

ENSIIE 3A – SEC 2

AUDITS DE CYBERSÉCURITÉ

Support de cours
Evry, 17 Novembre 2023

Introduction


- Etude des risques et de leur traitement
 - Analyse de risques
 - Objectifs de sécurité
 - Politique de sécurité
- Démarche d'ingénierie
 - Choix des fonctions de sécurité
 - Choix des produits de sécurité
 - Intégration des produits de sécurité

Introduction

- Garanties ?
 - Efficacité des mesures
 - Choix des solutions de sécurité adaptées
 - Paramétrage
 - Entretien du niveau de sécurité dans le temps

L'audit est l'un des moyens à disposition de tout organisme pour éprouver et s'assurer du niveau de sécurité de son système d'information.

Introduction

Ce qu'il est	Ce qu'il n'est pas
	

Introduction

Ce qu'il est	Ce qu'il n'est pas
Constat partagé Climat de confiance – accord	

Introduction

Ce qu'il est	Ce qu'il n'est pas
Constat partagé Climat de confiance – accord	Inspection / Contrôle Sanctions éventuelles

Introduction

Ce qu'il est	Ce qu'il n'est pas
Constat partagé Climat de confiance – accord	Inspection / Contrôle Sanctions éventuelles
Examen Evaluation d'une situation	

Introduction

Ce qu'il est	Ce qu'il n'est pas
Constat partagé Climat de confiance – accord	Inspection / Contrôle Sanctions éventuelles
Examen Evaluation d'une situation	Diagnostic Recherche de causes et de remèdes

Introduction

Ce qu'il est	Ce qu'il n'est pas
Constat partagé Climat de confiance – accord	Inspection / Contrôle Sanctions éventuelles
Examen Evaluation d'une situation	Diagnostic Recherche de causes et de remèdes
Evaluation Par rapport à des exigences internes ou externes	

Introduction

Ce qu'il est	Ce qu'il n'est pas
Constat partagé Climat de confiance – accord	Inspection / Contrôle Sanctions éventuelles
Examen Evaluation d'une situation	Diagnostic Recherche de causes et de remèdes
Evaluation Par rapport à des exigences internes ou externes	Test de résistance Test de vulnérabilité

Introduction

Ce qu'il est	Ce qu'il n'est pas
Constat partagé Climat de confiance – accord	Inspection / Contrôle Sanctions éventuelles
Examen Evaluation d'une situation	Diagnostic Recherche de causes et de remèdes
Evaluation Par rapport à des exigences internes ou externes	Test de résistance Test de vulnérabilité
Processus systématique	

Introduction

Ce qu'il est	Ce qu'il n'est pas
Constat partagé Climat de confiance – accord	Inspection / Contrôle Sanctions éventuelles
Examen Evaluation d'une situation	Diagnostic Recherche de causes et de remèdes
Evaluation Par rapport à des exigences internes ou externes	Test de résistance Test de vulnérabilité
Processus systématique	Processus aléatoire

Définitions

AUDIT

- Processus méthodique, indépendant et documenté permettant d'obtenir des **preuves objectives** et de les évaluer de manière objective pour déterminer si les **critères d'audit** sont satisfaits.

CRITERES D'AUDIT

- Ensemble d'exigences utilisées comme références vis-à-vis desquelles les preuves objectives sont comparées.

Définitions

PERIMETRE D'AUDIT

- Etendue et limites d'un audit
 - Périmètre technique
 - Périmètre fonctionnel

PROGRAMME D'AUDIT / CAMPAGNE D'AUDIT

- Dispositions relatives à un ensemble d'un ou plusieurs audits planifié pour une durée spécifique et dirigé dans un but spécifique.

Définitions

PREUVES D'AUDIT

- Enregistrements, énoncés de faits ou autres informations pertinents pour les critères d'audit et vérifiables

La preuve d'audit est toujours obtenue avec le consentement de l'audité

Définitions

ACTEURS

L'auditeur



- La personne qui réalise l'audit

L'audité



- L'organisme qui est audité

Le client de l'audit

- L'organisme ou la personne demandant l'audit



Référentiels / Critères d'audit

- Il s'agit du ou des documents de référence pour l'audit
 - Référentiel client
 - Référentiel étatique / ANSSI
 - Bonnes pratiques
- Permet d'établir la « checklist » d'audit
 - TD cet après-midi



Principes de l'audit

L'audit est caractérisé par la confiance accordée aux principes suivants. Le respect de ces principes est indispensable pour que les conclusions d'audit soient pertinentes et suffisantes.

Déontologie

- Ethique, honnêteté, responsabilité
- Compétences requises
- Impartialité
- Sensibilité aux influences pouvant être exercées

Restitution impartiale

- L'obligation de rendre compte de manière sincère et précise

Conscience professionnelle

- L'attitude diligente et avisée au cours de l'audit

Principes de l'audit

Confidentialité

- Sécurité des informations

Indépendance

- Indépendance des auditeurs vis-à-vis de l'activité auditée
- Etat d'esprit objectif
- Constatations et conclusions uniquement fondées sur des preuves d'audit

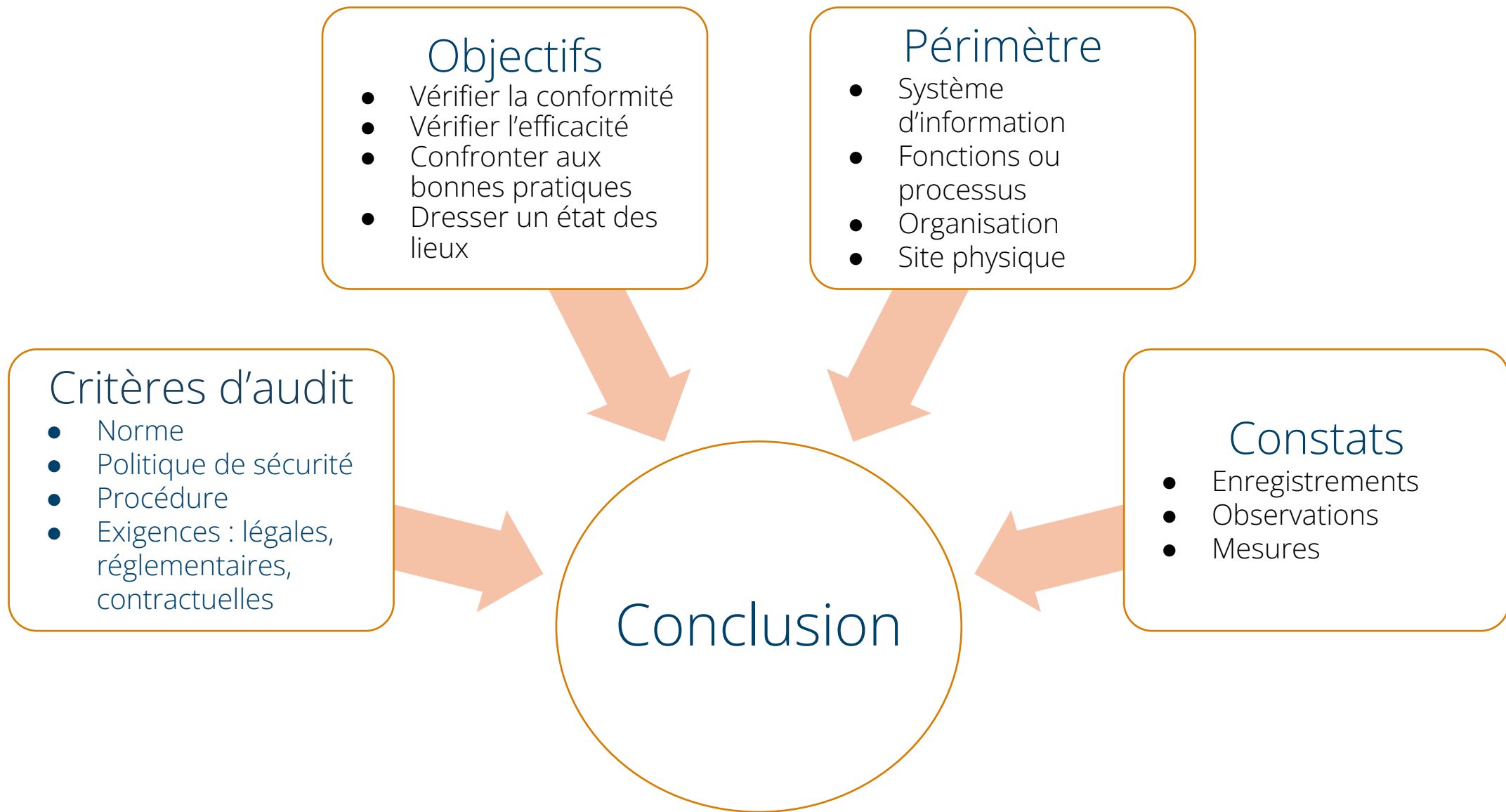
Approche fondée sur la preuve

- Les preuves d'audit sont vérifiables, tangibles, et s'appuient sur des échantillons disponibles et pertinents

Approche fondée sur les risques

- Approche d'audit prenant en considération les risques et les opportunités liés à l'audit

Principes de l'audit - Synthèse



Phase préparatoire

NÉCESSITÉ DE LA PRÉPARATION

- Connaître au mieux le système à auditer avant d'y avoir accès
- Minimiser les efforts à fournir lors de l'audit sur site
- Aller vite dans les manipulations répétitives pour maximiser le temps de compréhension et d'interviews

Phase préparatoire

ÉLÉMENTS A ANALYSER AU PRÉALABLE

- Compréhension du besoin
 - Contexte
 - Objectifs et attendus de l'audit
- Référentiel de sécurité de l'entreprise / du système
 - Règles de sécurité
 - Recommandations
 - Interdictions (et dérogations)
- Documentation du système à auditer
 - Architecture physique
 - Architecture logique
 - Détail des postes, serveurs, équipements réseau

Phase préparatoire

DOCUMENTS A PRÉPARER

- Squelette du support de restitution
 - Restitution rapide le jour même
- Liste des points nécessitant vérification lors de l'audit sur site (cahier de tests)
 - Tester les commandes de récupération des configurations
- Squelette de rapport d'audit

Réalisation de l'audit

LES DIFFÉRENTES ÉTAPES



Réalisation de l'audit

LES DIFFÉRENTES ÉTAPES



Réalisation de l'audit

VÉRIFICATION DES PRÉREQUIS

- S'assurer que les auditeurs ont les prérequis nécessaires
 - Accès physiques (postes et équipements réseau)
 - Comptes
 - Mots de passe
 - Droits
 - Disponibilités des sachants du système

Réalisation de l'audit

AUDIT ORGANISATIONNEL ET INTERVIEWS

- Se faire expliquer le système par les sachants
- Déterminer les personnes responsables du système
 - Propriétaires
 - Responsables de l'exploitation
 - Responsable du maintien en conditions opérationnelles
 - Responsable du maintien en conditions de sécurité (màj, backup & restore, ...)
 - Utilisateurs
 - Autres parties prenantes (TMA, constructeurs, État, ...)

Réalisation de l'audit

AUDIT TECHNIQUE

- Identifier l'échantillon représentatif
- Récupérer les configurations des postes et des équipements réseau
 - Politiques de sécurité Windows
 - Versions des applications et des systèmes d'exploitation
 - Utilisateurs et droits
 - Configurations des pare-feux système (Windows firewall, iptables)
 - Revue des règles de filtrage
- Repérer et identifier les éléments qui s'écartent des normes de sécurité et des bonnes pratiques

Réalisation de l'audit

DÉBRIEFING – réunion de synthèse à chaud

- Le débriefing a lieu à la fin de la journée d'audit et dure moins d'une heure
- Il s'appuie sur un PPT préparé pendant la journée
 - Rappel des objectifs
 - Rappel de la méthodologie
 - Périmètre
 - Synthèse des résultats (quelques statistiques)
 - Résultats détaillés : points forts et points faibles

Réalisation de l'audit

SAVOIR VIVRE – SAVOIR ETRE

- Avec les audités :
 - Toujours faire preuve de respect et d'humilité
 - Reformuler pour s'assurer d'avoir bien compris
 - Remercier les audités pour leur temps, leur disponibilité et leur coopération
 - Ne pas montrer de « fierté » lors de la découverte de vulnérabilités
- Au sein de l'équipe d'audit :
 - L'équipe doit faire preuve de cohésion et de consistance face à l'audité.
 - En cas d'erreur ou de désaccord, régler les points en privé.
 - Ne pas hésiter à utiliser les tournures:
 - « Je parle sous ton contrôle »
 - « Pour compléter ce que dis »



TRAVAIL POST-AUDIT

TRAVAIL POST-AUDIT

LES DIFFÉRENTES ÉTAPES

- Reprise et analyse des extractions des configurations
- Analyse des vulnérabilités et créations des fiches vulnérabilités
- Rédaction du rapport d'audit

TRAVAIL POST-AUDIT

REPRISE ET ANALYSE DES EXTRACTIONS DES CONFIGURATIONS

- Lister les éléments qui diffèrent des référentiels utilisés
- Effectuer les recherches de back-office
 - Versions de logiciels et de systèmes d'exploitation
 - Vulnérabilités connues
 - Récupération des preuves d'audit
- Évaluer le niveau de risque de chaque élément
- Déterminer les recommandations à appliquer

TRAVAIL POST-AUDIT

ANALYSE DES VULNERABILITÉS - FICHES VULNÉRABILITÉS

- Donner pour chaque vulnérabilité différents éléments (fiche vulnérabilité)
 - Référence de la vulnérabilité
 - Machines concernées
 - Catégorie de vulnérabilité
 - Description factuelle de la vulnérabilité
 - Preuve (capture d'écran)
 - Impact de la vulnérabilité sur la production
 - Niveau de risque (information, faible, moyen, élevé)
 - Rappel de l'exigence (référentiel)
 - Recommandation(s)

TRAVAIL POST-AUDIT

RÉDIGER UNE VULNÉRABILITÉ

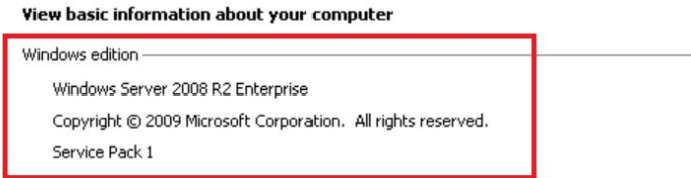
- Description factuelle
- Impacts sur le système
- Rédaction d'un risque :

Un attaquant ayant **[un prérequis]** en utilisant **[la vulnérabilité]** sur **[la machine X]** va pouvoir **[résultat technique]** et donc **[latéralisation]**, ce qui a comme effet sur le métier de **[conséquence métier]**

- Exigences (référentiel, bonnes pratiques)
- Recommandations

TRAVAIL POST-AUDIT

FICHE VULNÉRABILITÉ : EXEMPLE

Vuln-003	Fin de support de Microsoft Windows 2008	Serveur XX	Niveau de risque : Faible
<p><u>Description</u> : Le serveur XXXX exécute le système d'exploitation Microsoft Windows Server 2008 R2, dont le support standard s'est arrêté en janvier 2015, et la fin de support étendu sera en janvier 2021</p>			
			
<p><u>Impact</u> : L'arrêt de support Microsoft implique que ce serveur ne reçoit plus les mises à jour et correctifs de sécurité.</p>			
<p><u>Risque</u> : Un attaquant ayant un accès utilisateur va pouvoir utiliser la vulnérabilité XX connue sur Windows 2008 pour obtenir les droits administrateurs du poste et ainsi modifier le comportement du logiciel YY afin d'avoir un impact sur la production</p>			
<p><u>Règle XX du référentiel YY</u> : Les serveurs du système doivent utiliser une version Windows Server 2012 ou plus récent</p>			
<p><u>Recommandation</u> : Étudier la possibilité de migrer le serveur vers une version plus récente de Windows Server</p>			

TRAVAIL POST-AUDIT

RAPPORT D'AUDIT - ENJEUX

- C'est le document qui sera retenu par l'entreprise cliente. Il servira de référence pour
 - Les remédiations à mettre en place et leurs priorités
 - Les prises de décision relatives au système
- C'est également la trace laissée par les auditeurs au sein de l'organisme client (enjeu de réputation)

TRAVAIL POST-AUDIT

RAPPORT D'AUDIT - CONTENU

- Introduction
- Synthèse
- Méthodologie appliquée
- Rapport détaillé
- Synthèse des vulnérabilités

TRAVAIL POST-AUDIT

RAPPORT D'AUDIT - INTRODUCTION

- Le contexte
 - Rappel du système audité et de son utilité

TRAVAIL POST-AUDIT

RAPPORT D'AUDIT - INTRODUCTION

- Le contexte
 - Rappel du système audité et de son utilité
- Les objectifs
 - À quoi va servir l'audit et ses conclusions ?
 - Objectif du document (« ce document a pour objectif de détailler les résultats issus de [...] »)

TRAVAIL POST-AUDIT

RAPPORT D'AUDIT - INTRODUCTION

- Le contexte
 - Rappel du système audité et de son utilité
- Les objectifs
 - À quoi va servir l'audit et ses conclusions ?
 - Objectif du document (« ce document a pour objectif de détailler les résultats issus de [...] »)
- Le périmètre
 - Liste des machines et équipements concernés par l'audit

TRAVAIL POST-AUDIT

RAPPORT D'AUDIT - INTRODUCTION

- Le contexte
 - Rappel du système audité et de son utilité
- Les objectifs
 - À quoi va servir l'audit et ses conclusions ?
 - Objectif du document (« ce document a pour objectif de détailler les résultats issus de [...] »)
- Le périmètre
 - Liste des machines et équipements concernés par l'audit
- Les définitions et abréviations employées dans le document

TRAVAIL POST-AUDIT

RAPPORT D'AUDIT – SYNTHÈSE

- Contexte plus détaillé, notamment sur les utilités des machines du périmètre

TRAVAIL POST-AUDIT

RAPPORT D'AUDIT – SYNTHÈSE

- Contexte plus détaillé, notamment sur les utilités des machines du périmètre
- Rappel des dates d'audit + périmètre (important pour le suivi si plusieurs jours)

TRAVAIL POST-AUDIT

RAPPORT D'AUDIT – SYNTHÈSE

- Contexte plus détaillé, notamment sur les utilités des machines du périmètre
- Rappel des dates d'audit + périmètre (important pour le suivi si plusieurs jours)
- Scénario d'attaque : proposer un scénario d'attaque concret s'appuyant sur les vulnérabilités découvertes lors de l'audit

TRAVAIL POST-AUDIT

RAPPORT D'AUDIT – SYNTHÈSE

- Contexte plus détaillé, notamment sur les utilités des machines du périmètre
- Rappel des dates d'audit + périmètre (important pour le suivi si plusieurs jours)
- Scénario d'attaque : proposer un scénario d'attaque concret s'appuyant sur les vulnérabilités découvertes lors de l'audit
- Synthèse bons points / mauvais points pour chaque catégorie de vulnérabilité, de manière rédigée
 - Trouver pour chaque catégorie au moins un bon point
 - Donner quelques mauvais points (les plus importants)
 - Donner la/les recommandations principales

TRAVAIL POST-AUDIT

RAPPORT D'AUDIT – MÉTHODOLOGIE APPLIQUÉE

- Plan de test : rappel des différentes catégories de tests qui ont été réalisés :
 - Organisation
 - Documentation
 - Réseau
 - Systèmes Windows
 - Etc

TRAVAIL POST-AUDIT

RAPPORT D'AUDIT – MÉTHODOLOGIE APPLIQUÉE

- Plan de test : rappel des différentes catégories de tests qui ont été réalisés :
 - Organisation
 - Documentation
 - Réseau
 - Systèmes Windows
 - Etc
- Description des résultats : liste et descriptions des points qui vont pouvoir caractériser chaque vulnérabilité

TRAVAIL POST-AUDIT

RAPPORT D'AUDIT – RAPPORT DÉTAILLÉ

- Périmètre détaillé (oui, encore) : liste des machines et équipements audités
- Fiches vulnérabilités, triées par catégories

TRAVAIL POST-AUDIT

RAPPORT D'AUDIT – SYNTHÈSE DES VULNÉRABILITÉS

- La synthèse des vulnérabilités est un tableau récapitulatif des différentes vulnérabilités découvertes pendant l'audit
- Celles-ci sont triées par niveau de risque

Référence	Périmètre	Intitulé de la vulnérabilité	Niveau de risque	Recommandation
XXX-YYY-ZZ1	Configuration systèmes Windows	Utilisation de mots de passe faibles	Élevé	Augmenter la complexité des mots de passe utilisés
XXX-YYY-ZZ2	Architecture	Absence de ségrégation entre X et Y	Moyen	Étudier la possibilité de créer une ségrégation entre X et Y
...	Faible	...
...	Information	...