/01/25/midnight-blizzard-guidance-for-responders-on-nation-state-attack/

MIDNIGHT BLIZZARD'S RECENT IDENTITY-CENTRIC ATTACK PATH



DISSECTING MIDNIGHT BLIZZARD (1/3)

Attack Anatomy



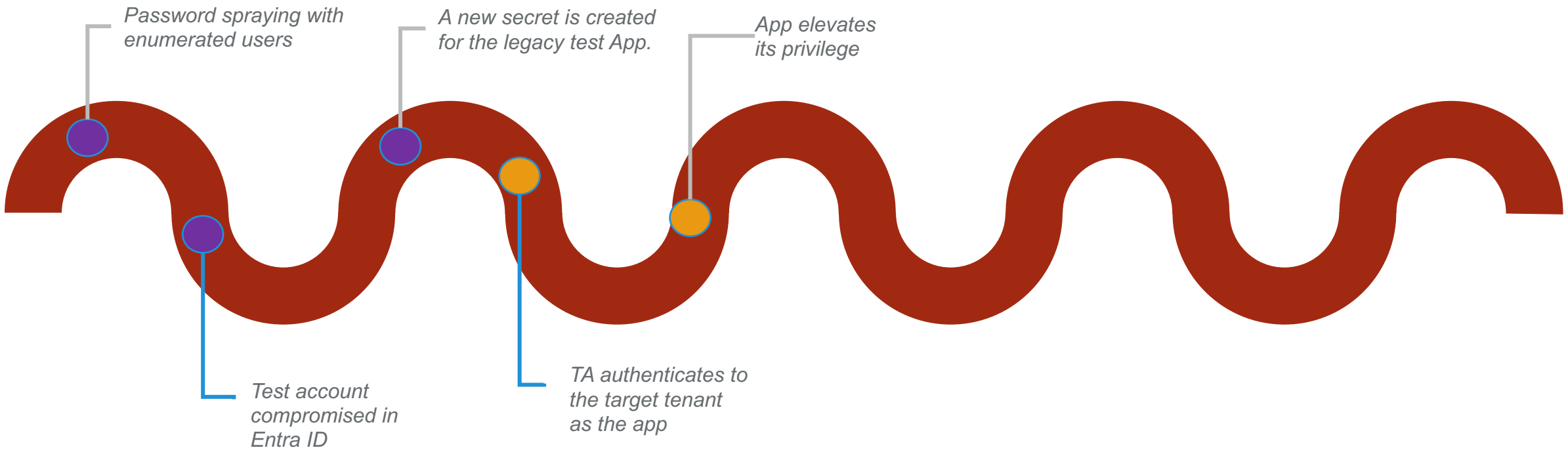
Can I have a Suspicious Sign-on event for an application authenticating itself using a non-interactive sign-on; a certificate or secret?

Not without additional diagnostic settings!

Even then; the challenge will be the high alert volume (noise) as it covers applications that authenticate programmatically as well AND this behavior is not even covered by a single event…

DISSECTING MIDNIGHT BLIZZARD (2/3)

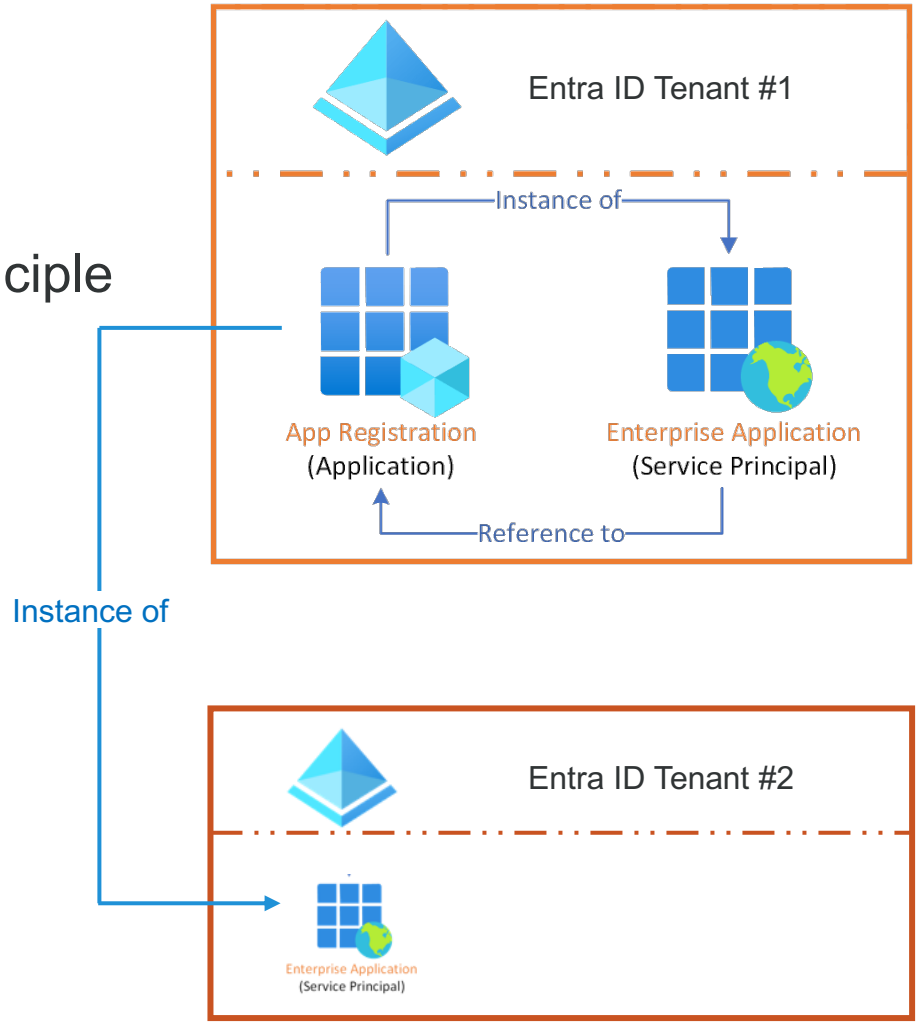
Attack Anatomy



ENTRA ID APPS

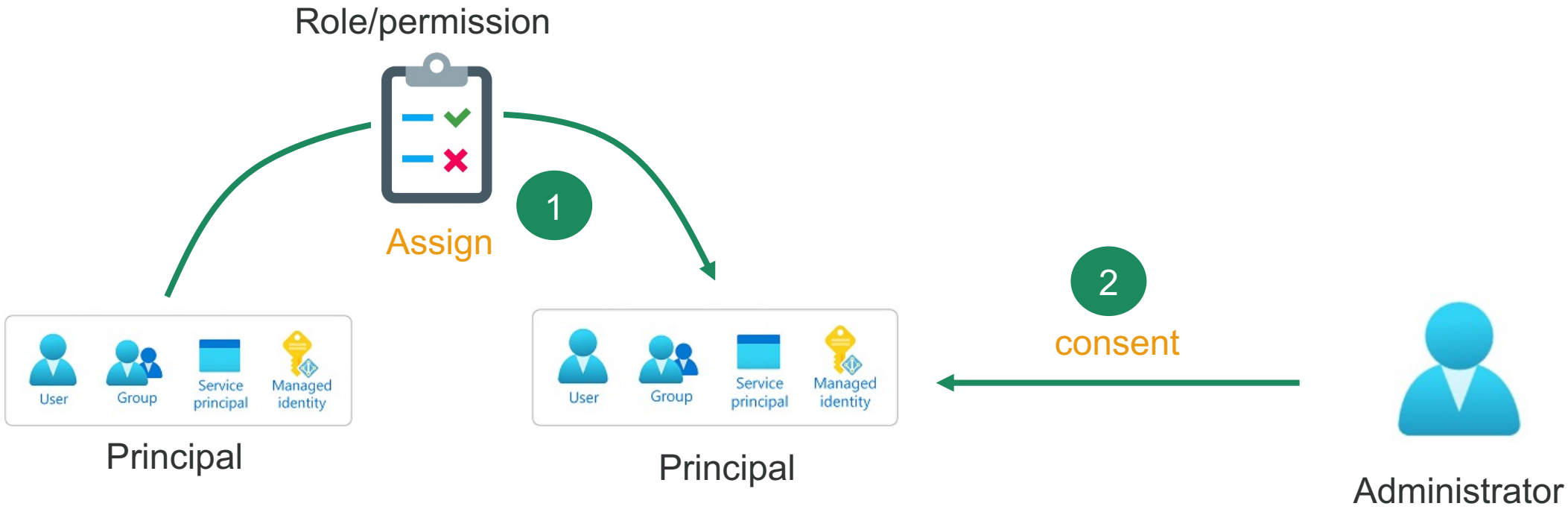
Basic concepts

1. Entra ID App registration (aka Oauth App)
   - > Global representation of the app across all tenants
2. Enterprise application object principle or service principle
   - > Local representation
   - > Owned and foreign
3. App Role
4. API Permission
   - > Delegated (on behalf of a user)
   - > Application (app itself)



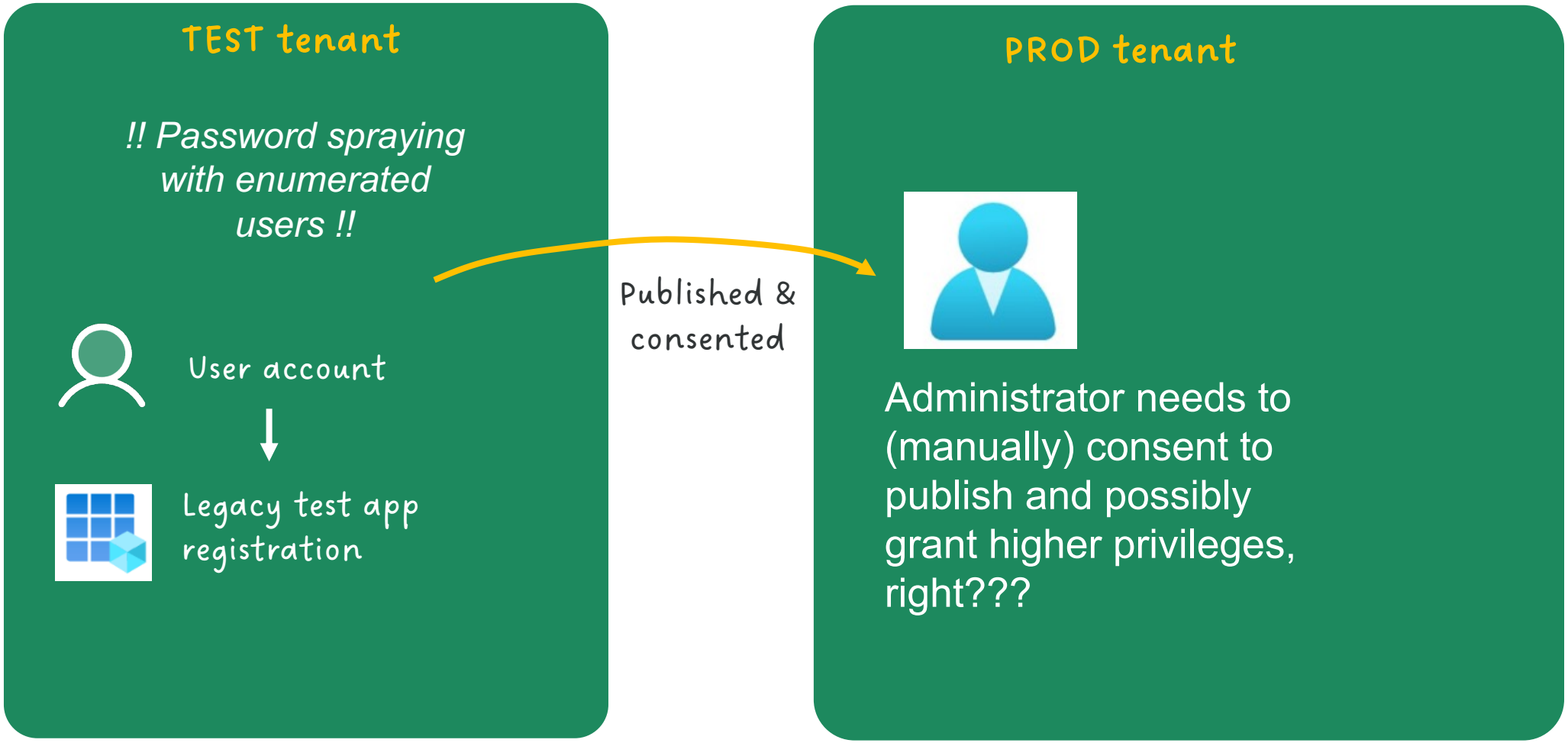
ASSIGNING NEW PERMISSIONS

A 2 steps process



CROSSING THE TRUSTED BOUDNARY

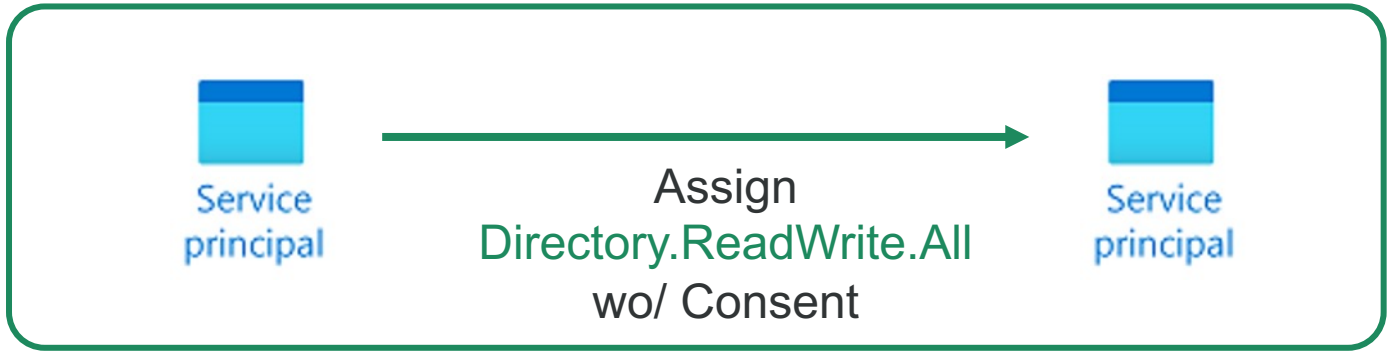
Access to TEST tenant was found. - A test app with high privileges was published to the PROD Tenant.

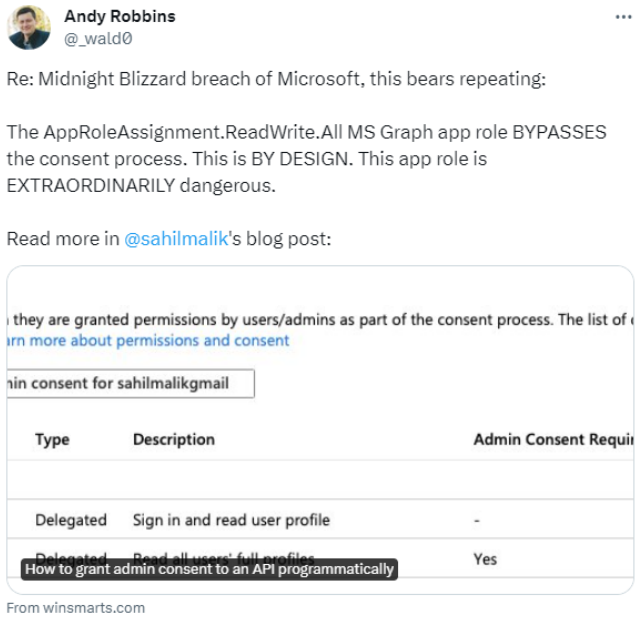


CONSENT PROCESS BYPASS

AppRoleAssignment.ReadWrite.All
MS Graph app roles

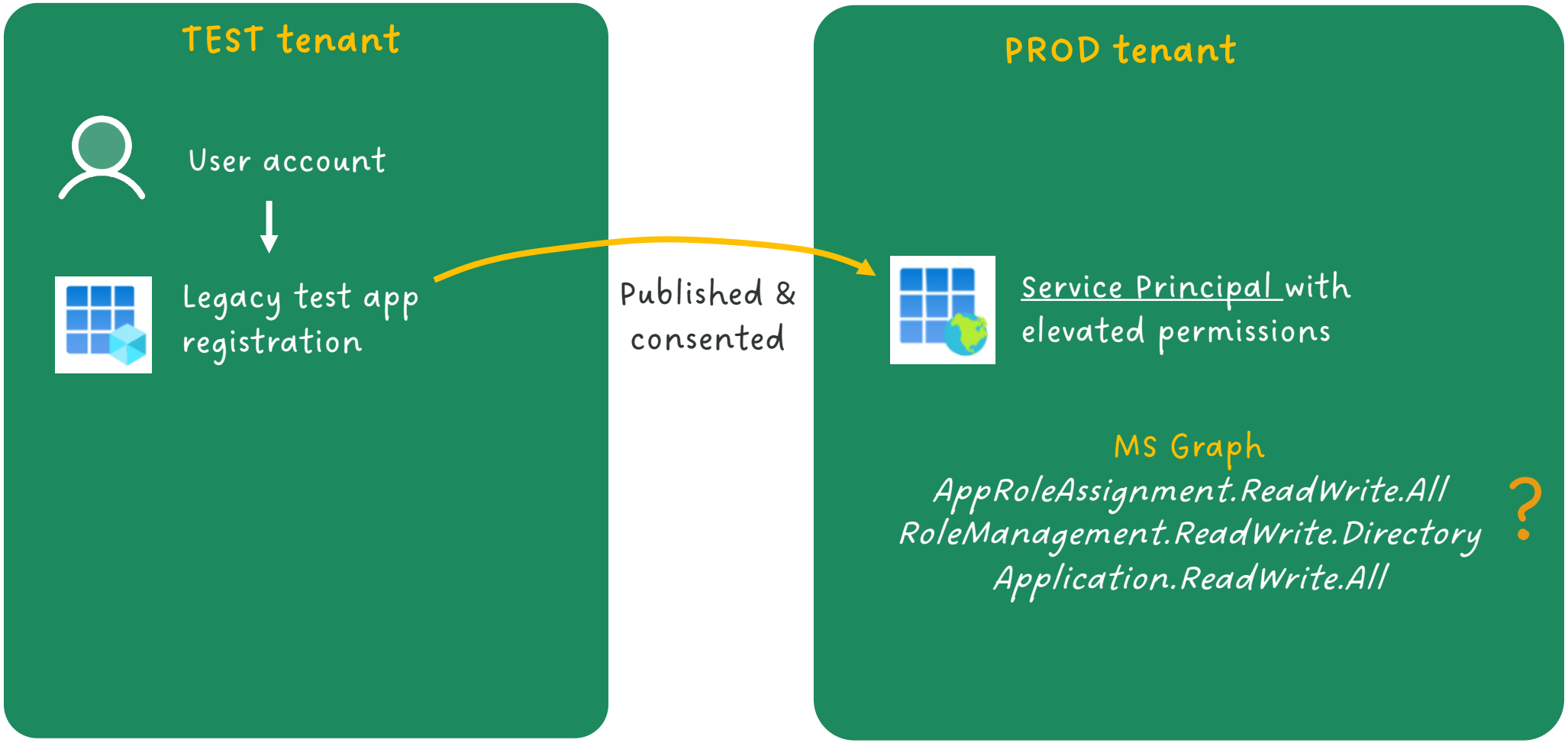
BYPASS Consent Process





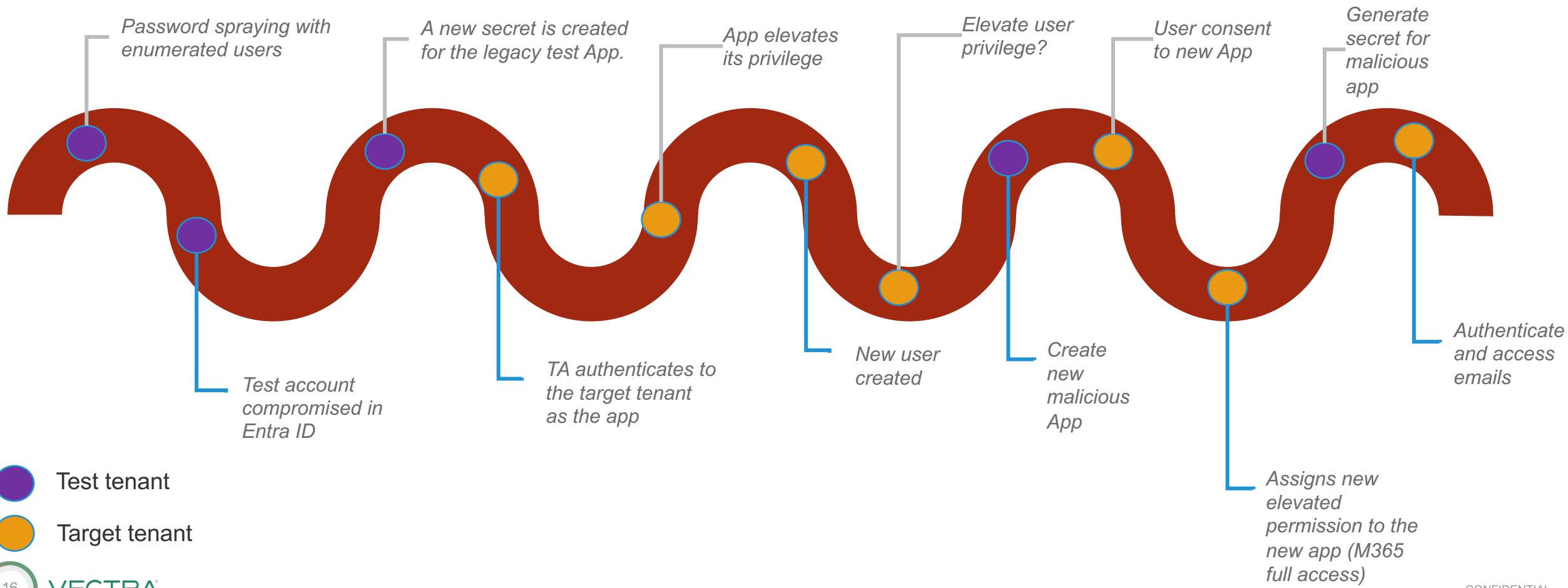
CONSENT

A test app with high privileges was published to the PROD Tenant



DETECTING MIDNIGHT BLIZZARD (3/3)

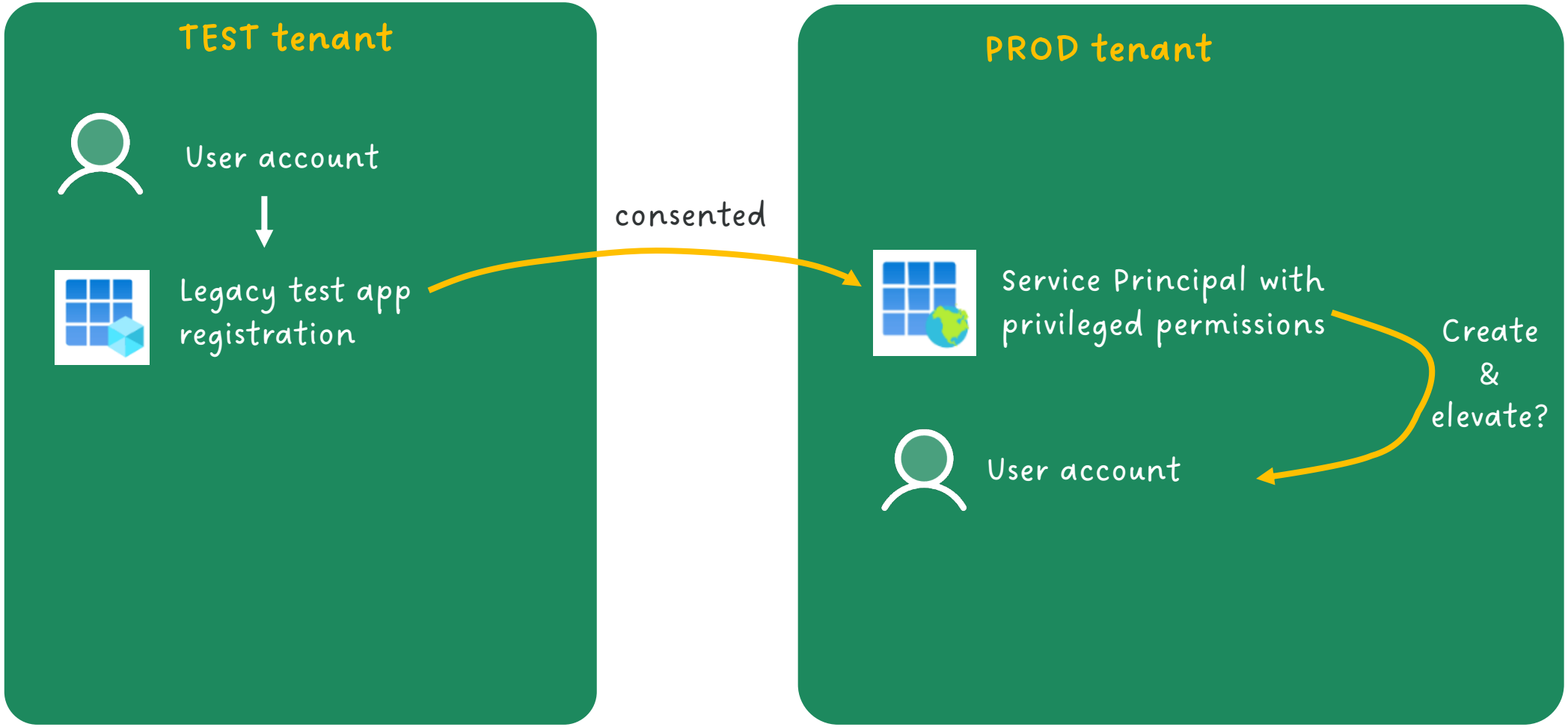
Attack Anatomy



VECTRA

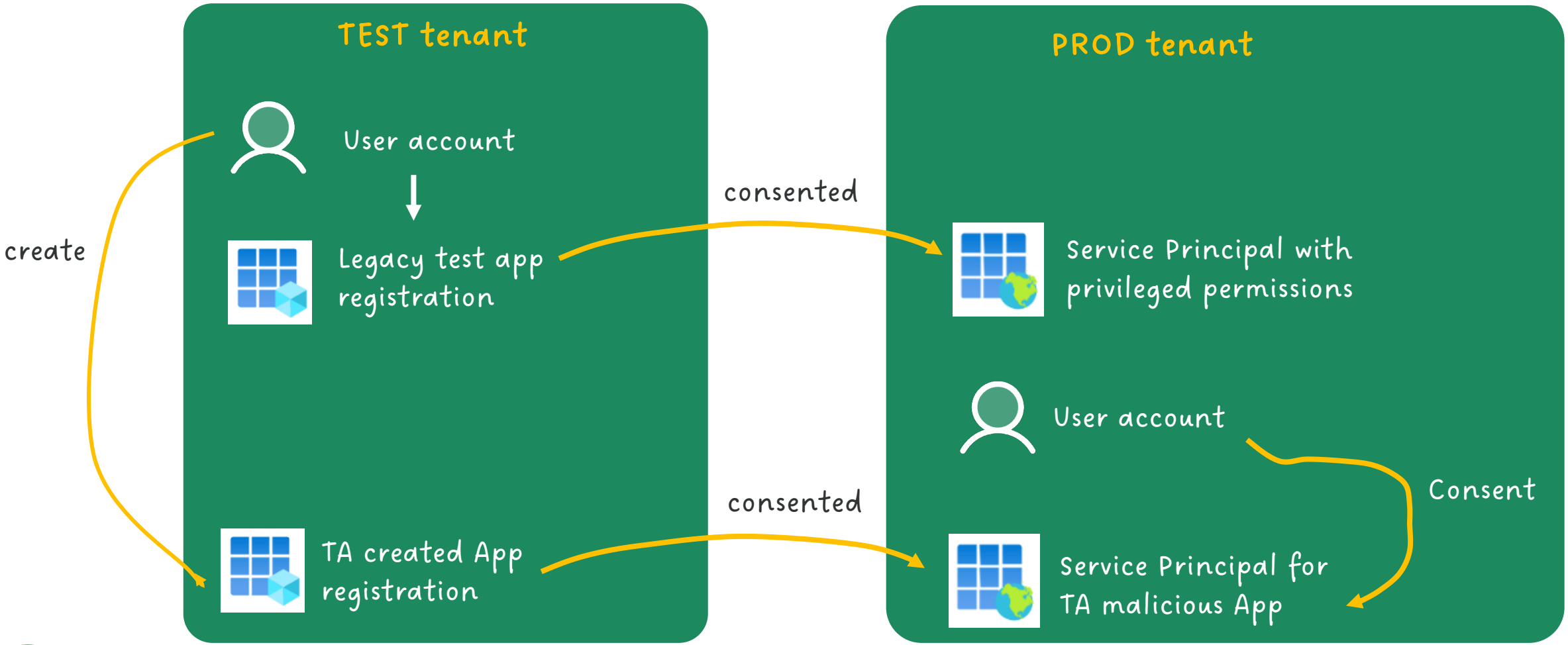
CREATE NEW USER

In the TARGET tenant that would be used to consent the malicious app



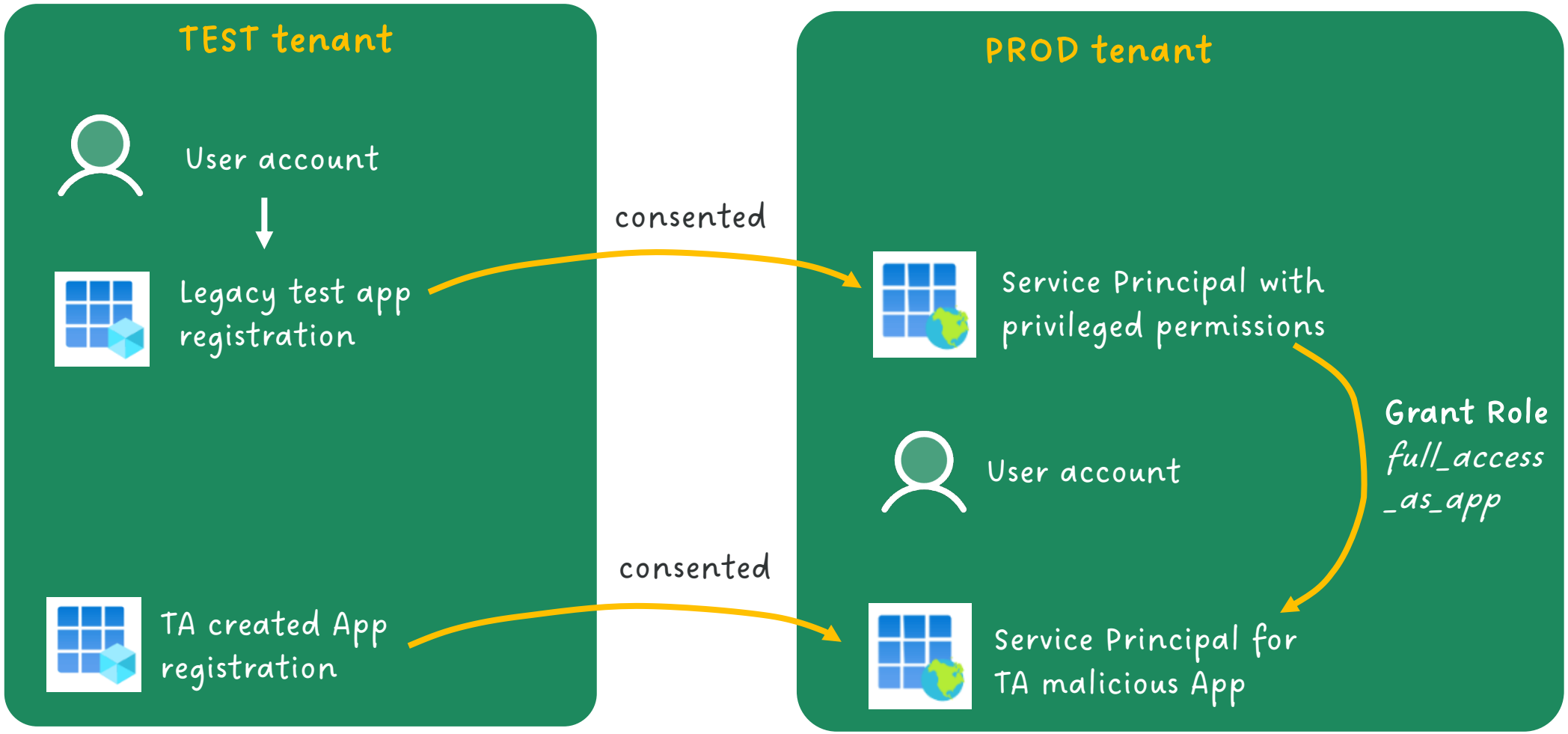
NEW MALICIOUS APP AND CONSENT

Newly created user consent the new malicious app



PRIVILEGE ESCALATION

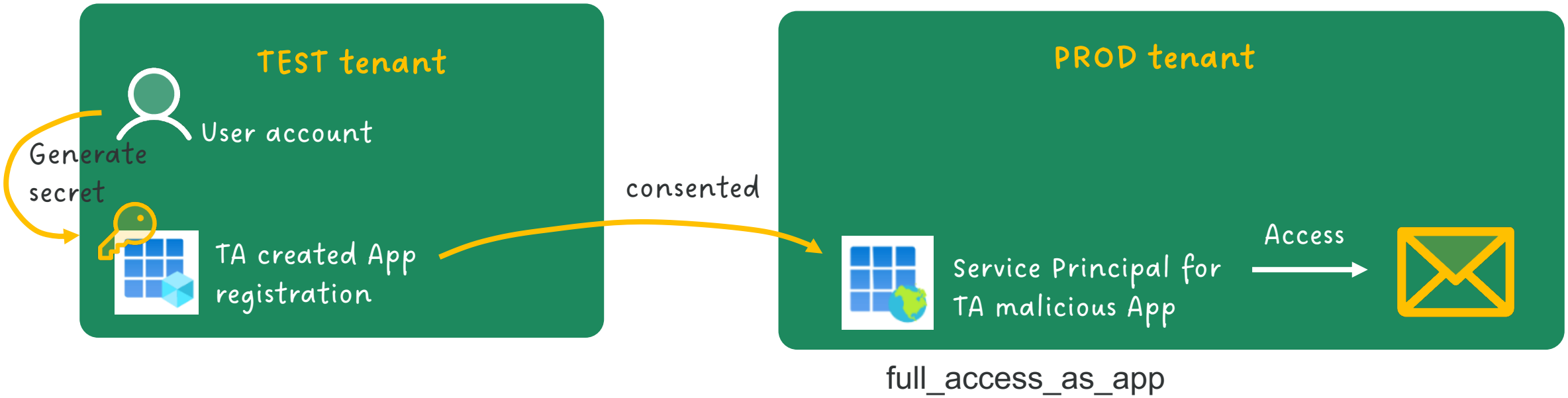
Grant Office 365 Exchange Online: full_access_as_app permission



IMPACT: M365 EMAILS

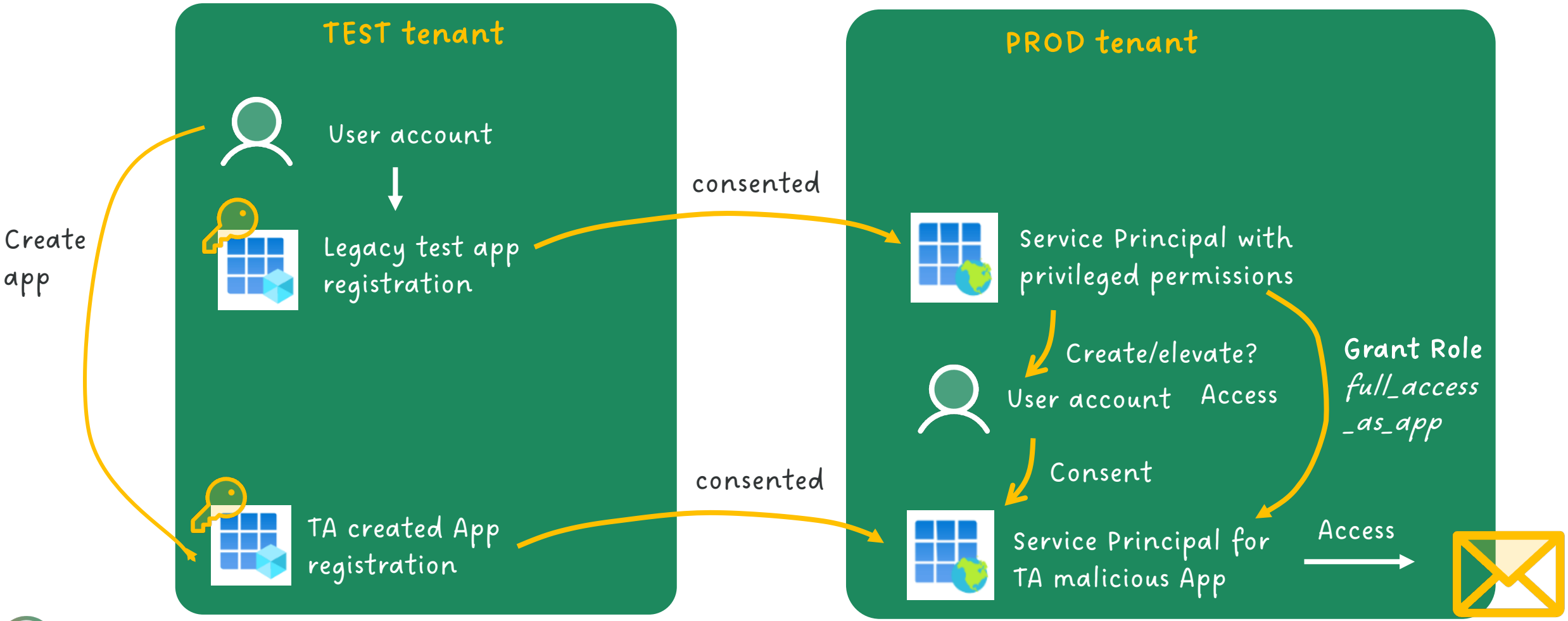
Access to All Email Inboxes!!

1. Through TA created App that has high permission with Office 365 Exchange Online access



PRIVILEGE ESCALATION

Grant Office 365 Exchange Online: full_access_as_app permission

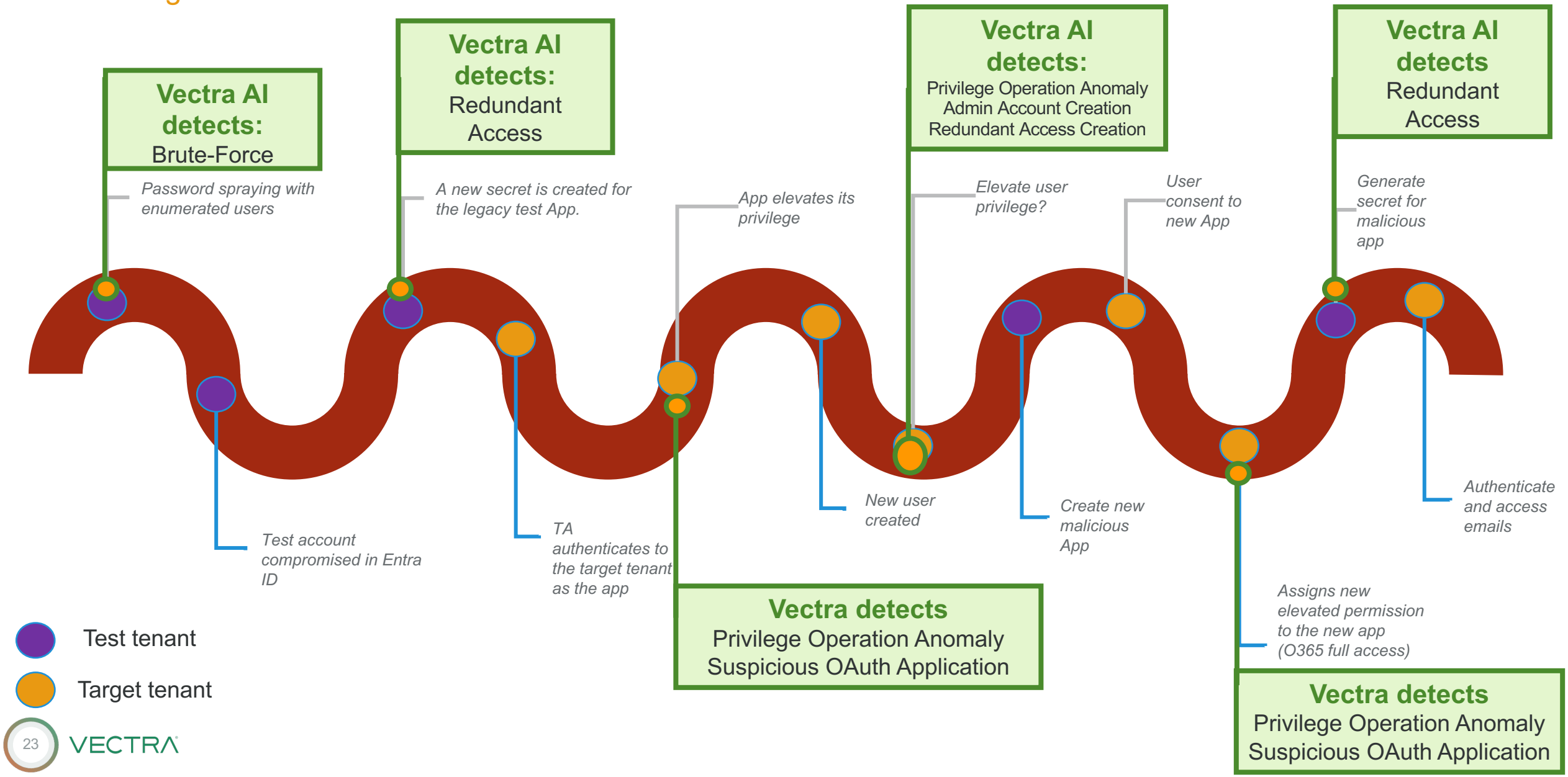


VECTRA®

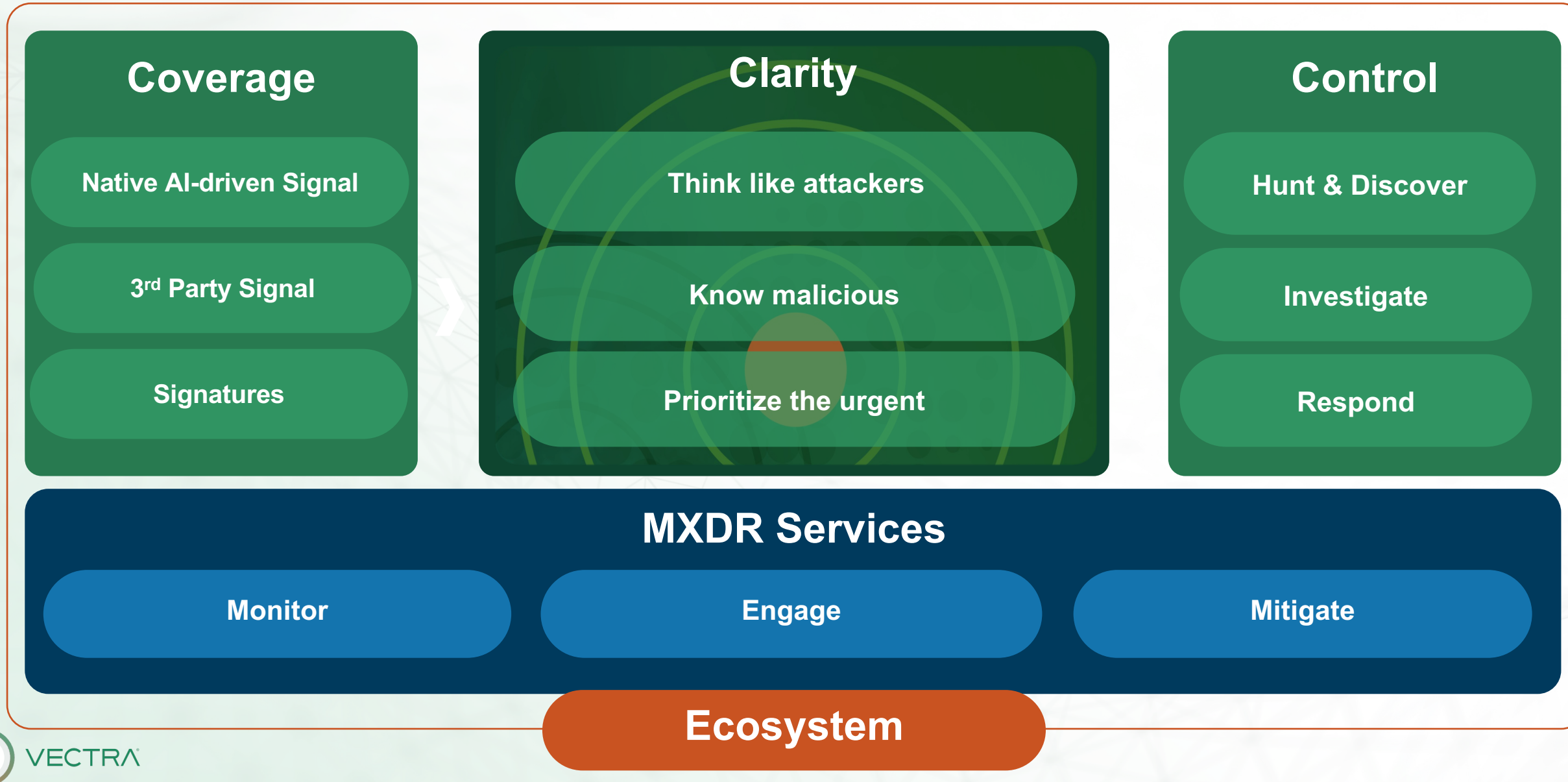
HOW DO WE DO IT

VECTRA AI CAN **DETECT** AND **STOP** MIDNIGHT BLIZZARD ATTACKS

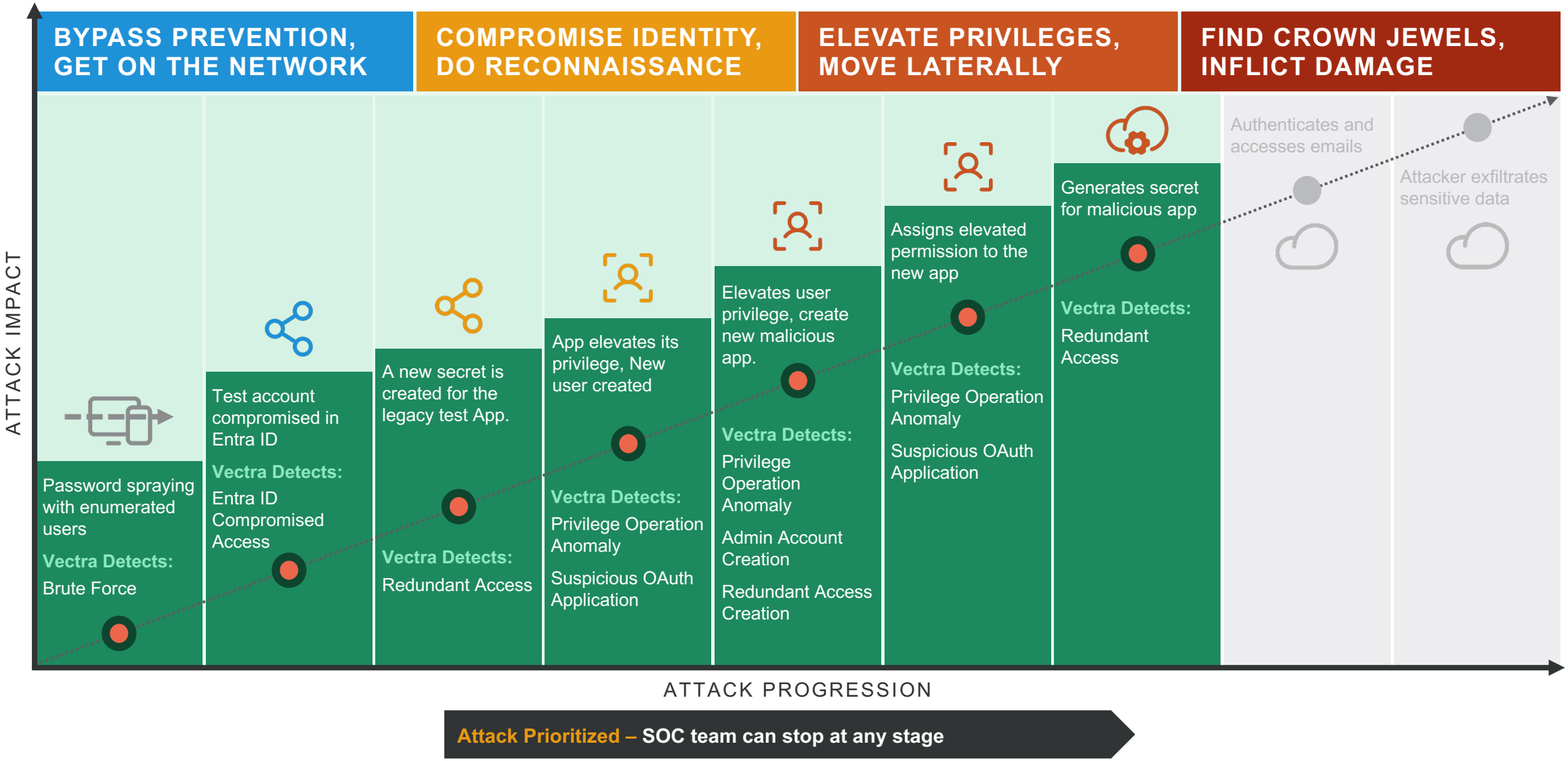
Coverage across the attack



HOW WE DO IT – VECTRA AI PLATFORM, MXDR, ECOSYSTEM



MIDNIGHT BLIZZARD APT29 WITH VECTRA AI



VECTRA AI AND MIDNIGHT BLIZZARD

Coverage

- Early-stage Identity tactics
  - ITDR for Azure AD
  - CDR for M365
- Cloud-centric tactics
  - NDR for Cloud
  - CDR for AWS
  - CDR for Azure*
- Datacenter tactics
  - NDR
  - ITDR for Network AD

Clarity

- AI Prioritization
  - Prioritization based on *known* attack paths (Think like an Attacker)
  - Correlation of Network and Cloud Identity

Control

- Native Response
  - Azure AD (via Azure AD)
    - Disable account
    - MFA re-prompt
  - AD (via Network AD)
    - Disable account
  - Host Isolation (via EDR)
    - Disable endpoint
- Vectra Automated Response Framework
  - Firewalls, Cloud, SASE, etc.

*Planned 2024