PARTENARIAT MICROSOFT

Bezet-Torres Jérôme – CC BY NC SA – Date de l'article

Introduction

Le réseau Certa est en partenariat avec Microsoft et propose des parcours destinés aux enseignants et aux étudiants. Avec deux grands axes :

- Le Cloud,
- La cybersécurité dans l'écosystème Microsoft.

Microsoft Security

I. Cloud

Microsoft propose aux enseignants du BTS SIO le programme [Programme Microsoft Learn pour les enseignants | Microsoft Learn] (MSLE). Vous pouvez retrouver plus d'informations sur la page dédiée au partenariat entre Microsoft et le site du Certa [Lien.]

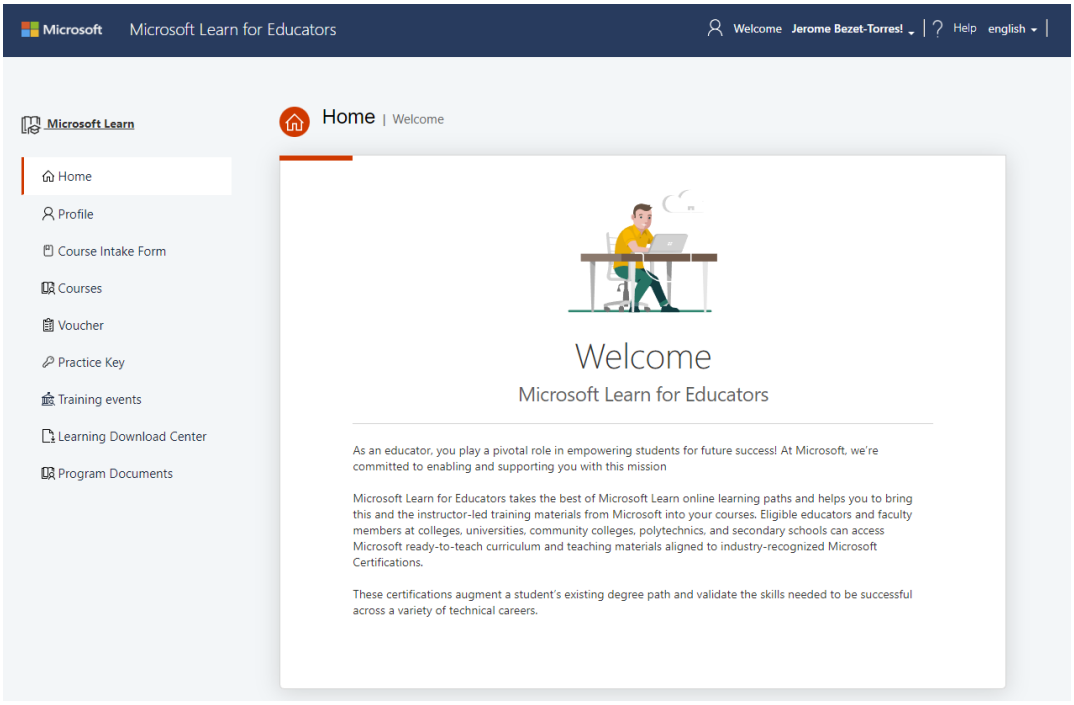

Figure 1 : portail MSLE

Plusieurs niveaux de certifications sont disponibles Fondamentales et Avancées basés sur les rôles. Je pense que les certifications fondamentales correspondent plus à notre publique.

A. Certifications fondamentales

La listes des certifications fondamentales sont assez nombreuses mais pour les SIO il me semble intéressant de leur enseigner quelques notions importantes sur le Cloud, il y a deux certifications à coloration SLAM et une certification à coloration SISR.

- AI-900 Artificial Intelligence Fundamentals (SLAM) lien
- AZ-900 Azure Fundamentals (SISR et SLAM) lien
- DP-900 Azure Data Fundamentals (SLAM) lien
- MS-900 Microsoft 365 Fundamentals lien
- SC-900 Security, compliance and Identity Fundamentals lien

Pour ma part cette année je me suis formé activement sur la partie Azure pour pouvoir enseigner à terme des notions fondamentales extraites des formations **AZ-900** et **SC-900.**
L'avantage du programme MSLE, est qu'il nous permet d'avoir les cours officiels de Microsoft ainsi que l'ensemble des travaux pratiques. Un autre avantage et non des moindres c'est que nous pouvons avoir des bons de passages pour des certifications Microsoft pour nos étudiants. Sachant que ces certifications correspondent à des besoins identifiés en entreprises.

B. Certifications Basées sur les rôles

Ces certifications sont beaucoup plus avancées pour nos étudiants, cependant pour les poursuites d'études comme ICS (Ingénieur en Cybersécurité) en partenariat avec l'école CPE de Lyon, la formation **AZ-104** semble très intéressante. Voici les compétences acquises par les étudiants après cette formation.

- Gérer les identités et la gouvernance Azure
- Implémenter et gérer le stockage
- Déployer et gérer les ressources de calcul Azure
- Configurer et gérer des réseaux virtuels
- Superviser les ressources Azure et en assurer la maintenance

Voici le chemin de certification que Microsoft propose lien.

II. La cybersécurité

Microsoft nous met à disposition une plateforme de formation pour les enseignants ainsi que pour les étudiants avec certaines restrictions (les laboratoires ou travaux pratiques sont payants pour les étudiants).

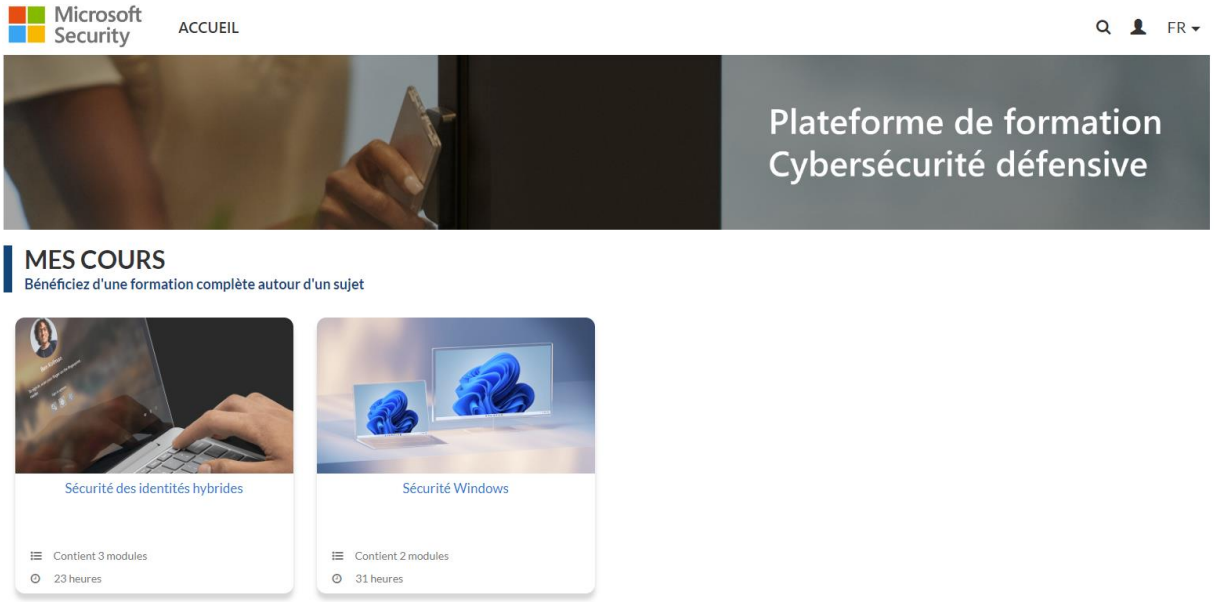

Figure 2 : MOOC Plateforme Cybersécurité défensive

Ces deux formations nous proposent des vidéos à destination de nos BTS SIO option SISR les PowerPoint sont en anglais.

- Sécurité Windows de : 31 heures
- Sécurité des identités Hybrides : 23 heures

A. Sécurité Windows

Ce cours permet à des apprenants déjà sensibilisés aux bases de la sécurité informatique de compléter leurs compétences avec les thématiques spécifiques au système Windows. Les différents enseignements sont regroupés autour de deux modules qui ciblent les différentes activités professionnelles en lien avec la sécurité informatique. Au cours de cette formation, l'apprenant est sensibilisé à l'administration des mécanismes de sécurité Windows et leur fonctionnement. À partir de cette base, l'apprenant acquiert ensuite des compétences opérationnelles pour contrer les attaques rencontrées couramment dans les environnements professionnels. Elle se décompose en deux modules :

- Sécurité Windows, dans ce module, l'apprenant se familiarise avec les éléments **fondamentaux** de la **sécurité Windows**. Le fonctionnement des composants de sécurité tels que **l'authentification**, le **contrôle d'accès**, **l'audit** et la **cryptographie** sont abordés, ainsi que leur configuration. Ce module constitue également une base de connaissances élémentaire pour les modules suivants.
- Menaces et **contre-mesures**, Ce module détaille les menaces auxquelles doit faire face un système **Windows** aujourd'hui. L'approche thématique reprend les principaux développements récents concernant les attaques de tous niveaux. L'apprenant est sensibilisé aux risques induits par les vulnérabilités associées et acquiert les compétences pour activer les contre-mesures proposées nativement par le système Windows.

B. Sécurité des identités Hybrides

Le cours traite des enjeux de sécurité des environnements hybrides en se concentrant sur les différentes phases d'attaques contre les plateformes d'identité. Il fournit une compréhension des composants des **annuaires** Microsoft (**Active Directory** et **Azure Active Directory**) et des bonnes pratiques et contre-mesures à mettre en place. Le cours aborde également les pratiques de gestion recommandées pour administrer des identités **hybrides** et **Cloud** de façon sécurisée, ainsi que les avantages et les alternatives à l'utilisation d'un mot de passe pour authentifier une identité. Elle se décompose en trois modules :

- Les fondations de l'identité hybride, Ce module introduit les composants principaux des environnements d'annuaire et de gestion des identités **Active Directory** (**AD DS**) et **Azure AD** (**AAD**). Ces notions sont essentielles pour comprendre, analyser et se défendre contre les menaces qu'ils pourraient subir. À l'issue de ce module, l'apprenant sera en mesure d'expliquer les mécanismes de sécurité de base présents dans les environnements **AD DS** & **AAD**.
- Les menaces ciblant la plateforme d'identités **hybrides** & **Cloud**, Ce module aborde les différentes phases d'attaques contre les plateformes d'identité. La **connaissance de ces attaques** est primordiale pour pouvoir recommander des bonnes pratiques et des contres mesures. À l'issue de ce module, l'apprenant sera en mesure de décrire les attaques modernes et mettre en place des défenses efficaces.
- La gestion sécurisée des identités hybrides, Ce module aborde les pratiques de gestion recommandées pour administrer des identités hybrides et cloud de façon sécurisée. La bonne compréhension de ces pratiques est essentielle afin de pourvoir prioriser des recommandations de sécurité. À l'issue de ce module, l'apprenant sera

en mesure de recommander des pratiques de gestion alignées sur l'approche Zéro Trust.

III. Retour d'expérience

A. Mon analyse du MOOC

Pour avoir suivis ces formations en autonomie j'ai décidé de créer un outil pour évaluer la difficulté des séquences vidéo et ainsi pouvoir évaluer si ces formations sont adaptées à nos BTS SIO option SISR.

L'outil qui me permet d'évaluer la difficulté des notions abordées en me basant sur trois critères distincts :

- Niveau de difficultés : langage utilisés, abréviations, démonstrations…
- Longueur : durée de la vidéo
- Thèmes : natures des thèmes abordés

MOOC Cybersécurité - Microsoft

Module 1 - Sécurité Windows	Niveau de difficulté	Longueur	Thème	Score
Introduction du cours	N/A	N/A	N/A	
Introduction du module	N/A	N/A	N/A	
Séquence 1 : Service d'authentification				
Introduction				1
Structures fondamentales de l'identité				60
La base de compte - SAM				48
Services du sous-système LSA				60
Cycle de vie de la session				125
Module d'authentification AP				75
Services SSPI				100
UAC				36
Comptes de service				24
Conclusion				

66

Module 2 - Menaces et contre-mesures	Niveau de difficulté	Longueur	Thème	Score
Introduction du cours	N/A	N/A	N/A	
Séquence 1 : Failles matérielles				
Introduction				0
Attaques visant le CPU				60
Attaques visant les unités mémoires				60
Périphérique malveillants				100
Firmwares				60
Conclusion				0
Séquence 2 : Corruption de windows				
Introduction				0
Analyse de risque				32
Séquence de démarrage				32

70

Figure 3 : Outil d'analyse des vidéos.

Légende					
	N/A	Facile	Correct	Dur	Avancé
Niveau de difficulté	1	2	3	4	5
	N/A	Courte	Normal	Long	Trop Long
Longueur	1	2	3	4	5
	N/A	Intéréssant	bon	Très bien	Excellent
Thème	1	2	3	4	5

75 Niveau Avancé

Figure 4 : Échelle d'évaluation.

Chacun sur une échelle de 1 à 5, ainsi en multipliant les trois valeurs je trouve ainsi un score qui me permet d'évaluer le degré de difficulté de la vidéo. J'estime que lorsque que le score obtenu est supérieur ou égale à **75** le niveau de la vidéo est difficile ou pas adapté ou alors il faut ajouter des compléments pour que l'ensemble des apports soit compris par les étudiants.

J'ai également suivi le vendredi 6 janvier la formation dispensée par les créateurs des Modules Microsoft, qui ont apprécié le retour ainsi que l'outil. Je vous partage donc aujourd'hui deux fichiers le premier correspond à mon analyse et ma perception des deux formations et le même fichier vide qui vous permettra à votre tour d'évaluer la difficulté des deux formations.

B. Objectifs

Je me suis fixé plusieurs objectifs, le premier, construire une plateforme pour réaliser les travaux pratiques car pour rappel l'accès aux TPs pour les étudiants est **payant**, les enseignants ont un accès pour 6 mois dès **leurs inscriptions**. Après avoir échangé avec les personnes de **Microsoft**, il est décidé qu'ils nous donneront accès aux sources des travaux pratiques au format **Markdown**. Ce format est très intéressant car avec un outil open-source de Microsoft nous pouvons générer un site web static (outil Docfx – open source) assez facilement pour avoir les travaux protiques dans un format agréable à utiliser.

Figure 4 : Exemple de l'outil Docfx – site web static

- En **A** une barre de navigation totalement personnalisable
- En **B** une table des matières de l'ensemble des documents du site static
- En C une table des matières du document que nous suivons…

Les formateurs nous mettrons à dispositions les disques durs des machines virtuelles mais cela représente un volume très important de machines virtuelles 1 To de durs virtuelles.

Conclusion

Microsoft nous met à disposition de belles ressources pour nos étudiants il faut cependant les retravailler et construire des TP pour permettre à nos étudiants de s'approprier ces nouveaux concepts de sécurité qui interviennent en Bloc 3 du référentiel du BTS SIO.