BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2023**

Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

ANNEXE 8-A : Outil d'aide à l'appréciation de l'environnement technologique mobilisé par la personne candidate

CONTRÔLE DE L'ENVIRONNEMENT TECHNOLOGIQUE

En référence à l'annexe II.E « Environnement technologique pour la certification » du référentiel du BTS SIO

Identification[1]	**IPSSI PARIS** **25 Rue Claude Tillier, 75012 Paris**	**SISR**

1. Environnement commun aux deux options

1.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

Éléments	**Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)**	**Remarques de la commission d'interrogation**
Un service d'authentification	OpenLDAP / Active Directory / (P)EAP	
Un SGBD	MySQL, MariaDB / SQLite	
Un accès sécurisé à internet	Firewall au cœur de réseau / Chiffrement asym. de flux avec SSL/TLS / Proxy Squid	
Un environnement de travail collaboratif	Github, Gitlab / Google Drive / Dropbox / Trello / Planner	
Deux serveurs, éventuellement virtualisés, basés sur des systèmes d'exploitation différents, dont l'un est un logiciel libre (*open source)*	Proxmox VE / VMware ESXi / Distributions Linux (Debian, Ubuntu, CentOS) / Windows Server 2019 / Windows Server 2022	

[1] Nom et adresse du centre d'examen ou identification de la personne candidate individuelle (numéro, nom, prénom)

ANNEXE 8-A (suite) : Modèle d'attestation de respect de l'annexe II.E – « Environnement technologique pour la certification » du référentiel

Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

Éléments	**Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)**	**Remarques de la commission d'interrogation**
Une solution de sauvegarde	Proxmox Backup Server / Serveur rsync / TrueNAS	
Des ressources dont l'accès est sécurisé et soumis à habilitation	Proxy Squid avec authentification / Reverse Proxy avec authentification	
Deux types de terminaux dont un mobile (type *smartphone* ou encore tablette)	Utilisation de PC fixes et portables, Téléphones IP, smartphones et tablettes via un réseau filaire VMPS ou via des canaux Wi-Fi sécurisés via SSID-to-VLAN	

1.2 Des outils sont mobilisés pour la gestion de la sécurité :

Éléments	**Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)**	**Remarques de la commission d'interrogation**
Gestion des incidents	GLPI	
Détection et prévention des intrusions	NIPS Snort / HIPS OSSEC	
Chiffrement	Chiffrement de flux par certificats TLS v1.2 à v1.3 / Chiffrement pair-à-pair de donner via des mécanismes asymétrique GPG / Chiffrement de stockage via des mécanismes symétriques AES, Twofish, Serpent	
Analyse de trafic	Analyse de trafic inter-VLAN, NAT et PAT via PFSense, utilisation de Wireshark	

Rappel : les logiciels de simulation ou d'émulation sont utilisés en réponse à des besoins de l'organisation. Ils ne peuvent se substituer complètement à des équipements réels dans l'environnement technologique d'apprentissage.

Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

ANNEXE 8-A (suite) : Modèle d'attestation de respect de l'annexe II.E « Environnement technologique pour la certification » du référentiel

2. Éléments spécifiques à l'option « Solutions d'infrastructure, systèmes et réseaux » (SISR)

Rappel de l'annexe II.E du référentiel : **« *Une solution d'infrastructure réduite à une simulation par un logiciel ne peut être acceptée.* »**

2.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

Éléments	**Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)**	**Remarques de la commission d'interrogation**
Un réseau comportant plusieurs périmètres de sécurité	Zones : MZ, DMZ, Guest et IT Utilisation de VLAN et filtrage de niveau 3 et 4, utilisation d'ACL	
Un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en termes de sécurité et de haute disponibilité	Hébergement d'une application Web métier dans un serveur de haute disponibilité par réplication et répartition de charge, incluant une Web Application Firewall	
Un logiciel d'analyse de trames	TCP dump et Wireshark	
Un logiciel de gestion des configurations	OCS Inventory / Fusion Inventory / Serveur TFTP	
Une solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès	Windows : RDP over VPN UNIX / Linux : SSH Autres : VNC over VPN Utilisation d'un Bastion	
Une solution permettant la supervision de la qualité, de la sécurité et de la disponibilité des équipements d'interconnexion, serveurs, systèmes et services avec remontées d'alertes	EyesOfNetwork / ZABBIX Scripts d'automatisation de scan NMAP avec NSE	
Une solution garantissant des accès sécurisés à un service, internes au périmètre de sécurité de l'organisation (type intranet) ou externes (type internet ou extranet)	OpenVPN avec authentification par certificat X.509 Intégration et gestion d'une PKI privée	

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution garantissant la continuité d'un service	Réplication de service sur un hyperviseur secondaire pour un PRA	
Une solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion	Pacemaker / Heartbeat / Corosync / STP	
Une solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion	HAProxy / NGINX	

2.2 La structure et les activités de l'organisation s'appuient sur au moins une solution d'infrastructure opérationnelle parmi les suivantes :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution permettant la connexion sécurisée entre deux sites distants	OpenVPN / IPSEC / L2TP / Wireguard	
Une solution permettant le déploiement des solutions techniques d'accès	GPO / Script d'automatisation à l'échelle d'un parc informatique	
Une solution gérée à l'aide de procédures automatisées écrites avec un langage de *scripting*	Script de filtrage de niveau 3 (Netfilter via iptables) Script de backup (rsync)	
Une solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau	NIPS Snort	