BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2025**

Fiche descriptive de réalisation professionnelle (recto)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation :**
Nom, prénom : Noah NICOLAU	**N° candidat :**
Épreuve ponctuelle **Contrôle en cours de formation**	**Date :** 20 / 04 /2026

Organisation support de la réalisation professionnelle

Le Port de Cherbourg est une infrastructure maritime stratégique assurant le transit de passagers, le transport de marchandises et l'accueil de croisières. L'organisation s'appuie sur un système d'information (SI) complexe comprenant environ 150 postes de travail, des serveurs de bases de données critiques et des équipements réseaux répartis sur plusieurs zones géographiques du port.

Intitulé de la réalisation professionnelle

Mise en œuvre d'une plateforme de gouvernance d'infrastructure : Supervision, Gestion de parc automatisée et Audit de vulnérabilités.

Période de réalisation : 05/09/25 – 22/05/26 **Lieu :** Saint Raphaël

Modalité : **X Seul(e)** **En équipe**

Compétences travaillées

X Concevoir une solution d'infrastructure réseau

X Installer, tester et déployer une solution d'infrastructure réseau

X Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation (ressources fournies, résultats attendus)

Ressources fournies :

- Accès à l'infrastructure : Serveur physique sous Linux (Debian) et Switch manageable Cisco 2950.
- Cahier des charges : Note de cadrage de la DSI sur les objectifs de supervision et de sécurité.
- Documentation technique : Accès aux documentations communautaires (Docker, Icinga, GLPI, Greenbone).
- Comptes administrateurs : Accès aux machines du domaine pour le déploiement des agents d'inventaire.

Résultats attendus :

- Automatisation de l'inventaire : Remontée automatique des caractéristiques matérielles et logicielles des postes de travail dans GLPI via OCS Inventory.
- Supervision opérationnelle : Mise en place d'un tableau de bord Icinga surveillant l'état des services.
- Audit de sécurité : Génération d'un rapport de vulnérabilités complet (via Greenbone) listant les failles critiques du réseau interne.
- Conteneurisation des services : Déploiement de l'ensemble des outils sous forme de conteneurs Docker pour garantir une infrastructure isolée, stable et facilement maintenable.
- Documentation technique : Rédaction d'une procédure d'exploitation pour le suivi des alertes et la gestion du cycle de vie du matériel.

Description des ressources documentaires, matérielles et logicielles utilisées

Ressources Documentaires :

- Documentation Icinga 2 : Pour la mise en place des "checks" de supervision et des notifications.
- Documentation GLPI/OCS Inventory : Pour la liaison entre l'agent d'inventaire et la base de données de gestion.
- Documentation Greenbone (OpenVAS) : Pour la configuration des scans de sécurité et l'interprétation des rapports de vulnérabilités.
- Mémento Cisco : Pour la configuration des communautés SNMP sur le switch 2950.

Matériel spécifique utilisé :

- Serveur physique : Hôte de virtualisationalloué pour supporter l'ensemble des services.
- Switch Cisco

Production finale :

- Icinga 2 : Outil de supervision utilisé pour surveiller la disponibilité des serveurs du port et l'état des ports du switch Cisco en temps réel.
- GLPI & OCS Inventory : Couple de logiciels permettant l'inventaire automatique des postes de travail et la gestion des tickets d'assistance (Helpdesk).
- Greenbone : Scanner de vulnérabilités utilisé pour identifier les failles de sécurité (OS obsolètes, services mal configurés) sur le rése--au interne.
- Docker : Utilisé pour conteneuriser les services de supervision et d'inventaire, facilitant ainsi leur déploiement et leurs futures mises à jour.

Modalités d'accès aux productions et à leur documentation

https://noah-nicolau.fr/

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2025**

Fiche descriptive de réalisation professionnelle (verso)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs

Plan proposée :

Le Port de Cherbourg disposait d'un inventaire manuel (tableur Excel) souvent obsolète, ce qui rendait la gestion du cycle de vie des machines impossible. De plus, les techniciens n'étaient informés des pannes que par les appels des utilisateurs, faute d'un système d'alerte. Enfin, aucune analyse régulière des failles de sécurité internes n'était effectuée, exposant le port à des risques d'intrusion via des logiciels non mis à jour.

Solution envisagée :

- Supervision : Étude de solutions comme Nagios ou Icinga (plus moderne).
- Inventaire : Mise en place d'un système automatisé OCS/GLPI pour supprimer la saisie manuelle.
- Audit : Utilisation de Greenbone pour réaliser des scans de vulnérabilités périodiques.

Solution Retenue :

L'ensemble des solutions retenues est **Open Source**, permettant une grande flexibilité sans coût de licence. Le déploiement via **Docker** a été choisi pour isoler les services et garantir la stabilité du serveur de gestion.

La réalisation :

La mise en œuvre a été découpée en trois phases techniques majeures :

1. Gestion du parc : Installation du serveur OCS Inventory couplé à GLPI. Déploiement des agents OCS sur les postes du domaine pour remonter automatiquement les configurations matérielles et logicielles.
2. Supervision réseau : Configuration d'Icinga pour surveiller le switch Cisco 2950 via le protocole SNMP. Création d'alertes mail en cas de saturation de bande passante ou de coupure d'un lien critique.
3. Audit de sécurité : Installation de Greenbone Security Assistant. Lancement d'un scan complet du réseau pour identifier les machines présentant des failles critiques (CVE) et rédaction d'un plan d'action pour les correctifs.

Conclusion :

Cette réalisation apporte une visibilité complète sur l'infrastructure du port. Les techniciens interviennent désormais de manière **proactive** grâce aux alertes Icinga. L'inventaire est toujours à jour, ce qui facilite la planification des budgets de renouvellement matériel. Enfin, les audits Greenbone ont permis de durcir la sécurité du réseau interne en corrigeant les failles avant qu'elles ne soient exploitées.