WEBINAIRE

Thème:
Préparation d'audit de sécurité technique et organisationnel d'une infrastructure IT

@cybernetic-security.com

EQUIPES

CyberNetic-Security

Dr Papa Mory GUEYE

Expert en Cybersécurité

Spécialiste:

- **Méthodes et Systèmes de Protection de l'Information**
- **Directeur des Systèmes d'information - CNS (DSI)**
- **Responsable de Sécurité des Systèmes d'information (RSSI)**
- **Consultant en Cybersécurité**
- **Enseignant Chercheur**

Issiaga KALTAMBA

Spécialiste en Cybersécurité

Spécialiste:

- **Audit de Sécurité Technique et Organisationnel**

Spécialiste:

- **SOC Niveau 1**
- **SOC Niveau 2**
- **Responsable SOC (Centre d'Opération et de Sécurité) Chef de Projet**
- **Consultant en Cybersécurité**

ERHARD FALEU

Spécialiste en Cybersécurité

Ingénieur en Cybersécurité
Ethical Hacker

Spécialiste:

- **RISK MANAGER**
- **Consultant en Cybersécurité**

Trois (3) Phases

Phase 1

- **Objectif du webinaire**

Phase 2

- **Introduction à l’audit de Sécurité Technique et Organisationnel**

Phase 3

- **Méthodologie d'Audit**

Phase 1

objectifs du webinaire

Ce webinaire vise à fournir une compréhension approfondie de l'audit de sécurité technique et organisationnel d'une infrastructure IT. Vous apprendrez les principes de base, les méthodologies d'audit, et les meilleures pratiques pour évaluer la sécurité des systèmes et des processus organisationnels.

Phase 2

Introduction et Objectifs à l’audit de Sécurité Technique et Organisationnel

Définition

Un audit de sécurité est une évaluation systématique des systèmes d'information, des processus, et des politiques d'une organisation pour identifier les vulnérabilités, les risques, et les faiblesses potentielles en matière de sécurité. Il vise à garantir que les mesures de sécurité mises en place sont efficaces, conformes aux normes, et adaptées aux besoins de l'organisation.

Importance de l'audit de sécurité

L'audit de sécurité est crucial pour protéger les infrastructures IT contre les menaces et les vulnérabilités. En évaluant de manière systématique les systèmes, les contrôles et les politiques de sécurité, un audit permet de :

Identifier les Failles de Sécurité : Détecter les vulnérabilités potentielles avant qu'elles ne soient exploitées par des attaquants.

Assurer la Conformité : Vérifier que les pratiques de sécurité respectent les normes et les régulations en vigueur, telles que ISO 27001 ou le RGPD.

Améliorer la Résilience : Renforcer les mécanismes de protection et les processus organisationnels pour mieux résister aux incidents de sécurité.

Optimiser les Ressources : Prioriser les actions correctives et les investissements en fonction des risques identifiés, afin d'utiliser les ressources de manière plus efficace.

Objectifs Principaux d'un Audit de Sécurité

Identification des Vulnérabilités
Détecter les failles de sécurité dans les systèmes informatiques, les réseaux, les applications, et les pratiques organisationnelles.

Évaluation des Risques
Analyser les risques associés aux vulnérabilités identifiées et leur potentiel impact sur l'organisation.

Conformité aux Normes et Régulations
Vérifier que l'organisation respecte les lois, régulations, et standards de sécurité, comme ISO 27001, le RGPD, ou NIST

Amélioration Continue
Recommander des actions correctives pour renforcer la sécurité et améliorer les pratiques de gestion des risques.

Prévention des Incidents de Sécurité
Proposer des mesures préventives pour éviter les violations de sécurité, les attaques cybernétiques, et les pertes de données.

Protection des Actifs
S'assurer que les informations sensibles et les actifs critiques de l'organisation sont protégés contre les accès non autorisés et les menaces.

Normes et Régulations

1 ISO/IEC 27001

L'ISO/IEC 27001 est une norme internationale qui spécifie les exigences pour établir, mettre en œuvre, maintenir, et améliorer un système de management de la sécurité de l'information (SMSI).

2 NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY) CYBERSECURITY FRAMEWORK

Le NIST Cybersecurity Framework est un cadre de référence développé par le gouvernement américain pour aider les organisations à gérer et à réduire les risques liés à la cybersécurité.

3 RGPD (RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES)

Le RGPD est une régulation de l'Union Européenne visant à protéger les données personnelles des individus et à renforcer les droits à la vie privée.

4 PCI DSS (PAYMENT CARD INDUSTRY DATA SECURITY STANDARD)

Le PCI DSS est une norme de sécurité pour les organisations qui traitent des informations de cartes de paiement.

Composantes d'un Audit de Sécurité Technique

01

ÉVALUATION DES SYSTÈMES

Comment évaluer la sécurité des systèmes informatiques (serveurs, réseaux, etc.).

02

ANALYSE DES VULNÉRABILITÉS

Techniques théoriques pour identifier les vulnérabilités potentielles.

03

CONTRÔLES TECHNIQUES

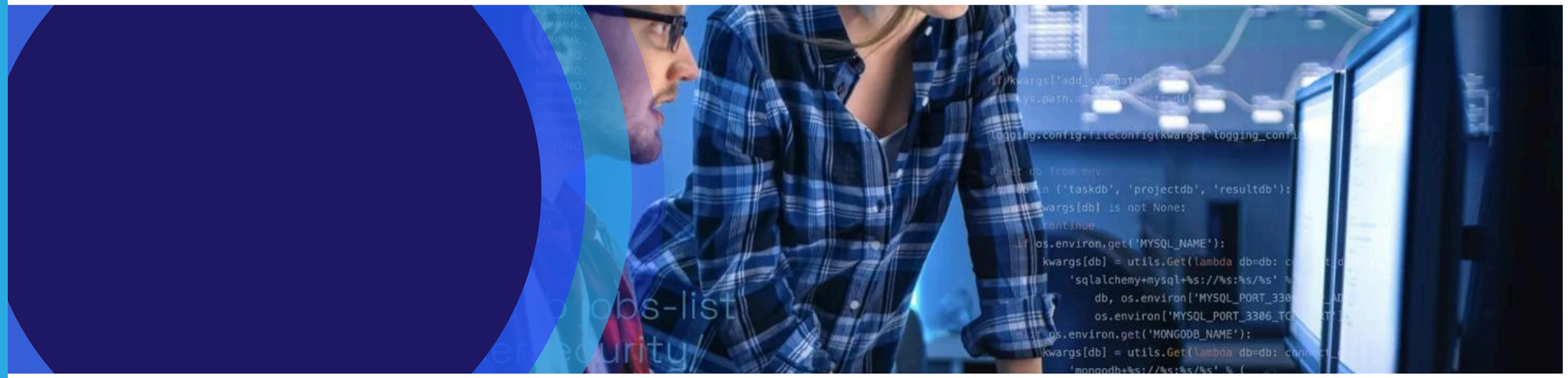
Principes des contrôles techniques, comme les pare-feu, les systèmes de détection d'intrusion.

Audit de Sécurité Organisationnel

CyberNetic-Security

Un audit de sécurité organisationnel est une évaluation systématique des politiques, procédures, et pratiques d'une organisation pour identifier les faiblesses, les vulnérabilités, et les lacunes en matière de sécurité. Contrairement à un audit technique qui se concentre sur les systèmes informatiques, l'audit organisationnel examine comment les pratiques de sécurité sont intégrées dans la culture et les opérations de l'entreprise.

Objectifs Principaux de l'Audit de Sécurité Organisationnel :



01 Évaluation des Politiques de Sécurité

02 Analyse des Procédures et Processus

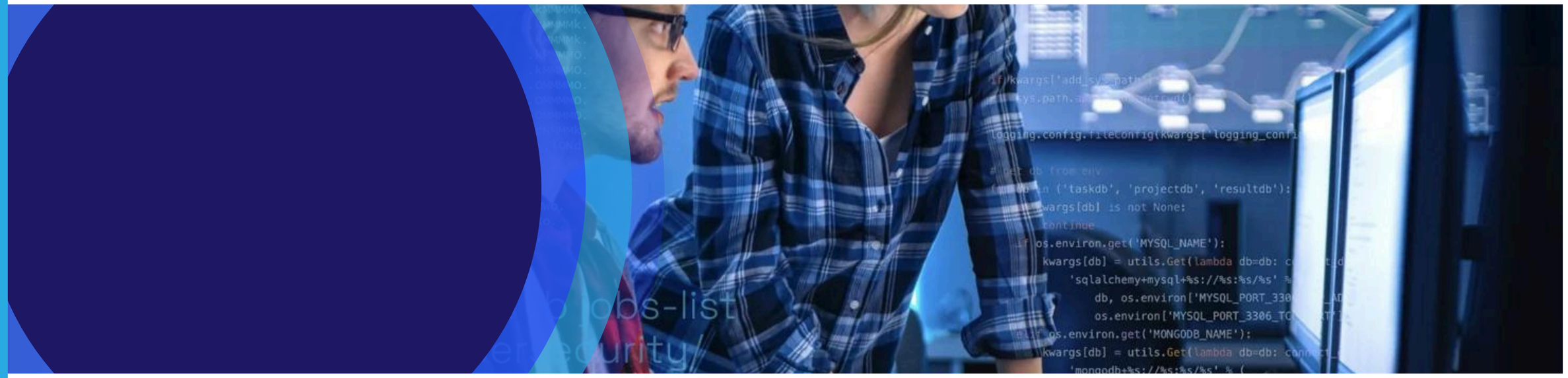
03 Vérification de la Conformité Réglementaire

04 Évaluation de la Sensibilisation de la Formation

05 Gestion des Risques et Gouvernance

06 Examen des Incidents de Sécurité Passés

Importance de l'Audit de Sécurité Organisationnel

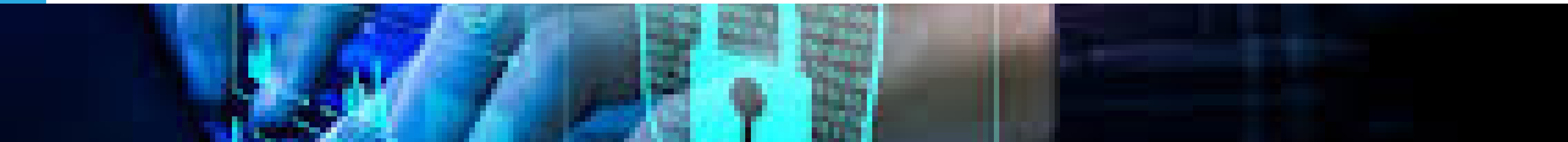


01 Renforcement de la Sécurité Globale

02 Réduction des Risques

03 Conformité et Réputation

04 Amélioration Continue



thor: Mageshkumar Aadhinathan

Phase 3

Méthodologie d'Audit

Composants Clés d'une Méthodologie d'Audit :

Une méthodologie d'audit est un ensemble structuré de processus, de techniques, de normes et de meilleures pratiques utilisées pour planifier, exécuter et rapporter les résultats d'un audit. Elle sert de guide pour les auditeurs afin de garantir que l'audit est mené de manière systématique, cohérente, efficace, et conforme aux normes de l'industrie.

01

Planification : Comment planifier un audit (définition de la portée, objectifs, ressources nécessaires).

Planification de l'Audit

Objectifs de l'Audit : Définir clairement les objectifs de l'audit, ce qui doit être réalisé, et les résultats attendus.

Portée de l'Audit : Déterminer les domaines spécifiques à auditer, les processus ou les systèmes concernés, et les limites de l'audit.

Calendrier et Ressources : Établir un calendrier pour l'audit et allouer les ressources nécessaires, y compris l'équipe d'audit et les outils requis.

02

Exécution :
Méthodes théoriques pour la conduite de l'audit, y compris les techniques d'analyse et de collecte de données.

Évaluation des Risques

Identifier et évaluer les risques potentiels qui pourraient affecter les objectifs de l'audit.

Prioriser les risques en fonction de leur probabilité et de leur impact potentiel pour concentrer les efforts d'audit sur les domaines les plus critiques.

03

Collecte de Données

- Utiliser diverses techniques pour collecter des informations pertinentes, telles que les entretiens, les observations, la revue de documents, et les tests techniques.
- Assurer la fiabilité et la précision des données recueillies pour une analyse valide.

04

Évaluation et Analyse

- Comparer les données collectées aux critères de référence, tels que les normes, les politiques, et les réglementations pertinentes.
- Analyser les écarts, les faiblesses, et les non-conformités pour évaluer l'efficacité des contrôles existants et identifier les domaines à améliorer.

05

Documentation des Résultats

- Documenter systématiquement toutes les constatations de l'audit, y compris les preuves collectées, les analyses effectuées, et les conclusions tirées.
- Assurer la traçabilité des résultats en maintenant une documentation complète et organisée.

06

Rapport d'Audit

- Préparer un rapport d'audit détaillé qui résume les objectifs, la portée, les méthodologies utilisées, les constatations, les conclusions, et les recommandations.
- Présenter les résultats de manière claire et concise, avec des recommandations d'amélioration basées sur les meilleures pratiques.

07

Suivi Post-Audit

- Effectuer un suivi pour vérifier que les recommandations de l'audit ont été mises en œuvre correctement et efficacement.
- Revoir les actions correctives prises pour s'assurer qu'elles adressent bien les problèmes identifiés et améliorent le contrôle global.

Importance de la Méthodologie d'Audit :

Cohérence et Efficacité :
Une méthodologie d'audit bien définie assure que les audits sont conduits de manière cohérente et efficace, avec une approche standardisée qui minimise les erreurs et les omissions.

Crédibilité et Confiance :
En suivant une méthodologie rigoureuse, les auditeurs peuvent fournir des résultats d'audit crédibles et fiables, renforçant la confiance des parties prenantes dans les conclusions et recommandations.

Amélioration Continue :
La méthodologie d'audit permet une évaluation structurée et répétable, facilitant l'amélioration continue des processus et des contrôles dans une organisation.

@reallygreatsite

MERCI!

Plus d’informations

SITE WEB: CYBERNETIC-SECURITY.COM

EMAIL: INFO@CYBERNETIC-SECURITY.COM

TÉLÉPHONE:

+221 78 833 88 47

+221 78 896 49 96

+221 76 355 19 09

@CYBERNETIC-SECURITY

@CYBERNETIC-SECURITY

@CYBERNETIC-SECURITY