Contrôle de la Sécurité des S.I.

Les investigations

Les investigations et résultats

- ⇨Les méthodes d'investigation
- ⇨Les entretiens
- ⇨La gestion de la preuve
- ⇨Les résultats
- ⇨Points clefs

⇨*Mise en pratique : identifications des investigations à réaliser*

Les objectifs des investigations

⇨ Les investigations peuvent avoir plusieurs objectifs souvent complémentaires :

- ✓ Recueillir des éléments de preuves permettant de s'assurer de la conformité ou de la non-conformité de tout ou partie du S.I. par rapport à un référentiel
- ✓ S'assurer de la robustesse des mesures de sécurité vis-à-vis d'une menace
- ✓ Enquêter suite à un incident de sécurité

Types et natures d'investigation

- Le type d'investigation peut se caractériser en fonction de la méthode, démarche, … utilisée
- Exemple :

CS1	**Contrôler les Infrastructures**	→ Analyse d'architecture → Contrôle de configuration → Tests d'intrusion
CS2	**Contrôler les Applications**	→ Analyse de code → Tests des fonctions de sécurité → Tests de vulnérabilités
CS3	**Contrôler les Process**	→ Contrôle environnements → Contrôle des procédures → Contrôle des méthodes

Types et natures d'investigation

⇨ Le type d'investigation peut se caractériser par les méthodes à mettre en œuvre pour les réaliser :

- ✓ Des observations visuelles
- ✓ Des relevés techniques
- ✓ Des entretiens
- ✓ Des relevés de paramètres fonctionnels
- ✓ Des analyses documentaires
- ✓ Des tests techniques

CS1 - Analyse d'architecture

⇨ **Contenu du contrôle :**

✓ Analyser d'architecture des infrastructures afin d'évaluer la cohérence des orientations techniques retenues pour garantir la sécurité du système.

⇨ **Méthodes**

✓ Ces investigations s'appuient essentiellement de l'analyse documentaire et des entretiens

CS1 - Analyse d'architecture

⇨ **Démarche et outils :**

✓L'analyse s'appuie sur le relevé des écarts observés entre :

- La mise en œuvre de l'architecture
- Les documents liés à l'architecture : DAT, Dossier d'administration, manuel d'exploitation ...
- Le référentiel documentaire SSI de la Banque Postale

✓L'analyse pourra porter notamment sur :

- Plan d'adressage et de nommage IP
- Plan de routage
- Cloisonnement
- Exploitabilité
- Choix des fonctions de sécurité
- …

CS1 - Analyse d'architecture

⇨ **Exemple de preuves recherchées :**

- Absence d'identification d'objectifs de sécurité
- Absence de modules de Sécurité
- Choix techniques non optimal (chiffrement bas, annuaire sans contrôle, …)
- L'absence de cloisonnement
- …

CS1 – Contrôle de configuration

⇨ **Contenu du contrôle**

✓Le contrôle doit permettre de mettre en évidence :

- Les vulnérabilités issues des écarts des configurations par rapport au référentiel de l'entité et à l'état de l'art ;
- L'origine de ces écarts (erreurs humaines, vulnérabilité du processus…).

⇨ **Méthodes**

✓Ces investigations s'appuient essentiellement sur des relevés de paramètres techniques et fonctionnels

CS1 – Contrôle de configuration

⇨ Démarches et outils

✓L'analyse s'appuie sur le relevé des écarts observés entre la réalité et :

- Les normes de l'entité
- L'état de l'art
- Le référentiel technique interne

✓Les éléments contrôlés sont notamment :

- Les serveurs, Les postes de travail
- les infrastructures réseaux
- Les équipements de sécurité

✓Les contrôles peuvent porter sur notamment :

- Les versions des équipements en matière de sécurité
- La configuration des services de sécurité
- Le contrôle des paramétrages (activation ou non de services sensibles par exemple)
- Revue de droits
- Gestion des privilèges

CS1 – Contrôle de configuration

⇨ **Exemple de preuves recherchées :**

- Version de pach Sécurité non à jour
- Ports non utiles ouverts
- Des paramètrages « par défaut »
- L'absence de gestion de profil
- Des fonctions de sécurité non activés, ou non présentes (ex de l'antivirus)
- …

CS1 – Contrôle de configuration

⇨ Exemple d'outil : Poste de travail

Règle	Famille	Question	Action à effectuer	Réponse attendue	Réponse observée	Conformité (O/N/_)	Evaluation (+/-/_)
	AQ -- Acquisition d'équipements et de prestations						
AQ-7	Paramètres de sécurité des utilisateurs	Possibilité d'ajouter/modifier des programmes ?		On ne doit pas avoir la possibilité d'ajouter, supprimer et modifier des programmes.			
	CL -- Contrôle d'accès logique						
CL-2	Comptes utilisateurs et administrateur	Vérification la désactivation ou l'absence du compte invité		Le compte Invité est absent ou désactivé			
CL-3	Comptes utilisateurs et administrateur	Présence de comptes utilisateurs locaux ?		NON : il n'y a aucuns comptes utilisateurs locaux présents			
CL-4	Comptes utilisateurs et administrateur	Vérification de la non utilisation d'un compte générique / Utilisation personnel du compte ?	Question	NON : le compte utilisé n'est pas partagé par un ensemble de personne			
CL-4	Firewall personnel	Le poste est t-il en pocession d'un firewall personnel ?	Question et observation	OUI : le poste est équipé d'un firewall personnel			
CL-4	Firewall personnel	Qui fixe les règles du firewall : l'utilisateur, l'administrateur ? Diffusion automatique des règles ?	Question et observation	Les règles du firewall personnel sont "pushés" par l'administrateur			
CL-4	Firewall personnel	Les règles peuvent t'elles être modifier ?	Question et observation	NON : l'utilisateur ne peut pas modifier lui-même les règles firewall			
CL-7	Stratégie de verouillage de comptes	Nombre de tentatives autorisé ?		Les comptes sont vérrouiller après 3 tentatives infructueuses			
CL-11	Stratégie de verouillage de comptes	Verrouillage de compte accepté ?	Sélectionner dans le "Panneau de configuration" / "Outils d'administration" / "Stratégie de sécurité locale" / "Statégie de vérouillage de comptes", observer les	OUI : en cas d'erreur répétitive lors de la frappe du mot de passe, le compte se verrouille pendant une certaine durée			
CL-11	Ecran de veille	L'utilisateur peut-il désactivé le verouillage automatique par mot de passe de son poste ?	Propriété du bureau "ecran de veille"	NON : l'utilisateur ne peut pas désactivé la fonction de verouillage automatique du mot de			
CL-11	Ecran de veille	En cas d'inactivité prolongé, le poste est-il verouillé automatiquement par un mot de poste ?	Propriété du bureau "ecran de veille"	OUI : en cas d'inactivité prolongé, le poste se bloque et la saisie du mot de passe est			
	CS -- Continuité de service						
	GC -- Gestion de la configuration						
GC-5	Gestion	Le poste est-il suivi et administré par l'équipe d'administration des postes bueautiques ?	Question	OUI : la cellule informatique administre le poste			

CS1&2 – Tests d'intrusion / vulnérab.

⇨ **Contenu du contrôle :**

– Le contrôle doit permettre d'évaluer le potentiel de nuisance d'un ou plusieurs attaquants, externe ou interne, possédant différents niveaux de privilèges :

✓**Tests d'intrusions sur les infrastructures** : évaluation de la capacité d'un attaquant de s'introduire au sein de l'infrastructure cible avec suffisamment de privilèges pour recueillir de l'information sensible, modifier l'intégrité du système ou installer des logiciels tiers, et ceci en exploitant toute nature de vulnérabilité.

✓**Tests de vulnérabilité des applications** : évaluation de la capacité de contourner les protections et contrôles inhérents à une application afin de recueillir des informations sensibles ou de modifier son intégrité, et ceci en exploitant des vulnérabilités d'ordre applicatif.

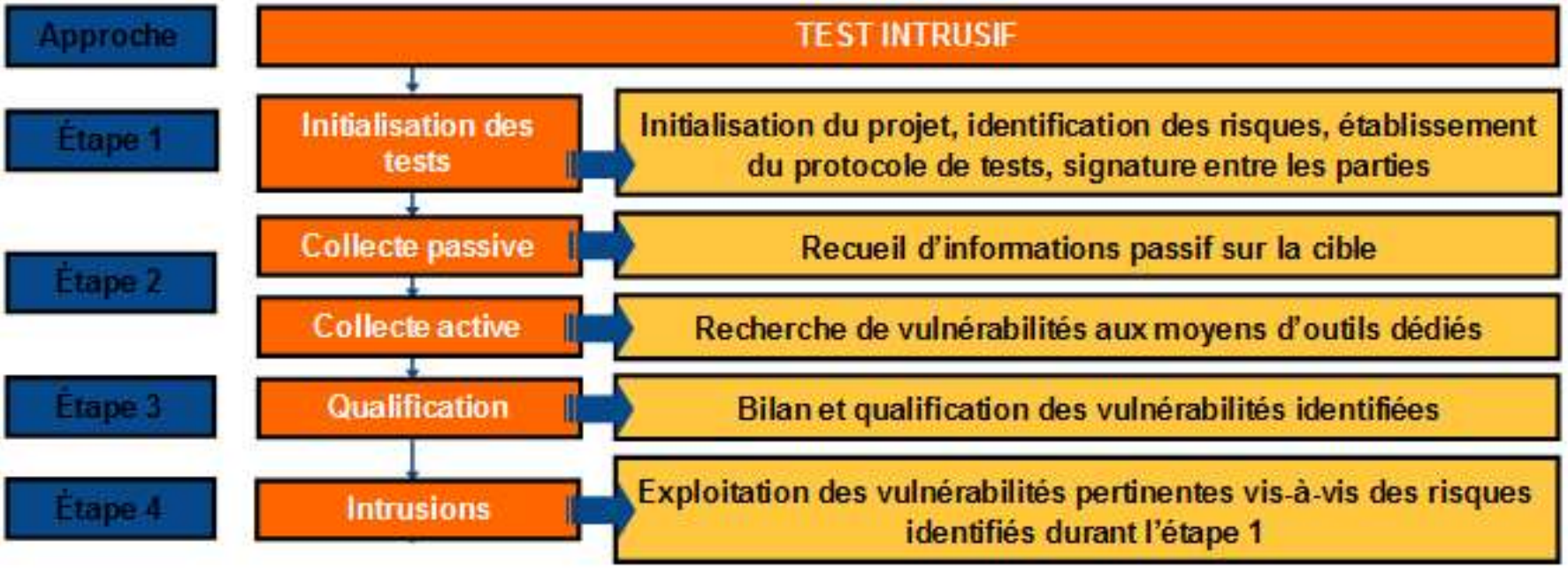
CS1&2 – Tests d'intrusion / vulnérab.

⇨**Méthode**

- ✓L'approche dépend des risques à évaluer
  - ✓**Boite noire** : aucune information
  - ✓**Boite Blanche** : l'auditeur dispose des informations techniques de la cible
  - ✓**Interne** : à partir du réseau interne
  - ✓**Externe** : à partir d'Internet

CS1&2 – Tests d'intrusion / vulnérab.

⇨ **Démarches et outils :**



CS2 – Analyse de code

⇨ **Contenu du contrôle** :

✓Le contrôle de code doit permettre permettant d'identifier les failles issues de l'ensemble des erreurs de développement

⇨ **Méthode**

✓Ces investigations s'appuient essentiellement sur des analyses documentaires et des tests techniques

CS2 – Analyse de code

Principe OWASP

OWASP
The Open Web Application Security Project

L'injection (SQL, shell, LDAP, etc…)	Exploitation du manque de contrôle dans un champs USR
Broken Authentication and Session Management	Vols d'authentification, de la session
Cross-Site Scripting:	Exploitation du manque de contrôle dans un champs USR
Insecure Direct Object References	Exploitation d'un manque de contrôle d'accès aux données
Security Misconfiguration:	Outils mal configuré, non à jour, …
Sensitive Data Exposure	Mauvais chiffrement de données sensibles, mdp en cache, …
Missing Function Level Access Control	Exploitation d'un manque de contrôle d'accès aux fonctions
…	

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

CS2 – Analyse de code

Principe OWASP

Recommandation des points à tester

1. Validation des entrées
2. Conception du code source
3. Fuite d'informations et gestion incorrecte des erreurs
4. Référence d'objet direct
5. Utilisation des ressources
6. Utilisation de l'API
7. Violation des bonnes pratiques
8. Gestion de session faible

CS2 – Analyse de code

Plusieurs approches sont envisageables :

⇨L'analyse statique qui consiste à une revue du code à la recherche d'erreurs de développement classiques :

- débordements de mémoires tampons;
- l'utilisation de fonctions système incontrôlées ;
- etc.

⇨L'analyse dynamique qui consiste à utiliser le code et d'orienter les tests en injectant des entrées pouvant impacter l'exécution normale du composant ;

⇨Des solutions combinant les deux approches ou ciblant des parties sensibles du code :

- les fonctions d'authentification,
- les algorithmes de chiffrement,
- etc.

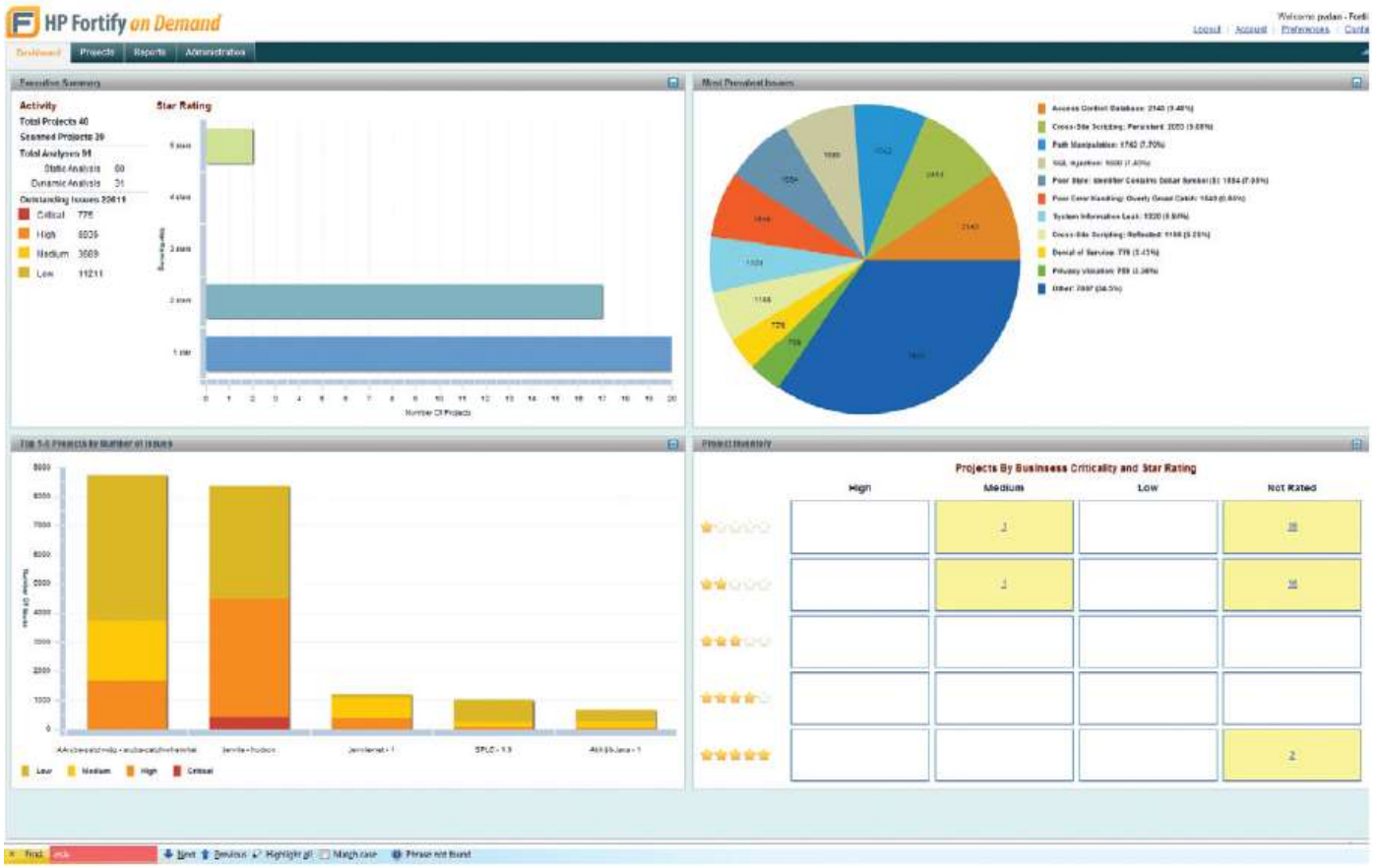
CS2 – Analyse de code

Outils

Figure 1. Magic Quadrant for Application Security Testing

CS2 – Analyse de code

Outils



CS2 – Tests des fonctions de sécurité

⇨ **Objectifs :**

✓Vérifier la robustesse des fonctions de sécurité notamment par l'analyse des écarts lors de leur mise en œuvre vis-à-vis des normes de développement,de l'état de l'art (retour d'expérience, veille sécurité, recommandations, standard …), et du référentiel de l'entité

⇨ **Méthodes**

✓Ces investigations s'appuient essentiellement sur des analyses documentaires, des tests fonctionnels et des tests techniques

CS2 – Tests des fonctions de sécurité

⇨**Méthode et outils :**

✓Une première étape permet de recenser de manière exhaustive toutes les fonctions de sécurités implémentées au niveau applicatif. notamment :

- Contrôle d'intégrité
- Authentification applicative
- Chiffrement de données
- Signature numérique, Horodatage
- Non-répudiation
- Chaînage des événements
- Auditabilité.

✓Une deuxième étape permet de définir et de dérouler un plan de test applicatif des fonctions de sécurité en décrivant l'environnement, le déroulement, et les résultats attendus.

- Définir les données de test
- Etablir des scénarios
- Protocole de tests

CS3 – Contrôle des environnements

⇨ **Contenu du contrôle :**

✓Le contrôle de l'environnement doit permettre d'évaluer les moyens mis en œuvre pour répondre aux risques physiques en analysant les paramètres d'environnement des bâtiments, locaux, … hébergeant les ressources des systèmes.

⇨**Méthodes**

✓Ces investigations s'appuient essentiellement sur des analyses documentaires, des tests fonctionnels, des tests techniques, des observations visuelles et des entretiens

CS3 – Contrôle des environnements

⇨ **Démarche et outils:**

✓Les risques à prendre en compte sont les suivants :

- Les risques naturels (Inondations ou infiltrations, foudre, température,..) ;
- Les risques industriels (proximité d'industries) ;
- Les risques liés à l'énergie (fourniture et secours) ;
- Les risques liés aux télécommunications (fourniture et secours) ;
- Les risques liés aux accès (filtrage, contrôles, surveillance, …)

✓Les contrôles concernent notamment :

- Les salles d'hébergement des S.I., principal et secondaire
- Les locaux où se déroulent les activités autours du S.I. :
- Les bureaux des utilisateurs
- Les locaux techniques hébergeant du matériel spécifique
- Les locaux techniques dédié aux ressources (Electricité, Climatisation, …)

CS3 – Contrôle des environnements

⇨ **Exemple de preuves recherchées :**

- Dossier techniques d'équipements de sécurité (vidéosurveillance, Contrôle d'accès, …) comme des dossiers d'installation et des contrats de maintenance
- Les dossiers techniques des utilities (énergie, eau, télécom,…) et leur moyens de secours
- Les dossiers techniques des hébergements techniques
- Les tests de basculement (périmètres, fréquence, …)
- Plan d'exposition aux risques du secteur géographique
- Les procédures d'accès
- …

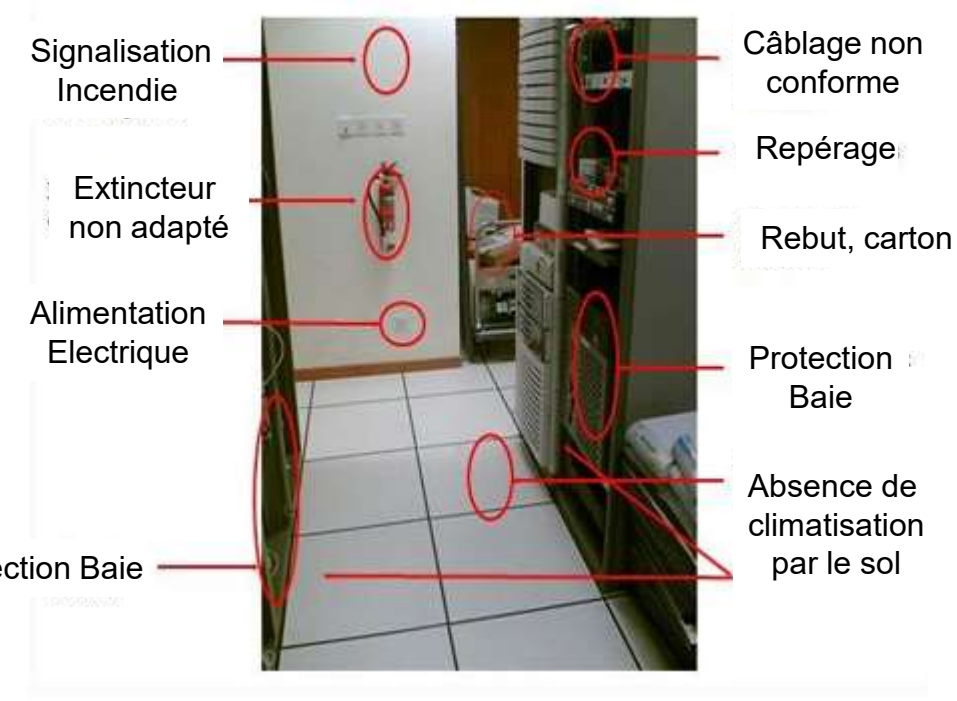
CS3 – Contrôle des environnements

Audit Salle informatique			
Thème	**Point de contrôle**	**Preuve recherchée**	**Constats**
Sécurité physique périmètrique	Mur resistant à l'intrusion	Mur épais et plein, absence de vitrage vers l'extérieur, ...	
	Porte resistante à l'intrusion	Porte épaisse, pleine, serrure solide, ...	
	Contrôle d'accès	Verrous avec une clef, lecteur de carte	
	Détecteur d'intrusion	Détecteur (contact d'alarme, radar) sur les accès	
Sécurité Physique Intérieure	Baies sécurisées	Baies fermées à clefs	
	Equipements sécurisés	Matériels hors baie protégés	
	Matériel fixé	Fixation baie, présence limitée de matériel hors baie	
	Implantations	Faux plancher et faux plafond	
Normes câblage	Disposition	Rangés, étiquetés, ...	
	Intégrité du câble	Absence de cables denudés, ..	
	Matériel / matériaux non utiles	Absence de réseaux anciens non déposé	
	Séparation des différents réseaux	Cheminement / chemin de cable différent	
Organisation Salle	Accessibilité	Accès aux équipements sans difficultés	
	Matériel / matériaux non utiles	Absence de carton, absence de cafetiere, ...	

CS3 – Contrôle des environnements

Thème	Point de contrôle	Preuve recherchée	Constats
Protection dégats des eaux	Etanchéité vis-à-vis de l'exterieur	Absence de fuite	
	Fuite d'eau potientiel	Absence de canalisation (alimentation ou évacuation dans la salle)	
	Placement de la salle	Minimum d'exposition au risque	
	Détection	Presence d'un détecteur d'humidité	
Protection incendie	Détection	Détecteur de fumée	
	Extinction	Extincteur adapté	
Alimentation Electrique	Tableau aux normes		
	Alimentation de secours		
	Onduleur/batterie		
	Distribution au norme	Absence de nourrice	
Climatisation	Climatisation	Présence d'un climatiseur	
	Contrôle de l'environnement	Capteur de temperature / humidité	
	Isolation du local		
Procédures et documentation	Regles d'accès sécurisée au local		
	Plan d'implantation		
	Documentation technique pour la maintenance		
	Plan de câblage, schéma, ...		

CS3 – Contrôle des environnements



CS3 – Contrôle des procédures

⇨ **Contenu du contrôle :**

✓Le contrôle consiste à porter un diagnostic sur la définition, la mise en œuvre et le contrôle des procédures de sécurité appliquée sur le périmètre de la cible de contrôle, telles que :

- La recette des fonctions de sécurité
- La gestion des incidents
- Les procédures de sauvegardes
- La gestion des configurations de sécurité
- …

⇨ **Méthodes**

✓Ces investigations s'appuient essentiellement sur des analyses documentaires, des observations visuelles et des entretiens

CS3 – Contrôle des procédures

⇨**Démarche et outils:**

✓La démarche comprend des entretiens avec les catégories suivantes:

- Maîtrise d'ouvrage
- Maîtrise d'œuvre
- Responsable Sécurité
- Exploitant
- Administrateur
- Utilisateur
- …

⇨**Exemple de preuves recherchées :**

- Procédures écrites
- CR de réalisation de procédure (Bordereaux de traitement, …)
- …

CS3 – Contrôle des procédures

N°	Thème	Famille	ID	intitulé	ISO	Exigences	D	I	C	T	Conseils	Constats	Eval Constat
	Sécurité physique des infrastructures												
		PP -- Protection Physique											
			PP-1	Procédures de protection physique	15.1.1	Chaque service doit documenter les dispositions prises pour assurer la protection physique des locaux contenant les composants physiques nécessaires au fonctionnement des systèmes d'information et la manière dont il met en place les moyens afférents, et diffuser cette documentation	1	1	1	1	La documentation peut correspondre à des processus ou des procédures. Lorsqu'un local héberge des composants de plusieurs systèmes, les exigences de protection physique le concernant sont établies à partir des valeurs maximales de disponibilité, d'intégrité, de confidentialité et de traçabilité des systèmes hébergés.	Les dispositions prises pour assurer la protection physique des locaux contenant les composants physiques nécessaires au fonctionnement des systèmes d'information et la manière dont il met en place les moyens afférents ne sont pas formalisées	3
			PP-1A1	Procédures de protection physique	15.1.1	**A1 :** Lorsque qu'un composant d'un système d'information est hébergé dans un local partagé par plusieurs services, l'exploitant doit s'assurer auprès du chef du service responsable du local et contrôler régulièrement que les protections physiques appliquées à ce local respectent les exigences de sécurité du système d'information concerné.	1	1	1	1			N/A
			PP-2	Autorisations d'accès	9.1.2 9.1.6	Le service doit établir et tenir à jour les listes des personnes autorisées à accéder aux locaux contenant les composants physiques du système d'information y compris les composants, les supports de données et les équipements de liaisons. Cette exigence n'est pas applicable aux parties des locaux dûment identifiées comme accessibles sans contrôle par le public.	2	2	2	2		La liste des personnes ayant un badge pour accéder au locaux est connues. Il n'y a pas de formalisation des procédures liées à la sécurité physique.	3

CS3 – Contrôle des méthodes

⇨ **Contenu du contrôle :**

✓Le contrôle des méthodes consiste à vérifier la prise en compte dans la démarche projet des problématiques de sécurité au sein des infrastructures et des applications. Sera évaluée notamment la prise en compte de la sécurité au niveau :

- Des expressions de besoins (analyse de risques)
- Des études d'architectures
- Des méthodes de développement
- Des tests et recette
- Des phases de mise en production
- Des phases d'exploitation
- Des phases de maintenances correctives ou évolutives

⇨ **Méthodes**

✓Ces investigations s'appuient essentiellement sur des analyses documentaires et des entretiens

CS3 – Contrôle des méthodes

⇨**Démarche et outils:**

✓La démarche comprend des entretiens avec les catégories suivantes:

- Maîtrise d'ouvrage
- Maîtrise d'œuvre
- Responsable Sécurité
- Exploitant
- Administrateur
- …

⇨**Exemple de preuves recherchées :**

- PV de recette sécurité
- Analyse de risques
- Expression de besoin SSI
- …

Les entretiens

⇨**Quelques recommandations :**

- ✓S’assurer que l’entretien a bien lieu avec les personnes adéquates
- ✓Mener l’entretien dans l’environnement de travail de l’interloccuteur
- ✓Mettre à l’aise
- ✓Rappeler le contexte et les objectifs
- ✓Permettre à l’interlocuteur de se présenter et de présenter son rôle
- ✓Reformuler et valider les éléments recueillis lors de l’Entretien
- ✓Ne pas juger au cours de l’Entretien
- ✓Remercier à l’issu de l’Entretien
- ✓Diffuser un Compte-Rendu

La gestion de la preuve

⇨**La preuve (ou l'enregistrement) doit :**

- ✓Avoir été vérifiée
- ✓Reproductible
- ✓Être clairement identifiée
- ✓Pouvoir être fournis à la demande
- ✓Être protégés en confidentialité et en intégrité
- ✓Avoir été obtenus dans le cadre du mandat « honnêtement »
- ✓Répondre aux exigences légales de conservation
- ✓…

⇨ **On m'a dit que …, la probabilité que…, un sentiment que, … n'est pas une preuve. Si l'auditeur à conviction qu'une situation (positive ou négative) existe, il ne peut en faire état que si il peut fournir une preuve.**

Points clés

- Les investigations ont principalement pour objectif de recueillir des éléments de preuve pour établir un constat, et sont identifiées en fonction de la nature de la preuve et de la cible
- Les preuves doivent être protégées
- Les entretiens et le recueil des preuves doivent être menés en respectant les règles de déontologie

Mise en pratique

Contexte

Dans le cadre de sa stratégie de développement, l'entreprise LUXOR de vente de camions utilitaires évolue dans un contexte à très forte intensité concurrentielle. Elle souhaite améliorer ses taux de succès de réponses aux appels d'offres. Cette ambition doit passer par une professionnalisation des réponses aux appels d'offres émis par les communes, les conseils généraux, ... LUXOR se doit d'être vigilante sur le contenu et sur l'image qu'elle véhicule à travers ses propositions.

LUXOR va se doter d'un progiciel permettant de concevoir rapidement des propositions commerciales de qualité adaptées à ces futurs clients. Ce progiciel devra permettre notamment de :

- Gérer le contenu des réponses
- d'optimiser le format des propositions commerciales
- de réduire le temps passé à répondre aux appels d'offres
- de responsabiliser le vendeur en l'impliquant dans l'élaboration de la proposition, ceci dans une volonté de mise en concurrence.
- d'homogénéiser les réponses en capitalisant sur les bonnes pratiques
- fournir **un niveau de sécurité adapté** à la sensibilité des informations qu'il détiendra et produira (prix, secret de fabrication, ...)

Mise en pratique

Le système à contrôler

Le système informatique permettant de fournir le service de gestion des propositions commerciales est constitué des éléments principaux suivants :

- Une application proposée en mode SAS par l'Entreprise TBV qui assure le développement de la solution et sa maintenance.
- Une infrastructure informatique de type client / serveur sous un environnement « Linux », exploitée par TBV et hébergée chez un tiers TBH.
- Un client léger de type « web » installé sur les postes utilisateurs de LUXOR;

Des éléments techniques sont détaillés dans le tableau suivant :

Ressources informatiques		
Type	**Système exploitation**	**Technologies**
Serveurs	GNU/ Linux Debian	PHP, XML, Apache PostgreSQL
Clients	Windows/ I.E.	HTML JAVASCRIPT

Mise en pratique

⇨ **PROPOSEZ LES DIFFERENTES INVESTIGATIONS QUE POURRAIT TRAITER UN AUDIT**

Mise en pratique - Correction

Au regard des risques, les investigations susceptibles de répondre aux attentes sont :

- ⇨ Contrôle documentaire et architecture cible
- ⇨ Contrôle sécurité applicative
  - ⇨ Revue de code pour identifier l'absence de bombe logique ou cheval de troie
  - ⇨ Tests applicatifs de type OWASP
  - ⇨ Test des fonctions de sécurité pour tester notamment :
    - ⇨ Le cloisonnement applicatif, pour s'assurer que chaque vendeur n'a pas accès aux travaux d'un autre vendeur
    - ⇨ Le contrôle d'accès des utilisateurs et traçabilité de leurs accès
- ⇨ Contrôle de l'environnement
  - ⇨ D'hébergement pour s'assurer du bon niveau de continuité d'activité
  - ⇨ D'exploitation pour vérifier les protections physiques de l'environnement à partir duquel les exploitants accèdent au dispositif

Mise en pratique - Correction

- Contrôle des procédures
  - Procédures d'exploitation
  - Procédure d'accès des exploitants pour vérifier le niveau de la politique de contrôle d'accès, les outils de traçabilité, la protection des postes de travail
  - Procédures de sauvegarde, notamment la fréquence, la protection des données, les tests de restauration
- Contrôle des méthodes de développement
  - Tests et recette de sécurité
  - Gestion des versions
- Contrôle de sécurité technique sur les matériels désignés
  - Revue de vulnérabilité des serveurs
- Tests d'intrusion externe boite noire ;