bechtle

Cybersécurité en 2025:

Analyses et tour d'horizon des tendances afin d'assurer votre protection.

Bechtle Suisse SA
Rita Dib, Security Consultant, Modern Workplace & Security
Karim Trivier, Solution Architect, Modern Workplace & Security

Speakers.

Rita Dib

Security Consultant
Security, Bechtle Suisse SA

rita.dib@bechtle.com

Karim Trivier

Solution Architect
Security, Bechtle Suisse SA

karim.trivier@bechtle.com

Agenda

1. Introduction

2. Cybersécurité en 2024 et évolution des menaces technologiques

Les acteurs de la menace

Les tendances marquantes et leurs implications pour 2025

Attaques sur les infrastructures critiques, attaques sur les infrastructures de crypto-monnaie, démantèlement des groupes cybercriminels, hacktivisme et attaques DDoS, Cybersécurité et intelligence artificielle.

3. MFA sous pression

Pourquoi l'authentification multifactorielle ne suffit plus et comment contrer le vol d'identifiants et de jetons

4. Construire une stratégie de cybersécurité robuste

Aligner votre plan d'action sur les menaces actuelles et vos enjeux métiers

Introduction.

1

Bechtle Suisse SA.
Professional Services.

+500 projets / an	***5*** centres de complétences	***>20*** partenaires	***Organisation centrale avec PMO***
>300 clients	***20*** années d'expérience	***Conseils*** personnalisés	***+40*** Experts en Suisse Romande

Professional Services.

Nos centres de compétences :

Grâce à nos compétences de services dans les domaines du **Professional Services** nous accompagnons nos clients dans leur réflexion **stratégique**, puis dans les phases de **planification** et de **conception** jusqu'à **l'intégration** de leurs solutions informatiques.

Datacenter

Rendre agile votre IT en automatisant les nouvelles générations des Datacenters

Network

L'épine dorsale intelligente de l'entreprise

Modern Workplace

Expérimenter dès aujourd'hui le poste de travail de demain

Business Applications

Relever les exigences digitales d'entreprise modernes

Security

Protéger votre entreprise de toutes sortes de dangers et d'attaques

Cyberattaques en 2024 et évolution des menaces technologiques.

2

Les acteurs de la menace.

États-Nations

Contexte géopolitique

Sabotage
Espionnage

Cybercriminels

Profit financier

Extorsion
Fraude
Exfiltration de données

Hacktivistes

Idéologie

Sabotage
Désinformation

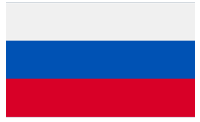
Insiders

Internes
Mécontentement
Vengeance

Sabotage
Exfiltration de données

Les attaques États-Nations.

Alors que les alliances internationales fluctuent, les cyberattaques se transforment en outils au service des objectifs géopolitiques des nations.




Type d'attaques				
Attaquants	Aqua Blizzard Midnight Blizzard Seashell Blizzard Secret Blizzard	Flax Typhoon Granite Typhoon Nylon Typhoon Raspberry Typhoon	Citrine Sleet Jade Sleet Moonstone Sleet Sapphire Sleet	Cotton Sandstorm Mint Sandstorm
Régions cibles	Europe & Asie Centrale Amérique du Nord	Asie de l'Est & Pacifique Amérique du Nord	Amérique du Nord Asie de l'Est & Pacifique	Moyen Orient & Afrique du Nord Amérique du Nord
Domaines cibles	Gouvernement IT ONG	Gouvernement IT Education & Recherche	IT Education & Recherche Industrie	Gouvernement IT Education & Recherche

Attaques sur les infrastructures critiques.

Les infrastructures critiques sont une cible privilégiée des États-Nations

Une cyberattaque russe contre l'Ukraine a interrompu ses services gouvernementaux essentiels

Une usine de bioénergie espagnole victime d'un ransomware

RansomHub

Les systèmes d'eaux des Etats-Unis visés par plusieurs cyberattaques

Cyber Av3ngers

CARR

Les attaques sur les infrastructures critiques ont un impact au-delà de l'infrastructure en elle même. Elles mettent en péril des secteurs entiers et fragilisent les communautés touchées.

Attaques sur les infrastructures critiques.

Cas des systèmes d'eaux et d'eaux usées (WWS) aux Etats-Unis

Interactions entre IT et OT

IT : gestion des données

OT : Supervision, SCADA présente des vulnérabilités dues à leur architecture vieillissante

Obsolescence

Systèmes obsolètes non supportés par les éditeurs

Absence de standardisation

153'000 systèmes d'eau potable, 16'000 stations de traitement des eaux usées. Pas de planification ou de gestion centralisée

Accès distants

SCADA permet un accès distant pour la supervision hors site. Augmentation de la surface d'attaque

Absence de segmentation

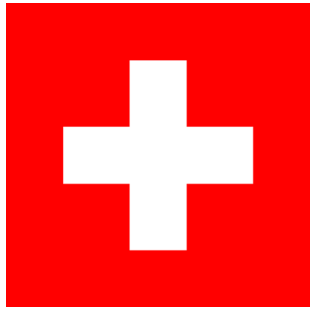
Passage d'une agence municipale à une autre jusqu'à atteindre les WWS

Faiblesses dans la chaîne d'approvisionnement

Dépendance des tiers
Accès à privilèges
Modules prêts à l'emploi mal configurés
Vendor Email Compromise

Attaques sur les infrastructures critiques.

Lois nationales et réglementations européennes



Loi sur la Sécurité de l'Information – LSI

Entrée en vigueur le 1er janvier 2024.

Assurer la protection des informations et des systèmes informatiques au sein de l'administration fédérale et des organisations associées.

Obligation de signaler les cyberattaques contre les opérateurs d'infrastructures critiques dans les 24h à l'OFCS à partir du 1er avril 2025.

Directive Européenne NIS2

Entrée en vigueur le 16 janvier 2023. Transposition en lois dans les différents pays de l'UE.

Applicable à un périmètre plus large d'entreprises dans des secteurs dits essentiels et importants.

Obligations étendues : gestion des risques, chaîne d'approvisionnement, gestion des incidents, sécurité des réseaux et des systèmes.

Obligation de signaler les cyberattaques dans les 72h.

Entreprises suisses concernées : clients au sein de l'UE, chaînes d'approvisionnement, filiales dans l'UE soumis à la directive.

Attaques sur les infrastructures de crypto-monnaie.

Les crypto-monnaies sont une cible privilégiée des attaques nord-coréennes

10 juin 2024
Cyberattaque contre Lykke :
vol de plus de 22 millions de dollars en crypto-monnaies et suspension des opérations.

10 septembre 2024 :
Une série d'attaques majeures secoue l'écosystème des crypto-monnaies et des services financiers en quelques jours.

21 février 2025 :
La plateforme Bybit victime d'un vol d'1,46 milliard de dollars, le plus important de l'histoire.

Attaques sur les infrastructures de crypto-monnaie.

Cas de ByBit

Attaque de la Supply-Chain

Gouvernance

Accès Initial

✖ Téléchargement d'un projet docker malveillant par un développeur de Safe Wallet

Compromission de son poste de travail

Détournement de jetons de session AWS pour contourner les contrôles MFA

Accès au tenant AWS de Safe

Accès au tenant AWS de Safe et à l'interface utilisateur de Safe Wallet

Injection du code malveillant

Injection d'un payload JavaScript dans l'interface utilisateur sur Safe:

- Activation du code uniquement si la transaction provient de Bybit ou de l'attaquant
- Redirection des fonds vers Lazarus

Signature de ByBit

Validation de la transaction par 3 signataires de ByBit, via des hardware wallet, la croyant légitime

✖ **Blind Signing**

Pas de vérification des champs (DelegateCall, adresse de destination)

Exfiltration des fonds

Accès des attaquants aux fonds de ByBit.

Exfiltration de 9$ pour un test puis de 1,4B$ en ETH

Suppression des traces

Restauration de l'ancienne version de l'interface utilisateur

Suppression des traces

Déplacement des fonds

Dispersion des fonds sur plusieurs wallets pour brouiller la traçabilité de la Blockchain

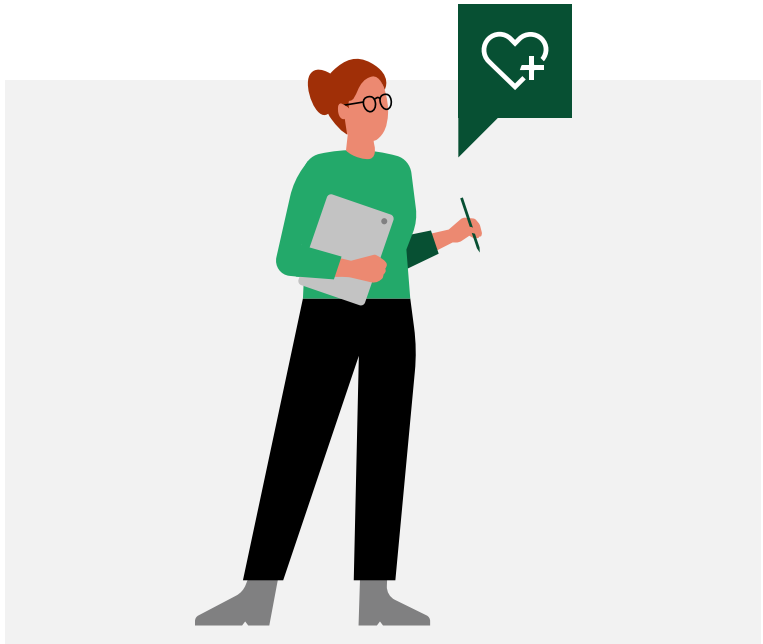
Ingénierie sociale

Attaque sur les environnements Cloud

✚ **Gestion de crise maîtrisée :** Communication immédiate et transparente, maintien des retraits utilisateurs, préservation de la confiance

Attaques sur les infrastructures de crypto-monnaie.

Cas de Bybit, Sécurité de la Supply-Chain

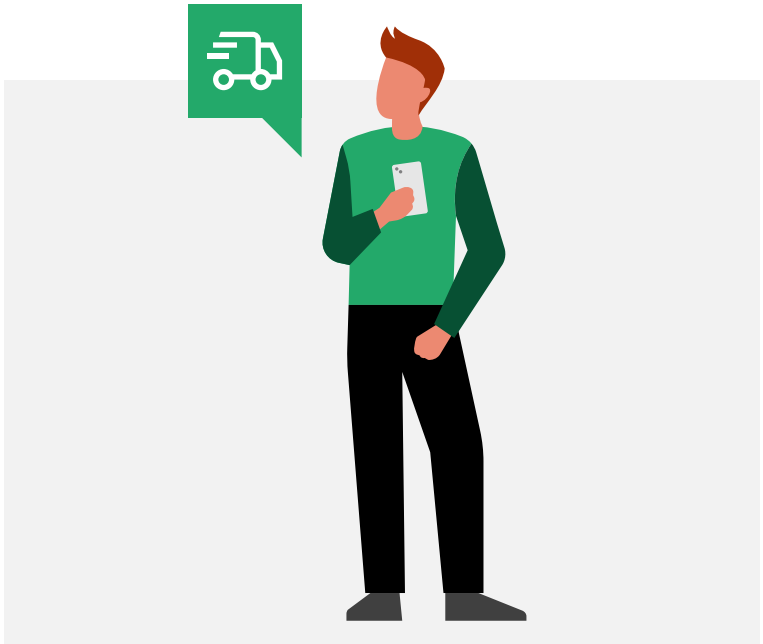


Security By Design

Evaluer le niveau de maturité des fournisseurs dès le RFP.

Intégrer des clauses de sécurité dans les contrats.

Définir les SLAs liés à la sécurité.

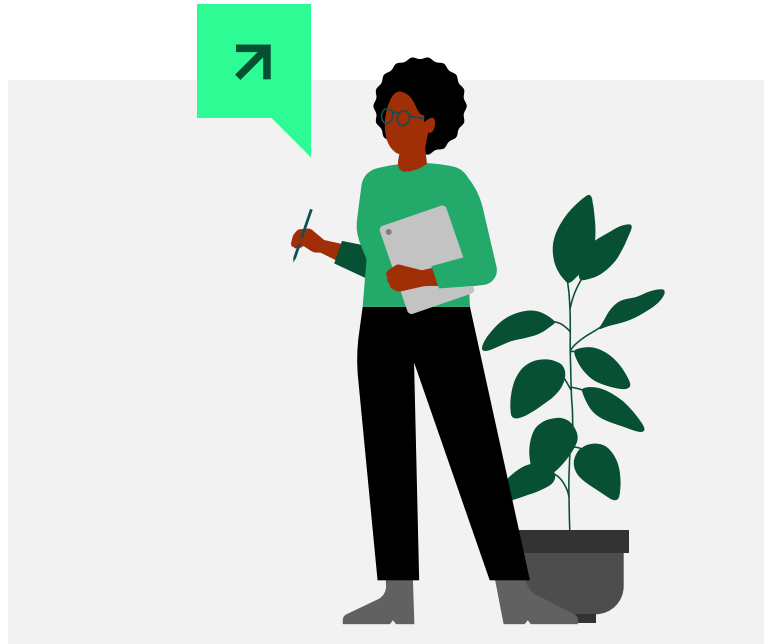


Approche basée sur les risques

Tenir un inventaire de tous les fournisseurs ainsi que les interconnexions et les accès aux équipements et données.

Cartographier les fournisseurs par ordre de criticité.

Identifier les risques liés à chaque fournisseur et envisager les mesures nécessaires.



Gestion des incidents

Surveiller les connexions et les échanges et détecter les évènements à risques.

Collaborer pour préparer un plan de réponse aux incidents communs.

Les cybercriminels en 2024.

LockBit3

23%

Play

10%

RansomHub

8%

Akira

6%

Black Basta

6%

8Base

6%

Baisse du chiffrement dans les attaques par ransomware

x3

Cybercrime-as-a-Service

Ransomware-as-a-Service

Phishing-as-a-Service

19 nouveaux sites de fuites

Zoom sur la Suisse

La Suisse est parmi les top 15 des pays les plus attaqués

Top 3 des acteurs cybercriminels en Suisse :

- Akira réalise des attaques opportunistes, sur divers secteurs d'activités et tailles d'entreprises
- 8Base recourt au chiffrement et aux techniques name and shame
- Black Basta, cible des prestigieuses entreprises et organisations pour réclamer des rançons élevées

Démantèlement de groupes de cybercriminels.

Opération Cronos

Une collaboration internationale contre le réseau LockBit

- Actif de 2019 au 19 février 2024
- Serveurs saisis, sites web sous-contrôle de Cronos, deux membres arrêtés.
- Infiltration dans le réseau, renseignements, collecte massive de données.
- Publication de l'identité du leader, LockBitSupp
- LockBit n'a pas été complètement démantelé mais opère avec une capacité réduite.

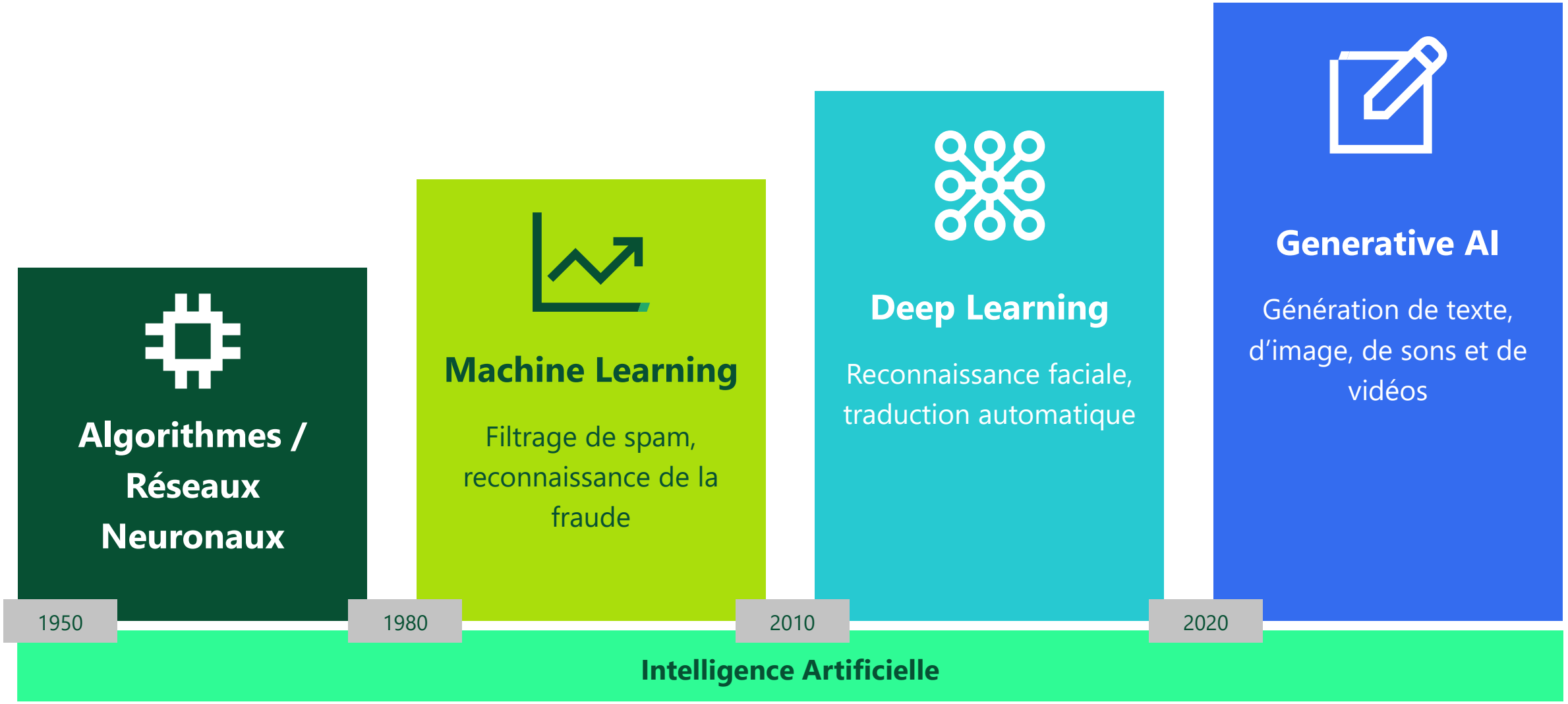
Opération Endgame

Arrêt des infrastructures de diffusion de logiciels malveillants

- Coordination judiciaire européenne, britannique et américaine nommée Endgame.
- Entre le 27 et le 29 mai des infrastructures de diffusion de logiciels malveillants (BumbleBee, IcedID, Pikabot, SmokeLoader et SystemBC) ont été dématelées.
- Plusieurs arrestations en Europe, 100 serveurs arrêtés, 2000 domaines sous contrôles des forces de l'ordre.
- Un montant important d'actifs en cryptomonnaies a été saisi.
- Plusieurs pays dont la Suisse ont aidé dans les arrestations et les interrogations de suspects.

- Succès de la coopération internationale des forces de l'ordre dans la lutte contre la cybercriminalité.
- Démantèlement de véritables entreprises cybercriminelles, longtemps considérées comme intouchables avant ces arrestations.
- Émergence et montée en puissance de nouveaux groupes de ransomware tels que Ransomhub, Akira, Black Basta, Hunters, Play, BianLian, Qilin, Medusa, et BlackSuit….
- La poursuite des opérations d'arrestation reste essentielle pour éradiquer définitivement ces réseaux criminels.

Cybersécurité et intelligence artificielle.



Cybersécurité et intelligence artificielle.

Generative AI double réalité entre protection et menaces

Assistance IA

Security Operations

Utilisation de par les cybercriminels

Fuite de données

Hallucinations de l'IA

Non-conformité

Exploiter l'IA intelligemment, c'est allier performance, contrôle rigoureux et sensibilisation des collaborateurs.

MFA sous pression.

3

L’identité comme nouveau périmètre.

600 millions attaques sur l’identité par jour

99% attaques sur les mots de passe

Faible utilisation du MFA

41% des clients Microsoft utilisent le MFA

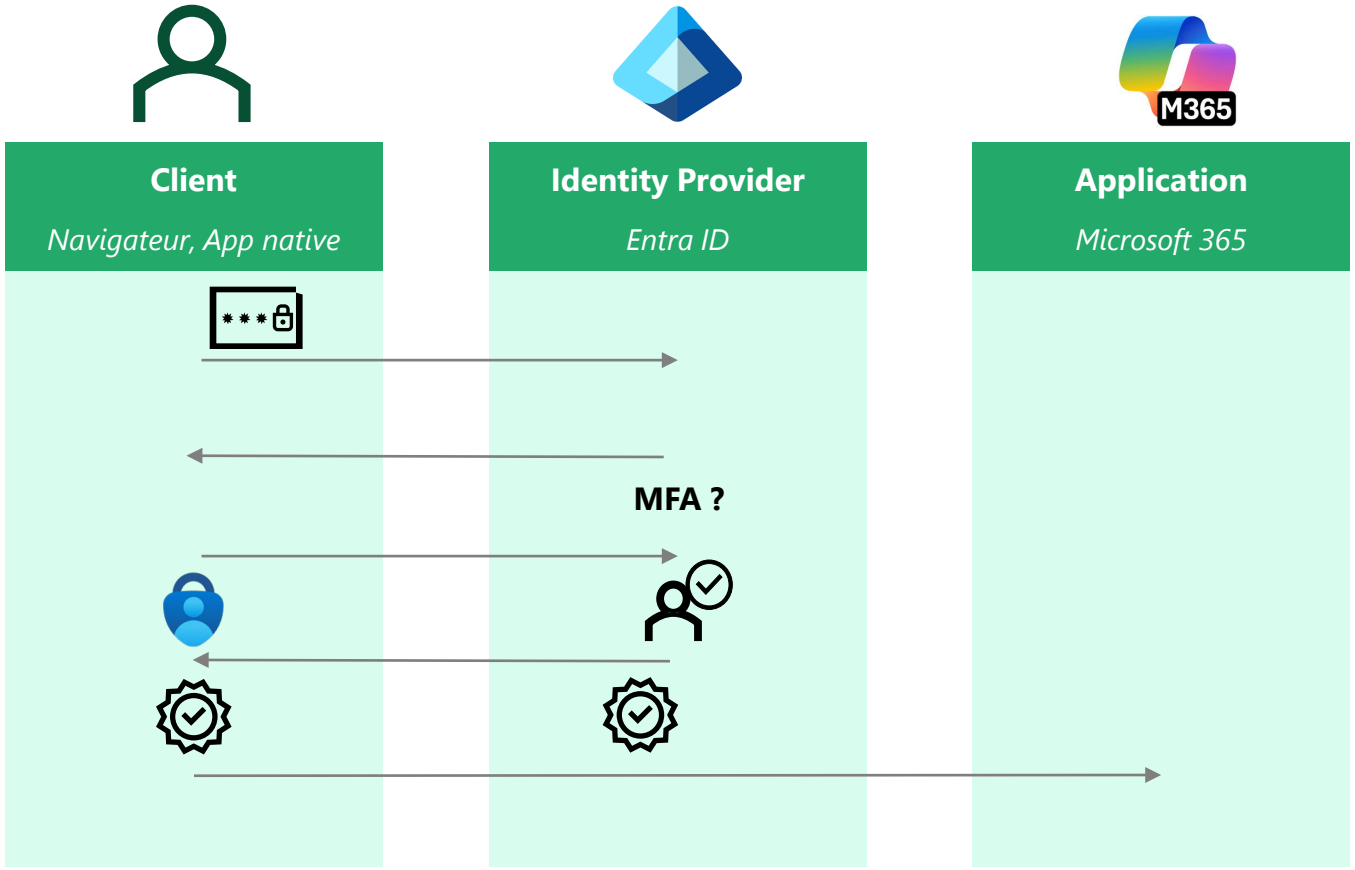
39’000 attaques de Token Theft par jour

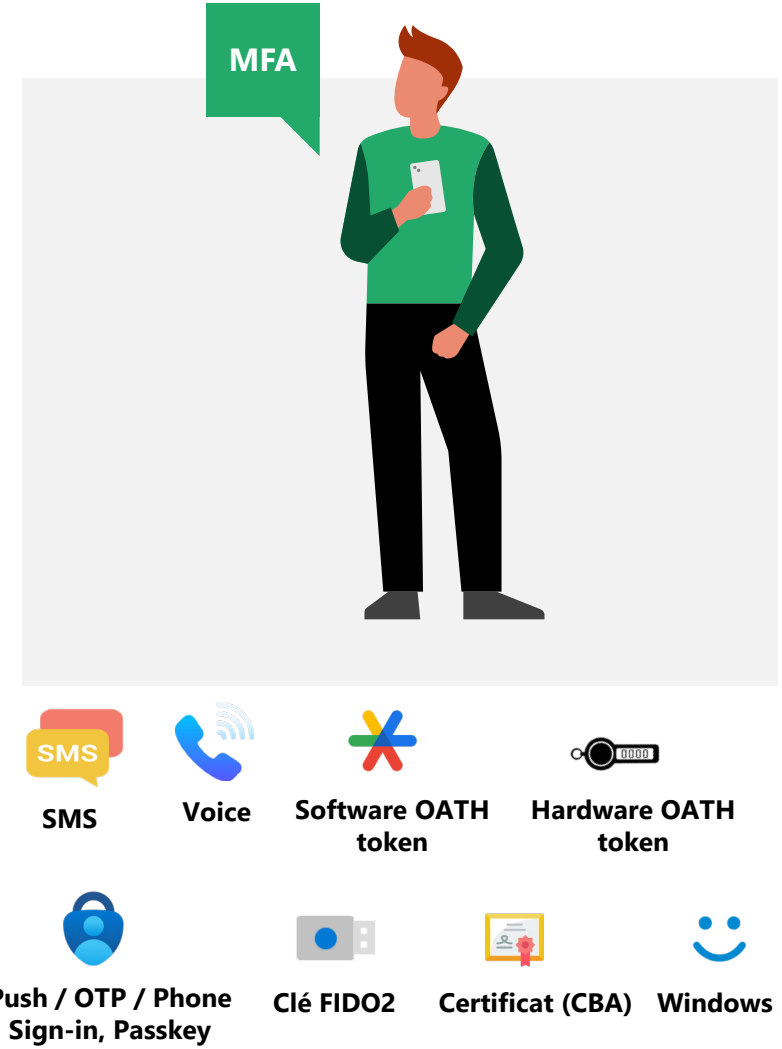
146% taux d’augmentation des phishing AiTM par rapport à l’an dernier

Tycoon, Rockstar, et EvilProxy sont les kits de PhaaS les plus utilisés

0-300 prix mensuel d’un kit PhaaS

Authentification par MFA.





Authentification par MFA.

SIM swapping

SMS / Appels

SMS

Voice

Notifications et OTP

MS Authenticator (Push)

MS Authenticator (OTP)

Software OATH token

Hardware OATH token

Passwordless Phone Sign-in

MS Authenticator (Phone Sign-in)

Phishing resistant

MS Authenticator (Passkey)

Clé FIDO2

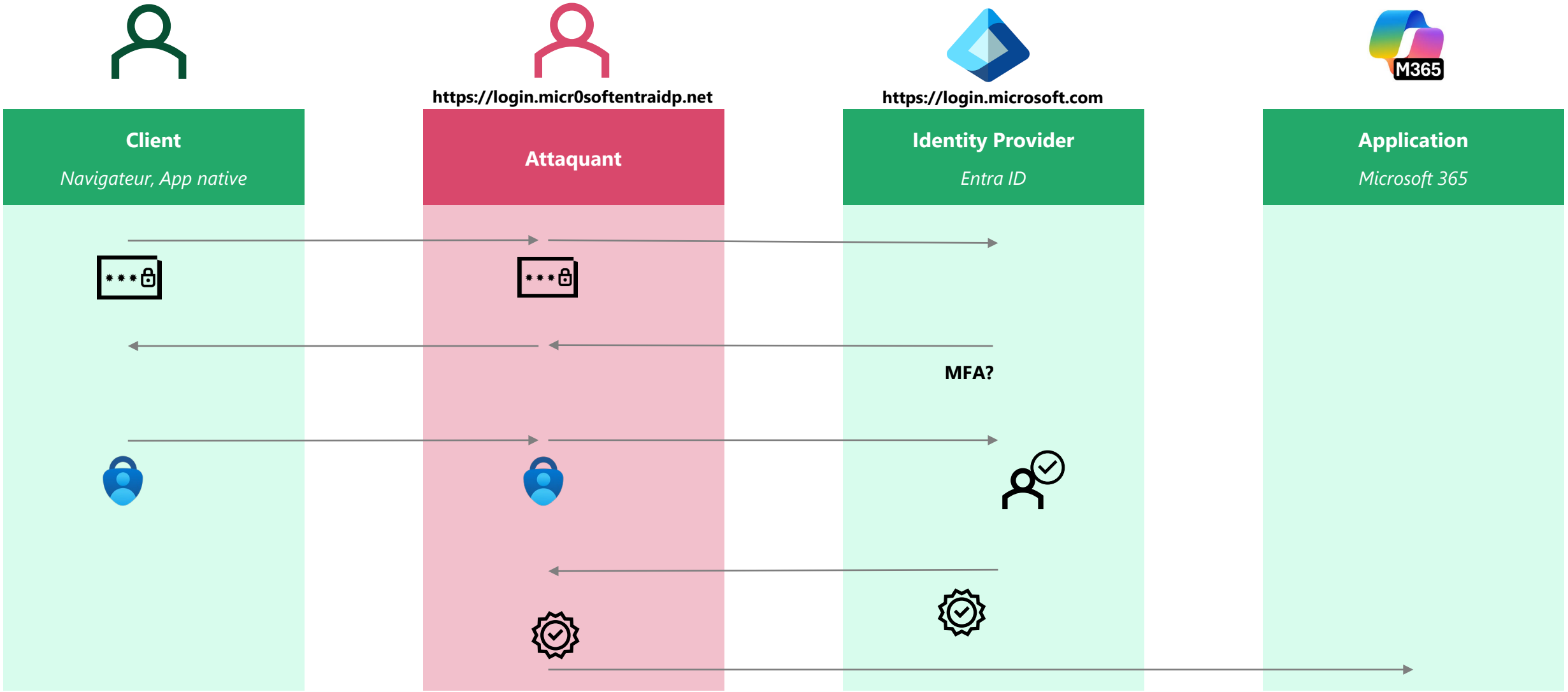
Certificat

Windows Hello

Vishing

Adversary-in-the-middle (AITM) – phishing, smishing

AiTM contre le MFA.



Authentification par MFA.

SIM swapping

SMS / Appels

SMS

Voice

Notifications et OTP

MS Authenticator (Push / OTP)

Software OATH token

Hardware OATH token

Passwordless Phone Sign-in

MS Authenticator (Phone Sign-in)

Phishing resistant

MS Authenticator (Passkey)

Clé FIDO2

Certificat (CBA)

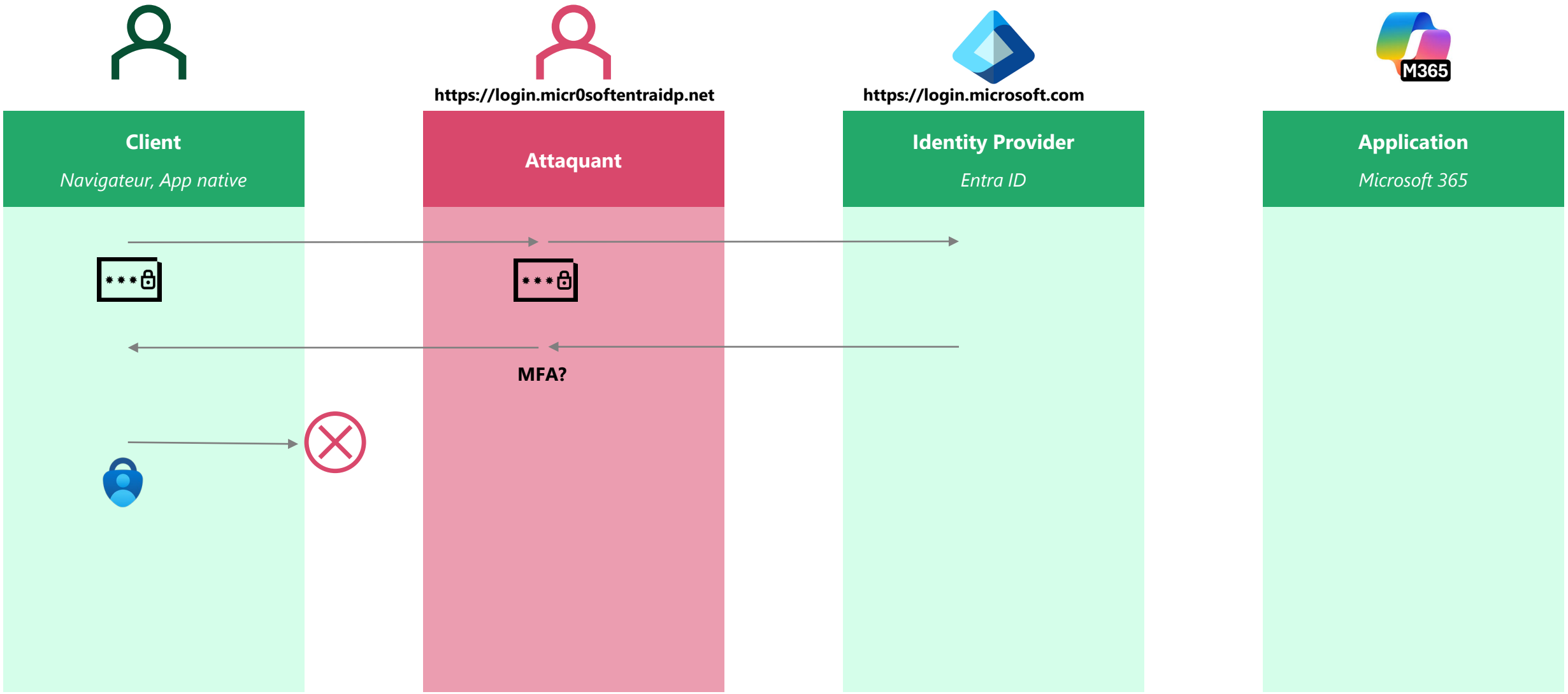
Windows Hello

Vishing

Adversary-in-the-middle (AITM) – phishing, smishing

Phishing Resistant

MFA phishing-resistant.



Authentification par MFA.

Comment sécuriser les authentification quand nous n'avons pas du Phishing-Resistant MFA ?

SIM swapping

SMS / Appels

SMS

Voice

Notifications et OTP

MS Authenticator (Push / OTP)

Software OATH token

Hardware OATH token

Passwordless Phone Sign-in

MS Authenticator (Phone Sign-in)

Phishing resistant

MS Authenticator (Passkey)

Clé FIDO2

Certificat (CBA)

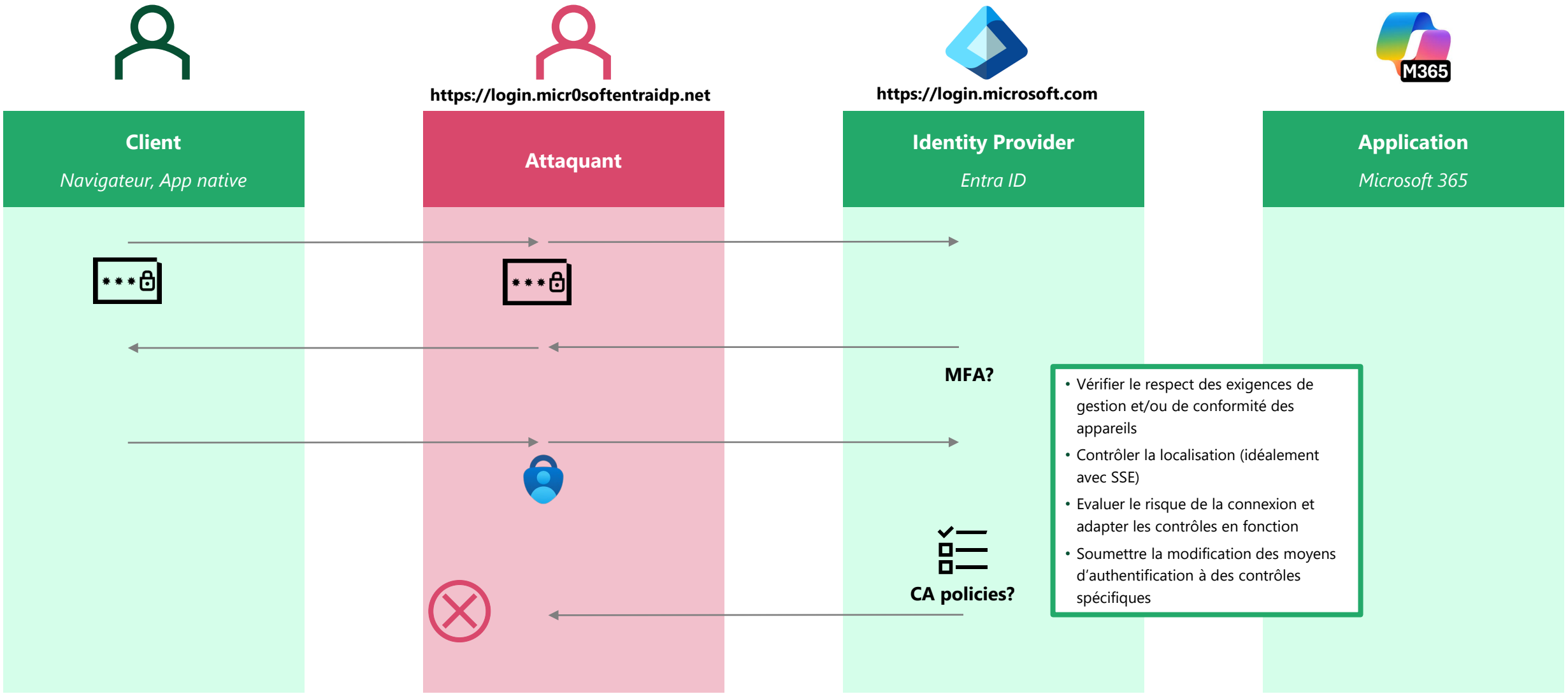
Windows Hello

Vishing

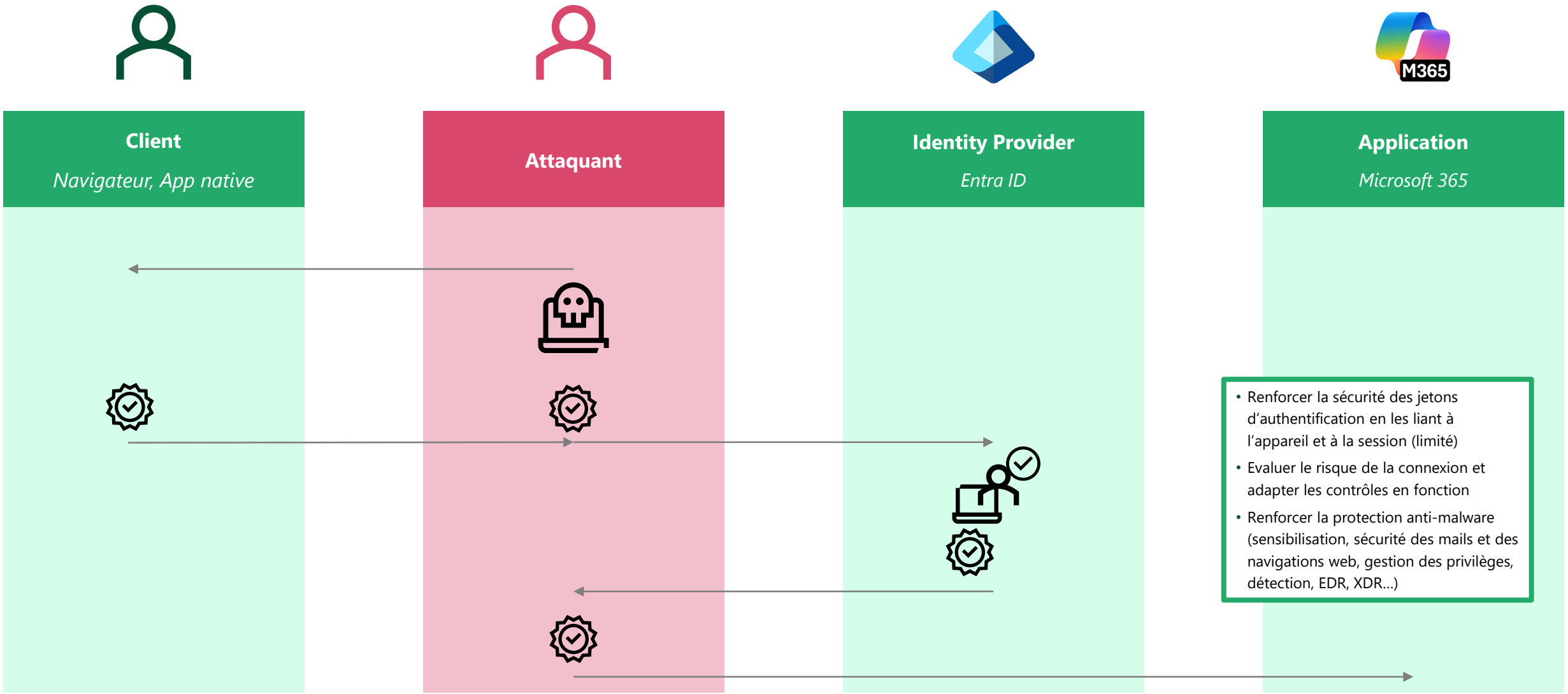
Adversary-in-the-middle (AITM) – phishing, smishing

Phishing Resistant

Protection MFA non Phishing-Resistant.



Pass-the-PRT.


Client
Navigateur, App native
Attaquant
Identity Provider
Entra ID
Application
Microsoft 365
• Renforcer la sécurité des jetons d'authentification en les liant à l'appareil et à la session (limité)
• Evaluer le risque de la connexion et adapter les contrôles en fonction
• Renforcer la protection anti-malware (sensibilisation, sécurité des mails et des navigations web, gestion des privilèges, détection, EDR, XDR…)

Authentification par MFA.

Récapitulatif

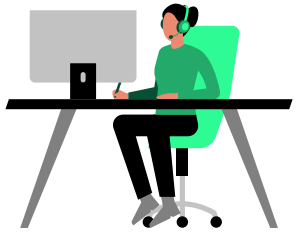
Authentification par mot de passe	Authentification à double facteur *(vulnérable au phishing)*	Authentification à double facteur et accès conditionnel	Authentification à double facteur résistante au phishing
• Phishing, social engineering • Guessing, password spraying • Shoulder surfing, keylogging • Credential stuffing	• SIM swapping • Vishing • Adversary-in-the-Middle	• Token Theft via un malware	• Token Theft via un malware
• Définir une politique de mot de passe stricte. • Sensibiliser les utilisateurs aux attaques, et au phishing en particulier.	• Sensibiliser les utilisateurs aux attaques SIM swapping et Vishing • Privilégier un deuxième facteur autre que les SMS ou les appels	• Appliquer une politique d'accès conditionnel de gestion des appareils : - Soumettre la modification des moyens d'authentification à des contrôles spécifiques - Contrôler la localisation (idéalement avec SSE) - Evaluer le risque de la connexion et adapter les contrôles en fonction - Vérifier le respect des exigences de conformité sur les appareils - Limiter la durée des sessions	• Renforcer la sécurité des jetons d'authentification en les liant à l'appareil et à la session (limité) • Evaluer le risque de la connexion et adapter les contrôles en fonction
• Adopter une authentification à double facteurs	• Combiner la double authentification avec une politique d'accès conditionnel	• Renforcer la sécurité des jetons d'authentification en les liant à l'appareil et à la session (limité) • Utiliser du phishing-resistant MFA	• Renforcer la protection anti-malware (sensibilisation, sécurité des mails et des navigations web, gestion des privilèges, détection, EDR, XDR…)

Construire une stratégie de cybersécurité robuste.

4

Construire une stratégie de cybersécurité robuste.

Les cyberattaques se professionnalisent :
Les attaquants consacrent davantage de temps à préparer leurs offensives. Ils ne cessent d'innover dans les techniques d'attaque et de contournement des défenses, exploitant les nouvelles technologies pour accroître leur efficacité.



La protection des environnements se complexifient :
Les environnements de travail deviennent toujours plus interconnectés (IT, OT, IoT, Cloud, on-premise), ce qui accroît les vulnérabilités et complique les opérations de patching. Les méthodes de protection évoluent sans cesse, mais peuvent parfois elles-mêmes servir de vecteurs d'attaque.

Vers une réglementation plus stricte :
Les réglementations européennes en cybersécurité se multiplient, affectant les entreprises suisses. La Confédération renforce ses exigences en matière de signalement des incidents et fait de la cybersécurité une priorité de la stratégie « Suisse numérique » 2025.

Moins de réactif, plus de proactif

Approche basée sur les risques

Les outils seuls ne suffisent plus

Construire une stratégie de cybersécurité robuste.

Approche basée sur les risques : Cybersecurity Assessment par Bechtle

Connaître son périmètre

- Identifier les processus métiers et leurs besoins en sécurité (DIC)
- Cartographier les assets qui supportent les processus métiers (logiciel, matériel, infrastructure…)
- Identifier les profils des attaquants
- Choisir un référentiel de sécurité adapté au niveau de maturité, exigences réglementaires, secteur d'activité…

Identifier les vulnérabilités et les risques

- Evaluer les mesures de sécurité en place
- Identifier les vulnérabilités présentes
- Analyser les risques

Construire une feuille de route

- Formaliser un plan d'actions sur le court, moyen et long terme à la fois ambitieux et atteignable
- Prioriser les actions qui réduisent les risques critiques et qui agissent sur les activités métiers prioritaires
- Calculer le budget et les ressources nécessaires pour la réalisation des actions

Obtenir la validation de la Direction

- Présenter les résultats à la Direction
- Œuvrer à obtenir son soutien et son engagement dans la stratégie de sécurité

Suivre et Mettre à jour

bechtle

Bechtle IT Forum

"BRINGING INNOVATIONS, TRANSFORMING FUTURES".

24 Juin 2025 - SwissTech Convention Center

https://www.bechtle.com/ch-fr/a-propos-de-bechtle/evenements/bechtle-it-forum-2025

#BITF25


bechtle