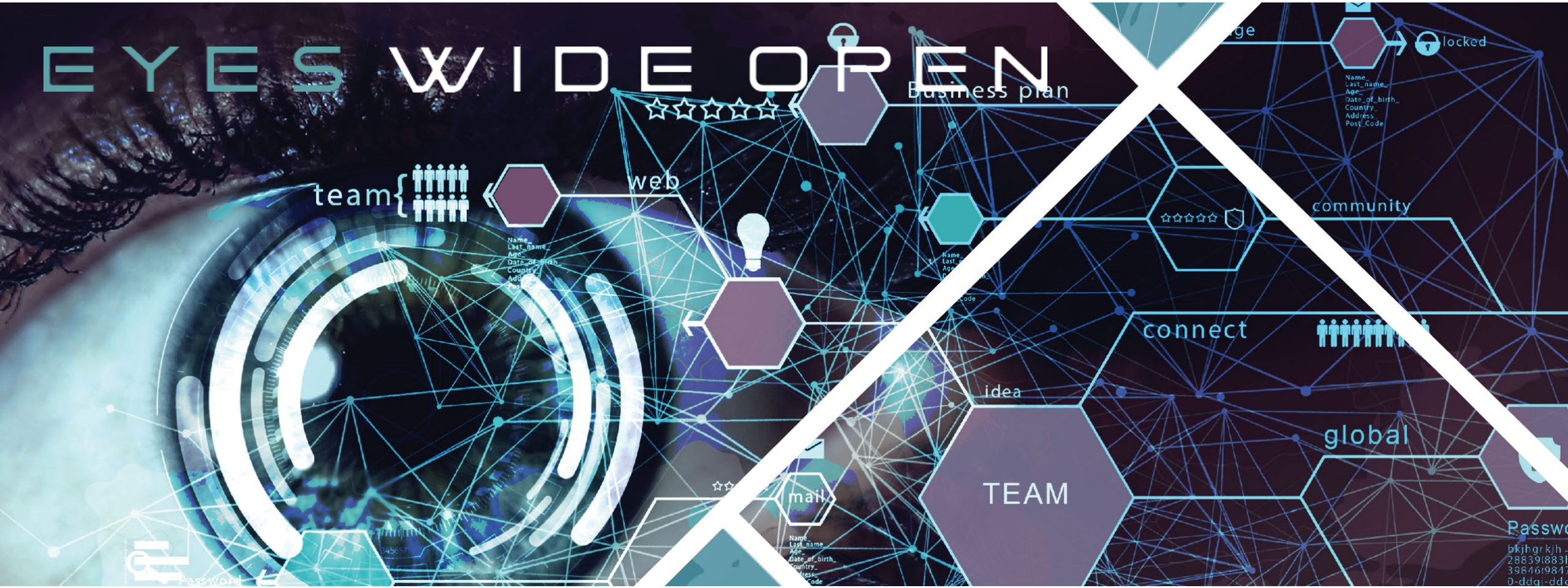
12TH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

TITLE SPONSOR

Island



whoami

- Father and Husband
- CTO @ ProCircular
- CISSP, G|CIH, GWAPT, CCFP
- 18 years of IT experience; 10 in cybersecurity consulting
- I like to golf; my scorecard says otherwise
- Bourbon - with or without ice?

Today's Session

1. What is Zero Trust?
2. A brief history of Zero Trust
3. Current Zero Trust Misconceptions
4. DEMOS ☺
5. Quick Wins
6. Where do we go from here?

What is Zero Trust?

A collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.

Source: NIST 800-207

Principles of Zero Trust

1

Verify explicitly

2

Use least privilege access

3

Assume breach

Zero Trust Timeline

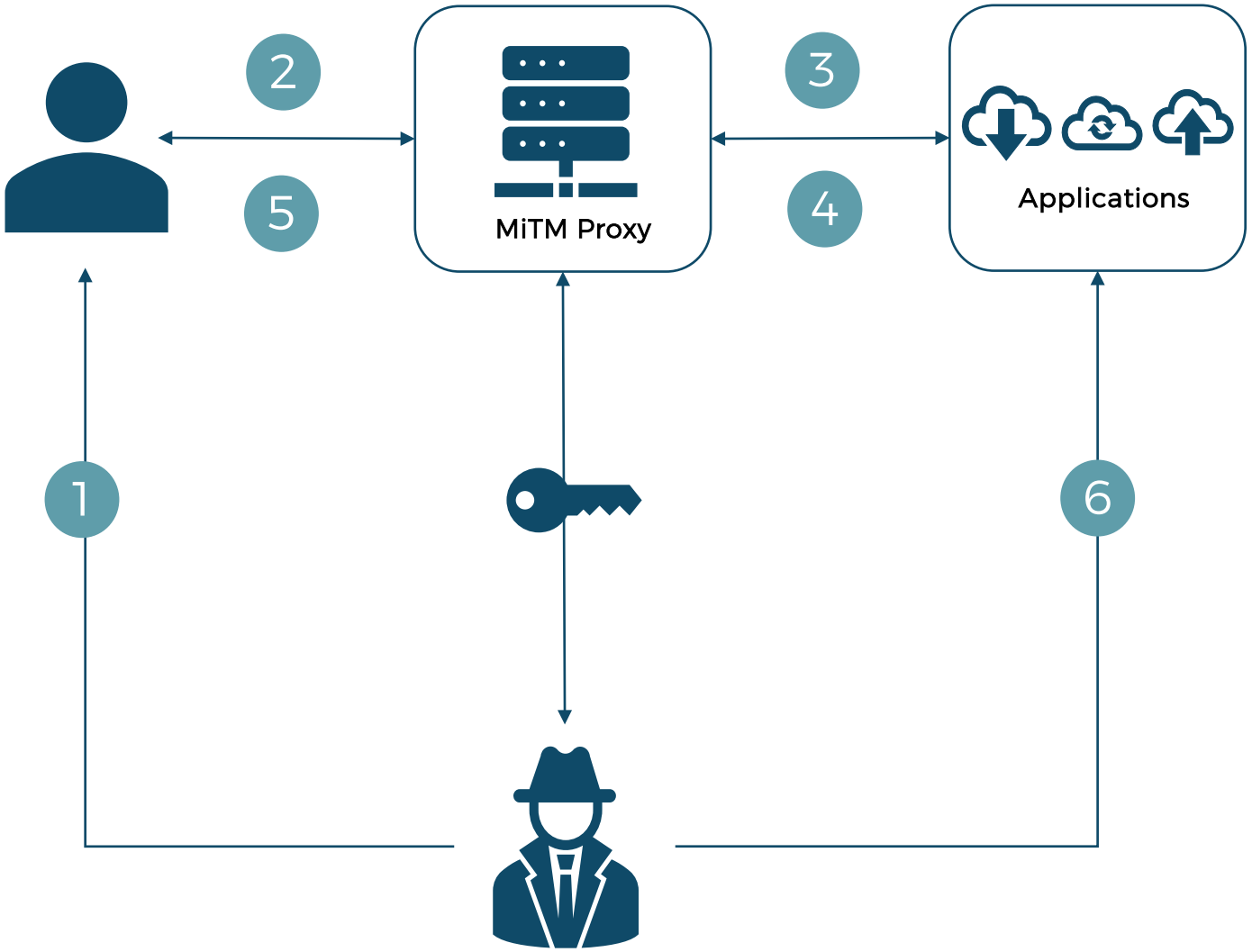
2004	2009	2014	2017	2019
Jericho Forum	Zero Trust is Born	Google & BeyondCorp	Gartner's CARTA	Zero Trust Rebirth

Zero Trust Misconceptions

- SSO + MFA = Zero Trust
- Zero Trust is only about user and device identity
- Applications are trusted once initially vetted
- SaaS apps are ‘out of scope’
- SASE can solve Zero Trust

ATTACK #1

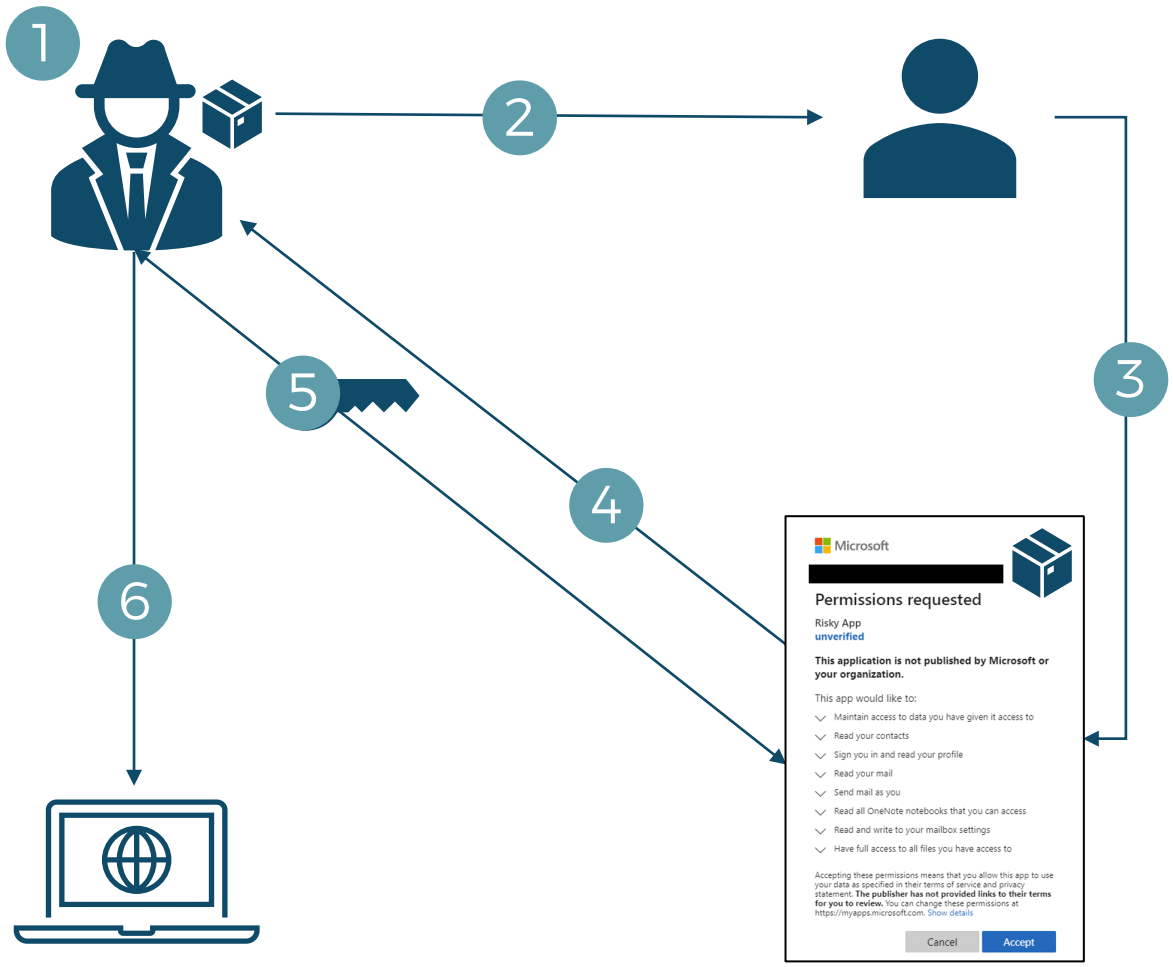
Adversary-in-The-Middle aka MFA Session Riding Bypass



1. Attacker sends phishing email to user.
2. User logs into phishing site.
3. MiTM proxy intercepts and relays request to service or website.
4. Service or website sends MFA request and proxy relays to the user.
5. User inputs additional authentication factor and proxy intercepts session token.
6. Attacker uses captured session token to authenticate as user

ATTACK #2

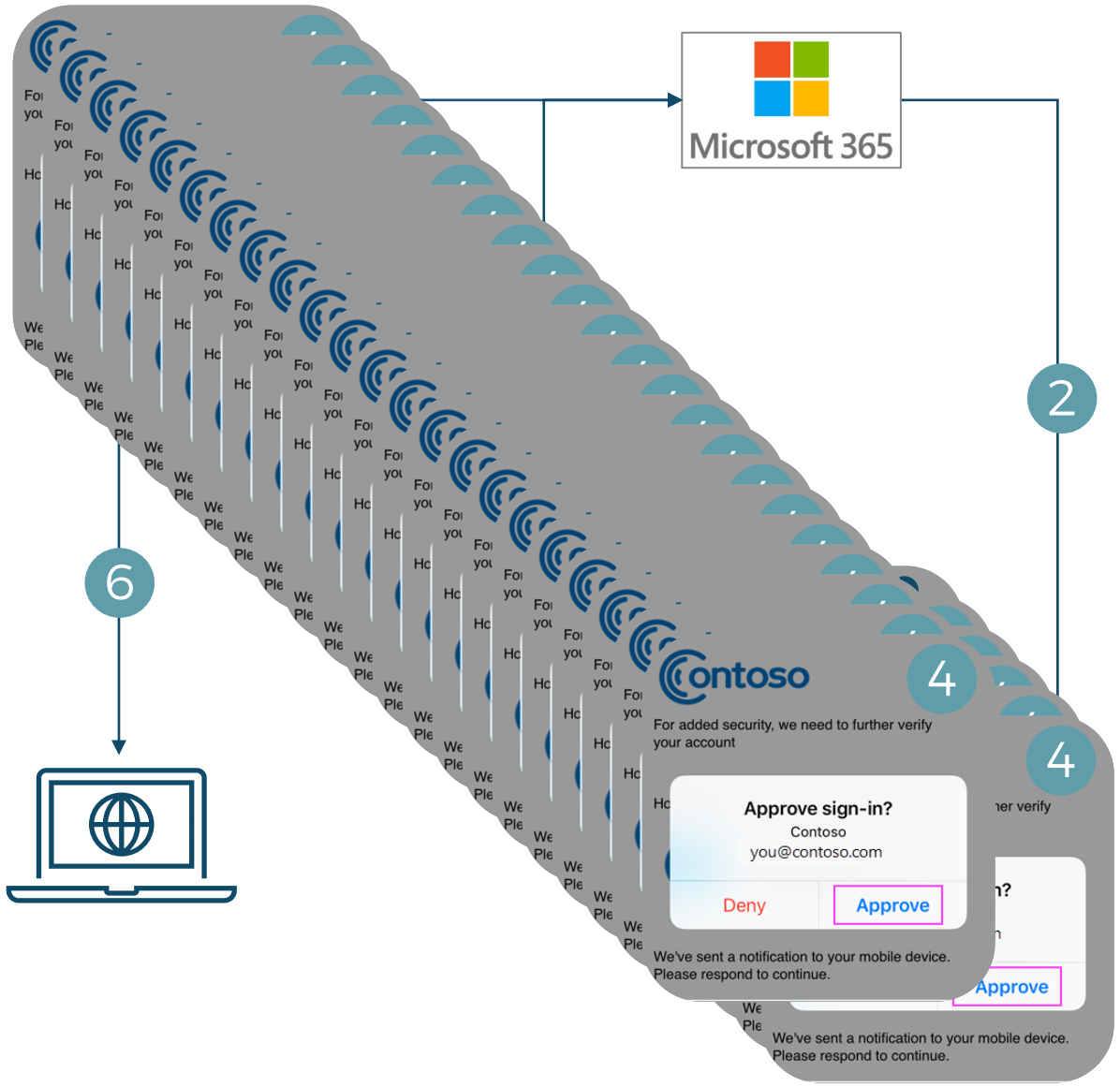
Illicit Application Consent Grant



1. Attacker creates malicious Azure-registered application
2. Attacker sends link via phish to user
3. User authenticates to attacker site and authorizes app consent
4. App sends authorization code to attacker
5. Attacker requests access token through app
6. Attacker uses access token to access systems without MFA prompt

ATTACK #3

MFA Fatigue



1. Attacker authenticates to site with compromised credentials
2. User receives *Push* notification to a mobile device
3. User denies sign-in approval
4. Attacker sends another MFA approval request ….and another, and another…….
5. User approves login request due to 'fatigue'
6. Attacker uses authorized session to access resources and establish MFA persistence

Quick Wins

Session Token Stealing

- Leverage conditional access or authentication policies to restrict access based on multiple factors.
- Robust session time out policies can mitigate long-term or persistent access.
- Leverage behavioral detection technologies to prompt for additional authentication or invalidate duplicate sessions.

Illicit Consent Grant

- Prevent users and group owners from approving application consents.
- Require admin approvals for authorizing consents or limit those that can be auto-approved by granular permissions.
- Continuously monitor your environment for app consents and perform routine audits if unable to block user consents.

MFA Fatigue

- Configure detection rules in your SIEM or data lake to monitor for multiple denies from a user.
- Consider passwordless authentication methods as an alternative to generic push notifications.
- Train users to report these attempts to the IT & security teams.

Where do we go from here?

Verify explicitly

Always validate all available data points:

- User identity and location
- Device health/type
- Service account context
- Data classification

Use least privilege access

Secure both data and user productivity by using a combination of the following:

- Just-in-time (JIT)
- Just-enough-access (JEA)
- Data protection
- Adaptive risk policies

Assume breach

Assume compromise and limit the blast radius:

- Consider identity-based segmentation
- Set default access lists to “deny”
- Include SaaS apps!
- Lean heavily on risk-based monitoring and threat detection

Questions


STAY SASSY
MY FRIENDS
imgflip.com