Teams Pills

Lesson 4:

Sicurezza & compliance

in Teams

Microsoft 365

Teams Pills – Lesson 4
Security & Compliance in Teams
3 use cases

Rebecca Travasi
Technical Specialist Security & Compliance
Microsoft Italy

Donato Salamina
Technical Specialist Security & Compliance
Microsoft Italy

Teams Security & Compliance

Identity & access management

Conditional Access Policy

Multi Factor Auth

Sign-in Risk

User Risk

Threat Protection

URL detonation

Malware Detection

File detonation

Information Protection & Governance

Information protection

Retention policies

DLP (files)

DLP (chat)

Insider Risk Management

Supervisory review

Information barriers

Discover & Respond

Audit log searches

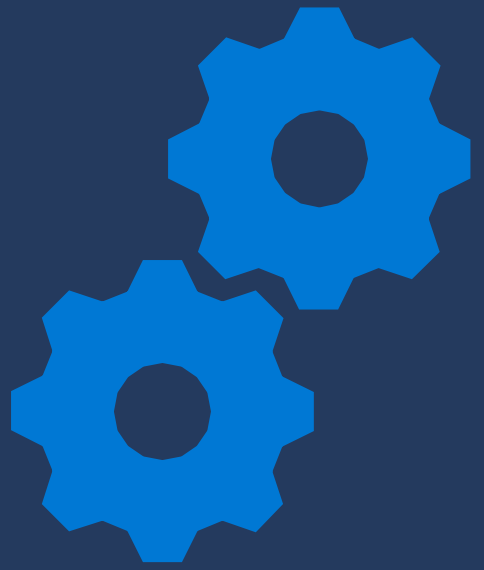
Data Investigations

Data subject requests

Advanced eDiscovery

Microsoft 365

Conditional access e Teams: protezione dell'identità tramite 2 esempi di policy



Microsoft 365

Come usare il Conditional Access per restringere l’utilizzo di Teams agli impiegati:

Il CA è una funzionalità di Azure AD che consente alle organizzazioni di definire condizioni specifiche per la modalità di autenticazione degli utenti e l'accesso ad applicazioni e servizi. Le policy si configurano sul portale Azure.

Si noti che il CA richiede Azure AD Premium P1 o P2.

(Nota, è disponibile anche una versione di valutazione di 30 giorni).

Microsoft 365

Scenario: una società fittizia Contoso, desidera concedere ai propri dipendenti venditori al dettaglio l'accesso a Microsoft Teams, tuttavia hanno requisiti che devono essere soddisfatti.

- I dipendenti al dettaglio vengono pagati ogni ora e lavorano presso un punto vendita aziendale. Quando il dipendente lascia il lavoro ed è "fuori orario", non gli è consentito accedere a Microsoft Teams.
- Quando il dipendente lascia il lavoro, l'app non deve consentire loro di accedere a dati o servizi.
- Quando il dipendente torna al lavoro, l'app deve consentire loro di accedere a tutti i dati e i servizi all'interno dell'app.
- Questi requisiti si applicheranno a tutte le piattaforme in cui un dipendente può accedere a Microsoft Teams (app per smartphone, Windows, Mac, browser web, ecc.)

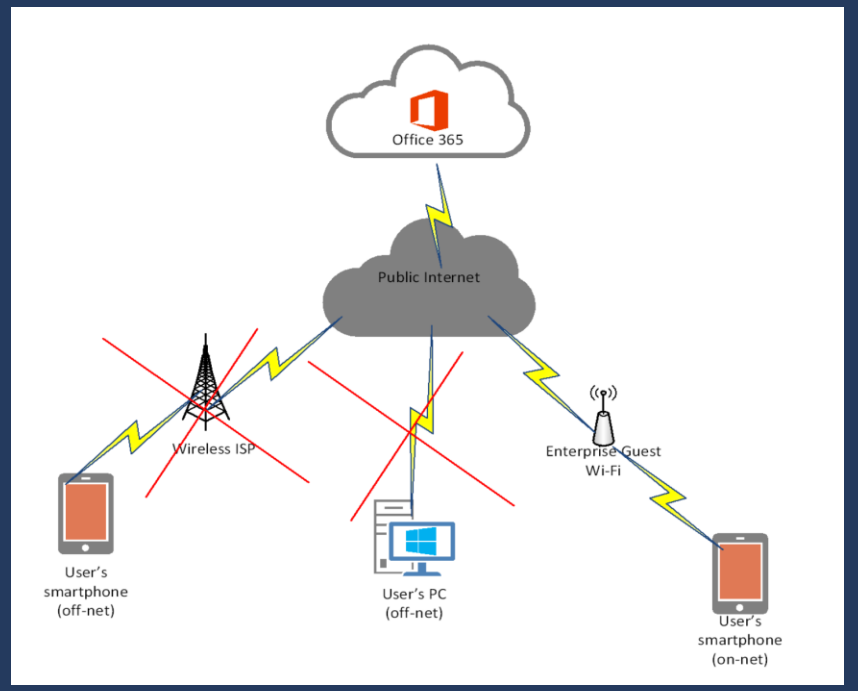
Microsoft 365

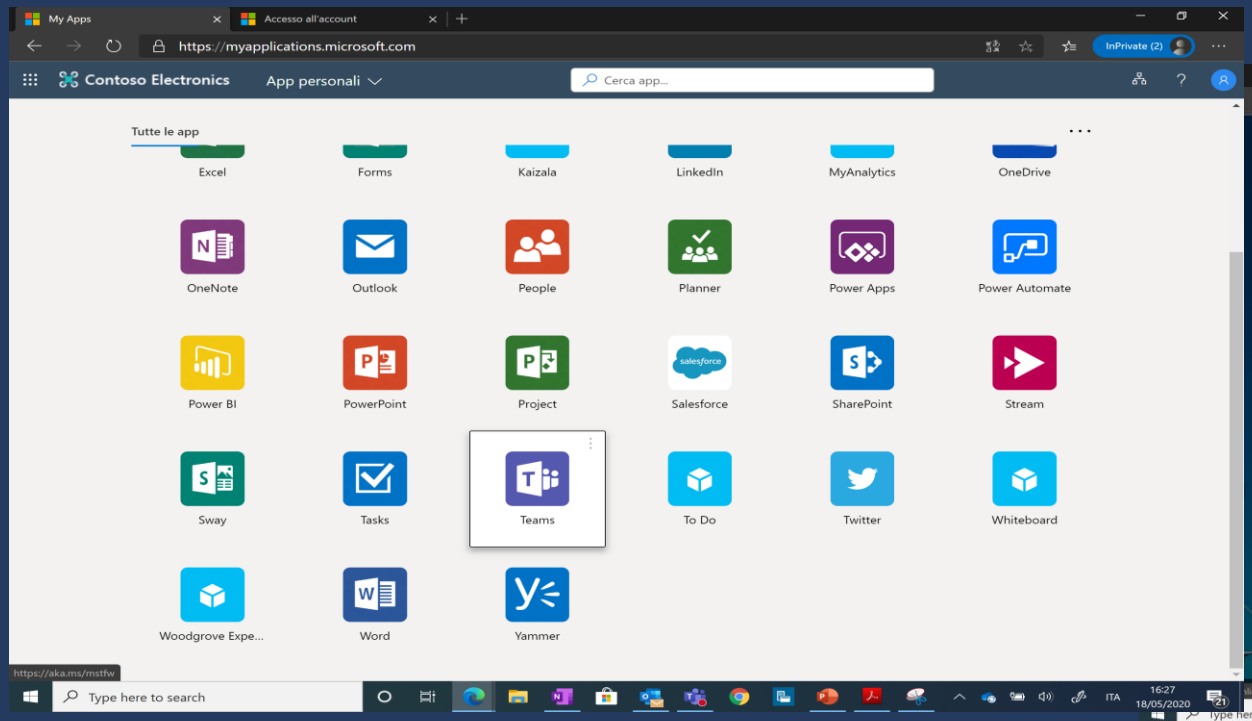
Note di design:

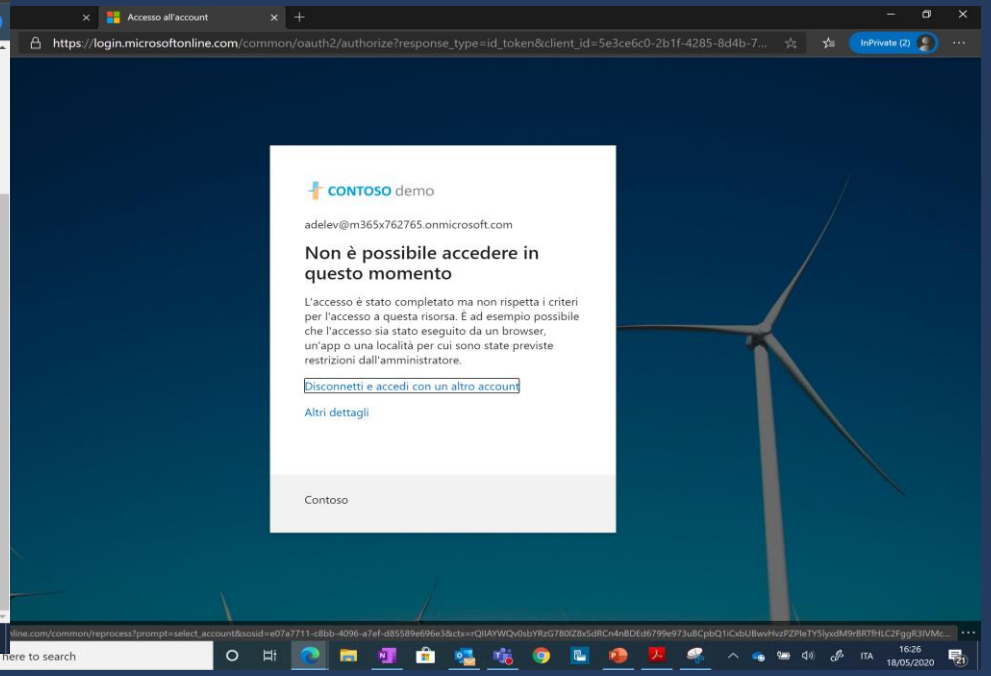
- Tutti i venditori al dettaglio verranno assegnati a un gruppo di sicurezza denominato «Personale di vendita». I criteri di accesso condizionale verranno applicati solo ai dipendenti membri di questo gruppo di sicurezza.
- Il criterio verrà applicato solo a Microsoft Teams e includerà tutte le piattaforme (Android, iOS, Windows Phone, Windows, Mac OS e così via).
- Il criterio verrà applicato a qualsiasi location (indirizzo IP), ma verranno escluse le location con indirizzi IP attendibili. (Contoso aggiungerà la propria subnet IP pubblica all'elenco di indirizzi IP attendibili.)
- Il criterio verrà applicato a browser, app per dispositivi mobili e client desktop.
- I controlli di accesso verranno impostati nel primo caso per bloccare l’accesso, nel secondo con richiesta di secondo fattore di autenticazione (MFA).

Microsoft 365

- Controllare assegnazione Licenze utenti
- Aggiungere il dipendente al gruppo di sicurezza «Retail Employees»
- Creare Policy di CA
- Scenario 1 con blocco
- Scenario 2 con MFA







Microsoft 365

Demo

portal.azure.com

Microsoft 365

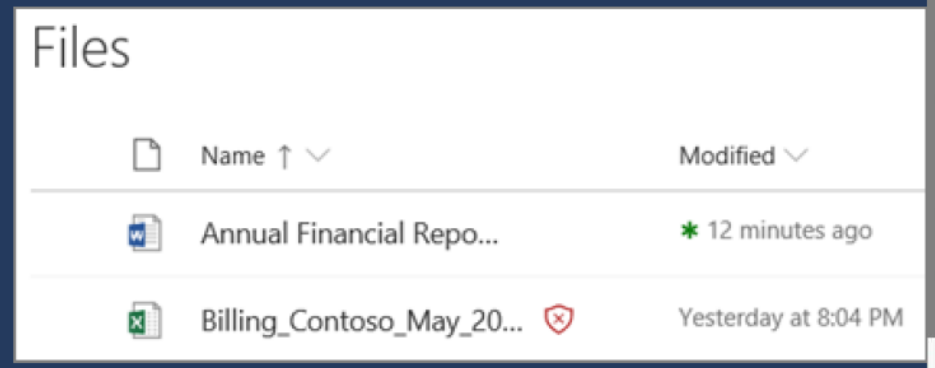
Protezione contro malware e phishing con office 365 ATP in Teams

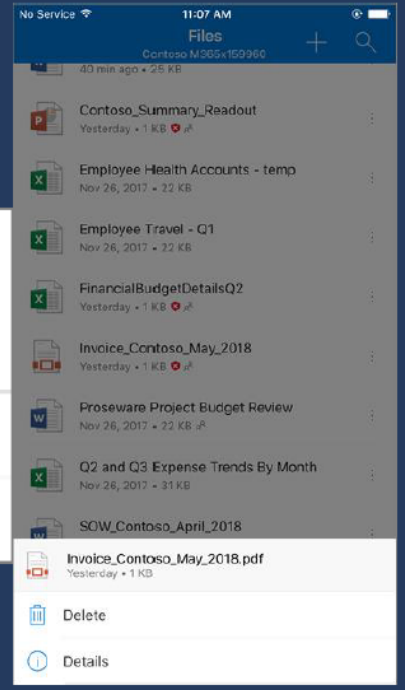
Microsoft 365

Note di design:
Ipotizzate che assumiate un'agenzia di marketing e che la invitiate come ospite di un team in Microsoft Teams a collaborare. Cosa succede se l'account dell'ospite viene compromesso e un attore malintenzionato ottiene l'accesso al team in Microsoft Teams? L'organizzazione sta avendo conversazioni sensibili lì, il caricamento di file sensibili, e se i dati dovessero essere divulgati pubblicamente, potrebbe danneggiare l'organizzazione. Ancora più importante, un cattivo attore può pubblicare collegamenti ipertestuali a siti Web di "phishing" e caricare file dannosi in Microsoft Teams - da lì gli utenti possono aprire i collegamenti o eseguire i file, ponendo una grave minaccia per la sicurezza dell'organizzazione.

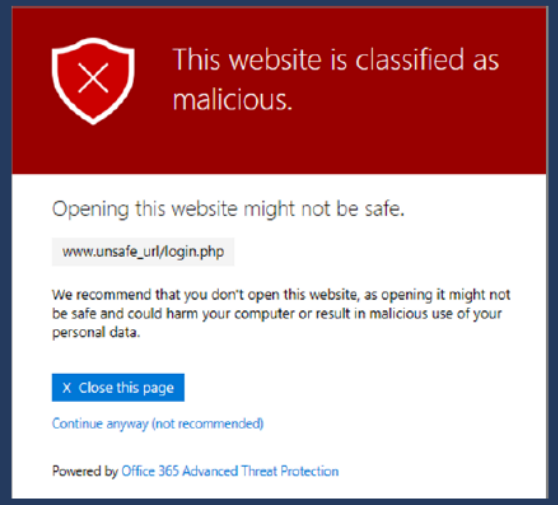
Microsoft 365

ATP Documenti:
quando un file ATP Documenti:
quando un file su SharePoint Online, OneDrive for Business, e Microsoft Teams
su SharePoint Online, OneDrive for Business, e Microsoft Teams viene ritenuto malevolo, ATP integra direttamente con il file store per bloccare il file. Anche se il file viene bloccato è comunque presente nella library sia in app web che desktop, il file non può essere aperto , copiato, spostato o condiviso
può solo essere eliminato.



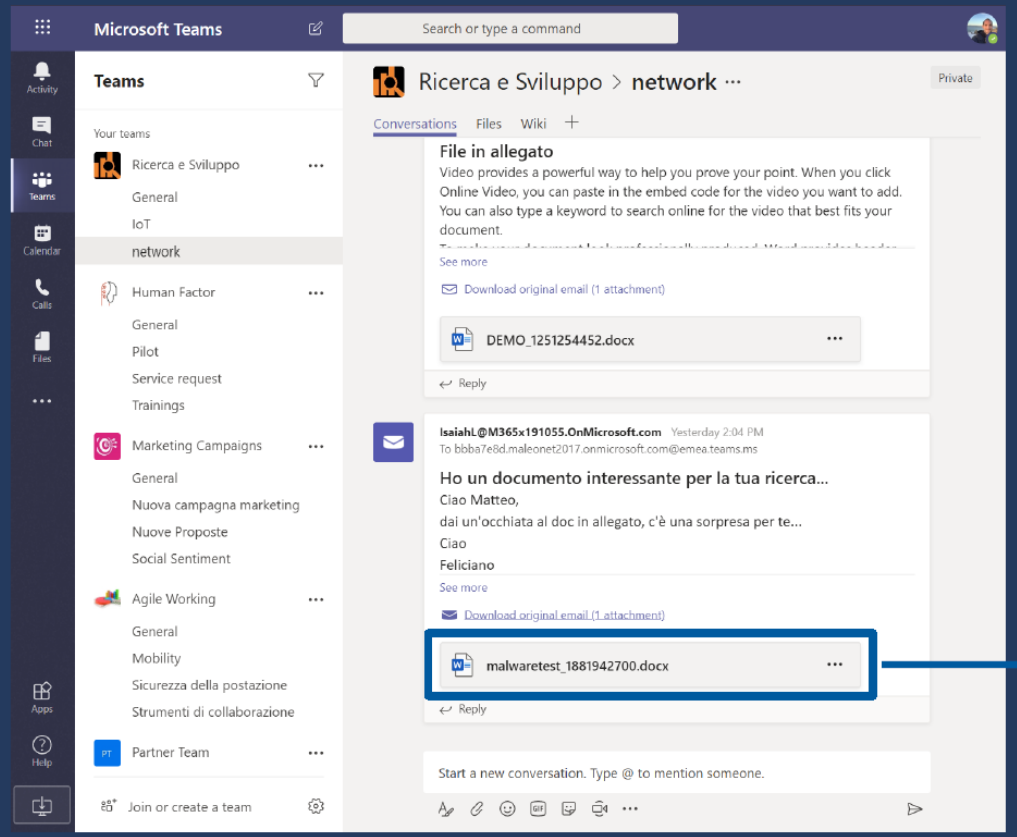


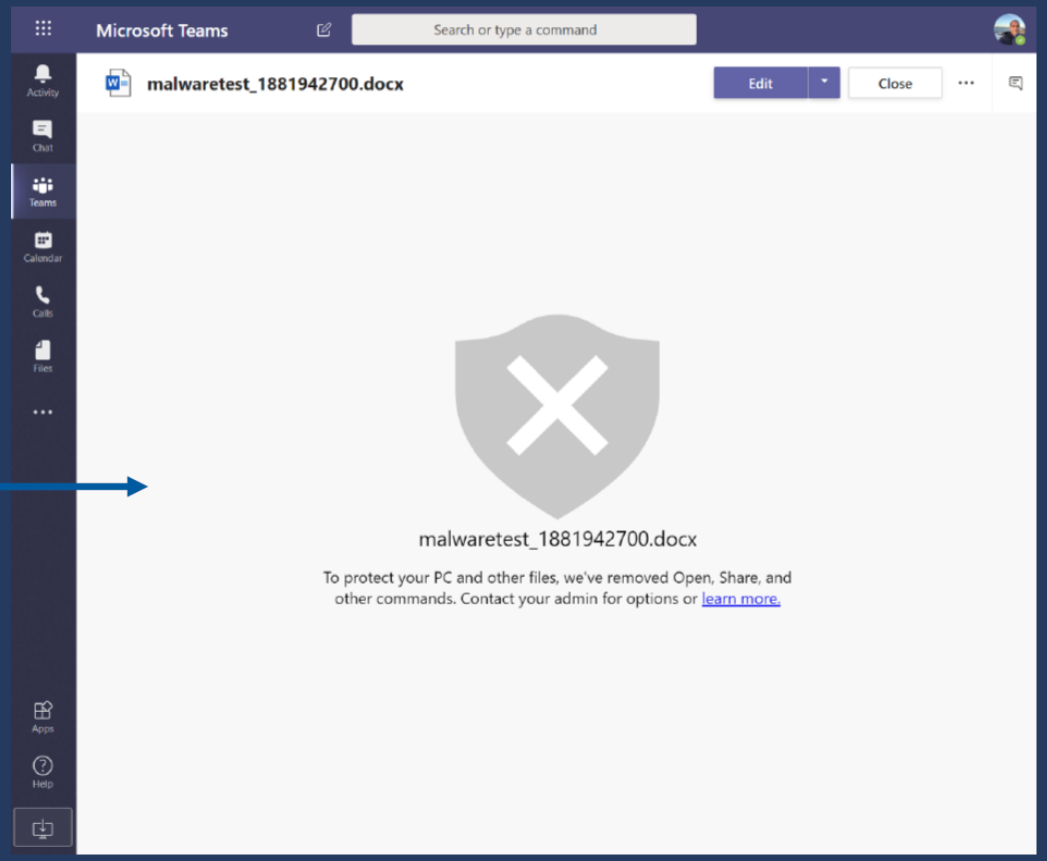
ATP Safe Links:
Questa funzione può aiutare a proteggere l'organizzazione fornendo una verifica time-of-click degli indirizzi web (URLs) anche nelle chat di Teams. Le policy si impostano sul Security center dagli amministratori.



Microsoft 365

ATP in Teams

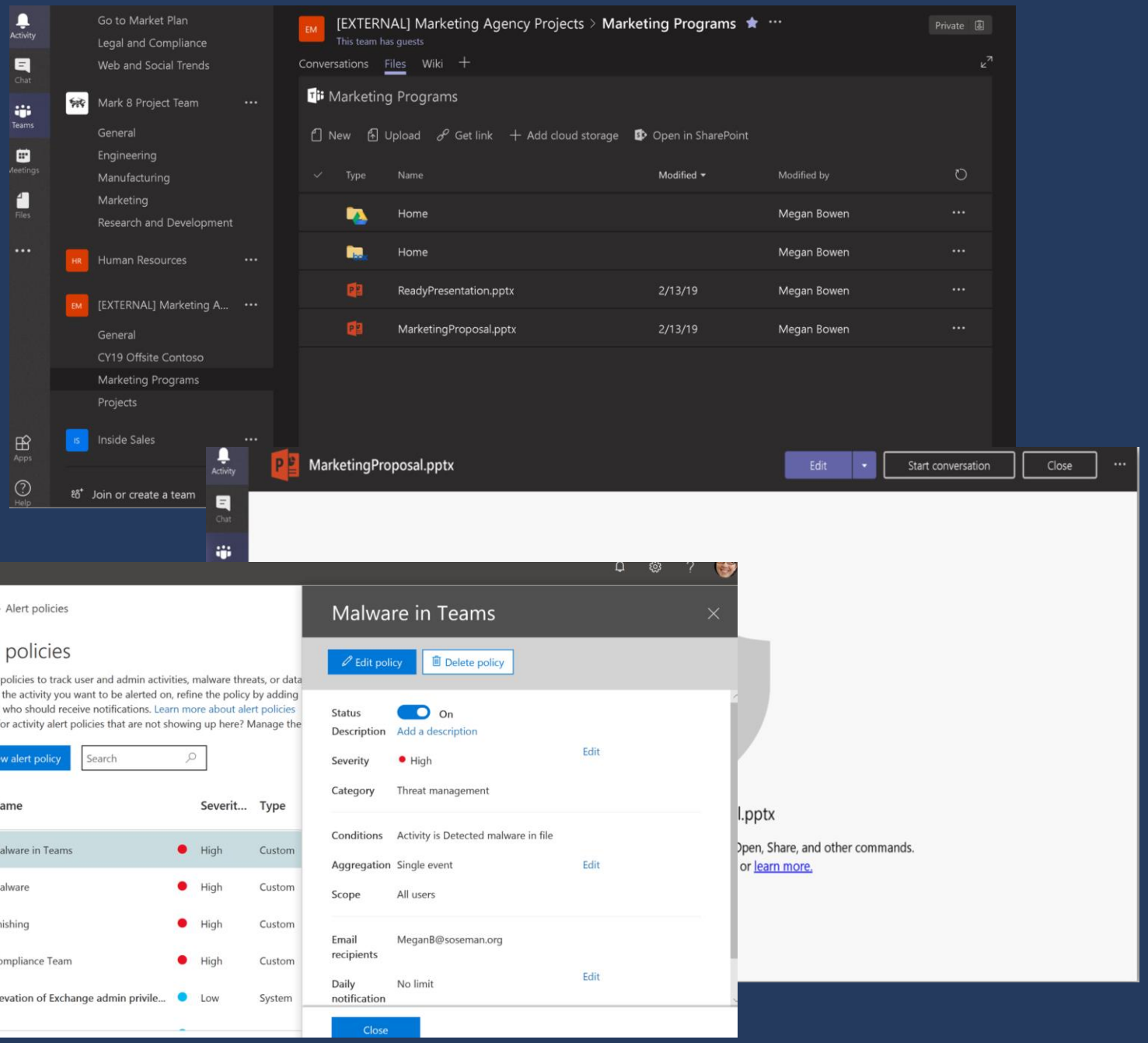




Microsoft 365

Safe Attachments blocca l'utente e non dà mai la possibilità di avviare il file. Questo stesso comportamento si verifica anche quando il file viene eseguito direttamente da SharePoint. Se si usano gli avvisi di Office 365 (nel Centro sicurezza e conformità) questi possono essere configurati per notificare all'amministratore che il malware è stato caricato in Microsoft Teams.

*Con MCAS si può inviare una notifica via SMS e volendo si integra con vostri SIEM.

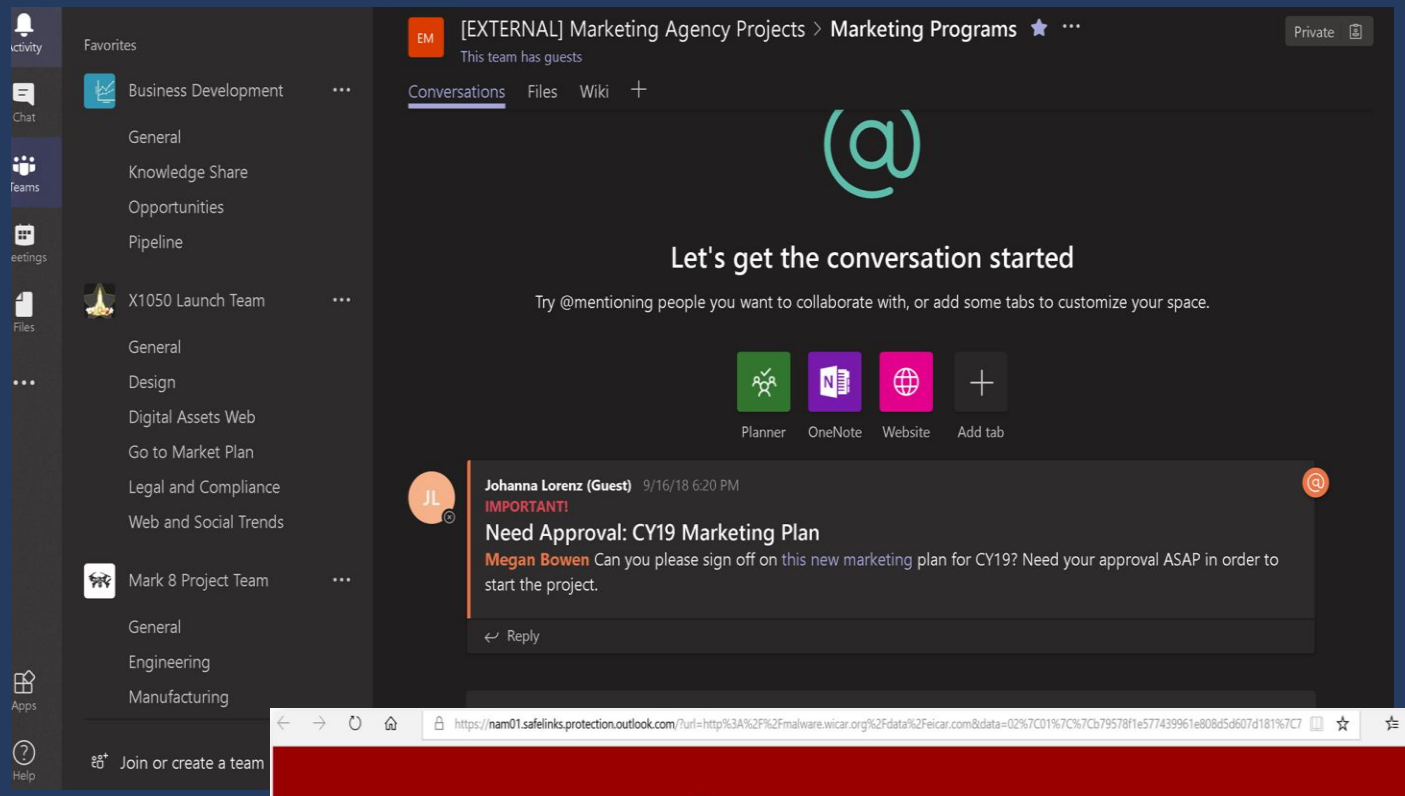


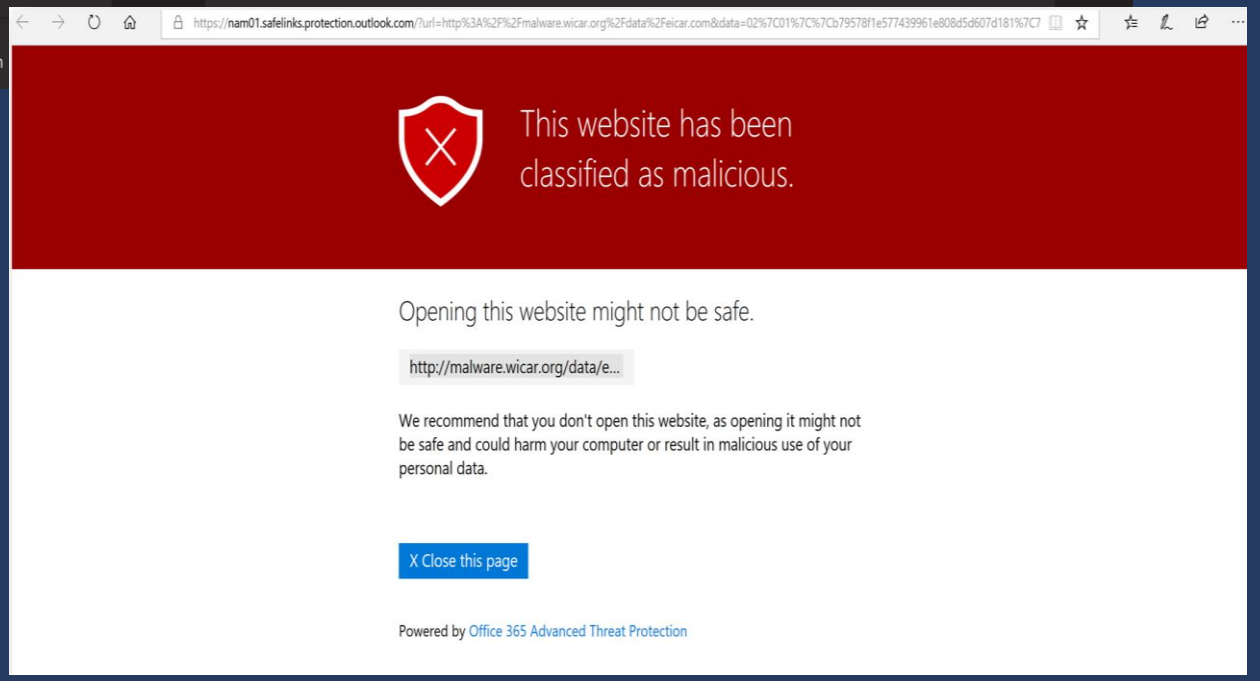
Microsoft 365

Tentativi di phishing in Teams:

Se la policy di ATP Safe Links è configurata correttamente, quando viene condiviso un URL malevolo, l'utente riceverà un messaggio di blocco quando tenta di fare clic sul link.

Quando l'utente fa clic sul collegamento, ATP Safe Links e Intelligent Security Graph entrano in azione per fornire protezione. ATP riconosce il sito come dannoso, e ferma l'utente non dando loro la possibilità di fare clic attraverso il sito originale. (questo può essere modificato nella policy rendendola più lasca e permettndo nonostante l'avviso di proseguire sul sito.)





Microsoft 365

Demo

Protection.office.com

Microsoft 365

Conformità in Teams: Microsoft Information Protection per proteggere dati sensibili con DLP policy

Microsoft 365

Note di design:

- Un gruppo di lavoro con funzioni trasversali sta lavorando su un nuovo prodotto in fase di progettazione e sviluppo
- Viene creato un Team ad-ho riservato per il gruppo di lavoro
- Al gruppo di lavoro partecipano solo persone dipendenti dell'azienda
- Il Team contiene informazioni sensibili relative al prodotto in via di sviluppo
- Il Team è classificato come Highly Confidential
- Il personale lavora in mobilità, sia con dispositivi aziendali che personali
- E' necessario proteggere l'intellectual property ed evitare che informazioni sensibili entri in mani di persone non autorizzate

Funzionalità di Compliance per Microsoft Teams

Information Protection & Governance

Data Loss Prevention
Permette di identificare contenuti sensibili non appena creati, usati o condivisi ed aiuta a prevenire la perdita del dato accidentale

Information Protection
Permette di identificare, classificare e proteggere dati sensibili e critici attraverso il ciclo di vita, l'intera organizzazione e l'esterno

Information Governance
Permette di gestire il ciclo di vita del dato, usando soluzioni per importare, memorizzare dati critici in modo che si possa mantenere ciò di cui si ha bisogno e cancellare ciò che non serve

Records Management
Utilizza una classificazione intelligente per automatizzare e semplificare la schedulazione del mantenimento dei record in ambito regolatorio, legale e del dato critico

Insider Risk Management

Communication Compliance
Permette di minimizzare i rischi legati alle comunicazioni aiutando a catturare messaggi inappropriati, investigare possibili violazioni di policy e intraprendere azioni per rimediare

Insider Risk Management
Permette di rilevare attività rischiose all'interno dell'organizzazione per aiutare a identificare, investigare e intraprendere azioni per il rimedio di rischi e minacce interne.

Information Barriers
Criteri che permettono di impostare delle barriere per impedire a singoli utenti o gruppi di utenti di comunicare tra loro, scambiarsi file

Discover & Respond

Audit
Registra le attività degli utenti e degli amministratori e permette la ricerca e l'investigazione di una lista completa di attività tra i servizi

Data Investigations
Permette di effettuare delle ricerche per identificare dati sensibili, malevoli, o mal posizionati tra i servizi in modo da investigare e rimediare (per esempio Data spillage)

Data Subject Requests
Permette di ricercare ed esportare dati personali e di rispondere all'esigenza del DSR per il GDPR

eDiscovery
Aiuta a rispondere alle richieste di ricerca per fini legali utilizzando le soluzioni Core e Advanced per identificare, preservare, analizzare ed esportare i dati

Microsoft 365

Demo

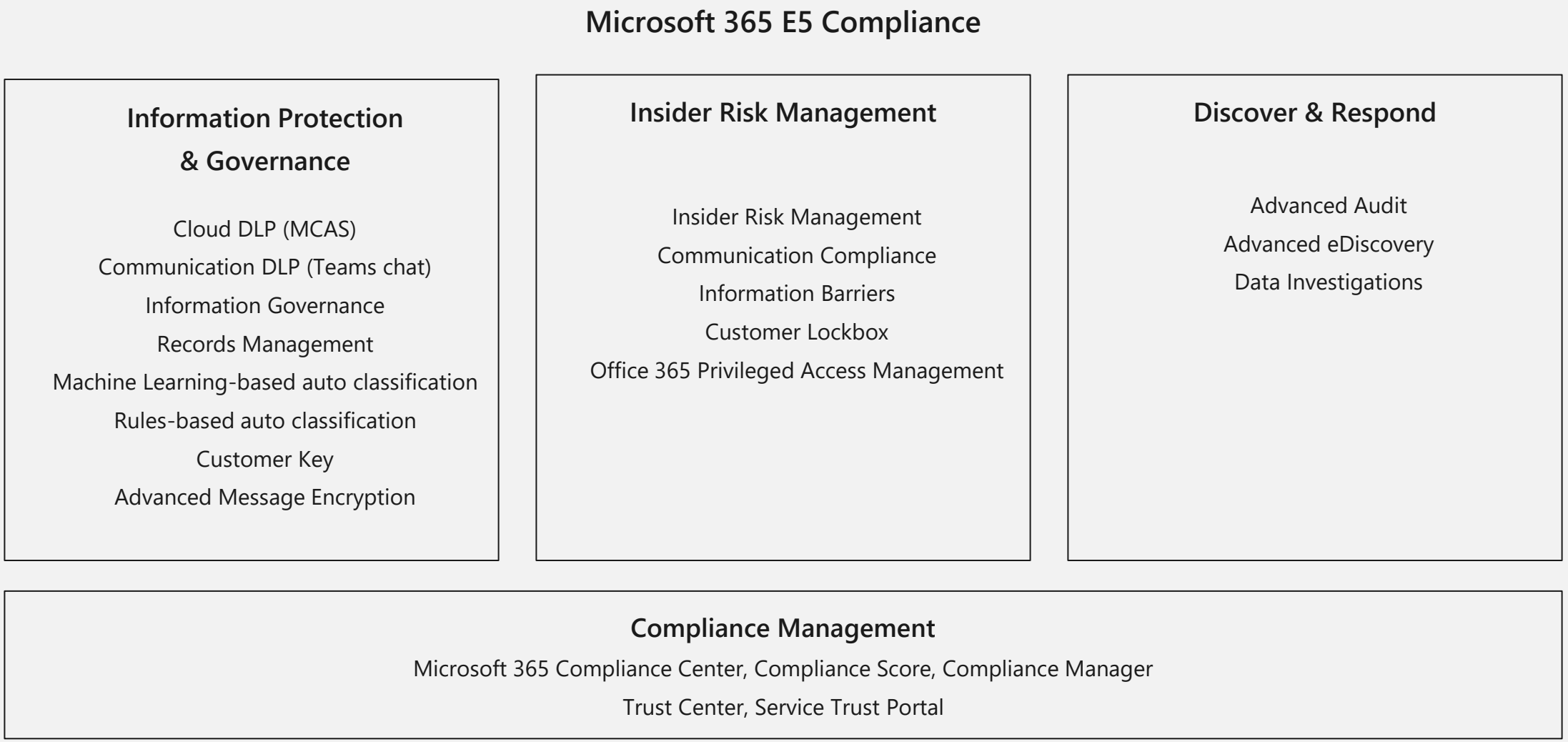
Microsoft 365

Licensing Microsoft 365 Security & Compliance

Microsoft 365 E5 Security

	Microsoft 365 E5 Security	Microsoft 365 E5	Office 365 E5	EMS E5	Windows E5
Office 365 ATP Plan 2	●	●	●		
Microsoft Defender ATP	●	●			●
Azure Active Directory Plan 2	●	●		●	
Azure ATP	●	●		●	
Microsoft Cloud App Security	●	●		●	

Microsoft 365 E5 Compliance



Microsoft 365

Link Utili e Community

Resta sempre aggiornato con le ultime news di **Microsoft 365:**
https://www.microsoft.com/microsoft-365/partners/

Scenari di utilizzo di **Teams** per ogni specifica **Industry**
https://www.microsoft.com/microsoft-365/partners/teamwork

Area dedicata alla practice su Teams
https://www.microsoft.com/microsoft-365/partners/teamwork

Accedi alla community di **Microsoft 365**:
https://www.microsoft.com/microsoft-365/partners/community

Visita l'area **Partner Hub** dedicata all'Italia:
https://aka.ms/Italy_Partner_Hub

Iscriviti alla **Partner Newsletter:**
https://aka.ms/Italy_MPN_News

Visita **la Microsoft Partner Zone** per tutte le ultime notizie, gli eventi e la formazione nella tua zona.
https://www.microsoftpartnercommunity.com/t5/Italy-Partner-Zone/ct-p/ITPZ

Microsoft 365 Roadmap
https://www.microsoft.com/en-us/microsoft-365/roadmap?filters=

Visita il **Partner Training Calendar:**
https://www.microsoft.com/it-it/partner-training/default.aspx

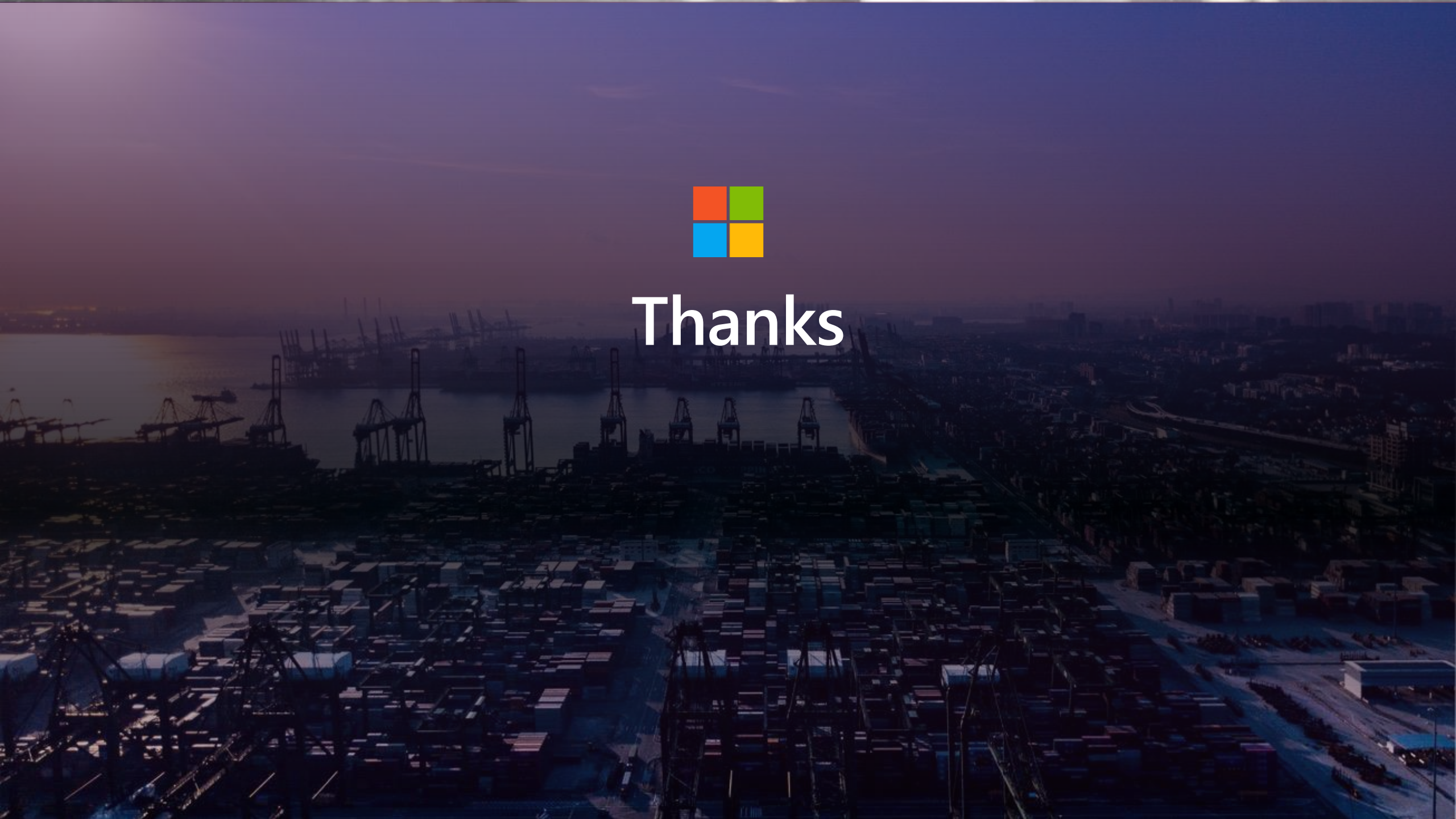
Microsoft 365

Next Session – 27.05.2020
Teams: migrazione da Skype, funzionalità voce e integrazione della funzionalità Meeting con Surface Hub

Presentazione degli scenari di coesistenza per la migrazione da Skype a Teams al fine di chiarire le varie funzionalità disponibili nelle varie modalità e path di migrazione.
Presentazione dell'architettura Direct Routing per implementare scenari di integrazione di telefonia. In chiusura vedremo come utilizzare al meglio Microsoft Teams con Surface Hub"

Agenda

- Path di migrazione da Skype for Business to Teams
- Esperienza utente durante la migrazione
- Introduzione su Direct Routing
- Esempio di migrazione da PBX a Teams
- Teams & Surface Hub


Thanks