Microsoft 365 Defender

Simulation d’attaque, détection et réponse

WEBINAR | 29.03.2022

Chérif Tunkara – Solution Architect
Killian Bebel – Senior IT Project Engineer
Karim Trivier – IT Project Engineer

Agenda.

1. Bechtle
2. M365 Defender
3. Attack Scenario
4. Attack Demo
5. Detect and Respond Demo
6. Prevention
7. Customer integration use case
8. Q&A

Bechtle Suisse SA.

Bechtle Suisse SA – en Romandie

>250
EMPLOYES

+65 EXPERTS
SUISSE ROMANDE

4
BUSINESS UNITS

PROFESSIONAL SERVICES
MANAGED SERVICES
DATA & ANALYTICS
SKILLS MANAGEMENT

>300 CLIENTS en Suisse Romande

>20
PARTENAIRES

Top-level certifications

- CITRIX
- CISCO
- DELL
- FORTINET
- HPE
- MICROSOFT
- NINTEX
- POWELL
- TRENDMICRO
- VEEAM
- VMWARE
- …

CONSEILS
PERSONNALISES

20
ANNEES D' EXPERIENCE

ORGANISATION CENTRALE AVEC **SPOC**

PME, ENTERPRISE ET PUBLIC

PLAN
BUILD
RUN

NOS PROPRES DATA CENTERS
En SUISSE

+500
PROJETS / AN

M365 Defender.

Microsoft 365 Defender

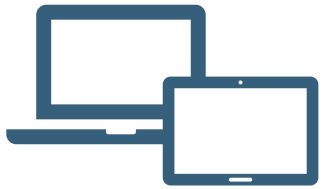
Solutions overview

EMAIL & DOCS

Microsoft Defender for Office 365

IDENTITIES

Microsoft Defender for Identity



ENDPOINTS

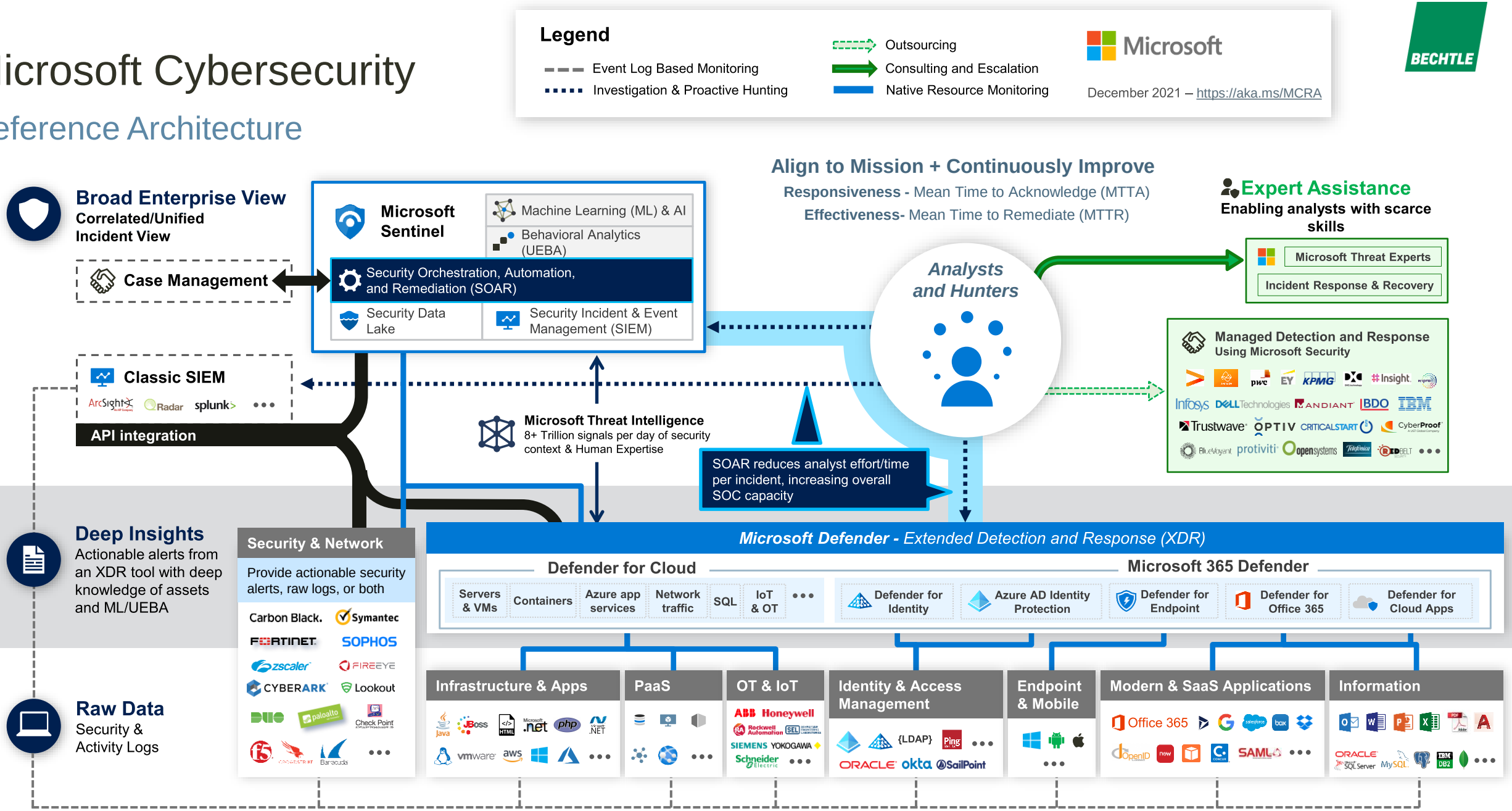
Microsoft Defender for Endpoint

APPS & CLOUD APPS

Microsoft Defender for Cloud Apps

Microsoft Cybersecurity

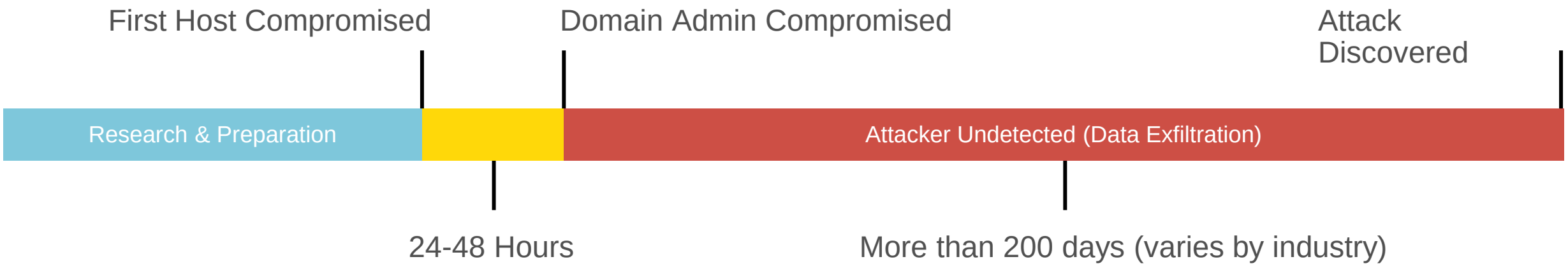
Reference Architecture



Attack Scenario.

Typical attack

Timeline & observations



ATTACK SOPHISTICATION

Attack operators exploit any weakness

Target information on any device or service

TARGET AD & IDENTITIES

Active Directory controls access to business assets

Attackers commonly target AD and IT Admins

ATTACKS NOT DETECTED

Current detection tools miss most attacks

You may be under attack (or compromised)

RESPONSE AND RECOVERY

Response requires advanced expertise and tools

Expensive and challenging to successfully recover

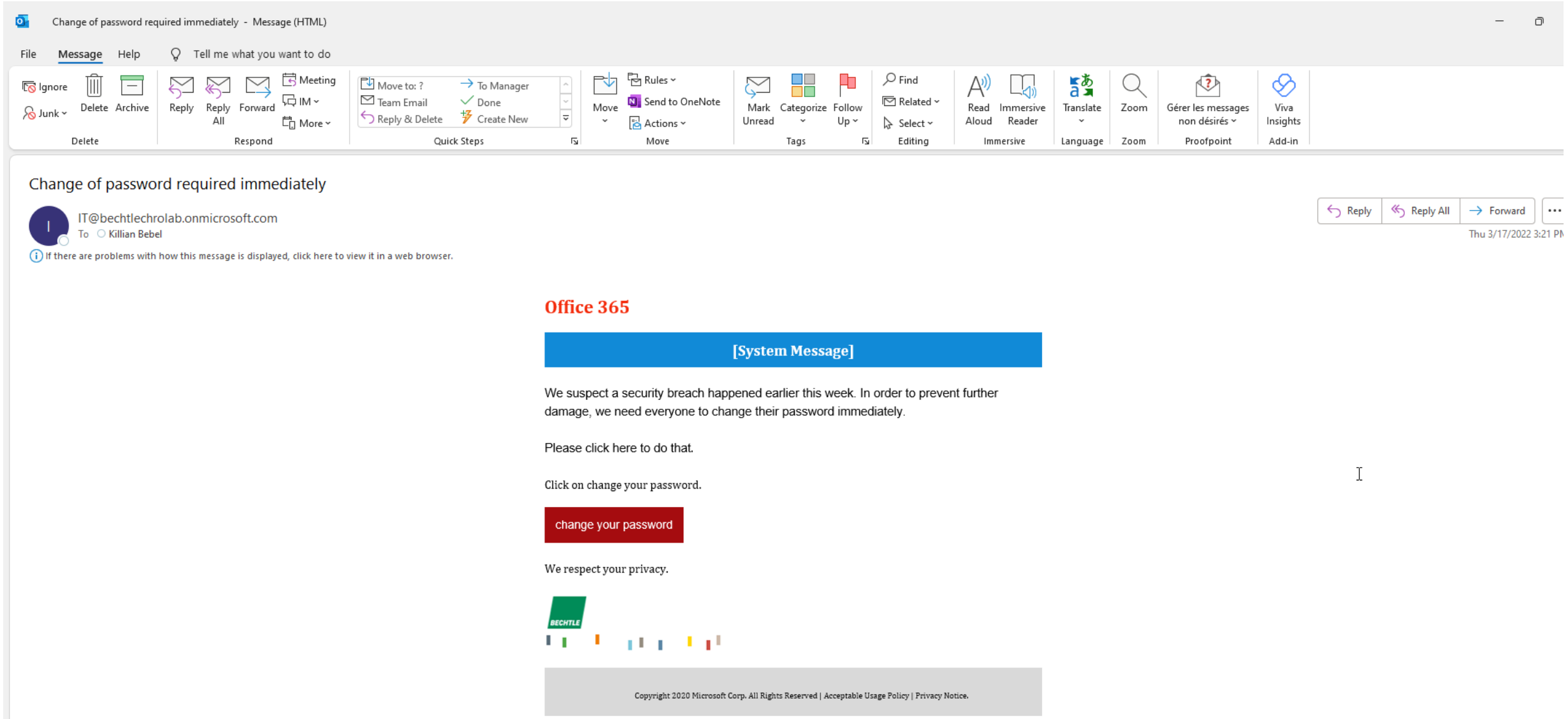
Attack scenario

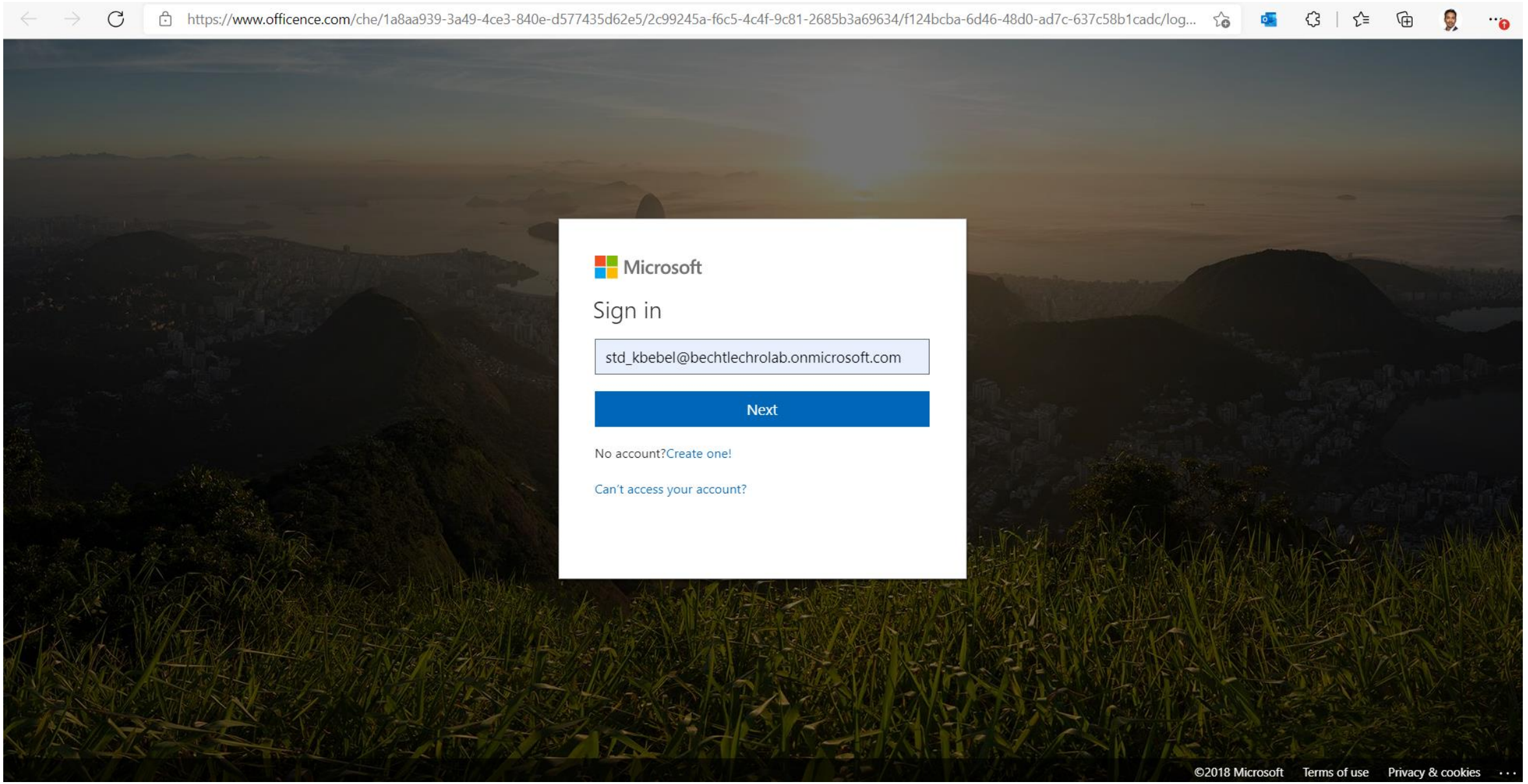
Architecture and steps

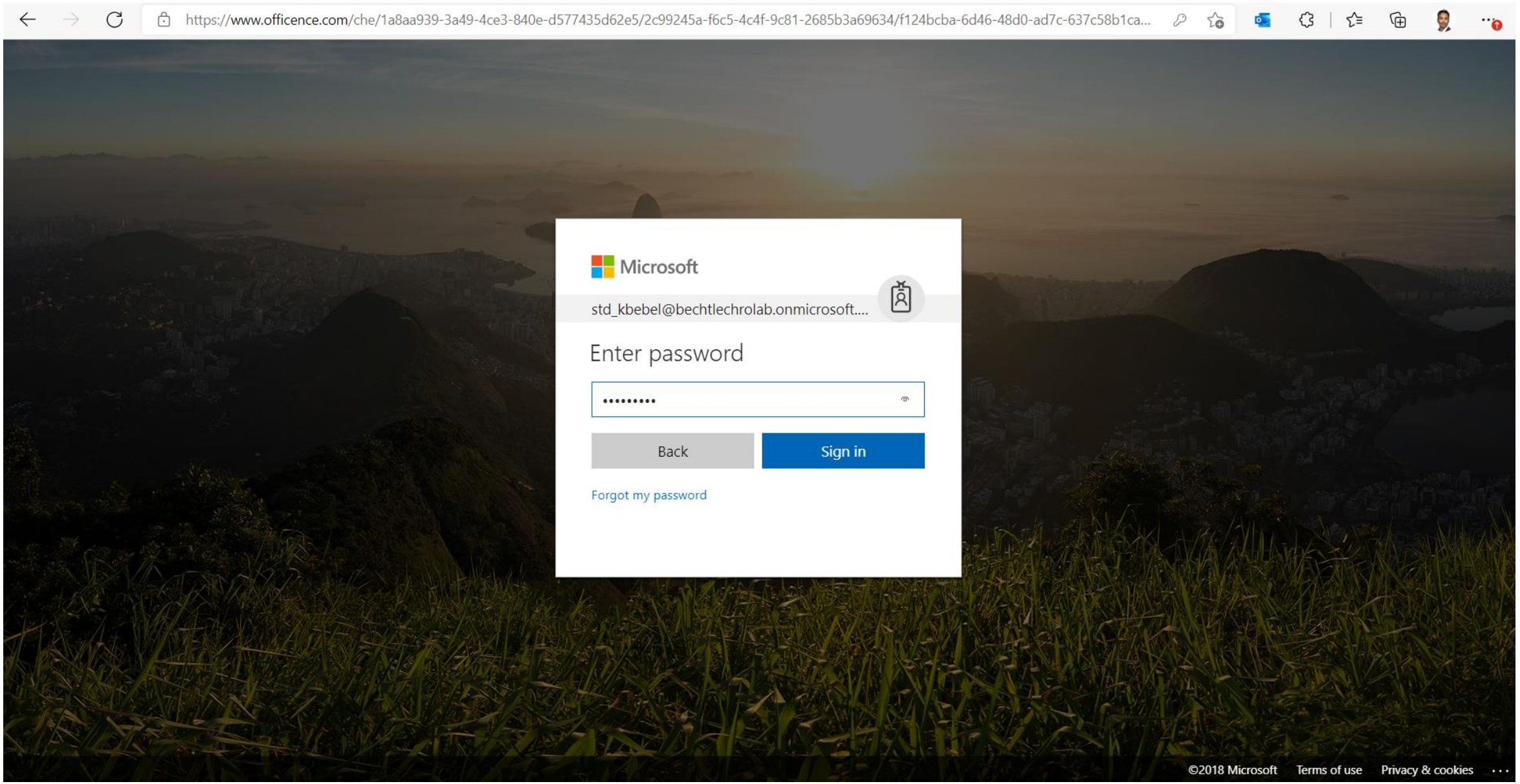
BCHTEST.COM

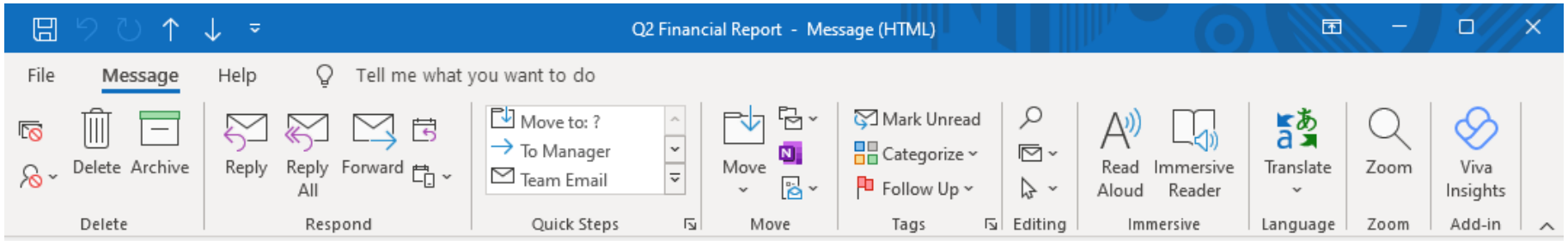
Tier 0	 WINDCBCH Domain Controller, Windows Server 2016	Domain Admins adm_<user>
Tier 1	 WIN2016SRV Application Server, Windows Server 2016	Service Accounts Helpdesk Admins hdesk_<user> svc_<service>
Tier 2	 WIN10TEST1 Workstation, Windows 11  WIN10TEST2 Workstation, Windows 11	Helpdesk Admins Domain Users hdesk_<user> std_<user>

Attack Demo.


Change of password required immediately - Message (HTML)
File
Message
Help
Tell me what you want to do
Ignore
Junk
Delete
Archive
Reply
Reply All
Forward
Meeting
IM
More
Move to: ?
Team Email
Reply & Delete
To Manager
Done
Create New
Move
Rules
Send to OneNote
Actions
Mark Unread
Categorize
Follow Up
Find
Related
Select
Read Aloud
Immersive Reader
Translate
Zoom
Gérer les messages non désirés
Viva Insights
Delete
Respond
Quick Steps
Move
Tags
Editing
Immersive
Language
Zoom
Proofpoint
Add-in
Change of password required immediately
IT@bechtlechrolab.onmicrosoft.com
To Killian Bebel
If there are problems with how this message is displayed, click here to view it in a web browser.
Reply
Reply All
Forward
Thu 3/17/2022 3:21 PM
Office 365
[System Message]
We suspect a security breach happened earlier this week. In order to prevent further damage, we need everyone to change their password immediately.
Please click here to do that.
Click on change your password.
change your password
We respect your privacy.
Copyright 2020 Microsoft Corp. All Rights Reserved | Acceptable Usage Policy | Privacy Notice.


https://www.officence.com/che/1a8aa939-3a49-4ce3-840e-d577435d62e5/2c99245a-f6c5-4c4f-9c81-2685b3a69634/f124bcba-6d46-48d0-ad7c-637c58b1cadc/log...
Microsoft
Sign in
std_kbebel@bechtlechrolab.onmicrosoft.com
Next
No account?Create one!
Can't access your account?
©2018 Microsoft
Terms of use
Privacy & cookies


https://www.officence.com/che/1a8aa939-3a49-4ce3-840e-d577435d62e5/2c99245a-f6c5-4c4f-9c81-2685b3a69634/f124bcba-6d46-48d0-ad7c-637c58b1ca...
Microsoft
std_kbebel@bechtlechrolab.onmicrosoft....
Enter password
Back
Sign in
Forgot my password
©2018 Microsoft
Terms of use
Privacy & cookies



Q2 Financial Report

KB

Killian Bebel
To Karim Trivier

Reply | Reply All | Forward | ...

Mon 21/03/2022 01:25

BCHTEST-Q2-FinancialReport.xlsm
21 KB

Hello Karim,

Please have a look on our Q2 financial report. It is highly confidential, I am not even sure I am allowed to forward it to you.
I trust you, so keep it for you and let's end the conversation about it here.

Best regards,
Killian

Killian Bebel
Deputy CFO
Bchtest SA
Avenue des Rootkits 1337
1228 Plan-les-Ouates

Phone: +41 21 123 45 67
Mobile: +41 79 123 45 67

E-Mail: killian.bebel@bchtest.com
Web: bechtest.com
DSGVO/GDPR: Privacy Policy Art. 13,14

Detect and Respond Demo.

Prevention.

The Cybersecurity Bell Curve

Basic security hygiene still protects against 98% of attacks

Enable multifactor authentication

Make it harder for bad actors to utilize stolen or phished credentials by enabling multifactor authentication. Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.

Apply least privilege access

Prevent attackers from spreading across the network by applying least privilege access principles, which limits user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive polices, and data protection to help secure both data and productivity.

Keep up to date

Mitigate the risk of software vulnerabilities by ensuring your organization's devices, infrastructure, and applications are kept up to date and correctly configured. Endpoint management solutions allow policies to be pushed to machines for correct configuration and ensure systems are running the latest versions.

Utilize antimalware

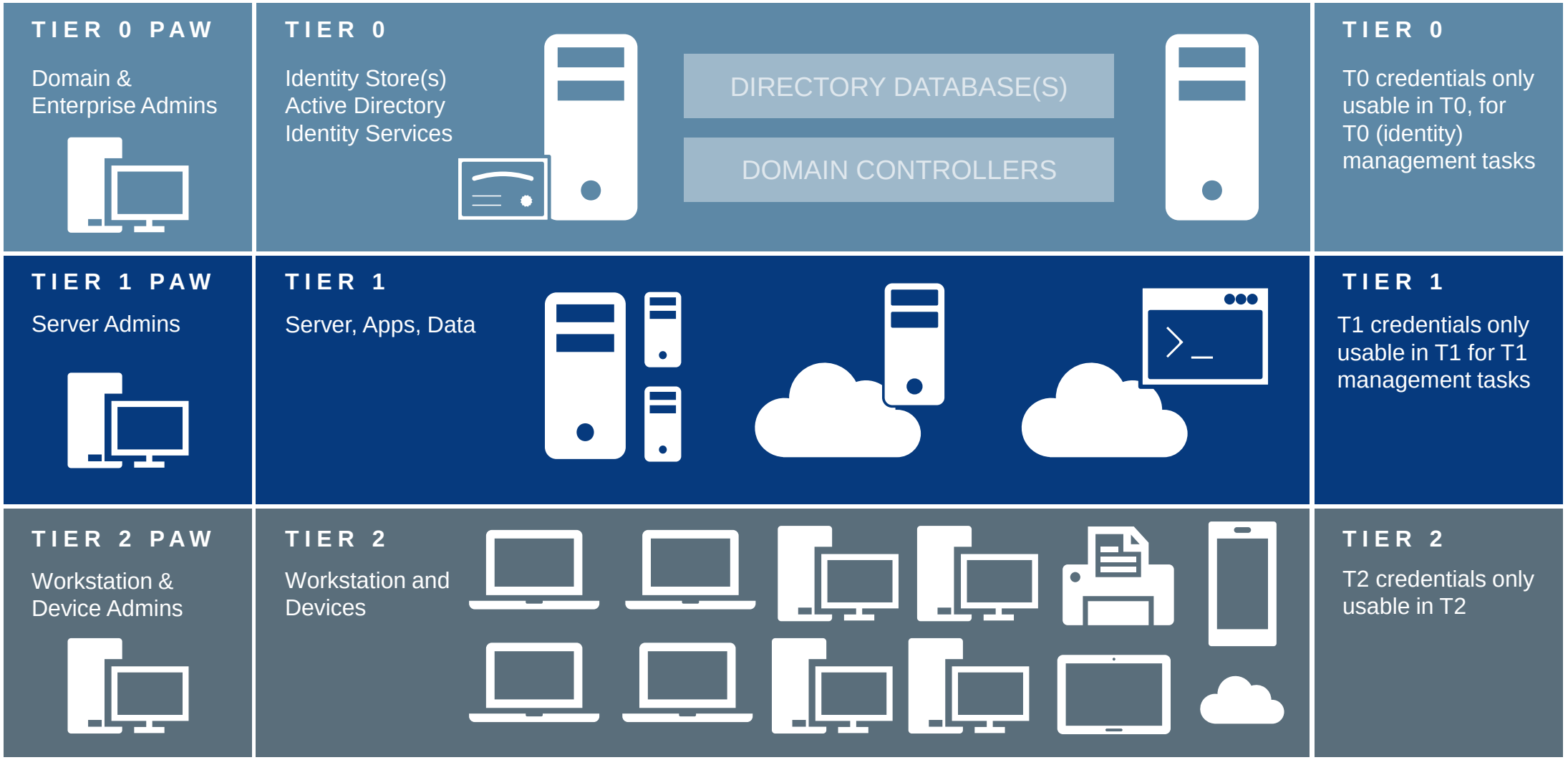
Stop malware attacks from executing by installing and enabling antimalware solutions on endpoints and devices. Utilize cloud-connected antimalware services for the most current and accurate detection capabilities.

Protect data

Know where your sensitive data is stored and who has access. Implement information protection best practices such as applying sensitivity labels and data loss prevention policies. If a breach does occur, it's critical that security teams know where the most sensitive data is stored and accessed.

Protecting Active Directory and Admin privileges

Tiering model



Ecole Hôtelière de Lausanne

Projet Microsoft Defender for Endpoint

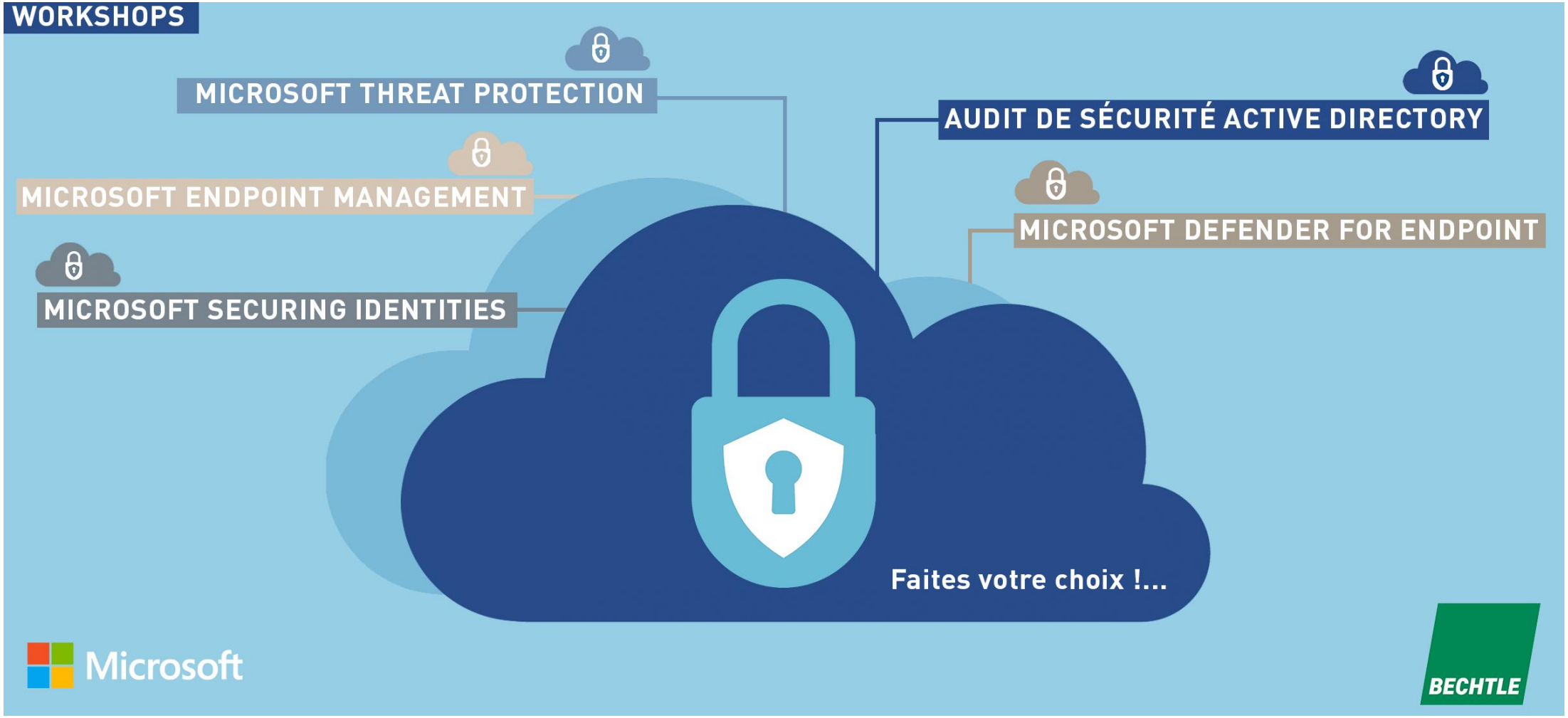
- Définition et accompagnement à l'exécution de la stratégie de déploiement pour
  - Windows 10
  - Windows Server 2008R2, 2012R2, 2016 et 2019
  - Linux Server
- Configuration Microsoft Defender for Endpoint et Microsoft Defender Antivirus selon best practices
- Déploiement de System Center Endpoint Protection sur Windows Server 2012
- Formation Security Analysts
  - Gestion et réponse aux incidents
  - Gestion du cycle de vie des appareils
  - Gestion des vulnérabilités

> *Microsoft a pris une belle envergure avec la mise à disposition de ses solutions MDE qui concurencent allègrement les meilleures solutions de sécurité du marché. Naturellement nous avons fait confiance à ces produits qui en plus de répondre à nos attentes en terme de protection de notre IT, s'intégrent parfaitement dans notre eco-système nous permettant ainsi une très bonne optimisation et standardisation de notre gamme de solutions."*
>
> *Marco Grosso - Digital Services Delivery Manager*

Ecole Hôtelière de Lausanne

> *Les équipes Bechtle ont une fois encore fait preuve de l'efficacité et de la compétence qui les caractérisent en nous supportant dans ce projet. Ils nous ont aidé, formé et amené à l'autonomie de gestion de cette solution. Bechtle a une réelle plus-value, notamment dans son agilité, sa capacité à répondre aux besoins et sa facilité d'intégration dans nos équipes. Ils nous apportent toujours le petit plus qui fait grandir l'équipe."*
>
> *Marco Grosso - Digital Services Delivery Manager*

Workshop Microsoft Security.



AVRIL

- **7 avril 2022** | Bechtle & VMware - Offrez à vos collaborateurs la possibilité de travailler n'importe où (Anglais)
- **28 avril 2022** | Bechtle & VMware – Modernisation du datacenter et gestion du cloud avec VMware Cloud Foundation (Anglais)

Merci !

Des questions?

Nous restons à votre disposition pour vous accompagner dans vos projets futurs.