Sujet n° 5

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS
Sous-épreuve E12- Expression et communication en langue anglaise
Session 2023

Coefficient 1

Durée maximale de l'épreuve : 20 minutes
Préparation : 20 minutes

Déroulement de l'épreuve :

1) Expression orale en continu (5 minutes maximum)

   Présentation en anglais de l'analyse du dossier et de la situation en lien avec le secteur professionnel

2) Expression orale en interaction (15 minutes maximum)

   Échange en anglais avec l'examinateur à partir de l'analyse du dossier et des réponses apportées au questionnement accompagnant la mise en situation

L'usage d'un dictionnaire n'est pas autorisé.

Composition du dossier du candidat

Document A	**Texte**: Importance of Cybersecurity in Consumer Goods Business
Document B	**Infographie**: Need for ethical hackers
Document C	**Video**: Wizlynx ethical hacking services (1'15)
Mise en situation et questionnement	

Ce sujet comporte 4 pages. Il est conseillé au candidat de vérifier que le sujet est complet.

DOSSIER DU CANDIDAT : ETHICAL HACKING

Document A

Importance of Cybersecurity in Consumer Goods Business

The consumer sector is big business – for shareholders as well as hackers. Large companies with multiple brands operate with an unprecedented amount of valuable data, which means a single cyber incident could cost assets and a reputation worth billions of dollars. Consumer businesses are always in danger from cyber-attacks, so their defenses must be strong and resilient to deal with them. […]

Be prepared

It's simply not worth the risk of not having strong cybersecurity measures in place within a consumer goods business. One incident can lead to irreparable damage to reputation and significantly impact the bottom line through long-term loss of customers, customer compensation, and compliance fines. We've seen this time and time again.

As business productivity is returning to pre-pandemic levels but with the added cyber risk of more remote working, cybersecurity priorities need to be:

- Manage cyber risk as a team with a strong balance between the rapid adoption of technology and appropriate cyber risk management.
- Increase preparedness with cyber risk management strategies in the enterprise and emerging technologies as they are deployed.
- Monitor people, applications, systems and the external environment to detect incidents more effectively.
- Develop threat intelligence to understand harmful behavior and top risks.
- Be prepared and decrease the business impact of incidents before they escalate.
- Capture lessons learned to improve security controls.

In a nutshell, always #BeCyberSmart.

Carol Watson, *enhalo.co,* December 7, 2021

Document B

https://www.vpnmentor.com/blog/ultimate-guide-to-ethical-hacking/

Document C

Vidéo : Wizlynx ethical hacking services (1'15)

Wizlynx group, August 2, 2021

MISE EN SITUATION

You are an IT technician. Your manager is worried about potential cyber-attacks and he would like to know more about penetration testing ethical hackers. You give him advice.

QUESTIONNEMENT

- What is the difference between malicious and ethical hackers?
- What is the purpose of ethical hacking?
- What about penetration tests?