

Les éléments à télécharger sont disponibles à l'adresse suivante :

**<http://www.editions-eni.fr>**

Saisissez la référence de l'ouvrage **EPSECMIC** dans la zone de recherche et validez. Cliquez sur le titre du livre puis sur le bouton de téléchargement.

## Chapitre 1 Introduction

1.	Présentation du livre . . . . .	11
1.1	Le cloud . . . . .	12
1.2	Les différents modèles du cloud. . . . .	13
1.2.1	IaaS . . . . .	13
1.2.2	PaaS. . . . .	14
1.2.3	SaaS. . . . .	15
1.3	Les modèles de déploiement du cloud . . . . .	15
1.3.1	Le cloud public . . . . .	15
1.3.2	Le cloud privé. . . . .	16
1.3.3	Le cloud hybride. . . . .	16
1.4	Les enjeux du cloud . . . . .	17
1.5	La sécurité dans le cloud. . . . .	17
1.5.1	Crise sanitaire COVID-19 et la sécurité. . . . .	17
1.5.2	La responsabilité . . . . .	20
1.5.3	Microsoft Azure. . . . .	21
1.5.4	Le cloud Microsoft offre-t-il plus de sécurité ? . . . . .	23
1.6	Les acteurs sur le marché . . . . .	25
1.7	Microsoft Azure . . . . .	29
1.8	Microsoft 365 . . . . .	30

## Chapitre 2

### Microsoft 365 Defender

1.	Introduction . . . . .	31
1.1	Azure Defender . . . . .	35
1.2	Microsoft 365 Defender . . . . .	38
2.	Point sur les licences . . . . .	39
2.1	Microsoft 365 . . . . .	40
2.2	Enterprise Mobility + Security . . . . .	41
2.3	Microsoft 365 . . . . .	42
3.	Modèle de sécurité cloud Microsoft . . . . .	44
3.1	Le modèle Zero Trust . . . . .	44
3.2	Zero Trust journey . . . . .	46
3.3	Sécuriser son environnement cloud en neuf étapes . . . . .	47
4.	Introduction à Microsoft 365 . . . . .	51
5.	Enterprise Mobility + Security . . . . .	54
5.1	Azure Active Directory . . . . .	54
5.2	Azure Information Protection . . . . .	55
5.3	Microsoft Cloud App Security . . . . .	57
5.4	Endpoint Manager . . . . .	58
5.5	Microsoft Advanced Threat Analytics . . . . .	58
5.6	Microsoft Defender for Identity . . . . .	59
6.	Présentation du bac à sable . . . . .	61
6.1	Partie Azure . . . . .	61
6.1.1	Groupes de ressources . . . . .	63
6.1.2	Réseau virtuel . . . . .	66
6.1.3	Network Security Group . . . . .	69
6.1.4	Machine virtuelle . . . . .	75
6.1.5	L'environnement Microsoft 365 . . . . .	91

## Chapitre 3

### Sécurité des identités avec Azure AD

1.	Azure Active Directory .....	97
1.1	Les éditions d'Azure Active Directory .....	99
1.2	Les limitations d'Azure Active Directory .....	101
2.	Zero Trust avec Azure Active Directory .....	102
3.	Microsoft et l'identité .....	104
3.1	ADDS et Azure Active Directory .....	104
3.2	L'identité dans le cloud Microsoft .....	105
3.2.1	Azure Active Directory .....	106
3.2.2	ADDS sur une machine virtuelle dans Azure .....	106
3.2.3	Azure Active Directory Domain Services .....	106
4.	L'identité hybride .....	108
4.1	Les usages .....	109
4.1.1	Microsoft 365 .....	109
4.1.2	Intégration avec les applications SaaS .....	110
4.2	L'identité hybride et l'authentification .....	110
4.2.1	Synchronisation du hash de mot de passe .....	111
4.2.2	Le Pass-through - Authentification directe .....	113
4.2.3	La fédération avec Active Directory Federation Services .....	115
4.2.4	PingFederate .....	115
4.3	Comment choisir son moyen d'authentification ? .....	116
4.3.1	Résumé .....	118
4.3.2	Bac à sable .....	119
5.	Microsoft Secure Score .....	119
5.1	Introduction .....	119
5.1.1	Interface .....	121
5.1.2	Utilisation .....	128
5.2	Secure Score pour l'identité .....	130
6.	Azure authentication multifacteur .....	133
6.1	Introduction à Azure MFA .....	136
6.2	Configuration .....	140
6.2.1	Activation du MFA sur un utilisateur .....	143
6.2.2	Paramètres Azure MFA - portail Azure AD .....	146
6.2.3	Activation d'Azure MFA en PowerShell .....	155

6.2.4 Activation Azure MFA via les accès conditionnels . . . . .	158
6.2.5 État des lieux . . . . .	177
6.2.6 Gestion du MFA pour les utilisateurs. . . . .	178
6.2.7 Rapport d'utilisation MFA . . . . .	183
6.2.8 MFA et stratégie d'accès conditionnel - conditions . . . . .	192
6.2.9 Bonnes pratiques . . . . .	198
6.3 MFA et utilisateur. . . . .	199
6.3.1 Enregistrement MFA . . . . .	199
6.3.2 Portail MyAccount. . . . .	206
7. Gestion des mots de passe et des comptes . . . . .	214
7.1 Azure Active Directory Password Protection . . . . .	214
7.1.1 Configuration Azure Active Directory. . . . .	215
7.1.2 Configuration pour Active Directory - On-premises. . . . .	218
7.2 PasswordLess avec FIDO2 . . . . .	230
7.2.1 Introduction . . . . .	232
7.2.2 FIDO2. . . . .	232
7.2.3 PasswordLess et les méthodes d'authentification . . . . .	233
7.2.4 Activation du PasswordLess avec FIDO2 . . . . .	236
7.3 Comptes brise-glaces. . . . .	250
7.3.1 Introduction . . . . .	250
7.3.2 Bonnes pratiques . . . . .	251
7.3.3 Création des comptes brise-glaces. . . . .	251
7.3.4 Surveillance des comptes brise-glaces. . . . .	259
7.4 Self-Service Password Reset . . . . .	267
7.4.1 Introduction . . . . .	267
7.4.2 Prérequis . . . . .	269
7.4.3 Activation du SSPR . . . . .	269
7.4.4 Réinitialisation de mot de passe via SSPR . . . . .	284
7.4.5 Le mode combiné . . . . .	286
8. Conditional access . . . . .	291
8.1 Introduction . . . . .	291
8.1.1 Design et Matrix . . . . .	299
8.1.2 Mise en place . . . . .	304
8.2 Reporting. . . . .	310
8.2.1 Insights et rapports . . . . .	310
8.2.2 Logs Azure Active Directory . . . . .	312

8.3 Report Only et What If .....	315
8.3.1 What If.....	315
8.3.2 Report Only.....	320
8.4 Conditional access et PowerShell .....	322
8.5 Bonnes pratiques.....	326
9. Azure Identity Protection.....	332
9.1 Introduction .....	333
9.1.1 Configuration Azure AD Identity Protection .....	335
9.1.2 Simulation .....	353
10. Privileged Identity Management .....	355
11. Conclusion.....	387

## Chapitre 4

### Hardening Microsoft 365

1. Introduction.....	389
2. Introduction à Microsoft Defender .....	391
3. Microsoft Defender for Identity.....	411
3.1 Introduction .....	411
3.2 Architecture .....	413
3.2.1 Capacity planning.....	418
3.2.2 Choix de l'architecture .....	421
3.2.3 Prérequis.....	423
3.3 Déploiement .....	428
3.3.1 Création de l'espace Microsoft Defender for Identity.....	428
3.3.2 Administration.....	436
3.3.3 Timeline alerts.....	445
3.3.4 Recherche.....	447
3.3.5 Délégation .....	452
3.3.6 Les rapports .....	454
3.3.7 Log des capteurs.....	457
3.4 Les alertes .....	458
3.5 SecOps.....	466

4.	Microsoft Defender for Office 365 . . . . .	471
4.1	Introduction . . . . .	471
4.2	Stratégies . . . . .	473
4.2.1	Activation des stratégies prédéfinies. . . . .	475
4.2.2	Analyseur de configuration . . . . .	479
4.2.3	Paramètres des stratégies prédéfinies . . . . .	482
4.3	Configuration de stratégies personnalisées . . . . .	485
4.3.1	Antihameçonnage . . . . .	485
4.3.2	Pièces jointes fiables . . . . .	495
4.3.3	Liens fiables . . . . .	498
4.3.4	Logiciel anticourrier indésirable . . . . .	501
4.3.5	Logiciel antiprogramme malveillant . . . . .	501
4.3.6	DKIM . . . . .	502
4.3.7	DMARC . . . . .	502
4.3.8	Envois des utilisateurs . . . . .	503
4.4	Simulateur d'attaques . . . . .	503
4.4.1	Prérequis . . . . .	505
4.4.2	Simulation d'attaques . . . . .	505
4.4.3	Administration . . . . .	515
4.5	Tour d'horizon de l'outil . . . . .	517
5.	Microsoft Defender for Endpoint . . . . .	518
5.1	Introduction . . . . .	518
5.1.1	Prérequis . . . . .	519
5.1.2	Systèmes . . . . .	520
5.2	Déploiement Defender for Endpoint . . . . .	521
5.2.1	Création de l'espace Defender for Endpoint . . . . .	521
5.2.2	Tour d'horizon de l'interface . . . . .	529
5.2.3	Alertes . . . . .	534
5.3	Design déploiement . . . . .	541
6.	Microsoft Cloud App Security . . . . .	542
6.1	Introduction . . . . .	543
6.1.1	Architecture Cloud App Security . . . . .	544
6.1.2	Prérequis . . . . .	546
6.2	Démarrage . . . . .	546
6.2.1	Découverte Cloud App Security . . . . .	546
6.2.2	Interaction SecOps. . . . .	553
6.2.3	Examiner . . . . .	555

6.3 Stratégies .....	561
6.3.1 Exemple de stratégies .....	566
6.3.2 Contrôle d'application par accès conditionnel .....	569
7. État des lieux .....	573

## Chapitre 5

### Protection des données

1. Introduction .....	575
2. Microsoft Information Protection .....	576
3. Classifier et protéger .....	576
3.1 Introduction .....	576
3.2 Découverte des étiquettes de confidentialité .....	578
3.2.1 Introduction .....	578
3.2.2 Prérequis .....	579
3.3 Design .....	581
3.3.1 Préparation .....	581
3.3.2 Définition - Taxonomie Label .....	582
3.4 Création et configuration .....	584
3.5 Client Unified Label .....	598
3.5.1 Prérequis .....	599
3.5.2 Installation .....	600
3.5.3 Classification et protection de documents .....	602
3.5.4 Protection via l'Explorer .....	609
3.5.5 Actions utilisateurs .....	614
3.5.6 Actions pour les administrateurs .....	618
3.5.7 Suivi et monitoring .....	622
3.5.8 Android et iOS .....	625
3.5.9 Fichiers PDF .....	627
3.5.10 Envoi d'e-mails protégés .....	632
3.5.11 Envoi d'e-mails vers l'extérieur .....	635
3.5.12 Paramètres avancés .....	641
3.6 Étiquetage automatique .....	644
3.6.1 Étiquetage automatique client .....	645
3.6.2 Étiquetage automatique service .....	655

3.7	Étiquettes de confidentialité avec Teams, SharePoint et groupes Microsoft 365 . . . . .	666
3.7.1	Activation . . . . .	666
3.7.2	Application d'une étiquette dans Teams . . . . .	672
3.7.3	Application d'une étiquette sur un site SharePoint . . . . .	673
3.7.4	Application d'une étiquette sur un groupe Microsoft 365 . . . . .	674
3.8	Activation des étiquettes sur des fichiers dans SharePoint . . . . .	675
3.9	Chiffrement . . . . .	675
3.9.1	Introduction . . . . .	675
3.9.2	Chiffrement à double clé . . . . .	677
3.9.3	DuoKey . . . . .	678
3.9.4	Activation de la protection à double clé . . . . .	678
3.10	Super user . . . . .	681
3.11	Protection contre la perte de données . . . . .	682
3.11.1	Introduction au DLP . . . . .	683
3.11.2	Stratégie de DLP . . . . .	685
3.11.3	Création d'une stratégie DLP pour Microsoft Teams . . . . .	686
3.11.4	Expérience utilisateur DLP Teams . . . . .	693
3.11.5	Alertes . . . . .	695
3.12	Windows 10 et le DLP . . . . .	698
3.12.1	Introduction . . . . .	698
3.12.2	Création d'une stratégie DLP pour Windows 10 . . . . .	700
3.12.3	Expérience utilisateur . . . . .	712
3.12.4	Monitoring . . . . .	713
3.13	Conclusion . . . . .	715

## Chapitre 6

### Sécuriser Microsoft Azure

1.	Introduction Microsoft Azure . . . . .	717
1.1	Responsabilités . . . . .	719
2.	Azure Defender . . . . .	720
2.1	Introduction . . . . .	720
2.1.1	Ce que supporte Azure Defender . . . . .	723
2.1.2	Abonnement Azure . . . . .	724
2.1.3	Prise en main . . . . .	725

2.1.4 Activation . . . . .	728
2.1.5 Machines virtuelles - Just In Time Access . . . . .	735
2.1.6 Détection d'attaque - Azure machine virtuelle . . . . .	743
2.1.7 Notification . . . . .	752
2.1.8 Transition . . . . .	754
2.2 Azure Sentinel . . . . .	754
2.2.1 Introduction . . . . .	754
2.2.2 Composants . . . . .	756
2.2.3 Prérequis . . . . .	761
2.2.4 Mise en route . . . . .	761
2.2.5 Connecter une source de données . . . . .	767
2.2.6 Investigation . . . . .	772
2.2.7 Création d'une règle personnalisée . . . . .	775
2.2.8 Création d'une règle à partir d'un modèle . . . . .	780
2.2.9 Création d'un playbook . . . . .	782
2.3 Sécurité des machines virtuelles dans Azure . . . . .	788
2.3.1 Connexion . . . . .	788
2.3.2 Azure Bastion . . . . .	790
2.3.3 Azure Security Center/Defender . . . . .	796
2.3.4 Azure Backup . . . . .	796
2.3.5 Monitoring et mise à jour . . . . .	796
2.3.6 Firewall . . . . .	797
3. Conclusion . . . . .	797

## Chapitre 7

### Sécurité des accès privilégiés

1. Introduction . . . . .	799
1.1 Stratégie de sécurité On-premises et cloud . . . . .	799
1.1.1 Vulnérabilités . . . . .	800
1.1.2 Protection . . . . .	801
1.1.3 Sécurisation et isolation des comptes à privilèges . . . . .	802
1.1.4 Appareils depuis Endpoint Manager - utilisateurs standards .	804
1.1.5 Synchronisation des comptes . . . . .	806
1.1.6 Azure AD et Service - authentification . . . . .	806
1.1.7 Recommandations générales . . . . .	807

2.	Sécurité des accès depuis le cloud . . . . .	808
2.1	Zéro Trust et au-delà . . . . .	809
2.1.1	Stratégie d'accès privilégiés . . . . .	809
2.1.2	Appareils d'accès privilégiés . . . . .	812
2.1.3	Plan de sécurité rapide . . . . .	813
2.2	Modèle d'accès . . . . .	814
3.	Conclusion . . . . .	816

## Conclusion

1.	Introduction . . . . .	817
2.	Zero Trust . . . . .	818
3.	Ce que nous avons abordé . . . . .	819
3.1	Azure Active Directory . . . . .	820
3.2	Hardening Microsoft 365 . . . . .	820
3.3	La protection de données . . . . .	821
3.4	La sécurité des environnements Microsoft Azure . . . . .	821
3.5	Modèle d'accès privilégiés . . . . .	822
	Index . . . . .	823