Microsoft – Éducation Nationale

BTS cybersécurité et/des services informatiques aux organisations
BTS SIO

Les intervenants

Jérôme Bezet-Torres

Parcours Professionnel

- Microsoft MVP 3 x Cloud and Datacenter Management
- Microsoft Certified Trainer ++ 10 ans
- VMware vExpert 3 ans
- Instructeur Cisco CCNA – IT - DevNet
- Auteur Éditions ENI – livres - vidéos

Mes passions - domaines

- Écosystème Microsoft
- Scripting PowerShell
- Automatisation
- Packer – Vault – Terraform - Ansible

Professeur d'informatique BTS SIO

Académie de Lyon
Formateur Académique
Institution des chartreux
BTS SIO option SISR 1ère Année – 2 ème Année

Contacter

@JM2K69

https://www.linkedin.com/in/jerome-bezettorres

Intervenants

Arnaud Jumelet

Karine Sanguinet

Alexandre Lafargue

Les Partenariats

AWS Academy

Le CERTA est un établissement membre d'AWS Academy.

CISCO Systems

Partenariat avec CISCO Systems autour du programme NetAcad.

MICROSOFT

Le réseau CERTA reconduit son partenariat avec Microsoft autour du CLOUD AZURE en BTS SIO.

Root-Me PRO

Des environnements pratiques en ligne dédiés à l'apprentissage éthique de la Cybersécurité

IBM

Le partenariat avec IBM : comprendre et maîtriser le cloud, la cybersécurité, l'IA.

ANSSI

Ressources ANSSI SecNum Académie et CyberEdu.

STORMSHIELD

Un partenariat avec Stormshield autour du programme de formation sur les pare-feux SNS.

Partenariat

Contact
Olivier Mondet – Inspecteur d'académie – Inspecteur pédagogique et régional – Rectorat de Créteil
Amal Hecker (amal.hecker@reseaucerta.org) – Professeure en BTS SIO – Lycée polyvalent de Cachan – Académie de Créteil
Mickaël Honvault (mickael.honvault@ac-lille.fr) - Professeur en BTS SIO - Lycée Gaston Berger - Lille

Éducation Nationale – Réseau Certa

Microsoft

Rénovation du BTS SIO

- Diplôme de niveau 5 le plus complet en cybersécurité
- Contenu cyber en systèmes et réseaux et en développement informatique

MOOC Microsoft Sécurité

- Windows Sécurité
- Sécurité des Identités hybrides

Quelques chiffres récents

1 heure
Pour accéder aux données

<2 heures
pour se déplacer

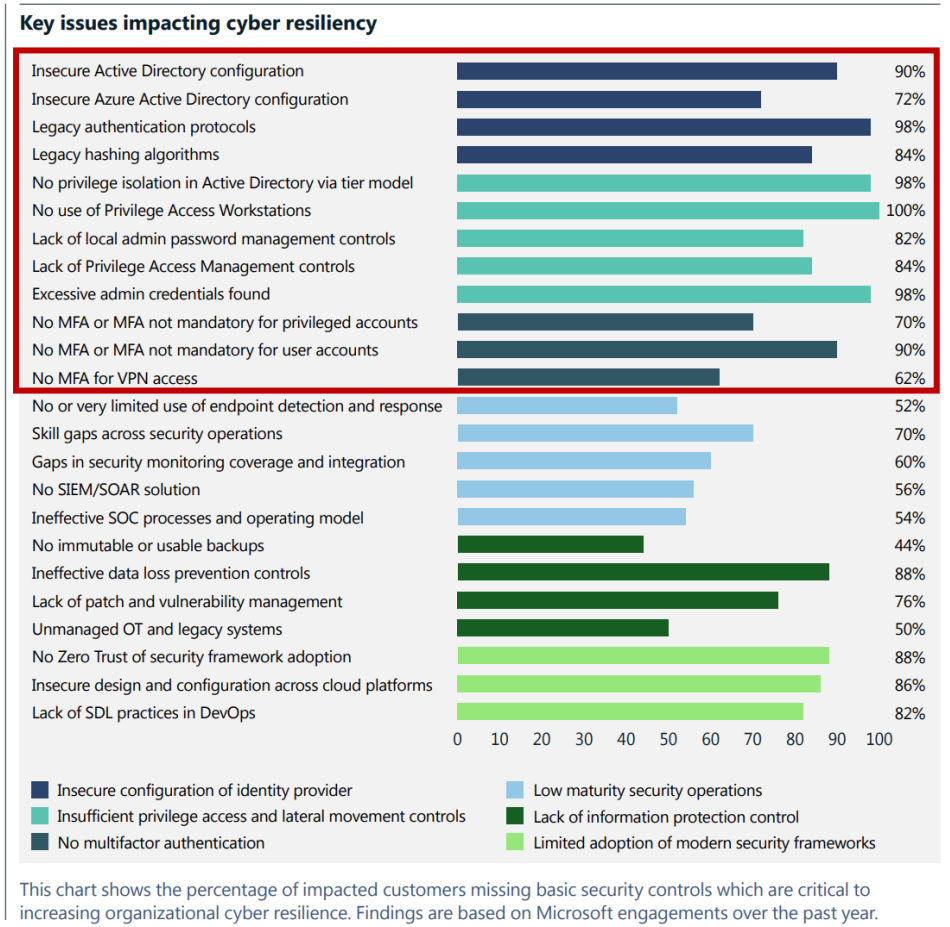
710 millions d'e-mails de phishing bloqués par semaine.

Appliquer les correctifs sans tarder

78% des appareils ont au moins un logiciel non patché alors que depuis

9 mois le correctif de sécurité est disponible.

Les menaces actuelles



This chart shows the percentage of impacted customers missing basic security controls which are critical to increasing organizational cyber resilience. Findings are based on Microsoft engagements over the past year.

Ce graphique montre le pourcentage de clients compromis qui n'ont pas appliqués les contrôles de sécurité de base essentiels pour accroître la cyber-résilience. Les résultats sont basés sur les engagements de Microsoft au cours de la dernière année.

Active Directory (AD) and Azure AD security

88%

of impacted customers did not employ AD and Azure AD security best practices. This has become a common attack vector as attackers exploit misconfigurations and weaker security postures in critical identity systems to gain broader access and impact to businesses.

Least privilege access and use of Privileged Access Workstations (PAW)

None of the impacted organizations implemented proper administrative credential segregation and least privilege access principles via dedicated workstations during the management of their critical identity and high-value assets, such as proprietary systems and business-critical applications.

Over 80 percent of security incidents can be traced to a few missing elements that could be addressed through modern security approaches.

Microsoft Digital Defense Report 2022

Aka.ms/mddr

Plateforme de formation

- Deux parcours pour nos étudiants
  - Sécurité Windows
  - Sécurité des identités hybrides

Plateforme de formation

MES COURS

Bénéficiez d'une formation complète autour d'un sujet

Sécurité Windows

Contient 2 modules

31 heures

Sécurité des identités hybrides

Contient 3 modules

23 heures

- Deux parcours pour nos étudiants
  - Sécurité Windows
  - Sécurité des identités hybrides

RÉSEAU CERTA

Sécurité des identités hybrides

Module 1 : Les fondations de l'identité hybride

Expliquer les mécanismes de sécurité de base présents dans les environnements Active Directory & Azure Active Directory.

Module 2 : Les menaces et les contre-mesures

Décrire les attaques modernes et mettre en place des défenses efficaces.

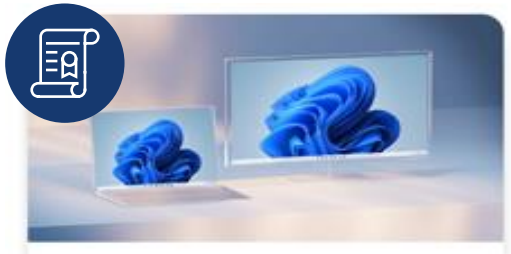
Module 3 : La gestion sécurisée des identités hybrides

Recommander des pratiques de gestion alignées sur l'approche Zero Trust.

- **6 heures de vidéos**
- **215 questions**
- **22 heures de labs**

Microsoft

RÉSEAU CERTA



Sécurité windows

Module 1 : Administrer la sécurité Windows

Découvrir comment utiliser les services d'authentification, de contrôle d'accès, d'audit et de chiffrement.

Module 2 : Les menaces et les contre-mesures

Décrire les contrôles de sécurité à configurer pour contrer les vulnérabilités matérielles, la corruption du système Windows, le vol d'identité et l'exploitation d'applications vulnérables.

Module 3 : Extraire des informations dans un contexte post-mortem

Savoir comment obtenir une image de la mémoire d'un système Windows et décrire comment extraire l'activité du système en cours, les données de la mémoire et les informations sur les périphériques.

- **7 heures de vidéos**
- **220 questions**
- **22 heures de labs**

Microsoft

Une analyse…

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	66
Services SSPI				100	
UAC				36	
Comptes de service				24	
Conclusion					
Séquence 2 : Contrôle d'accès					
Privilèges Windows				30	
Gestion des privilèges Windows				48	
Base de sécurité locale				24	
Lkit de ressources de confirmité de la sécurité SCT				80	68
Modèle DACL				125	
Modèles obligatoires et dynamiques				125	
Définir un contrôle d'accès				45	
Conclusion					

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	70	
Périphérique malveillants				100		
Firmwares				60		
Conclusion				0		
Séquence 2 : Corruption de windows						
Introduction				0		
Analyse de risque				32		
Séquence de démarrage				32		
Technique de démarrage sécurisée				48		
RootKits				45	50	
Sécurité basée sur la vrtualisation				48		
Contrôle d'intégrité du code				100		
Sécurité des environnemnts de scripts				45		
Conclusion				0		
Séquence 3 : Vol d'iendtité						
Introduction				0		
Vol d'information en mémoire				60		

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	***Intéressant***	***bon***	***Très bien***	***Excellent***
Thème	1	2	3	4	5

75 Niveau Avancé

Quels modules utiliser et quand…

Name	Duration	Temps Sequence	Proportion	Choix vidéo SIO1	Parcours SIO1	Bloc SIO1	Choix vidéo SIO2	Parcours SIO2	Bloc SIO2
1.0.0 Introduction du module.mp4	00:00:47								
1.1.0 Sequence 1 Services d'authentification - introduction.mp4	00:01:17								
1.1.1. Structures fondamentales de l'identité.mp4	00:07:41			x	00:07:41	B1			
1.1.2. La base de compte - SAM.mp4	00:03:24			x	00:03:24	B3			
1.1.3. Services du sous-système LSA.mp4	00:02:10								
1.1.4. Cycle de vie de la session.mp4	00:04:21	00:33:41	25%	x	00:04:21	B1			
1.1.5. Modules d'authentification AP.mp4	00:02:24						x	00:02:24	B2
1.1.6. Services SSPI.mp4	00:05:23								
1.1.7. UAC.mp4	00:04:52			x	00:04:52	B1			
1.1.8. Comptes de service.mp4	00:02:09						x	00:02:09	B2
1.1.9 Conclusion.mp4	00:01:33								
1.2.0 Séquence 2 Contrôle d'accès Introduction.mp4	00:01:05								
1.2.1. Privilèges Windows.mp4	00:04:08								
1.2.2. Gestion des privilèges Windows.mp4	00:02:07						x	00:02:07	B2
1.2.3. Base de sécurité locale.mp4	00:03:40								
1.2.4. Kit de ressources de conformité de la sécurité (SCT).mp4	00:04:51	00:33:46	26%				x	00:04:51	B3
1.2.5. Modèle DACL.mp4	00:08:58						x	00:08:58	B3
1.2.6. Modèles obligatoires et dynamiques.mp4	00:04:10								
1.2.7. Définir un contrôle d'accès.mp4	00:04:47			x	00:04:47	B1			
1.2.8. Conclusion.mp4	00:00:58								
1.3.0 Séquence 3 Services d'audits - Introduction.mp4	00:01:02								
1.3.1. Fonctionnement de l'audit.mp4	00:02:21						x	00:02:21	B3
1.3.2. Stratégies d'audit.mp4	00:03:53						x	00:03:53	B3
1.3.3. Audit des accès aux ressources.mp4	00:06:30	00:25:03	19%				x	00:06:30	B3
1.3.4. Audit des ouvertures de sessions.mp4	00:07:16						x	00:07:16	B3
1.3.5. Audit des changements dans la stratégie de sécurité.mp4	00:05:03						x	00:05:03	B3
1.3.6. Conclusion.mp4	00:00:52								
1.4.0 Séquence 4 Cryptographie - Introduction.mp4	00:01:17								

Parcours SIO1		Parcours SIO2	
B1	00:21:41	B1	00:00:00
B2	00:10:23	B2	00:06:40
B3	00:03:24	B3	00:46:59
Total	00:35:28	**Total**	00:53:39
tx d'utilisation	26,85%	**tx d'utilisation**	40,61%

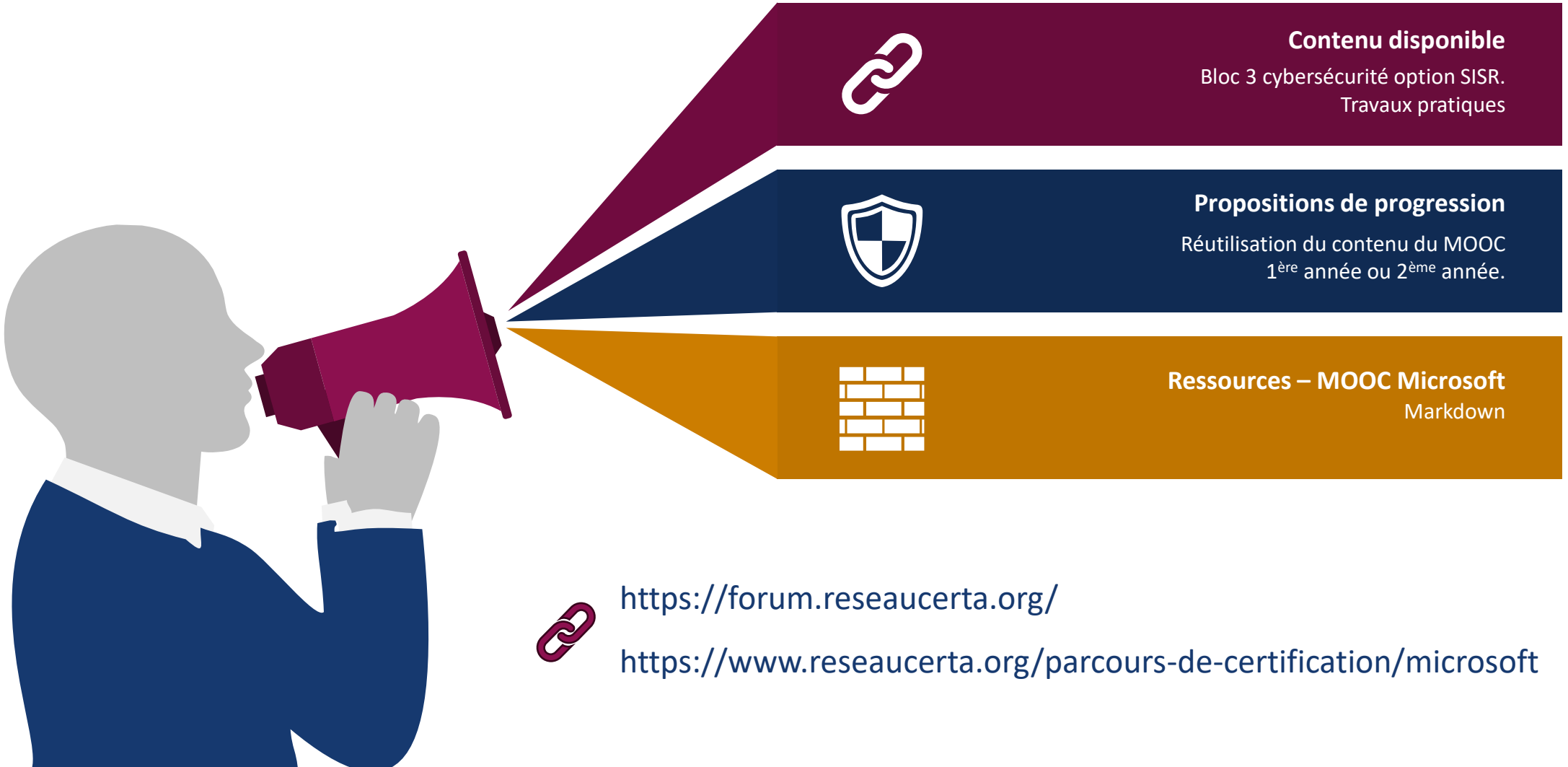
Synthèse	
B1	00:21:41
B2	00:17:03
B3	00:50:23
Total	01:29:07
tx d'utilisation	67,46%

RÉSEAU CERTA

Démonstrations

- Accès à la plateforme
- Travaux pratiques
- Docfx
- Terraform

Septembre – Décembre 2023



Contenu disponible

Bloc 3 cybersécurité option SISR.
Travaux pratiques

Propositions de progression

Réutilisation du contenu du MOOC
1ère année ou 2ème année.

Ressources – MOOC Microsoft

Markdown

https://forum.reseaucerta.org/

https://www.reseaucerta.org/parcours-de-certification/microsoft