CATALOGUE DE FORMATION

EDITION 2025-2027

Renforcez vos défenses, formez vos équipes, sécurisez votre avenir.

Des formations conçues par des experts, pour répondre aux défis concrets des organisations d'aujourd'hui

Formation et sensibilisation des employés

Administration des systèmes d'information

Sécurisation des systèmes d'information

+689 87 304 125 / +33 699 631 711

contact@tavita-cybersecurity.com

https://tavita-cybersecurity.com

À propos de TAVITA CYBERSECURITY

TAVITA CYBERSECURITY est une société experte dans la protection des actifs numériques des organisations publiques et privées. Elle offre une gamme complète de services en cybersécurité, reposant sur une expertise éprouvée.
Son savoir-faire s'appuie sur une double légitimité :

- 27 années d'expérience dans la gestion et la sécurisation des systèmes d'information,
- dont 23 années d'engagement opérationnel sur des infrastructures critiques au sein du ministère des Armées.

Cette expertise est consolidée par une parfaite maîtrise des référentiels de cybersécurité, acquise grâce à une pratique de terrain rigoureuse, une formation continue exigeante, et des collaborations étroites avec des acteurs publics et privés.

Nos domaines d'expertise :

- **Audit & conformité** : évaluation rigoureuse des infrastructures, logiciels et processus pour s'aligner avec les meilleures pratiques (ISO 27001, RGPD, PCI DSS, etc.)
- **Tests d'intrusion (pentesting)** : identification proactive des failles avec exploitation contrôlée pour renforcer la sécurité
- **Sécurité opérationnelle** : implémentation de pare-feu, SIEM, EDR/XDR, chiffrement, authentification forte (MFA), et segmentation réseau
- **Surveillance & réponse aux incidents** : détection en temps réel des menaces, investigation, remédiation et rapport
- **Sensibilisation & formation** : accompagnement des équipes par des sessions, ateliers et simulations de phishing

Notre vision :

Permettre à chaque organisation qu'elle soit PME, ETI ou grand compte de disposer d'une posture de sécurité proactive. En combinant rigueur technique, veille constante des cybermenaces et conseils adaptés, TAVITA CYBERSECURITY ambitionne de transformer la cybersécurité en un véritable atout stratégique.

TABLE DES MATIERES

SENSIBILISATION ET INITIATION A LA CYBERSECURITE

MODULE 1 - enjeux, menaces et cadre légal

OBJECTIFS :

- Comprendre les motivations à l'origine des exigences de sécurité dans les systèmes d'information
- Acquérir les notions fondamentales et la typologie des menaces
- Sensibiliser les utilisateurs et administrateurs aux risques et bonnes pratiques en cybersécurité

CONTENU :

1. **LES ENJEUX DE LA SECURITE DES SYSTEMES D'INFORMATION**
   - Introduction et préambule
   - Pourquoi la cybersécurité est devenue un enjeu majeur
   - Intérêts des cybercriminels pour les SI
   - L'économie souterraine du cybercrime
   - Impacts sur la vie privée et les données personnelles
   - Risques sur les infrastructures critiques
   - Études de cas et exemples d'attaques réelles

2. **IDENTIFICATION DES BESOINS DE SECURITE**
   - Introduction aux principes DIC (Disponibilité, Intégrité, Confidentialité)
   - Ajout du critère de Preuve (DICP)
   - Sécurité vs Sûreté : distinctions essentielles
   - Exemple d'analyse des besoins DICP
   - Mécanismes techniques et organisationnels associés

3. **NOTIONS DE VULNERABILITE, MENACES, ATTAQUE**
   - Définitions : vulnérabilité, menace, attaque
   - Cas concret de faille dans une application
   - Démonstration : usage légitime vs exploitation malveillante

4. **PANORAMA DE MENACES ACTUELLES**
   - Typologie des menaces et sources potentielles
   - Phishing, ingénierie sociale
   - Attaques ciblées et avancées (APT)
   - Fraudes internes, violations d'accès, DDoS, virus, botnets
   - Mise en situation illustrée

5. **LE DROIT DES T.I.C ET L'ORGANISATION DE LA SECURITE EN FRANCE**
   - Architecture de la cybersécurité en France
   - Le droit des technologies de l'information et de la communication (TIC)
   - Dispositifs de lutte contre la cybercriminalité
   - Le rôle de la CNIL et la protection des données personnelles

PUBLIC CONCERNE : Tout public (utilisateurs, personnels techniques, encadrants)

PRE-REQUIS : aucun

MOYENS PEDAGOGIQUES :

- Formation interactive, basée sur des retours d'expérience
- Utilisation de ressources officielles et de démonstrations en ligne
- Études de cas pratiques et mises en situation

INTERVENANT(S) : Consultant en cybersécurité

EVALUATION & ATTESTATION :

- Évaluation des acquis en fin de session via un quiz
- Évaluation de satisfaction à chaud
- Attestation de formation remise à chaque participant
- Support : Remis à chaque participant à l'issue de la session

MODALITES PRATIQUES :
Durée de la formation : 4h
Lieu de formation : INTER / INTRA (à définir)
Tarifs : Demander un devis
Conact : David TOUCHE au +689 87 304 125 / + 33 699 631 711 ou **contact@tavita-cybersecurity.com**

SENSIBILISATION ET INITIATION A LA CYBERSECURITE

MODULE 2 - Règles d'hygiène informatique

OBJECTIFS :

- Adopter les bonnes pratiques d'hygiène numérique essentielles pour renforcer la sécurité des systèmes d'information, à l'échelle individuelle comme organisationnelle.

CONTENU :

1. COMPRENDRE LE SYSTEME D'INFORMATION

- Identifier les composantes d'un SI (matériel, logiciel, humain, logique)
- Réaliser un inventaire des biens numériques
- Connaître les types de réseaux et leurs usages
- Comprendre les risques liés à l'interconnexion

2. MAITRISER LA SECURITE DU RESEAU

- Sécuriser le réseau interne (filtrage, segmentation, supervision)
- Gérer les terminaux personnels (BYOD)
- Contrôler les flux de données internes
- Protéger le réseau des menaces extérieures (pare-feu, proxy, VLAN, DMZ)
- Sécuriser les accès distants et l'administration des équipements
- Sécuriser les réseaux Wi-Fi

3. SECURISER LES EQUIPEMENTS ET LES DONNEES

- Séléctionner des applications fiables
- Maintenir les systèmes et logiciels à jour
- Protéger les terminaux avec antivirus / antimalware / antispyware
- Reconnaître les signes d'infection par un logiciel malveillant
- Protéger les données sensibles (chiffrement, sauvegarde)
- Durcir les configurations par défaut (principe du moindre privilège)

4. GERER LES UTILISATEURS ET LEURS ACCES

- Définir les rôles et les niveaux de privilèges
- Renforcer la politique de mot de passe
- Mettre en œuvre des méthodes d'authentification forte
- Sensibiliser les utilisateurs aux risques humains :
    - Spam
    - Phishing, spear phishing, ingénierie sociale
    - Réagir en cas d'incident ou de tentative d'arnaque

5. SECURISER PHYSIQUEMENT L'ENVIRONNEMENT DU SI

- Protéger les locaux et l'accès physique aux équipements
- Prendre en compte les risques liés aux périphériques partagés (imprimantes, copieurs)
- Sécuriser les équipements mobiles ou exposés

6. PILOTER LA SECURITE DU SYSTEME D'INFORMATION

- Comprendre l'organisation de la cybersécurité en France
- Formaliser les contrats, maintenances et interventions externes
- Mettre en place une supervision des activités et incidents
- Identifier et gérer les incidents de sécurité
- Élaborer un plan de continuité et de reprise d'activité (PCA/PRA)
- Conduire des audits réguliers de sécurité

PUBLIC CONCERNE : Tout public : utilisateurs, administrateurs, personnel encadrant

PRE-REQUIS : Connaissances générales des systèmes d'information (fonctionnement, composants)

MOYENS PEDAGOGIQUES :

- Méthode participative fondée sur les échanges et l'expérience terrain
- Navigation guidée sur des ressources en ligne de référence
- Études de cas, mises en situation, démonstrations concrètes

INTERVENANT(S) : Consultant en cybersécurité

EVALUATION & ATTESTATION :

- Quiz de validation des acquis en fin de session
- Évaluation de satisfaction à chaud
- Attestation de formation remise à chaque participant
- Support : Remis à chaque participant à l'issue de la session

MODALITES PRATIQUES :

Durée de la formation : 4h
Lieu de formation : INTER / INTRA (à définir)
Tarifs : Demander un devis
Conact : David TOUCHE au +689 87 304 125 / + 33 699 631 711 ou **contact@tavita-cybersecurity.com**

SENSIBILISATION ET INITIATION A LA CYBERSECURITE

MODULE 3 - Les aspects réseau et applicatifs

OBJECTIFS :

- Comprendre les vulnérabilités associées aux protocoles réseaux et aux applications
- Identifier les principales solutions techniques de sécurisation du SI
- Acquérir les bases de la cryptographie et de la sécurité des applications web

CONTENU :

1. LA SECURITE DU PROTOCOLE IP

- Introduction aux enjeux de sécurité des protocoles réseau
- Exemples concrets :
  - Attaque par réflexion
  - Écoute et interception de trafic
  - Altération du routage des datagrammes IP
- Principes de sécurisation du protocole IP

2. SECURISATION D'UN RESEAU

- Fonctionnement et rôle des dispositifs techniques :
  - Pare-feu
  - Répartiteur de charge (Load Balancer)
  - Anti-virus / Antimalware
  - Systèmes de détection et de prévention d'intrusions (IDS / IPS)
  - Réseaux privés virtuels (VPN)
  - Segmentation réseau (VLAN, DMZ)
- Illustration par un exemple de sécurisation sur un réseau simple

3. LES BASES DE LA CRYPTOGRAPHIE

- Définitions clés et terminologie
- Éléments historiques
- Chiffrement symétrique
- Chiffrement asymétrique
- Comparaison des deux approches
- Signature électronique et intégrité des données
- Certificats numériques et autorités de certification
- Jetons cryptographiques et usage courant

4. LA SECURITE DES APPLICATIONS WEB

- Vulnérabilités courantes :
  - Usurpation d'identité via manipulation de cookies
  - Injection SQL et compromission de bases de données
- Bonnes pratiques de développement sécurisé

PUBLIC CONCERNE : Tout public sensibilisé aux bases du fonctionnement des SI

PRE-REQUIS :

- Connaissances Connaissances générales en systèmes d'information
- Notions de base sur les réseaux, systèmes d'exploitation et applications

MOYENS PEDAGOGIQUES :

- Pédagogie Méthode interactive et participative
- Exploration de sites de référence et de ressources pédagogiques
- Études de cas pratiques et mises en situation

INTERVENANT(S) : Consultant en cybersécurité

EVALUATION & ATTESTATION :

- Quiz de validation des acquis en fin de session
- Évaluation de satisfaction à chaud
- Attestation de formation remise à chaque participant
- Support : Remis à chaque participant à l'issue de la session

MODALITES PRATIQUES :

Durée de la formation : 4h
Lieu de formation : INTER / INTRA (à définir)
Tarifs : Demander un devis
Conact : David TOUCHE au +689 87 304 125 / + 33 699 631 711 ou **contact@tavita-cybersecurity.com**

SENSIBILISATION ET INITIATION A LA CYBERSECURITE

MODULE 4 - La gestion de la cybersécurité au sein d'une organisation

OBJECTIFS :

- Comprendre les normes, méthodes et référentiels pour intégrer la cybersécurité à tous les niveaux d'une organisation
- Intégrer la sécurité dès la conception des projets et dans les processus métier
- Identifier les freins et contraintes organisationnelles à la mise en œuvre d'une politique de sécurité efficace
- Découvrir les différents métiers, compétences et perspectives professionnelles dans le domaine de la cybersécurité

CONTENU :

1. INTEGRER LA SECURITE AU SEIN D'UNE ORGANISATION

- Introduction
- Panorama des normes ISO de la famille 27000
  - ISO 27001 : Système de management de la sécurité de l'information
  - ISO 27002 : Code de bonnes pratiques
  - ISO 27005 : Gestion des risques
- Classification des informations sensibles
- Gestion des ressources humaines et sensibilisation interne

2. INTEGRER LA SECURITE DANS LES PROJETS

- Enjeux de la sécurité dans le cycle de vie d'un projet
- Cas d'intégration tardive de la sécurité (en fin de développement)
- Approche par l'analyse des risques et mise en œuvre de mesures correctives
- Élaboration d'un plan d'action de sécurité (PSSI, PRA, etc.)

3. ENJEUX ET FREINS A LA PRISE EN COMPTE DE LA CYBERSECURITE

- Manque de compréhension ou d'adhésion aux enjeux SSI
- Nécessité d'un pilotage stratégique par la direction
- Difficultés de décision en environnement incertain
- Arbitrage entre facilité d'usage et niveau de sécurité
- Adaptation constante aux évolutions technologiques
- Brouillage des limites entre sphères professionnelle, personnelle et publique

4. METIERS DE LA CYBERSECURITE

- Positionnement Positionnement des fonctions SSI dans les organisations
- Cartographie des métiers et des compétences (inspirée des référentiels ANSSI/France Compétences)
- Présentation de profils types : RSSI, analyste SOC, pentester, consultant GRC, etc.
- Perspectives d'évolution de carrière et besoins en recrutement

PUBLIC CONCERNE : Tout public souhaitant comprendre la gouvernance et les enjeux organisationnels de la cybersécurité

PRE-REQUIS : Connaissances de base sur les systèmes d'information (architecture, fonctionnement, actifs)

MOYENS PEDAGOGIQUES :

- Formation interactive fondée sur les retours d'expérience
- Accès à des ressources pédagogiques de référence (ANSSI, CNIL, etc.)
- Études de cas concrets et exercices de mise en situation

INTERVENANT(S) : Consultant en cybersécurité

EVALUATION & ATTESTATION :

- Quiz de validation des acquis en fin de session
- Évaluation de satisfaction à chaud
- Attestation de formation remise à chaque participant
- Support : Remis à chaque participant à l'issue de la session

MODALITES PRATIQUES :

Durée de la formation : 4h
Lieu de formation : INTER / INTRA (à définir)
Tarifs : Demander un devis
Conact : David TOUCHE au +689 87 304 125 / + 33 699 631 711 ou **contact@tavita-cybersecurity.com**

SENSIBILISATION ET INITIATION A LA CYBERSECURITE

MODULE 5 – Sécurisation Active Directory et lutte contre les ransomwares

OBJECTIFS :

- Comprendre Comprendre les enjeux de sécurité des systèmes d'information et les motivations des cyberattaquants
- Identifier les modes opératoires des ransomwares et les bonnes pratiques pour s'en prémunir
- Sensibiliser les administrateurs aux pratiques essentielles de sécurisation d'un environnement Active Directory

CONTENU :

1. LES ENJEUX DE LA SECURITE DES SYSTEMES D'INFORMATION

- Comprendre pourquoi les S.I. sont ciblés
- L'économie souterraine du cybercrime
- Conséquences sur la confidentialité et la continuité d'activité
- Études de cas : attaques marquantes sur des environnements Active Directory

2. COMPRENDRE LES RANSOMWARES

- Définition et typologie
- Principaux vecteurs d'infection (email, RDP, USB, vulnérabilités, etc.)
- Exemples de ransomwares (WannaCry, Ryuk, MAKOP, etc.)
- Déroulement type d'une attaque
- Mesures de réaction en cas d'infection
- Prévention, détection et stratégie de résilience

3. SECURISATION DE L'ENVIRONNEMENT ACTIVE DIRECTORY

- Rôle central d'Active Directory dans une infrastructure
- Pourquoi AD est une cible stratégique
- Mécanismes d'attaque sur AD : cinétique d'une compromission
- Exemples d'escalade de privilèges via AD

4. BONNES PRATIQUES POUR RENFORCER LA SECURITE D'ACTIVE DIRECTORY

- Mise en œuvre des composants de sécurité essentiels :
  - PKI, LDAPS, LAPS, DNSSEC, WSUS, Corbeille AD
  - gMSA (Group Managed Service Accounts)
  - Délégation de contrôle maîtrisée
  - PSO (Password Settings Objects)
  - Matrice de droits d'accès partagés
  - Surveillance des ports d'écoute AD
- Sécurisation des accès à distance : protocole RDP
- Suivi des entrées/sorties utilisateurs (procédures IN/OUT)
- Outils de gestion des mots de passe : KeePass, Dashlane, etc.
- Intégration d'un Plan de durcissement AD basé sur les guides ANSSI/Microsoft

PUBLIC CONCERNE : Techniciens, administrateurs systèmes et infrastructures, responsables SSI

PRE-REQUIS : Connaissances de base sur Active Directory (structure, rôles, fonctionnement)

MOYENS PEDAGOGIQUES :

- Formation interactive avec retours d'expérience
- Accès à des ressources et guides de sécurisation de référence
- Cas pratiques et recommandations applicables immédiatement

INTERVENANT(S) : Consultant en cybersécurité

EVALUATION & ATTESTATION :

- Quiz de validation des acquis en fin de session
- Évaluation de satisfaction à chaud
- Attestation de formation remise à chaque participant
- Support : Remis à chaque participant à l'issue de la session

MODALITES PRATIQUES :

Durée de la formation : 4h
Lieu de formation : INTER / INTRA (à définir)
Tarifs : Demander un devis
Conact : David TOUCHE au +689 87 304 125 / + 33 699 631 711 ou **contact@tavita-cybersecurity.com**

SENSIBILISATION A LA CYBERSECURITE

Pour les acteurs Techniques / Métiers IT

OBJECTIFS :

- Appréhender les menaces cyber dans un contexte géopolitique tendu (conflit Russie-Ukraine)
- Comprendre les motivations actuelles et futures des cyberattaquants
- Connaître les fondamentaux de la cybersécurité et la typologie des menaces
- Sensibiliser les professionnels SI aux nouvelles vulnérabilités et bonnes pratiques
- Identifier les outils et démarches de gouvernance de la cybersécurité en entreprise

CONTENU :

1. **NOTIONS FONDAMENTALES DE LA CYBERSECURITE**
   - Enjeux stratégiques de la cybersécurité
   - Impacts de la cybercriminalité sur la vie privée et les infrastructures critiques
   - Définitions essentielles : vulnérabilité, menace, attaque, fuite de données
   - Études de cas d'attaques notables

2. **PANORAMA DE LA CYBERCRIMINALITE**
   - Statistiques globales et focus local : la situation en Polynésie française
   - Typologie des menaces actuelles
   - Organisation du cybercrime et fonctionnement des groupes malveillants
   - Arnaque au président (FOVI), vente de données personnelles : un marché lucratif
   - Classement des 15 menaces les plus répandues

3. **FOCUS SUR LES RANCOMWARES**
   - Définition et fonctionnement
   - Vecteurs d'attaque courants
   - Conséquences d'une infection
   - Faut-il payer une rançon ? (enjeux éthiques et juridiques)

4. **ETUDE DE CAS : CYBERATTAQUE EN POLYNESIENNE**
   - Contexte de l'attaque
   - Déclenchement, déroulement et impacts
   - Enjeux techniques et organisationnels
   - Retours d'expérience : erreurs, investigations et plan de reprise (PCA/PRA)

5. **QUE FAIRE EN CAS DE CYBERATTAQUE ?**
   - Premiers réflexes
   - Gestion de crise : coordination, communication, priorités
   - Sortie de crise et retour à la normale

6. LES BONNES PRATIQUES D'HYGIENE INFORMATIQUE

- Politique de mot de passe et gestion des identités
- Sécurisation des accès et des communications
- Gestion des mises à jour et des périphériques mobiles
- Sauvegarde, accès distant et cyberassurance

7. LES OUTILS DE GESTION DE LA CYBERSECURITE AU SEIN DE L'ENTREPRISE

- Intégration de la cybersécurité dans l'organisation
- Panorama des normes ISO 27000 (27001, 27002, 27005)
- Intégration dans les projets : sécurité dès la conception
- Freins organisationnels et leviers d'action
- Introduction au SMSI (Système de Management de la Sécurité de l'Information)

PUBLIC CONCERNE : Responsables SI, DSI, RSSI, chefs de projets, administrateurs systèmes et réseaux, techniciens, ou toute personne impliquée dans la conformité CYBER ou la gouvernance SSI de l'entreprise.

PRE-REQUIS : Notions de base en cybersécurité ou souhait d'acquérir des réflexes d'hygiène informatique pour faire face aux menaces actuelles.

MOYENS PEDAGOGIQUES :

- Formation interactive fondée sur des cas concrets
- Échanges d'expérience et mises en situation
- Ressources officielles (ANSSI, CNIL, CERT-FR…)

INTERVENANT(S) : Consultant en cybersécurité

EVALUATION & ATTESTATION :

- Quiz de validation des acquis en fin de session
- Évaluation de satisfaction à chaud
- Attestation de formation remise à chaque participant
- Support : Remis à chaque participant à l'issue de la session

MODALITES PRATIQUES :
Durée de la formation : 4h
Lieu de formation : INTER / INTRA (à définir)
Tarifs : Demander un devis
Conact : David TOUCHE au +689 87 304 125 / + 33 699 631 711 ou **contact@tavita-cybersecurity.com**

SENSIBILISATION A LA CYBERSECURITE

Pour les collaborateurs et utilisateurs du système d'information

OBJECTIFS :

- Acquérir les notions fondamentales de la cybersécurité et comprendre les types de menaces existantes
- Prendre conscience des risques numériques liés à l'usage quotidien de l'outil informatique
- Intégrer les bonnes pratiques d'hygiène informatique pour adopter un comportement numérique responsable

CONTENU :

1. **NOTIONS DE BASE DE LA CYBERSECURITE**
   - Introduction : cybersécurité vs sécurité informatique
   - Les enjeux de la protection du numérique
   - Qu'est-ce que le cyberespace ?
   - Vulnérabilités, menaces, attaques : définitions essentielles
   - Qui sont les hackers ? (profils, motivations)
   - Fuite de données, malwares et virus : comment cela se produit ?
   - Typologie des cyberattaques les plus fréquentes
   - Le phishing (hameçonnage) : repérer les tentatives de fraude
   - Exemples concrets d'attaques et leurs impacts
   - Zoom : comprendre le fonctionnement d'un ransomware

2. **PANORAMA DE LA CYBERCRIMINALITE**
   - Données clés en France et en Polynésie française
   - Typologie et organisation de la cybercriminalité
   - Fonctionnement des cyber-gangs
   - Le commerce illégal des données personnelles : enjeux et risques

3. **QUE FAIRE EN CAS DE CYBERATTAQUE/ESCROQUERIE ?**
   - Réflexes essentiels à adopter immédiatement
   - À qui signaler l'incident ?
   - Comportement à adopter pour limiter les conséquences

4. **LES BONNES PRATIQUES POUR LIMITER LE RISQUE**
   - Règles essentielles d'hygiène numérique
   - Bien gérer ses mots de passe (et comprendre pourquoi !)
   - Sécuriser sa messagerie professionnelle
   - Nettoyer ses traces sur Internet
   - Activer l'authentification multifacteur (MFA)
   - Attention aux objets connectés (IoT) dans l'environnement de travail
   - Comportements à adopter lors de déplacements professionnels
   - Ressources utiles : plateformes de signalement, guides pratiques
   - Conclusion : adopter une culture de cybersécurité au quotidien

PUBLIC CONCERNE : Tous les collaborateurs, salariés ou agents utilisant un poste informatique, quel que soit leur niveau technique ou leur fonction.

PRE-REQUIS : Aucun. Cette formation est accessible à tous.

MOYENS PEDAGOGIQUES :

- Approche interactive basée sur des exemples concrets
- Navigation guidée sur des ressources officielles (ANSSI, Cybermalveillance.gouv.fr, CNIL…)
- Échanges et retours d'expérience entre participants

INTERVENANT(S) : Consultant en cybersécurité

EVALUATION & ATTESTATION :

- Quiz de validation des acquis en fin de session
- Évaluation de satisfaction à chaud
- Attestation de formation remise à chaque participant
- Support : Remis à chaque participant à l'issue de la session

MODALITES PRATIQUES :

Durée de la formation : 4h
Lieu de formation : INTER / INTRA (à définir)
Tarifs : Demander un devis
Conact : David TOUCHE au +689 87 304 125 / + 33 699 631 711 ou **contact@tavita-cybersecurity.com**

MICROSOFT WINDOWS SERVER 2019/2022

Administation

OBJECTIFS :

- Comprendre les évolutions clés de Windows Server 2019 et 2022
- Maîtriser l'installation, la configuration et l'administration des services Windows Server
- Déployer un environnement Active Directory sécurisé et résilient
- Exploiter les outils modernes d'administration (Windows Admin Center, PowerShell)
- Mettre en œuvre des solutions de stockage sécurisées et performantes (ReFS, Storage Spaces)
- Intégrer les services hybrides avec Microsoft Azure

CONTENU :

1. ARCHITECTURE ET INSTALLATION

- Évolutions fonctionnelles entre Windows Server 2016, 2019 et 2022
- Nouvelles interfaces et expérience utilisateur
- Scénarios d'installation : Core, Desktop Experience, Nano Server
- Configuration initiale, rôles et fonctionnalités

2. ADMINISTRATION ET OUTILS MODERNES

- Utilisation du Server Manager et des consoles classiques
- Déploiement et gestion via Windows Admin Center (WAC)
- Automatisation avec PowerShell (cmdlets AD, stockage, réseau, etc.)
- Intégration Azure Arc, Azure File Sync, sauvegarde dans le cloud

3. ACTIVE DIRECTORY ET AUTHENTIFICATION

- Installation et sécurisation d'Active Directory Domain Services (AD DS)
- Gestion des comptes, unités organisationnelles, stratégies GPO
- Utilisation d'ADAC, LAPS, gMSA, PSO
- Principes de durcissement AD (selon les recommandations ANSSI/Microsoft)
- Prévention des attaques type pass-the-hash / kerberoasting

4. STOCKAGE ET SYSTEMES DE FICHIERS

- ReFS (Resilient File System) : avantages et cas d'usage
- Espaces de stockage et Storage Spaces Direct (S2D)
- Storage Migration Services : modernisation des serveurs de fichiers
- Sécurité des fichiers, contrôles d'accès, audit

5. SECURITE, SUPERVISION ET MAINTENANCE

- Windows Defender Antivirus et Exploit Guard
- Détection et réponse avec Microsoft Defender for Endpoint
- Outils de performance : PerfMon, ResMon, Event Viewer
- Sauvegarde, restauration, snapshots VSS, récupération système

PUBLIC CONCERNE : Techniciens, administrateurs et ingénieurs systèmes et réseaux.

PRE-REQUIS : Bonne connaissance des environnements Windows poste client (Windows 10/11) et notions de base sur les réseaux et services d'annuaire.

MOYENS PEDAGOGIQUES :

- Alternance d'apports théoriques et de démonstrations en environnement de test
- Scénarios pratiques adaptés aux besoins des participants
- Accès à des ressources officielles Microsoft et guides de durcissement

INTERVENANT(S) : Consultant expert en cybersécurité et systèmes Microsoft

EVALUATION & ATTESTATION :

- Mise en application de chaque chapitre par des travaux pratiques sous forme de laboratoire
- Quiz de validation des acquis en fin de session
- Évaluation de satisfaction à chaud
- Attestation de formation remise à chaque participant

MODALITES PRATIQUES :

Durée de la formation : 4 jours
Lieu de formation : INTER / INTRA (à définir)
Tarifs : Demander un devis
Conact : David TOUCHE au +689 87 304 125 / + 33 699 631 711 ou **contact@tavita-cybersecurity.com**

MICROSOFT WINDOWS SERVER 2025

Administation

OBJECTIFS :

- Découvrir les nouveautés et évolutions de Windows Server 2025
- Maîtriser l'installation, la configuration et l'administration des rôles serveur
- Mettre en œuvre une infrastructure Active Directory sécurisée
- Gérer les services réseau, le stockage et les politiques de sécurité
- Exploiter les outils modernes (WAC, PowerShell, Azure Arc) pour une administration efficace
- Intégrer les fonctionnalités cloud hybrides dans un environnement maîtrisé

CONTENU :

6. ARCHITECTURE ET INSTALLATION

- Présentation de Windows Server 2025 et comparatif avec les versions précédentes
- Nouveautés majeures : sécurité, virtualisation, containerisation
- Modes d'installation : Core, Desktop Experience, Nano Server
- Installation automatisée (ISO, image de déploiement, unattended file)
- Licences, activation, et options d'abonnement cloud

7. OUTILS D'ADMINISTRATION ET DEPLOIEMENT

- Introduction à Windows Admin Center (WAC) 2025 : nouveautés et intégration avancée
- Utilisation avancée de PowerShell 7+ pour l'automatisation des tâches
- Supervision centralisée : événements, services, stockage, réseau
- Introduction à Azure Arc pour la gestion hybride
- Intégration avec Azure Automanage (nouveauté 2025)

8. ACTIVE DIRECTORY ET SERVICE D'ANNUAIRE

- Installation et promotion du contrôleur de domaine
- Gestion des utilisateurs, groupes, unités organisationnelles (OU)
- Déploiement de gMSA, LAPS, stratégie de mot de passe affinée (PSO)
- Mise en œuvre de la séparation des niveaux d'administration (Tiering Model)
- Gestion des accès privilégiés (PAM), MFA pour les admins
- Suivi de la cinétique d'attaque AD et recommandations ANSSI

9. STOCKAGE ET SYSTEMES DE FICHIERS

- Nouveautés du ReFS et prise en charge des snapshots améliorés
- Mise en œuvre des Storage Spaces Direct (S2D)
- Services de migration de fichiers et compatibilité avec Windows Server 2025
- Gestion des disques virtuels, quotas, FSRM (gestion anti-ransomware)
- Implémentation d'un plan de sauvegarde/restauration complet (VSS, Windows Server Backup)

10. SECURITE ET RESILIENCE DU SYSTÈME

- Renforcement de la sécurité par défaut (Secure-Core Server, Credential Guard activé nativement)
- Antivirus et antimalware natifs avec Microsoft Defender for Endpoint Server
- Configuration de RDP sécurisé, pare-feu, audit et journalisation centralisée
- Déploiement de politiques Zero Trust à travers les GPO
- Configuration de BitLocker sur les volumes système et données

11. SERVICES RESEAU ET ACCES

- Configuration des services DNS, DHCP et IPAM
- Intégration avec Azure DNS et DNSSEC
- Mise en place d'un VPN site-à-site et accès distant via NPS
- Gestion du firewall avancé et journalisation des flux
- Déploiement des serveurs RDS 2025 (Remote Desktop Services)

PUBLIC CONCERNE : Administrateurs systèmes, techniciens réseau, ingénieurs infrastructure, responsables IT souhaitant déployer ou migrer vers Windows Server 2025

PRE-REQUIS : Bonne connaissance de l'environnement Windows Server (2016 à 2022), notions en services réseau, AD, PowerShell recommandées

MOYENS PEDAGOGIQUES :

- Alternance théorie / démonstration / exercices sur environnements simulés
- Scénarios concrets adaptés aux problématiques de production
- Mise à disposition de VM Windows Server 2025 pour travaux pratiques

INTERVENANT(S) : Consultant expert en cybersécurité et systèmes Microsoft

EVALUATION & ATTESTATION :

- Mise en application de chaque chapitre par des travaux pratiques sous forme de laboratoire
- Quiz de validation des acquis en fin de session
- Évaluation de satisfaction à chaud
- Attestation de formation remise à chaque participant

MODALITES PRATIQUES :

Durée de la formation : 4 jours
Lieu de formation : INTER / INTRA (à définir)
Tarifs : Demander un devis
Conact : David TOUCHE au +689 87 304 125 / + 33 699 631 711 ou **contact@tavita-cybersecurity.com**

MICROSOFT WINDOWS SERVER 2019/2022

Initiation à l'administration de Active Directory

OBJECTIFS :

- Appréhender Comprendre les bases de l'administration d'un serveur Windows Server 2019 / 2022
- Savoir installer, configurer et gérer un domaine Active Directory
- Administrer les comptes, groupes et stratégies de sécurité dans un environnement d'entreprise

CONTENU :

1. ARCHITECTURE ET INSTALLATION

- Présentation de Windows Server (versions, rôles, éditions)
- Installation de Windows Server 2019/2022 (interface graphique ou mode Core)
- Configuration initiale du serveur (IP, hostname, mise à jour, rôles)

2. DEPLOIEMENT D'ACTIVE DIRECTORY

- Prérequis à l'installation d'AD DS
- Installation et promotion du contrôleur de domaine
- Découverte du Centre d'administration Active Directory (ADAC)

3. COMPTES DES COMPTES, GROUPES ET GPO

- Création et gestion des comptes utilisateurs et groupes de sécurité
- Délégation d'administration
- Introduction aux stratégies de groupe (GPO)
- Fonctionnement, héritage, filtrage, blocages
- Utilisation du magasin central
- Automatisation de la création d'objets avec PowerShell

4. INFRASTRUCTURE RESEAU ET INTEGRATION

- Introduction à DNS dans un environnement Active Directory
- Création de zones DNS et enregistrements
- Intégration d'un poste client au domaine
- Résolution des problèmes d'intégration

5. SECURITE ET BONNES PRATIQUES ACTIVE DIRECTORY

- Mise en œuvre d'une stratégie de mot de passe affinée (PSO)
- Activation et gestion de la corbeille Active Directory
- Mise en place de LAPS (gestion des mots de passe locaux)
- Journalisation et audit de sécurité
- Gestion avancée des GPO : durcissement, mise à jour, planification
- Introduction au déploiement de rôles sur Server Core

- Configuration avancée du pare-feu Windows avec règles spécifiques
- GPO de renforcement contre les attaques Active Directory (ex : restriction RDP, filtrage des droits)

PUBLIC CONCERNE : Techniciens, administrateurs systèmes, ingénieurs réseaux débutant sur Windows Server / AD

PRE-REQUIS : Connaissances de base de l'environnement Windows (poste client, réseau de base)

MOYENS PEDAGOGIQUES :

- Formation interactive avec démonstrations et travaux pratiques
- Études de cas inspirées de contextes réels
- Environnement de LAB fourni (VM locales ou distantes)

INTERVENANT(S) : Consultant expert en cybersécurité et systèmes Microsoft

EVALUATION & ATTESTATION :

- Évaluation des acquis à travers des exercices pratiques tout au long de la formation
- Attestation de formation délivrée à l'issue de la session

MODALITES PRATIQUES :

Durée de la formation : 2 jours
Lieu de formation : INTER / INTRA (à définir)
Tarifs : Demander un devis
Conact : David TOUCHE au +689 87 304 125 / + 33 699 631 711 ou **contact@tavita-cybersecurity.com**

MICROSOFT WINDOWS SERVER 2019/2022/2025

Installation, configuration et administration avancée des infrastructures

OBJECTIFS :

- Appréhender les nouveautés de Windows Server 2025 par rapport aux versions antérieures
- Installer et configurer Windows Server dans ses différentes déclinaisons (GUI, Core, Nano)
- Mettre en œuvre Active Directory et les services d'infrastructure
- Gérer les rôles avancés : stockage, virtualisation, clustering, sécurité
- Exploiter Windows Admin Center et les outils d'administration modernes
- Déployer Windows Server comme plateforme applicative (conteneurs, hybridation Azure)

CONTENU :

1. INTRODUCTION ET ARCHITECTURE

- Présentation de Windows Server 2025 : évolutions majeures par rapport à 2019/2022
- Nouveautés en matière de sécurité, de virtualisation, de performance et de supervision
- Comparatif des éditions (Standard, Datacenter, Azure Edition)
- Modèles d'activation classiques vs licences cloud-based (Azure Arc, CSP)
- Modes d'installation : Desktop Experience, Server Core, Nano Server
- Outils de déploiement automatisé : WDS, MDT, Sysprep, fichiers Unattend
- Nouveautés du mode Core sur 2025 (rôles supplémentaires, meilleure compatibilité WAC)

2. DISQUES, PARTAGES ET SYSTEME DE FICHIERS

- Revue des systèmes de fichiers : NTFS vs ReFS 3.x (améliorations WS2025)
- Disponibilité et tolérance aux pannes du stockage
- Configuration des Storage Pools / Storage Spaces Direct (évolutions dans WS2025)
- Mise en œuvre du contrôle d'accès dynamique (DAC) avec centralisation des règles
- Cryptage des volumes avec BitLocker + intégration au TPM / Azure Key Vault
- Storage Migration Services : migration inter-versions jusqu'à 2025
- Protection des données : sauvegardes, snapshots, intégration avec Azure Backup
- Introduction à Microsoft Defender for Servers dans Server 2025
- FSRM (File Server Resource Manager) : quotas, filtres, audit
- Bonnes pratiques de sécurité des fichiers et des partages

3. COMPTES UTILISATEURS ET GROUPES

- Gestion des comptes via ADAC, PowerShell, et Windows Admin Center 2025
- Intégration de la stratégie Zero Trust (séparation des privilèges, PAM)
- GPO : gestion, filtrage WMI, héritages, central store
- Synchronisation hybride avec Azure Active Directory
- Outils : Azure AD Connect v2, Microsoft Entra ID, SSO, MFA
- Gestion de l'extension de domaine local vers Azure
- Présentation des nouveaux outils : Entra ID Protection, Azure AD Join
- Sécurisation des comptes avec LAPS, gMSA, et stratégie affinée (PSO)

4. MICROSOFT ET HYPER-V 2019 VERS 2025

- Déploiement de Hyper-V 2025 : évolutions en matière de performance et compatibilité
- Gestion des VMs avec PowerShell 7+, intégration WAC
- Haute disponibilité avec Failover Clustering et Hyper-V Replica
- Nouveaux scénarios hybrides : Azure Stack HCI, Azure Automanage
- Sécurisation des VMs (shielded VMs, host guardian service)

5. CLUSTERING ET HAUTE DISPONIBILITE

- Architecture de Failover Clustering en 2025
- Nouveautés : maintenance prédictive, résilience améliorée, compatibilité Azure
- Intégration avec Storage Spaces Direct
- Sauvegarde/restauration avancées : Windows Server Backup, Azure Recovery Services
- Stratégies PRA/PCA dans un environnement hybride

6. INFRASTRUCTURE RESEAU ET SERVICE IP

- Configuration avancée des services DNS / DHCP / IPAM
- DHCP Failover, DNSSEC, sécurité DNS sur Windows Server 2025
- Intégration avec Azure DNS
- Automatisation des tâches réseau via PowerShell 7
- Gestion dynamique des IP avec IPAM
- Optimisation réseau : NIC Teaming, QoS, SDN
- Analyse réseau et supervision intégrée (WAC + intégration Azure Monitor)

7. PLATE-FORME D'APPLICATIONS ET CONTENEURS

- Présentation des rôles applicatifs dans WS2025
- Déploiement et gestion des conteneurs Windows & Linux sur WS2025
- Intégration avec Kubernetes, Docker, Azure Container Registry
- Bonnes pratiques de déploiement d'applications IIS / .NET / MS SQL
- Nouvelles options pour les microservices (isolation, sandboxing)
- Utilisation de Windows Server comme plateforme hybride

PUBLIC CONCERNE :

- Administrateurs systèmes et réseaux, ingénieurs infrastructure
- Responsables techniques impliqués dans la modernisation des SI
- Professionnels préparant une migration vers Windows Server 2025

PRE-REQUIS :

- Maîtrise de Windows Server (2016 à 2022)
- Connaissances solides en services réseau, AD et PowerShell
- Avoir suivi une formation d'introduction ou initiation Windows Server

MOYENS PEDAGOGIQUES :

- Alternance de théorie, démos et travaux pratiques
- Environnement de LAB virtualisé (Hyper-V / VMware / Azure Lab Services)
- Études de cas et simulations réalistes de déploiement

INTERVENANT(S) : Consultant expert en cybersécurité et systèmes Microsoft

EVALUATION & ATTESTATION :

- Quiz de validation des acquis en fin de formation
- Évaluation pratique (LAB final)
- Attestation de formation délivrée à l'issue de la session

MODALITES PRATIQUES :

Durée de la formation : 5 jours
Lieu de formation : INTER / INTRA (à définir)
Tarifs : Demander un devis
Conact : David TOUCHE au +689 87 304 125 / + 33 699 631 711 ou **contact@tavita-cybersecurity.com**

MICROSOFT WINDOWS SERVER 2019/2022/2025

Sécuriser votre infrastructure active directory

OBJECTIFS :

- Acquérir Maîtriser les techniques avancées de sécurisation d'une infrastructure Active Directory
- Mettre en œuvre les bonnes pratiques de durcissement système, réseau et applicatif
- Appliquer les recommandations issues des référentiels ANSSI, CIS Benchmarks et Microsoft Security Compliance Toolkit
- Savoir détecter et limiter les vecteurs d'attaque courants (pass-the-hash, Kerberoasting, persistence AD)
- Intégrer les nouveautés de Windows Server 2025 en matière de sécurité et de gouvernance

CONTENU :

1. **PRINCIPES DE SECURITE DANS UN SI WINDOWS**
   - Typologie des vulnérabilités et niveaux d'exposition
   - Risques majeurs ciblant Active Directory
   - Techniques de persistance, élévation de privilèges
   - Enjeux du durcissement dans une approche Zero Trust

2. **MISE EN PLACE D'UNE PKI SECURISEE (Public Key Infrastructure)**
   - Déploiement d'une infrastructure AD CS
   - Gestion des modèles de certificats, révocations, OCSP
   - Sécurisation des services Web : HTTPS, LDAPS
   - Bonnes pratiques de surveillance et d'audit de la PKI
   - Nouveautés Windows Server 2025 : compatibilité, politiques de cycle de vie des certificats

3. **SECURISATION D'ACTIVE DIRECTORY (AD)**
   - Authentification durcie via ADAC
   - Contrôleur de domaine en lecture seule (RODC)
   - Mise en place de LAPS, PSO, corbeille AD, DNSSEC
   - Journalisation avancée avec événements critiques
   - Utilisation d'outils de diagnostic : Microsoft Security Assessment, PingCastle, etc.
   - Installation sur Server Core / Nano pour minimiser la surface d'attaque

4. **SECURISATION DU SERVEUR DE FICHIERS – PROTECTION CONTRE LES RANSOMWARES**
   - Implémentation du modèle AGDLP
   - Configuration des alertes FSRM, extension de fichiers, filtrage par type
   - Déploiement du Contrôle d'Accès Dynamique (DAC)
   - Activation de l'énumération basée sur l'accès (EBA)

5. **SECURISATION DE L'ARCHITECTURE SYSTEME**
   - Déploiement de BitLocker avec récupération centralisée (TPM + AD)
   - Mise en œuvre de EFS et stratégies de récupération
   - Paramétrage du pare-feu Windows Defender avec règles avancées

6. **DURCISSEMENT D'ACTIVE DIRECTORY : DEFENSES AVANCEES**
   - Bloquer NetSession Enumeration, protection contre BloodHound
   - Désactivation ou restriction des protocoles faibles : SSLv3, LLMNR, NTLMv1
   - Sécurisation du spooler d'impression (PrintNightmare)
   - Désactivation de services à risque, gestion des services exposés
   - Configuration du cycle de rafraîchissement GPO, priorisation IPv4
   - Renforcement PowerShell + audit (transcription, logs)
   - Déploiement de Credential Guard, Device Guard
   - Application des packs de stratégie :
     - Pass-the-Hash Mitigation
     - Microsoft Security Compliance Toolkit (SCT)
     - MSS Legacy + Baselines
   - Restreindre l'énumération SAM-R (comptes AD)

7. **SECURISATION DE L'ADMINISTRATION DU DOMAINE**
   - Architecture N-Tier (Tier 0/1/2) et zones de sécurité
   - Durcissement des services d'identité (KDC, Kerberos, silos)
   - Restriction WinRM, WMI, RDP (port, restrictions)
   - Sécurisation des MSA/gMSA
   - Réduction de la surface d'attaque (désactivation de ports/services)
   - Analyse réseau avec Netstat, Wireshark
   - Implémentation de JEA (Just Enough Administration)

8. **GESTION DES CORRECTIFS DE SECURITE**
   - Déploiement d'un WSUS ou Microsoft Update for Business
   - Stratégie de mise à jour (test, production, pilote)
   - Suivi de la conformité et rapports d'application
   - Planification, maintenance, automatisation

PUBLIC CONCERNE :

- Administrateurs systèmes, ingénieurs infrastructure
- RSSI, DSI techniques, responsables de la gouvernance Active Directory
- Toute personne en charge de la sécurité du SI Microsoft

PRE-REQUIS :

- Expérience confirmée en administration Windows Server (2019 à 2025)
- Connaissances en Active Directory, GPO et PowerShell recommandées

MOYENS PEDAGOGIQUES :

- Formation interactive avec scénarios de menaces réalistes
- Références aux guides de durcissement ANSSI, CIS, Microsoft SCT 1.0
- Mises en situation avec environnement de LAB virtualisé
- Cas concrets issus d'incidents réels en entreprise,

INTERVENANT(S) : Consultant expert en cybersécurité et systèmes Microsoft

EVALUATION & ATTESTATION :

- Évaluation continue via des exercices pratiques
- Évaluation à chaud des acquis
- Attestation de formation remise en fin de session

MODALITES PRATIQUES :

Durée de la formation : 4 jours
Lieu de formation : INTER / INTRA (à définir)
Tarifs : Demander un devis
Conact : David TOUCHE au +689 87 304 125 / + 33 699 631 711 ou **contact@tavita-cybersecurity.com**

MICROSOFT WINDOWS SERVER 2019/2022/2025

Hyper-V Installation, stockage et virtualisation

OBJECTIFS :

- Comprendre les enjeux, l'architecture et les avantages d'Hyper-V dans l'écosystème Windows Server
- Acquérir les compétences nécessaires à l'installation, la configuration et la gestion des machines virtuelles
- Mettre en œuvre des environnements haute disponibilité et résilients avec clustering, réplication et conteneurs Hyper-V
- Savoir automatiser les tâches d'administration avec PowerShell

CONTENU :

1. INTRODUCTION A LA VIRTUALISATION AVEC HYPER-V

- Historique, concepts clés et types de virtualisation
- Hyperviseurs de type 1 / 2
- Intégration d'Hyper-V dans Windows Server 2025
- Éditions, licences, compatibilité avec Windows Server Core et Nano Server
- Gestion des OS invités, modes de déploiement

2. GESTION DU STOCKAGE LOCAL

- Gestion des disques et volumes sous Windows Server
- Présentation des systèmes de fichiers (NTFS, ReFS)
- Préparation du stockage pour les environnements virtualisés

3. ESPACES DE STOCKAGE ET DE LA DEDUPLICATIONS DE DONNEES

- Configuration des espaces de stockage (Storage Spaces)
- Mise en œuvre de la déduplication de données
- Surveillance et bonnes pratiques d'optimisation

4. INSTALLATION ET CONFIGURATION DE HYPER-V

- Prérequis matériels et logiciels
- Installation d'Hyper-V sur Windows Server 2019 à 2025
- Configuration du stockage et du réseau pour les hôtes Hyper-V
- Création, gestion et configuration des machines virtuelles

5. CONTENEURS DE WINDOWS ET HYPER-V

- Vue d'ensemble des conteneurs Windows Server
- Déploiement et gestion des conteneurs Hyper-V
- Scénarios d'usage : isolation, DevOps, microservices
- Comparaison Docker / Conteneurs Windows natifs

6. HAUTE DISPONIBILITE ET REPRISE D'ACTIVITE

- Concepts de tolérance aux pannes et de récupération
- Mise en œuvre de Windows Server Backup
- Planification de la reprise d'activité (PRA)
- Réplication Hyper-V entre deux hôtes

7. CLUSTERING DE BASCULEMENT

- Planification d'un cluster de basculement
- Création, configuration et maintenance d'un cluster
- Dépannage et surveillance du cluster
- Mise en place de clusters étendus entre sites

8. CLUSTERING AVANCE POUR MACHINES VIRTUELLES

- Intégration d'Hyper-V dans le cluster
- Déplacement dynamique de machines virtuelles
- Stockage partagé et CSV (Cluster Shared Volumes)
- Live Migration, Storage Migration et fonctionnalités avancées

9. REPARTITION DE CHARGES RESEAU (NLB)

- Présentation du Network Load Balancing (NLB)
- Configuration d'un cluster NLB
- Scénarios d'utilisation : frontaux Web, services applicatifs

10. AUTOMATISATION AVEC POWERSHELL

- Vue d'ensemble de PowerShell pour Hyper-V
- Commandes de base pour la gestion des VM
- Scripting avancé : snapshots, réplication, reporting

PUBLIC CONCERNE :

- Administrateurs systèmes et réseaux
- Ingénieurs virtualisation
- Responsables de production et techniciens infrastructures

PRE-REQUIS :

- Bonnes connaissances en administration Windows Server
- Une première expérience en virtualisation est recommandée

MOYENS PEDAGOGIQUES :

- Alternance de théorie et de mise en pratique
- Travaux dirigés et scénarios issus de cas réels
- Utilisation de machines virtuelles pour LAB et tests

INTERVENANT(S) : Consultant expert en cybersécurité et systèmes Microsoft

EVALUATION & ATTESTATION :

- Quiz de validation des acquis en fin de session
- Évaluation à chaud par les participants
- Attestation de formation remise à chaque participant

MODALITES PRATIQUES :

Durée de la formation : 3 jours
Lieu de formation : INTER / INTRA (à définir)
Tarifs : Demander un devis
Conact : David TOUCHE au +689 87 304 125 / + 33 699 631 711 ou **contact@tavita-cybersecurity.com**

MICROSOFT WINDOWS SERVER 2019/2022/2025

Mise en œuvre du service de certificats (PKI – Active Directory Certificate Services)

OBJECTIFS :

- Comprendre les concepts fondamentaux de la cryptographie appliquée aux environnements d'entreprise
- Déployer, configurer et administrer une autorité de certification (CA) sous Windows Server
- Délivrer et gérer des certificats numériques X.509 pour les utilisateurs, machines et services
- Mettre en œuvre une authentification forte basée sur certificat au sein d'une infrastructure Active Directory
- Appliquer les bonnes pratiques de sécurité, de révocation et d'administration dans un environnement PKI d'entreprise

CONTENU :

1. FONDAMENTAUX DE LA CRYPOGRAPHIE

- Chiffrement symétrique : principe et algorithmes (AES, DES...)
- Chiffrement asymétrique : RSA, ECC
- Fonction de hachage (SHA-2, SHA-3)
- Signature numérique et vérification d'intégrité
- Confidentialité en HTTPS : fonctionnement simplifié
- Attaque de type Man-in-the-Middle
- Notions de signature électronique et d'authentification forte

2. INTRODUCTION AUX INFRASTRUCTURES A CLES PUBLIQUES (PKI)

- Architecture PKI : rôles et composants (CA, RA, CRL, OCSP)
- Le certificat X.509 : structure et usages
- Rôle et hiérarchie d'une autorité de certification
- Protocole LDAPS et sécurisation des échanges LDAP
- Mécanismes de révocation : CRL, OCSP
- Typologies de déploiement PKI (Root CA, Subordinate CA, Offline CA)
- Bonnes pratiques ANSSI / Microsoft / CIS
- Gestion des clés : durée de vie, rotation, renouvellement

3. DÉPLOIEMENT ET CONFIGURATION D'UNE PKI AVEC AD CS

- Installation et configuration des rôles AD CS
- Création d'une autorité de certification entreprise ou autonome
- Définition des modèles de certificats personnalisés
- Configuration de l'enrôlement automatique (Autoenrollment)
- Archivage et récupération de certificats
- Déploiement de certificats utilisateurs, ordinateurs, services
- Intégration des certificats dans les services :
  - HTTPS (IIS)
  - LDAPS
  - VPN/IPsec

    - Smartcards / cartes à puce
    - EFS (chiffrement de fichiers)
- Mise en place du protocole OCSP (Online Certificate Status Protocol)
- Configuration des points de distribution de CRL (CDP/AIA)
- Gestion des délégations et rôles d'administration
- Automatisation de la gestion PKI avec PowerShell

PUBLIC CONCERNE :

- Administrateurs systèmes et infrastructures
- Responsables sécurité / IT
- Toute personne en charge de la sécurité des communications internes dans un environnement Microsoft

PRE-REQUIS :

- Maîtrise des fondamentaux de Windows Server (2019/2022/2025)
- Expérience en administration Active Directory

MOYENS PEDAGOGIQUES:

- Formation interactive basée sur l'expérience et l'échange
- Démonstrations en environnement virtualisé
- Exercices pratiques à chaque étape de la mise en œuvre
- Référentiels : ANSSI, CIS, Microsoft Security Compliance Toolkit

INTERVENANT(S) : Consultant expert en cybersécurité et systèmes Microsoft

EVALUATION & ATTESTATION :

- Évaluation des acquis par mise en pratique continue + quiz final
- Évaluation à chaud de la session par les participants
- Attestation de formation délivrée en fin de session

MODALITES PRATIQUES :
Durée de la formation : 2 jours
Lieu de formation : INTER / INTRA (à définir)
Tarifs : Demander un devis
Conact : David TOUCHE au +689 87 304 125 / + 33 699 631 711 ou **contact@tavita-cybersecurity.com**

MICROSOFT WINDOWS SERVER 2019/2022/2025

Configuration et gestion du service de mises à jour WSUS (Windows Server Update Services)

OBJECTIFS :

- Comprendre les mécanismes de mise à jour dans les environnements Windows Server récents (2019 à 2025)
- Savoir installer, configurer et maintenir une infrastructure WSUS sécurisée
- Maîtriser le déploiement de correctifs dans des environnements connectés et isolés
- Automatiser et superviser les mises à jour à l'aide des GPO, commandes PowerShell et outils natifs
- Renforcer la sécurité de la chaîne de distribution des mises à jour

CONTENU :

1. ARCHITECTURE ET INSTALLATION

- Les mises Fonctionnement du service Windows Update
- Rôles et évolutions de WSUS (versions 4.0 et 5.0)
- Compatibilité et nouveautés avec Windows Server 2025
- Choix du type d'installation : rôle complet ou console distante
- Base de données WSUS (WID ou SQL Server dédié)
- Intégration dans un projet de déploiement de correctifs à l'échelle d'un parc

2. ADMINISTRATION ET PARAMETRAGE

- Console WSUS : configuration initiale et bonnes pratiques
- Catégories de produits, classifications, langues
- Groupes d'ordinateurs : assignation manuelle et automatique
- Intégration avec Active Directory et stratégie de groupes (GPO)
- Commandes utiles : wsusutil, wuauclt, usoclient, PowerShell UpdateModule
- Mode autonome vs. mode connecté (synchronisation avec un WSUS maître)

3. SECURITE ET CHIFFREMENT DES FLUX

- Activation du protocole HTTPS (SSL/TLS) entre clients et serveur WSUS
- Création, exportation et déploiement du certificat racine (AD CS ou AC tierce)
- Sécurisation du transfert de métadonnées
- Sauvegarde/restauration de la base WSUS
- Stratégie de test et d'approbation des correctifs
- Cas d'usage pour environnements critiques ou sensibles

4. **DEPLOIEMENT ET MAINTENANCE OPERATIONNELLE**
   - Configuration de serveurs WSUS maître / réplica
   - Déploiement dans des sites distants ou isolés (mode offline)
   - Exportation de la base WSUS pour duplication (via wsusutil export/import)
   - Intégration avec Microsoft Endpoint Configuration Manager
   - Automatisation du déploiement via regedit, PowerShell, ou GPO

5. **REPORTING ET SUPERVISION**
   - Rapports d'état des clients et des mises à jour
   - Suivi de conformité et détection des postes non à jour
   - Gestion des alertes WSUS et audit des actions d'approbation
   - Bonnes pratiques de nettoyage et d'optimisation de la base WSUS

PUBLIC CONCERNE : Administrateurs systèmes, ingénieurs infrastructures, techniciens responsables du cycle de mise à jour Windows dans l'organisation.

PRE-REQUIS : Bonne connaissance de l'administration Windows Server et des principes Active Directory / GPO.

MOYENS PEDAGOGIQUES:

- Alternance d'apports théoriques et de travaux pratiques en environnement virtualisé
- Accès à un environnement WSUS de démonstration (mode maître/réplica)
- Support numérique remis à chaque participant
- Cas concrets de production et bonnes pratiques tirées d'expériences réelles

INTERVENANT(S) : Consultant expert en cybersécurité et systèmes Microsoft

EVALUATION & ATTESTATION :

- Évaluation des acquis par quiz final + exercices pratiques
- Évaluation à chaud par les participants
- Attestation de formation remise à l'issue de la session

MODALITES PRATIQUES :
Durée de la formation : 2 jours
Lieu de formation : INTER / INTRA (à définir)
Tarifs : Demander un devis
Conact : David TOUCHE au +689 87 304 125 / + 33 699 631 711 ou **contact@tavita-cybersecurity.com**

MICROSOFT WINDOWS SERVER 2019/2022/2025

Mise en œuvre et administration d'un serveur Exchange 2019

OBJECTIFS :

- Déployer, configurer et administrer une infrastructure de messagerie basée sur Exchange Server 2019
- Gérer les destinataires, boîtes aux lettres, politiques de transport et services d'accès client
- Implémenter la haute disponibilité, la continuité d'activité et la reprise après sinistre
- Sécuriser les échanges de messagerie (antivirus, antispam, RBAC, audit)
- Préparer la migration vers Exchange Online / Office 365 (hybridation ou transfert complet)

CONTENU :

1. DEPLOIEMENT DE MICROSOFT EXCHANGE SERVER

- Architecture et composants d'Exchange Server 2019
- Prérequis matériels, logiciels et dépendances Active Directory
- Scénarios de déploiement (mono/multi-serveurs, DAG, Edge Transport)
- Compatibilité avec Windows Server 2019/2022/2025
- Installation pas à pas et vérifications post-déploiement

2. ADMINISTRATION GENERALE DU SERVEUR

- Console Exchange Admin Center (EAC)
- Gestion des rôles serveur et services de boîtes aux lettres
- Planification de maintenance, configuration de journaux, protocoles, quotas
- Intégration avec les certificats SSL internes (PKI) ou publics

3. GESTION DES DESTINATAIRES

- Utilisateurs, boîtes aux lettres, groupes, contacts, ressources
- Stratégies d'adresse, listes d'adresses globales (GAL), politiques de boîte
- Gestion dynamique des groupes de distribution
- Délégation de permissions sur les objets Exchange

4. UTILISATION DE L'EXCHANGE MANAGEMENT SHELL (EMS)

- Principes et syntaxe PowerShell spécifique à Exchange
- Automatisation de tâches récurrentes (création, audit, supervision)
- Scripts d'administration avancée et gestion par lot

5. CONNECTIVITE ET SERVICES CLIENTS

- Configuration des services d'accès client (OWA, MAPI/HTTP, POP, IMAP)
- Intégration Outlook, autodiscover, publication via reverse proxy
- Gestion de la mobilité (ActiveSync, gestion à distance, sécurité mobile)
- Accès externe sécurisé via certificats et pare-feu

6. HAUTE DISPONIBILITE ET REPRISE D'ACTIVITE

- Architecture du transport dans Exchange
- Connecteurs de réception/envoi, routage des messages
- Règles de transport, limites, journalisation des flux
- Filtrage d'autorisation et stratégies de conformité

7. TRANSPORT ET FLUX DE MESSAGERIE

- Architecture du transport dans Exchange
- Connecteurs de réception/envoi, routage des messages
- Règles de transport, limites, journalisation des flux
- Filtrage d'autorisation et stratégies de conformité

8. PROTECTION DES MESSAGES (ANTIVIRUS / ANTISPAM)

- Rôle Edge Transport : filtrage entrant en périphérie
- Moteurs antivirus internes / externes (via API Exchange AV)
- Filtrage antispam : agents de transport, listes, SCL
- Intégration avec Microsoft Defender for Office 365

9. EXCHANGE ONLINE ET MIGRATION HYBRIDE

- Vue d'ensemble d'Exchange Online et Office 365
- Outils de migration : Cutover, Staged, Hybrid Configuration Wizard
- Synchronisation Azure AD (AADConnect)
- Gestion mixte d'un environnement hybride (on-prem / cloud)

10. SUPERVISION, SÉCURITÉ ET MAINTENANCE

- Supervision (queues, files d'attente, files d'achèvement)
- Audits : accès, boîte aux lettres, journaux d'administration
- Mise en œuvre du RBAC (contrôle d'accès basé sur les rôles)
- Scripts de diagnostic, outils de stress, analyse des performances
- Bonnes pratiques de maintenance corrective et préventive

PUBLIC CONCERNE : Administrateurs systèmes, ingénieurs IT, techniciens ou toute personne impliquée dans la gestion d'une messagerie d'entreprise Exchange Server.

PRE-REQUIS : Bonne maîtrise de l'environnement Windows Server 2012 à 2025 et de l'Active Directory.

MOYENS PEDAGOGIQUES:

- Formation orientée pratique sur un environnement Exchange virtualisé
- Travaux dirigés et mises en situation inspirées de cas réels
- Support numérique et scripts remis à l'issue de la session

INTERVENANT(S) : Consultant expert en cybersécurité et systèmes Microsoft

EVALUATION & ATTESTATION :

- Évaluation des acquis par quiz final et cas pratique
- Évaluation de satisfaction à chaud
- Remise d'une attestation de formation

MODALITES PRATIQUES :

Durée de la formation : 2 jours
Lieu de formation : INTER / INTRA (à définir)
Tarifs : Demander un devis
Conact : David TOUCHE au +689 87 304 125 / + 33 699 631 711 ou **contact@tavita-cybersecurity.com**

MICROSOFT WINDOWS SERVER 2019/2022/2025

Initiation et découverte des services essentiels

OBJECTIFS :

- Apprendre Savoir installer et administrer Windows Server 2019/2022/2025
- Comprendre l'intégration cloud hybride et Windows Admin Center
- Gérer et sécuriser les comptes utilisateurs et groupes
- Maîtriser le stockage et les partages de fichiers (NTFS, ReFS, SMB, NFS, iSCSI)
- Configurer l'impression réseau et le serveur d'impression
- Mettre en œuvre des stratégies de sécurité avancées (GPO, BitLocker, pare-feu, audit)
- Surveiller et optimiser les performances du serveur
- Installer et administrer les Remote Desktop Services (RDS)

CONTENU :

1. **INSTALLER WINDOWS SERVER 2019 / 2022 / 2025**
   - Préparation de l'installation (hardware, virtualisation, licensing)
   - Installation en mode GUI et Core
   - Nouveautés de Windows Server 2025 (Azure Arc, gestion hybride)

2. **UTILISER WINDOWS ADMIN CENTER ET LE SERVER MANAGER**
   - Présentation et prise en main
   - Gestion de grappes et serveurs distants
   - Gestion centralisée via Windows Admin Center
   - Ajout de rôles et fonctionnalités en local ou distant

3. **GERER LES COMPTES UTILISATEURS ET GROUPES**
   - Création et administration des comptes utilisateurs
   - Politique de mot de passe et MFA
   - Groupes de sécurité et groupes prédéfinis
   - Gestion des profils utilisateurs et répertoires de base

4. **CONFIGURER LES ACCES AUX RESSOURCES AVEC NTFS ET LES GROUPES**
   - Dossiers partagés et autorisations combinées NTFS/partages
   - Meilleures pratiques sur la délégation de droits
   - Implémentation de DFS (Distributed File System)
   - Gestion avancée FSRM (File Server Resource Manager)

5. **GERER ET OPTIMISER LE STOCKAGE**
   - Concepts et nouveautés NTFS / ReFS
   - Espaces de stockage, Storage Spaces Direct
   - Pools de stockage et résilience
   - Gestion unifiée avec Windows Admin Center

6. **CONFIGURER LE RESEAU ET LES SERVICES DE BASE**
   - Configurer l'adressage IP et le DHCP
   - Implémentation d'IPAM
   - Services DNS : haute disponibilité, diagnostics
   - Intégration aux services cloud hybrides

7. **CONFIGURER DES PERIPHERIQUES D'IMPRESSION**
   - Ajout et gestion d'imprimantes réseau
   - Serveur d'impression Windows Server
   - Gestion des files d'attente et sécurité d'impression

8. **SECURITE ET STRATEGIES DE GROUPE**
   - Mise en œuvre des stratégies de sécurité
   - Gestion des ACL et Dynamic Access Control
   - BitLocker et intégrité du système
   - Gestion de l'audit et des journaux
   - Configuration du pare-feu Windows avancé

9. **SURVEILLANCE ET OPTIMISATION**
   - Surveillance système (Perfmon, Event Viewer)
   - Gestion proactive des alertes
   - Outils d'analyse et de performance intégrés
   - Dépannage avancé

10. **INSTALLER ET CONFIGURER LES SERVICES RDS (REMOTE DESKTOP SERVICES)**
    - Présentation et architecture des RDS
    - Installation d'une ferme RDS avec broker
    - Gestion des licences
    - Publication d'applications RemoteApp et accès Web
    - Administration avec PowerShell

PUBLIC CONCERNE : Tout professionnel de l'informatique disposant de connaissances de base en environnement Windows et souhaitant découvrir ou mettre à niveau ses compétences sur Windows Server 2019, 2022 et 2025.

PRE-REQUIS : Connaissances de base en systèmes Windows et réseaux.

MOYENS PEDAGOGIQUES :

- Formation participative, échanges d'expériences
- Démonstrations techniques et ateliers pratiques
- Support numérique remis en fin de formation

INTERVENANT(S) : Consultant expert en cybersécurité et systèmes Microsoft

EVALUATION & ATTESTATION :

- Évaluation des acquis via quizz en fin de formation
- Attestation de formation remise au participant
- Évaluation « à chaud » de la satisfaction en fin de session

MODALITES PRATIQUES :

Durée de la formation : 4 jours
Lieu de formation : INTER / INTRA (à définir)
Tarifs : Demander un devis
Conact : David TOUCHE au +689 87 304 125 / + 33 699 631 711 ou **contact@tavita-cybersecurity.com**

MICROSOFT WINDOWS 10/11

Sécuriser les postes dans une infrastructure Active Directory

OBJECTIFS :

- Améliorer la sécurité des postes de travail Windows 10/11 dans un environnement Active Directory
- Optimiser les performances tout en respectant les exigences de sécurité et de conformité
- Mettre en œuvre des techniques et outils pour protéger les utilisateurs, les données et les réseaux

CONTENU :

1. INTRODUCTION ET CONTEXTE

- État des menaces actuelles sur Windows
- Évolution des architectures Windows et des usages collaboratifs
- Principes de la sécurité Windows 10/11
- Introduction au modèle Zero Trust

2. ATTAQUES ET AUTHENTIFICATION

- Panorama des attaques ciblant Windows et Active Directory
- Gestion de l'authentification (SSO, MFA, Kerberos)
- Déploiement et configuration de Microsoft LAPS
- Définition et application de Password Settings Objects (PSO)
- Bonnes pratiques pour le durcissement des comptes locaux

3. STRATEGIES ET MODELES DE SECURITE

- Bonnes pratiques ANSSI / CIS pour Active Directory
- Modèles d'administration (Tiering, ESAE, PAM)
- Gestion des environnements utilisateurs (profils, GPO)
- Sécurisation du Windows Store et des applications
- Configuration avancée d'UAC
- Gestion des ACL et Dynamic Access Control
- Mise en place de règles de sécurité pour les navigateurs

4. LA PROTECTION DES CONNEXIONS RESEAUX

- Sécuriser l'accès réseau dans un domaine Windows
- Configuration avancée du pare-feu Windows Defender
- Notions de Network Access Protection (NAP) et alternatives modernes (VPN Always On, Conditional Access)
- Introduction à DirectAccess
- Présentation de Windows To Go / Windows 365 Cloud PC

5. SECURITE DES DONNEES ET DES APPLICATIONS

- Mise en œuvre d'EFS pour la protection des fichiers
- Chiffrement avec BitLocker et BitLocker To Go
- Gestion des applications avec AppLocker
- Protection du poste avec Device Guard et Credential Guard
- Apports des mises à jour de sécurité récentes (Windows 11 Security Baselines)

6. SAUVEGARDES ET RESTAURATION

- Gestion de la protection système
- Automatisation des sauvegardes des postes
- Volume Shadow Copies et clichés instantanés
- Bonnes pratiques pour la restauration post-incident

7. OUTILS D'ANALYSE ET DE DIAGNOSTIC

- Analyse des performances et de la stabilité
- Utilisation des journaux d'événements et outils de diagnostic mémoire
- Présentation de Windows Performance Toolkit (WPT)
- Utilisation du Windows Assessment and Deployment Kit (ADK)
- Gestion de l'autonomie et consommation d'énergie des postes

PUBLIC CONCERNE : Techniciens, administrateurs systèmes et infrastructure, consultants sécurité

PRE-REQUIS : Maîtrise des fondamentaux de l'administration Windows 10 ou 11 en environnement d'entreprise

MOYENS PEDAGOGIQUES :

- Formation interactive orientée pratique
- Exercices appliqués à partir de cas réels
- Utilisation de guides de référence (ANSSI, CIS, Microsoft Baselines)

INTERVENANT(S) : Consultant expert en cybersécurité et systèmes Microsoft

EVALUATION & ATTESTATION :

- Quiz de validation des acquis en fin de formation
- Évaluation de satisfaction à chaud
- Attestation de formation remise au participant

MODALITES PRATIQUES :

Durée de la formation : 2 jours
Lieu de formation : INTER / INTRA (à définir)
Tarifs : Demander un devis
Conact : David TOUCHE au +689 87 304 125 / + 33 699 631 711 ou **contact@tavita-cybersecurity.com**

GESTION DE PARC INFORMATIQUE
Installation et administration de Microsoft Endpoint Configuration Manager (SCCM) 250x

OBJECTIFS :

- Installer et configurer Microsoft Endpoint Configuration Manager (Current Branch 250x)
- Déployer des systèmes d'exploitation Windows 10 / 11
- Distribuer et gérer des packages et applications d'entreprise
- Mettre en œuvre la gestion des mises à jour logicielles
- Superviser les inventaires matériels et logiciels, requêtes et rapports
- Sauvegarder et restaurer un site MECM

CONTENU :

1. **PLANIFICATION ET DEPLOIEMENT D'UN SITE PRIMAIRE**
   - Dimensionnement de l'infrastructure (on-premise, hybride, Cloud Attach)
   - Installation du site primaire et prérequis (SQL, certificats, comptes de service)
   - Configuration de la hiérarchie MECM
   - Intégration aux services cloud : Intune, Azure AD, Windows Autopilot
   - Stratégies de sécurité et modèles de rôles d'administration

2. **GESTION DES CLIENTS MECM**
   - Découverte et intégration des clients (Windows 10/11)
   - Méthodes de déploiement (push, GPO, script, co-management)
   - Applet Configuration Manager et Centre Logiciel
   - Suivi et analyse des logs côté client
   - Surveillance du cycle de vie des clients

3. **INVENTAIRE, REQUETES ET REGROUPEMENTS**
   - Inventaire matériel et logiciel avancé
   - Création et gestion des requêtes
   - Création et maintenance des regroupements dynamiques
   - Bonnes pratiques de structuration des collections

4. **DEPLOIEMENT D'APPLICATIONS**
   - Création de packages et d'applications modernes (MSIX, App-V)
   - Vue d'ensemble de la distribution et des points de distribution
   - Gestion de l'affinité utilisateurs/appareils
   - Analyse des déploiements (états, logs)
   - Stratégies de gestion et de sécurisation des applications

5. **GESTION DES MISES A JOUR LOGICIELLES**
   - Gestion des mises à jour CB / CBB / LTSC pour Windows 10 et 11
   - Plans de maintenance Windows
   - Intégration et configuration de WSUS
   - Automatisation des déploiements avec ADR (Automatic Deployment Rules)

- Diagnostic et supervision des mises à jourEtude des logs côté clients et serveurs.

6. DEPLOIEMENT DE SYSTEMES D'EXPLOITATION

- Préparation des images de référence (sysprep, MDT)
- Gestion des packages de pilotes et images de démarrage
- Création et optimisation des séquences de tâches
- Supervision et dépannage des déploiements de système

7. REPORTING, MAINTENANCE ET SECURITE

- Configuration de SQL Server Reporting Services (SSRS)
- Création et personnalisation des rapports
- Gestion des droits et sécurité des rôles MECM
- Tâches de maintenance du site
- Sauvegarde et restauration d'un site MECM
- Outils de dépannage et meilleures pratiques

PUBLIC CONCERNE : Administrateurs systèmes, techniciens IT, ingénieurs production ayant la responsabilité d'un parc informatique d'entreprise et souhaitant gérer efficacement Windows 10/11 via SCCM / MECM

PRE-REQUIS : Très bonnes connaissances de l'environnement Windows Server et des systèmes clients Windows 10/11.

MOYENS PEDAGOGIQUES:

- Formation interactive basée sur des mises en situation pratiques
- Études de cas et exercices sur des environnements proches de la production
- Support numérique remis en fin de formation

INTERVENANT(S) : Consultant expert en cybersécurité et systèmes Microsoft

EVALUATION & ATTESTATION :

- Quiz de validation des acquis en fin de session
- Évaluation de satisfaction à chaud
- Attestation de formation remise au participant

MODALITES PRATIQUES :
Durée de la formation : 4 jours
Lieu de formation : INTER / INTRA (à définir)
Tarifs : Demander un devis
Conact : David TOUCHE au +689 87 304 125 / + 33 699 631 711 ou **contact@tavita-cybersecurity.com**

GESTION DE PARC INFORMATIQUE

WAPT Entrerprise - Maintenez à jour votre parc informatique

OBJECTIFS :

À l'issue de la formation, le stagiaire sera capable :

- d'utiliser WAPT de manière efficace au quotidien
- de déployer des paquets WAPT
- de créer et maintenir des paquets personnalisés
- d'exploiter l'ensemble des fonctionnalités de la version Enterprise

CONTENU :

1. **INSTALLATION ET CONFIGURATION DE WAPT**
   - **Préparation de l'environnement serveur**
     - Dimensionnement recommandé
     - Paramètres système (nom, IP, prérequis logiciels)
   - **Installation du serveur WAPT**
     - Déploiement sur CentOS, Debian, Windows
     - Configuration des dépôts
     - Exécution du post-configuration
   - **Installation de la console et gestion des certificats**
     - Installation de la console
     - Génération du certificat administrateur
     - Prise en main et paramétrage de la console
   - **Génération et déploiement de l'agent WAPT**
     - Options de base de l'agent
     - Déploiement manuel et via GPO
   - **Configuration de l'agent WAPT**
     - Fichier wapt-get.ini
     - Utilisation en ligne de commande

2. **MAITRISER LES FONCTIONNALITES DE WAPT ENTERPRISE**
   - Mettre en place WAPT WUA
   - Déployer le Self-Service
   - Utiliser les fonctionnalités de reporting
   - Configurer les dépôts secondaires
   - Intégrer l'authentification Active Directory de la console
   - Paramétrer l'authentification Kerberos des agents
   - Configurer l'authentification par certificat client
   - Exploiter l'API WAPT pour l'automatisation
   - Mettre en œuvre le déploiement d'un système d'exploitation (Windows 10 / 11)

3. CREER ET MAINTENIR DES PAQUETS WAPT

- Créer des paquets simples
  - À partir d'un MSI
  - À partir d'un EXE
- Concevoir des paquets personnalisés
  - Structurer les besoins clients
  - Bonnes pratiques de gestion de versions

PUBLIC CONCERNE : Administrateurs systèmes, ingénieurs systèmes, exploitants et intégrateurs.

PRE-REQUIS :

- Bonnes connaissances de l'administration Windows
- Connaissances de base en réseau recommandées

MOYENS PEDAGOGIQUES :

- Formation interactive basée sur des cas pratiqueS
- Exercices d'application et mises en situation concrètes
- Support remis en fin de formation

INTERVENANT(S) : Consultant expert en cybersécurité et spécialiste WAPT

EVALUATION & ATTESTATION :

- Quiz d'évaluation des acquis en fin de formation
- Évaluation de satisfaction à chaud
- Attestation de formation remise au participant

MODALITES PRATIQUES :
Durée de la formation : 2 jours
Lieu de formation : INTER / INTRA (à définir)
Tarifs : Demander un devis
Conact : David TOUCHE au +689 87 304 125 / + 33 699 631 711 ou **contact@tavita-cybersecurity.com**

VMWARE VSPHERE 7.X/8.X

Installation, configuration et administration

OBJECTIFS :

- Installer et configurer une infrastructure VMware vSphere moderne (7.x / 8.x).
- Gérer et optimiser le réseau et le stockage virtuels.
- Déployer, administrer et superviser des machines virtuelles.
- Mettre en place la haute disponibilité, le DRS et les fonctionnalités avancées.
- Sécuriser l'accès et la gestion des ressources de l'infrastructure.
- Introduire les fonctionnalités récentes : vSphere Lifecycle Manager, vSAN, vSphere with Tanzu (containers/Kubernetes).

CONTENU :

1. INTRODUCTION À LA VIRTUALISATION ET À VSPHERE

- Présentation de VMware vSphere et des nouveautés (7.x / 8.x).
- Marché, enjeux et positionnement dans le cloud hybride.
- Licences et fonctionnalités associées.
- Intégration vSphere avec VMware Cloud et hyperscalers (AWS, Azure, GCP).

2. ARCHITECTURE, INSTALLATION ET VCENTER

- Architecture vSphere : ESXi, vCenter, PSC (évolution 7.x et 8.x).
- Installation et configuration de l'hyperviseur ESXi.
- Déploiement de vCenter Server Appliance (VCSA – Photon OS).
- Accès et gestion via vSphere Client HTML5.
- Migration de serveurs physiques vers VM (VMware Converter).

3. GESTION DU RESEAU VIRTUEL

- Concepts du réseau virtuel VMware.
  Switchs standards (vSwitch) et distribués (vDS).
  VLAN, sécurité, contrôle du trafic, QoS et load balancing.
  Gestion des ports et politiques de sécurité réseau.
  Nouveautés réseau dans vSphere 8 (DPDK, accélérations matérielles).

4. GESTION DU STOCKAGE VIRTUEL

- Types de stockage supportés : SAN FC, SAN iSCSI, NFS, vSAN.
- Volumes virtuels (vVols) et intégration avec le stockage externe.
- Création, gestion et optimisation des datastores.
- Politique de stockage basée sur les règles (SPBM).
- Nouveautés vSAN (compression, encryption, stretched clusters).

5. ADMINISTRATION DES MACHINES VIRTUELLES (VM)

- Installation et gestion des VMware Tools.
- Création et gestion de VM, clones, templates et snapshots.
- Migration à chaud (vMotion, Storage vMotion) et à froid.
- Optimisation du matériel virtuel (Thin Provisioning, VMDirectPath I/O).
- Réplication et continuité d'activité avec vSphere Replication et SRM (Site Recovery Manager).

6. HAUTE DISPONIBILITÉ ET OPTIMISATION DES RESSOURCES

- Mise en place et configuration d'un cluster HA et DRS.
- Resource Pools et contrôle de l'allocation des ressources.
- Optimisation CPU, mémoire et stockage.
- Nouveautés : DRS amélioré (basé sur les VM), vSphere Persistent Memory.
- Gestion des performances et bonnes pratiques.

7. SUPERVISION, SÉCURITÉ ET MAINTENANCE

- Alarmes par défaut et personnalisées.
- Alarmes et alertes personnalisées.
- Sécurisation des accès : rôles, permissions et RBAC.
- Authentification fédérée avec AD / ADFS / Identity Federation (SAML/OAuth).
- Gestion des mises à jour via vSphere Lifecycle Manager (remplaçant de VUM).
- Outils de dépannage et best practices.

PUBLIC CONCERNE : Administrateurs systèmes, ingénieurs virtualisation, architectes IT, responsables techniques souhaitant déployer et gérer une infrastructure VMware vSphere moderne.

PRE-REQUIS : Connaissance de base des environnements Windows ou Linux.
Notions en réseau et stockage recommandées.

MOYENS PEDAGOGIQUES :

- Formation interactive avec démonstrations et ateliers pratiques.
  Études de cas concrets et mises en situation.
  Support numérique remis en fin de formation.

INTERVENANT(S) : Consultant expert en virtualisation, infrastructures VMware et cybersécurité.

EVALUATION & ATTESTATION :

- Quiz de validation des acquis en fin de session.
- Évaluation de satisfaction à chaud.
- Attestation de formation délivrée aux participants.

MODALITES PRATIQUES :

Durée de la formation : 3 jours
Lieu de formation : INTER / INTRA (à définir)
Tarifs : Demander un devis
Conact : David TOUCHE au +689 87 304 125 / + 33 699 631 711 ou **contact@tavita-cybersecurity.com**

SECURITE INFORMATIQUE

Kaspersky Security Center : Les fondamentaux

OBJECTIFS :

- Décrire les possibilités offertes par Kaspersky Endpoint Security pour Windows et de Kaspersky Security Center
- Préparer et implémenter une solution de protection optimale de réseau Windows avec Kaspersky Endpoint Security et gérée à l'aide de Kaspersky Security Center
- Administrer ce système

CONTENU :

1. KASPERSKY - DEPLOIEMENT

- Préparation au déploiement
- Installation de Kaspersky Security Center
- Déploiement de la protection
- Gestion de la Structure d'Administration
- Lab 1.1 – Installation de Kaspersky Security Center
- Lab 1.2 – Déploiement de Kaspersky Endpoint Security
- Lab 1.3 – Installation de Kaspersky Endpoint Security sur un poste nomade
- Lab 1.4 – Surveillance du déploiement de la protection
- Lab 1.5 – Création de la structure des ordinateurs administrés
- Lab 1.6 – Création des stratégies et des tâches

2. ADMINISTRATION

- Notions fondamentales de Kaspersky Endpoint Security 10
- Protection du système de fichiers
- Protection du réseau
- System Watcher
- Diagnostics des menaces
- Diagnostics des statuts de protection
- Lab 2.1 – Test de l'Antivirus Fichiers
- Lab 2.2 – Identification des utilisateurs à risque
- Lab 2.3 – Configuration du Pare-feu
- Lab 2.4 – Traitement des incidents de virus
- Lab 2.5 – Configuration des exclusions

3. CONTROLE ENDPOINT

- Généralités
- Contrôle du lancement des applications
- Contrôle de l'activité des applications
- Contrôle des périphériques

- Filtrage de contenu
- Lab 3.1 – Contrôle du démarrage du navigateur
- Lab 3.2 – Contrôle du lancement d'application
- Lab 3.3 – Blocage de périphériques USB
- Lab 3.4 – Privilèges d'accès aux périphériques USB
- Lab 3.5 – Contrôle de l'accès à Internet

4. MAINTENANCE

- Introduction
- Gestion des licences
- Mises à jour
- Administration des ordinateurs itinérants
- Interaction avec l'utilisateur
- Sauvegarde et restauration
- Statistiques et rapports
- Lab 4.1 – Mise à Jour des bases de données et des modules
- Lab 4.2 – Configuration de la protection des ordinateurs itinérants
- Lab 4.3 – Protection par mot de passe de KES
- Lab 4.4 – Cacher la présence de KES
- Lab 4.5 – Sauvegarde et restauration

PUBLIC CONCERNE : Ce cours est destiné aux administrateurs réseau Microsoft Windows et aux spécialistes de la sécurité des informations.

PRE-REQUIS

- Compréhension de TCP/IP, du fonctionnement d'Internet et de l'e-mail, des connaissances de base dans l'administration de réseaux Windows et d'Active Directory
- Expérience des systèmes d'exploitation Microsoft Windows.

MOYENS PEDAGOGIQUES:

- Pédagogie par l'expérience fondée sur l'interaction dans le groupe.
- Exercices pratiques à partir de mise en situation,

INTERVENANT(S) : Consultant en cybersécurité et IT

EVALUATION & ATTESTATION :

- L'évaluation des acquis se fait en fin de formation au travers d'un Quiz. Une évaluation de la formation est faite à chaud par le participant à l'issue de la formation.
- L'attestation de formation est remise à la fin de la formation

MODALITES PRATIQUES :

Durée de la formation : 2 jours
Lieu de formation : INTER / INTRA (à définir)
Support de formation remis à l'issue
Tarifs : Demander un devis
Conact : David TOUCHE au 87 30 41 25 ou **contact@tavita-cybersecurity.com**

SECURITE INFORMATIQUE

Veeam Backup and Replication 9.5/12 : Installation, sauvegarde et restauration

OBJECTIFS :

- Installer Veeam et ses composants
- Connaître les améliorations par rapport aux versions précédentes
- Créer des tâches de sauvegarde d'un environnement virtuel
- Restaurer des fichiers sauvegardés dans un environnement virtuel

CONTENU :

1. LA SUITE LOGICIELLE DE VEEAM

- Présentation de la suite Veeam.
- Principales fonctionnalités de Veeam 9.5.
- Architecture générale Veeam.
- Composants de base et optionnels de l'architecture.
- Mise à jour des licences.

2. INSTALLATION ET CONFIGURATION

- Prérequis à l'installation de Veeam.
- Composants nécessaires pour le déploiement et l'utilisation de Veeam.
- Scénarios de déploiement.
- Mise à jour de Veeam Backup et réplication.

3. CONFIGURATION INITIALE DE L'ENVIRONNEMENT

- Découverte de l'interface utilisateur.
- Ajout de composants et d'éléments.
- Ajouter un proxy de sauvegarde VMware, Hyper-V.
- Réaliser des configurations de sauvegarde et de récupération.
- Ajouter des dépôts de sauvegarde.
- Gérer le réseau.

4. SAUVEGARDES ET RESTAURATIONS, REPLICATION ET PRA

- Création de tâches de sauvegarde et de points de restauration.
- Créer des tâches de copie de VM, fichiers, failover et PRA.
- Copies et réplications de machines virtuelles.
- Restaurations complètes ou rapides au niveau fichier.
- Créer des points de restauration avec VeeamZIP et Quick Backup.

5. FONCTIONNALITES AVANCEES

- Environnement isolé et protégé : outil Virtual lab.
- Restauration en un clic.
- Restauration des éléments fichiers via un explorateur et Veeam Explorer.
- Intégration client web.
- Sauvegarde des VM et VeeamZIP.
- Prise en charge des systèmes de stockage SAN.
- Sauvegarde et restauration des données à partir du cloud.

6. MAINTENANCE ET DEPANNAGE

- Auditer l'environnement.
- Analyse des dysfonctionnements de premier niveau de l'environnement.
- Rechercher des informations complémentaires

PUBLIC CONCERNE : Cette formation s'adresse aux administrateurs et ingénieurs systèmes amenés à travailler dans l'environnement de virtualisation VMware.

PRE-REQUIS : Avoir de l'expérience sur les systèmes Microsoft Windows ou Linux

MOYENS PEDAGOGIQUES :

- Pédagogie par l'expérience fondée sur l'interaction dans le groupe.
- Exercices pratiques à partir de mise en situation,

INTERVENANT(S) : Consultant en cybersécurité et IT

EVALUATION & ATTESTATION :

- L'évaluation des acquis se fait en fin de formation au travers d'un Quiz. Une évaluation de la formation est faite à chaud par le participant à l'issue de la formation.
- L'attestation de formation est remise au stagiaire à la fin de la formation

MODALITES PRATIQUES :

Durée de la formation : 2 jours

Lieu de formation : INTER / INTRA (à définir)

Support de formation remis à l'issue

Tarifs : Demander un devis

Conact : David TOUCHE au 87 30 41 25 ou **contact@tavita-cybersecurity.com**

SECURITE INFORMATIQUE

pfSense - Mettre en œuvre un firewall Open source pour sécuriser votre réseau d'entreprise

OBJECTIFS :

- A l'issue de cette formation, l'apprenant sera capable d'installer, de configurer et d'exploiter le firewall pfSense

CONTENU :

1. FONDAMENTAUX

- Installation
- Configuration de base
- Authentification
- Gestion des certificats
- Sauvegarde/Restauration
- Mise à niveau / Migration

2. GESTION DU RESEAU

- Interface
- VLAN
- Routage

3. CONFIGURATION DU FIREWALL

- Règles de base
- Alias
- Bonnes pratiques
- Options avancées
- DMZ Principe du stockage chiffré
- La délégation de confiance

4. NAT

- Interaction avec les règles de Firewall
- Port Forward
- NAT 1 :1
- NAT Outbound

5. SERVICES

- Interaction DNS over TLS
- DHCP
- DNS forwarding

- DNS resolver
- Dynamic DNS
- Portail captif
- Filtrage Web : Squid
- Detection d'intrusion : Snort
- QoS (Traffic Shaper)
- NTP

6. VPN

- Présentation des possibilités
- Clients nomades : OpenVPN, IPsec
- Sites à Sites : OpenVPN et IPsec

7. MULTI WAN/LAN

- Policy Routing
- Configuration CARP
- Load balancing

8. ADMINISTRATION

- Gestion des logs
- Terminal et/ou interface web
- Commandes système
- Gestion de paquets
- Mise à jour, sauvegarde et restauration

PUBLIC CONCERNE : Administrateur réseau ayant besoin d'une solution Firewall évolutive

PRE-REQUIS : Bonnes connaissances du fonctionnement d'un pare-feu et sur Linux

MOYENS PEDAGOGIQUES:

- Pédagogie par l'expérience fondée sur l'interaction dans le groupe.
- Exercices pratiques à partir de mise en situation,

INTERVENANT(S) : Consultant en cybersécurité et IT

EVALUATION & ATTESTATION :

- L'évaluation des acquis se fait en fin de formation au travers d'un Quiz. Une évaluation de la formation est faite à chaud par le participant à l'issue de la formation.
- L'attestation de formation est remise à la fin de la formation

MODALITES PRATIQUES :

Durée de la formation : 2 jours
Lieu de formation : INTER / INTRA (à définir)
Support de formation remis à l'issue
Tarifs : Demander un devis
Conact : David TOUCHE au 87 30 41 25 ou **contact@tavita-cybersecurity.com**

SECURITE INFORMATIQUE

Sécuriser l'infrastructure informatique de votre entreprise

OBJECTIFS :

- Mettre en œuvre les outils et les moyens nécessaires pour intégrer et assurer le maintien en condition opérationnelle de l'infrastructure informatique
- Sécuriser le système d'information de l'entreprise
- Intégrer des solution Open source afin d'optimiser les couts liés à la cybersécurité

CONTENU :

1. INTRODUCTION A LA SECURITE INFORMATIQUE

- Le système d'information
- Les principes de la sécurité informatique
- Point de situation sur les cyber-Attaques

2. GESTION ET SECURISATION DU PARC INFORMATIQUE AVEC ACTIVE DIRECTORY

- Optez pour la virtualisation intégrée de Microsoft - Installation de Hyper-V
- Déploiement d'Active Directory
- Déploiement d'un serveur WSUS
- Sécurisation via des stratégies de groupe
- Mise à jour des stratégies de groupe
- Stratégie de mise à jour logiciels
- Déploiement d'un PKI
- Authentification LDAPS
- Configuration RADIUS
- Création de compte de service gMSA
- Sécurisation du protocole RDP
- Sécurisation des serveurs
- Sécurisation des postes clients (LAPS)
- Mise en place d'une solution de sauvegarde local et cloud

3. METTRE EN PLACE UNE SOLUTION DE SAUVEGARDE INTEGREE

- Préparation Installation de la fonctionnalité Windows Backup
- Configuration d'une sauvegarde avec Windows Backup
- Restauration

4. SECURISATION DU RESEAU

- Notions de cloisonnement (VLAN, DMZ)
- Préparation Philosophie d'un firewall (règles)

- Philosophie et apport d'une DMZ
- Éléments de cryptographie
- Principes de fonctionnement d'un VPN (Virtual Private Network)
- Architecture et apports des certificats
- Architecture et apports d'un serveur d'authentification (RADIUS)

5. DEPLOIEMENT D'UNE SOLUTION ANTIVIRALE CENTRALISEE (EDR)

- Déploiement de Kaspersky Security Center (KSC)
- Création d'une tache de déploiement
- Création d'une stratégie Kaspersky Endpoint Security (KES)
- Déploiement et gestion à distance de KES sur les postes
- Supervision de KSC

6. SECURISATION INTERNET

- Déploiement et configuration d'un pare-feu Pfsense
- Mise en place d'un portail captif avec authentification RADIUS
- Flitrage Web (Proxy)
- Gestion des logs internet

7. WIFI ET SECURITE

- Vocabulaire et concepts (SSIS, canal, Point d'accès, WEP, WPA, WPA2, EAP, etc)
- L'authentification auprès d'un serveur Radius
- L'intérêt d'isoler le Wifi dans un VLAN
- Gestion des BYOD au sein de l'entreprise (équipements personnels)

8. MISE EN PLACE D'UNE SOLUTION DE TELETRAVAIL SECURISEE

- Implémentation de OpenVPN avec authentification LDAPS, RADUIS et certificats
- Mise en place d'une charte de télétravail

9. MISE EN PLACE D'UN SAS ANTIVIRUS

- Préparation d'un poste sur un réseau dédié avec une solution AV différente de celle des postes clients en réseau

PUBLIC CONCERNE : Administrateurs réseaux et systèmes concernés par les problèmes de sécurité, chefs de projets informatiques, techniciens et correspondants informatiques.

PRE-REQUIS : Connaissances sur les fondamentaux sur les systèmes d'information (réseau, système et sécurité). Avoir déjà travaillé sur un pare-feu, et des connaissances sur les OS serveurs de Microsoft (AD)

MOYENS PEDAGOGIQUES:

- Pédagogie par l'expérience fondée sur l'interaction dans le groupe.
- Exercices pratiques à partir de mise en situation,

INTERVENANT(S) : Consultant en cybersécurité et IT

EVALUATION & ATTESTATION :

- L'évaluation des acquis se fait en fin de formation au travers d'un Quiz. Une évaluation de la formation est faite à chaud par le participant à l'issue de la formation.
- L'attestation de formation est remise à la fin de la formation

MODALITES PRATIQUES :

Durée de la formation : 4 jours

Lieu de formation : INTER / INTRA (à définir)

Support de formation remis à l'issue

Tarifs : Demander un devis

Conact : David TOUCHE au 87 30 41 25 ou **contact@tavita-cybersecurity.com**

SECURITE INFORMATIQUE

OPNsense – Les bases

OBJECTIFS :

- L'objectif de la formation est d'appréhender le logiciel OPNsense, savoir le prendre en main, le configurer et réaliser les tâches d'administration du quotidien.

CONTENU :

Présentation du logiciel OPNsense
Installation et dimensionnement d'un firewall pour OPNsense
L'ordre des traitements effectués par OPNsense
Les règles de base du filtrage
La gestion complète du NAT
La gestion des alias
La gestion des VLAN
La gestion de la priorisation de trafic et des limiters
La gestion des VPN
La gestion des certificats
La gestion des utilisateurs locaux
La gestion des mises à jour
La gestion des sauvegardes

PUBLIC CONCERNE : Administrateurs réseaux et systèmes concernés par les problèmes de sécurité, chefs de projets informatiques, techniciens et correspondants informatiques.

PRE-REQUIS : Connaissances sur les fondamentaux sur les systèmes d'information (réseau, système et sécurité). Avoir déjà travaillé sur un pare-feu

MOYENS PEDAGOGIQUES:

- Pédagogie par l'expérience fondée sur l'interaction dans le groupe.
- Exercices pratiques à partir de mise en situation,

INTERVENANT(S) : Consultant en cybersécurité et IT

EVALUATION & ATTESTATION :

- L'évaluation des acquis se fait en fin de formation au travers d'un Quiz. Une évaluation de la formation est faite à chaud par le participant à l'issue de la formation.
- L'attestation de formation est remise à la fin de la formation

MODALITES PRATIQUES :

Durée de la formation : 2 jours
Lieu de formation : salle de formation SAGEST à ARUE
Support de formation remis à l'issue
Tarifs : Demander un devis
Conact : David TOUCHE au 87 30 41 25 ou **contact@tavita-cybersecurity.com**

SECURITE INFORMATIQUE

OPNsense – Administration avancée

OBJECTIFS :

- L'objectif de la formation est d'approfondir le fonctionnement du logiciel OPNsense, savoir réaliser des tâches d'administration complexes et apprendre à diagnostiquer par soi-même les problèmes pouvant être rencontrés.

CONTENU :

Le multi-WAN avec OPNsense
La gestion des adresses IP virtuelles
Configurer un OPNsense en haute-disponibilité (cluster d'OPNsense)
Configurer un portail captif
Diagnostiquer son OPNsense
Les plugins additionnels
Monter un VPN natté (overlap network)
Mettre en place un filtrage applicatif avec un proxy
Connecter le proxy à Active Directory pour faire du SSO
Mettre en place de la double-authentification (2FA)
Configurer l'IDS / IPS

PUBLIC CONCERNE : Administrateurs réseaux et systèmes concernés par les problèmes de sécurité, chefs de projets informatiques, techniciens et correspondants informatiques.

PRE-REQUIS : Connaissances sur les fondamentaux sur les systèmes d'information (réseau, système et sécurité). Avoir déjà travaillé sur un pare-feu

MOYENS PEDAGOGIQUES:

- Pédagogie par l'expérience fondée sur l'interaction dans le groupe.
- Exercices pratiques à partir de mise en situation,

INTERVENANT(S) : Consultant en cybersécurité et IT

EVALUATION & ATTESTATION :

- L'évaluation des acquis se fait en fin de formation au travers d'un Quiz. Une évaluation de la formation est faite à chaud par le participant à l'issue de la formation.
- L'attestation de formation est remise à la fin de la formation

MODALITES PRATIQUES :

Durée de la formation : 2 jours
Lieu de formation : INTER / INTRA (à définir)
Support de formation remis à l'issue
Tarifs : Demander un devis
Conact : David TOUCHE au 87 30 41 25 ou **contact@tavita-cybersecurity.com**

GOUVERNANCE SSI

Rédiger votre politique de sécurité des systèmes d'information (PSSI)

OBJECTIFS :

- Appréhendez identifier les enjeux d'une politique de sécurité
- Rédiger le document de PSSI
- Implémenter durablement cette PSI au sein de votre entreprise.

CONTENU :

1. IDENTIFIER LES ENJEUX D'UNE POLITIQUE DE SECURITE POUR VOTRE ENTREPRISE

- Prenez conscience des menaces visant le système d'information
- Identifiez les enjeux et objectifs d'une PSSI
- Équipez-vous pour concevoir une PSSI

2. REDIGER LA PSSI DE VOTRE ENTREPRISE

- Donnez un cadre à votre démarche
- Faites le bilan des biens à protéger
- Identifiez les principaux risques et la stratégie de mitigation
- Choisissez les exigences et les mesures de sécurité
- Entraînez-vous à rédiger une partie de la politique de sécurité de votre entreprise

3. IMPLEMENTER DURABLEMENT LA PSSI AU SEIN DE VOTRE ENTREPRISE

- Mettez en œuvre la PSSI efficacement
- Adoptez une démarche d'amélioration continue de la PSSI
- Appréhendez la mise en place d'un SMSI

PUBLIC CONCERNE : RSSI, DSI, Chefs de projet SMSI, responsables de la gestion de la sécurité de l'information, conseillers experts, consultants

PRE-REQUIS : Connaissances sur les fondamentaux sur les systèmes d'information et la cybersécurité.

MOYENS PEDAGOGIQUES:

- Pédagogie par l'expérience fondée sur l'interaction dans le groupe.
- Exercices pratiques à partir de mise en situation,

INTERVENANT(S) : Consultant en cybersécurité et IT

EVALUATION & ATTESTATION :

- L'évaluation des acquis se fait en fin de formation au travers d'un Quiz. Une évaluation de la formation est faite à chaud par le participant à l'issue de la formation.
- L'attestation de formation est remise à la fin de la formation

MODALITES PRATIQUES :

Durée de la formation : 2 jours

Lieu de formation : INTER / INTRA (à définir)

Support de formation remis à l'issue

Tarifs : Demander un devis

Conact : David TOUCHE au 87 30 41 25 ou **contact@tavita-cybersecurity.com**

MICROSOFT OFFICE 365

Administration

OBJECTIFS :

- Installer Le centre d'administration de la plateforme Microsoft 365 permet de gérer les utilisateurs et les licences, de créer/administrer des boîtes aux lettres Exchange Online, de configurer/gérer les sites SharePoint, de manager des équipes Teams/OneDrive.
- Cette formation vous donnera la maîtrise du centre d'administration.
- À l'issue de la formation, le participant sera en mesure de :
  - Connaître les possibilités d'administration d'une plateforme Microsoft 365
  - Gérer des comptes, synchroniser un Active Directory
  - Gérer des boîtes aux lettres via Exchange Online
  - Administrer des sites SharePoint Online
  - Paramétrer les fonctions essentielles de Skype Entreprise Online
  - Administrer le travail collaboratif sous Teams et OneDrive

METHODE PEDAGOGIQUE :

30% de cours et 70% de pratique avec exercices
En distanciel ou présentiel

CONTENU :

1. INTRODUCTION A MIRCROSOFT 365

- Présentation de Microsoft 365. Scénarios d'hybridation possible.
- Architecture côté Cloud, côté client.
- Évaluation gratuite Microsoft 365.
- Introduction au PowerShell. Administrer à distance : Azure AD PowerShell.

2. GERER LES UTILISATEURS, LES GROUPES ET LES LICENCES

- Manipuler les utilisateurs et les groupes.
- Notion de rôles. Attribution de rôles.
- Authentification. Mots de passe. Licences.

3. SYNCHRONISATION AD

- Les outils : IDFix, AD Connect.
- Synchronisation d'AD avec Azure AD.
- Azure Rights Management. Synchroniser avec ADFS.

4. ADMINISTRATION DE BASE EXCHANGE ONLINE

- Présentation d'Exchange Online.
- Utilisateur de messagerie. Contacts de messagerie.
- Boîte aux lettres partagée.

- Boîte aux lettres de ressources.
- Administration déléguée
- Stratégies d'accès clients
- Anti-spam.
- Troubleshooting

5. ADMINISTRATION DE BASE SHAREPOINT

- Présentation de SharePoint Online.
- Collections de sites. Gérer les utilisateurs. Gérer les droits.
- Accès aux données de l'entreprise. Accès externe.
- Gérer le magasin de termes. Gérer la recherche.
- Troubleshooting

6. ADMINISTRATION DE SKYPE ENTREPRISE

- Présentation de Skype for Enterprise Online.
- Paramétrer les utilisateurs. Fédération de domaines.
- Conférences téléphoniques.
- Troubleshooting

7. ADMINISTRATION DE BASE TEAMS ET ONEDRIVE

- Présentation de Teams et OneDrive.
- Equipes. Ajout d'utilisateurs.
- Notion de canal, de réunion.
- Partager des fichiers. Travail collaboratif. Recherche.
- Paramètres d'administration.
- Troubleshooting

8. SECURITE ET SUIVI

- Comprendre l'environnement de suivi.
- Stratégies de rétention.
- Prévention de la perte de données. Recherche de contenu.
- Menaces. Audit. Rapports.

PUBLIC CONCERNE : Administrateurs systèmes, ingénieurs systèmes, exploitants et intégrateurs.

PRE-REQUIS : Connaissances de base d'administration Windows. Expérience des composants de Microsoft 365 en tant qu'utilisateur, notamment Exchange et SharePoint.

MOYENS PEDAGOGIQUES :

- Pédagogie par l'expérience fondée sur l'interaction dans le groupe.
- Exercices pratiques à partir de mise en situation,

INTERVENANT(S) : Consultant en cybersécurité et IT

EVALUATION & ATTESTATION :

- L'évaluation des acquis se fait en fin de formation au travers d'un Quiz. Une évaluation de la formation est faite à chaud par le participant à l'issue de la formation. L'attestation de formation sera remise à la fin de la formation

MODALITES PRATIQUES :

Durée de la formation : 4 jours

Lieu de formation : INTER / INTRA (à définir)

Support de formation remis à l'issue

Tarifs : Demander un devis

Conact : David TOUCHE au 87 30 41 25 ou **contact@tavita-cybersecurity.com**

MICROSOFT OFFICE 365

Decouverte et prise en main des outils collaboratifs (niveau utilsateur)

OBJECTIFS :

- Découverte l'interface du portail Office 365
- Utiliser le lanceur d'applications
- Ecrire et gérer des courriels dans Outlook Web App
- Configurer l'interface de Outlook Web App
- Planifier des rendez-vous ou des tâches dans le calendrier Online
- Découverte des fonctionnalités essentielles
- Utiliser Microsoft 365 et des documents via le Cloud OneDrive
- Utiliser les possibilités de partage et de coédition en temps réel avec Microsoft SharePoint
- Organiser des réunions dans Teams avec des collaborateurs distants
- Développer les fonctionnalités de Teams

CONTENU :

1. OUTLOOK WEB APP

- Différence entre Outlook 365 et Outlook Web App
- Personnaliser l'interface Office Web App
- Configurer une signature
- Partager un calendrier
- Gérer ses contacts
- Configurer les réponses automatiques
- Gérer les courriers indésirables
- Configurer le transfert de courrier

2. MICROSOFT TEAMS

- Créer et gérer une équipe (Membres, Paramètres, Canaux, Applications, Balises)
- Ajouter et gérer les onglets
- Planifier, modifier et gérer une réunion
- Gestion des options de réunion (transcription, fonds, caméra, microphone, enregistrements, partage de documents, partage d'écran)
- Participer à une réunion
- Gérer le OneDrive de l'équipe

3. ONDRIVE BUSINESS

- Se connecter à OneDrive
- Découvrir l'environnement OneDrive en ligne
- Stockage de documents et gestion de contenu
- Partage de documents et gestion des droits
- Coéditer à plusieurs sur un même document (collaboration)
- Synchroniser les documents avec votre PC

4. DECOUVERTE DES AUTRES OUTILS

- Kaizala
- SharePoint
- Forms
- Planner
- Delve
- OneNote
- Tableau blanc
- Sway
- To Do
- Yammer
- List
- Project
- Visio

PUBLIC CONCERNE : Tout public

PRE-REQUIS : Connaissances de base sur Office 365

MOYENS PEDAGOGIQUES :

- Pédagogie par l'expérience fondée sur l'interaction dans le groupe.
- Démonstration

EVALUATION & ATTESTATION :

- L'attestation de formation sera remise à la fin de la formation

MODALITES PRATIQUES :

Durée de la formation : 1 jour

Lieu de formation : INTER / INTRA (à définir)

Tarifs : Demander un devis (tarif de groupe possible)

Contact : David TOUCHE au 87 30 41 25 ou **contact@tavita-cybersecurity.com**

MICROSOFT OFFICE 365

Sharepoint utilisateur et contributeur

OBJECTIFS :

- Découverte l'interface du portail Office 365
- Utiliser le lanceur d'applications
- Utiliser les fonctionnalités collaboratives de sites SharePoint (Online) sur Office 365 (bibliothèques de documents et listes)
- Retrouver rapidement des documents avec les outils de recherche
- Distinguer les interactions entre SharePoint et Office.

CONTENU :

1. INTRODUCTION A SHAREPOINT

- Qu'est-ce que SharePoint ?
- Structure : collection de site, sites et pages
- Le champ d'action en tant qu'utilisateur et contributeur
- Menu d'accès rapide, rubans et barre de navigation
- Présentation des applications et du "contenu du site"
- Présentation des listes et bibliothèques

2. LES BIBLIOTHEQUES DE DOCUMENTS

- Créer un favori dans l'explorateur vers la bibliothèque
- Utilisation des rubans et du menu du document
- Ouvrir un document dans une application Office Online
- Coédition dans une application Office Online
- Charger un document dans une bibliothèque
- Créer un document avec une application Office Online
- Envoi d'un lien d'un document par mail
- Trier et filtrer
- Organisation par dossiers et/ou par métadonnées (propriétés)
- Renseigner les métadonnées / propriétés
- Notions sur l'extraction et l'archivage d'un fichier
- Gestion des versions principales d'un même document
- Créer des affichages personnels
- Le mode "modification rapide"
- Créer des alertes sur un document, sur la bibliothèque
- Supprimer / récupérer un document (corbeille)

3. SYCHRONISATION DE FICHIERS SHAREPOINT AVEC ONEDRIVE

- Configurer la synchronisation
- Modifier les paramètres de synchronisation
- Télécharger à l'aide de l'explorateur de fichiers

4. LES LISTES

- Ouvrir une liste
- Le menu de l'élément
- Utiliser le mode "modification rapide"
- Visualiser le contenu d'une liste dans Excel

5. RECHERCHE

- Utiliser la recherche intégrée à SharePoint
- Affinage de la recherche (filtres)

PUBLIC CONCERNE : Tout utilisateur souhaitant utiliser un Intranet ou des solutions métiers développées avec les technologies SharePoint.

PRE-REQUIS : Avoir une bonne connaissance de Windows et d'Office

MOYENS PEDAGOGIQUES :

- Pédagogie par l'expérience fondée sur l'interaction dans le groupe.
- Démonstration

EVALUATION & ATTESTATION :

- L'attestation de formation sera remise à la fin de la formation

MODALITES PRATIQUES :

Durée de la formation : 1 jour

Lieu de formation : INTER / INTRA (à définir)

Tarifs : Demander un devis (tarif de groupe (10) possible)

Contact : David TOUCHE au 87 30 41 25 ou **contact@tavita-cybersecurity.com**

MICROSOFT OFFICE 365

Administration Microsoft Intune

Gestion d'un parc informatique moderne

OBJECTIFS :

- Comprendre les principes de l'administration moderne avec Microsoft Endpoint Manager (Intune).
- Enrôler et gérer des postes de travail Windows 10/11, terminaux mobiles iOS/Android et macOS.
- Déployer et sécuriser des applications d'entreprise.
- Mettre en œuvre les stratégies de configuration et de conformité.
- Gérer les mises à jour Windows via Windows Update for Business.
- Superviser, diagnostiquer et reporter sur l'état du parc.
- Intégrer Intune dans un environnement hybride avec Active Directory / Azure AD / MECM (co-management).

CONTENU :

1. INTRODUCTION À MICROSOFT INTUNE ET ENDPOINT MANAGER

- Concepts de MDM (Mobile Device Management) et MAM (Mobile Application Management).
- Architecture et prérequis d'Intune.
- Intégration avec Azure Active Directory et Microsoft 365.
- Scénarios de gestion : 100% Cloud vs Hybride (co-management avec MECM).
- Licences et périmètre fonctionnel.

2. ENRÔLEMENT ET GESTION DES APPAREILS

- Méthodes d'enrôlement Windows 10/11 (Azure AD Join, Autopilot, Hybrid Join).
- Enrôlement des terminaux mobiles (Android Enterprise, iOS/iPadOS, macOS).
- Gestion des profils d'enregistrement.
- Stratégies de sécurité de l'enrôlement (MFA, restrictions).
- Supervision et cycle de vie des appareils.

3. STRATÉGIES DE CONFIGURATION ET DE CONFORMITÉ

- Configuration des paramètres de sécurité Windows 10/11 et mobiles.
- Déploiement de profils (Wi-Fi, VPN, certificats, email, restrictions).
- Politiques de conformité et gestion conditionnelle avec Azure AD (Conditional Access).
- Bonnes pratiques de sécurisation Zero Trust.

4. DEPLOIEMENT ET GESTION DES APPLICATIONS

- Méthodes de distribution : Store, MSI, Win32, MSIX, applications Web.
- Déploiement d'applications Office 365 et applications métiers.
- Gestion des applications mobiles (MAM sans enrôlement).

- Attribution, ciblage et suivi des installations.
- Supervision et diagnostic des déploiements.

5. MISES À JOUR WINDOWS ET SÉCURITÉ

- Introduction à Windows Update for Business (WUfB).
- Configuration des anneaux de mise à jour (rings).
- Plans de maintenance et stratégies différenciées.
- Sécurité avancée : intégration avec Defender for Endpoint.
- Surveillance et dépannage des mises à jour.

6. WINDOWS AUTOPILOT ET AUTOMATISATION DU PARC

- Principes de Windows Autopilot.
- Préparation et import des profils.
- Déploiement Zero Touch et self-deploying.
- Séquences d'intégration avec Intune et Azure AD.
- Automatisation via PowerShell et Graph API.

7. REPORTING, SURVEILLANCE ET MAINTENANCE

- Utilisation du centre d'administration Intune et Endpoint Manager.
- Rapports intégrés et requêtes personnalisées.
- Intégration avec Microsoft Defender et Log Analytics (Azure Monitor).
- Bonnes pratiques de supervision et de troubleshooting.
- Sécurité des rôles et délégation d'administration dans Intune.

PUBLIC CONCERNE : Administrateurs systèmes, ingénieurs IT, responsables de parc informatique souhaitant gérer efficacement postes clients Windows 10/11 et terminaux mobiles via Microsoft Intune et Endpoint Manager.

PRE-REQUIS : Bonne connaissance de l'environnement Windows 10/11 et notions d'Active Directory / Azure AD.

MOYENS PEDAGOGIQUES :

- Formation interactive avec démonstrations et mises en pratique sur un tenant Microsoft 365.
- Études de cas concrets basés sur des scénarios de production.
- Support numérique remis en fin de formation.

INTERVENANTS : Consultant expert en cybersécurité et systèmes Microsoft.

EVALUATION & ATTESTATION :

- Quiz de validation des acquis en fin de session.
- Évaluation de satisfaction à chaud.
- Attestation de formation remise au participant.

MODALITES PRATIQUES :
Durée de la formation : 3 jours
Lieu de formation : INTER / INTRA (à définir)
Tarifs : Demander un devis
Contact : David TOUCHE +689 87 304 125 / +33 6 99 63 17 11 ou **contact@tavita-cybersecurity.com**

RESEAUX INFORMATIQUES

Base des réseaux locaux (débutant)

OBJECTIFS :

- Initier aux bases des réseaux pour être en mesure de choisir les meilleures approches de dépannage en vous aidant du modèle OSI et de vous apporter les connaissances nécessaires pour paramétrer correctement un hôte dans un réseau d'entreprise.
- Décrire les différents éléments d'un réseau
- Comprendre les mécanismes de routage
- Maîtriser l'adressage IPv4
- Paramétrer la configuration IP d'un poste réseau (adresse, masque, passerelle)
- Connaitre les protocoles les plus couramment utilisés (DHCP, DNS, NTP, SMTP, etc…)

CONTENU :

1. INTRODUCTION

- Qu'est-ce qu'un réseau ?
- Les éléments d'un réseau (équipements finaux, intermédiaires, les médias réseau)
- Les besoins des utilisateurs (communiquer sur site, entre sites distants, avec l'extérieur).
- Les différents types de réseaux (LAN, WAN, WLAN, etc…)
- Les grands enjeux des réseaux

2. LE MODELE OSI

- OSI, vue d'ensemble

3. LES FONDAMENTAUX DU RESEAU

- L'introduction à TCP/IP
- Les fondamentaux des LANs Ethernet
- Les fondamentaux de l'adressage et du routage IPv4
- La notation CIDR
- Les réseaux privés
- Le NAT
- Plusieurs débits de 10 Mo à plusieurs Go (10/100 base T/Gigabit Ethernet)
- Le protocole IP. L'adressage et la configuration
- Principes des protocoles TCP et UDP
- La notion de port
- Le modèle client/serveur
- Les commandes utiles (ARP, IPCONFIG, PING, NETSTAT, TRACERT)

4. LES DIFFERENTS EQUIPEMENTS

- Les ponts et commutateurs (switch).
- Les routeurs, rôles et intérêt.
- Point d'accès Wifi
- Les types de raccordements
- Concept de passerelle.

5. LES PRINCIPAUX SERVICES ET PROTOCOLES DE HAUT NIVEAU

- Le serveur de nom DNS. Rôles et intérêt
- Notions de domaine : principes de fonctionnement
- Le serveur DHCP
- Partager des ressources via FTP et NTFS
- Les protocoles de messagerie SMTP, POP3 et IMAP4
- Le http, https, ftp, telnet, SSH

PUBLIC CONCERNE : Tout informaticien étant amené à installer et paramétrer un réseau local en environnement TCP/IP.

PRE-REQUIS : Aucun

MOYENS PEDAGOGIQUES :

- Pédagogie par l'expérience fondée sur l'interaction dans le groupe.
- Exercices pratiques à partir de mise en situation

EVALUATION & ATTESTATION :

- L'attestation de formation sera remise à la fin de la formation

MODALITES PRATIQUES :

Durée de la formation : 1 jour

Lieu de formation : INTER / INTRA (à définir)

Tarifs : Demander un devis

Contact : David TOUCHE au 87 30 41 25 ou **contact@tavita-cybersecurity.com**

RESEAUX INFORMATIQUES

Base des réseaux locaux (avancée)

OBJECTIFS :

- Initier aux bases des réseaux pour être en mesure de choisir les meilleures approches de dépannage en vous aidant du modèle OSI et de vous apporter les connaissances nécessaires pour paramétrer correctement un hôte dans un réseau d'entreprise.
- Décrire les différents éléments d'un réseau
- Distinguer et mettre en œuvre les mécanismes de routage
- Maîtriser l'adressage IPv4
- Paramétrer la configuration IP d'un poste réseau (adresse, masque, passerelle)
- Connaitre les protocoles les plus couramment utilisés (DHCP, DNS, NTP, SMTP, etc…)

CONTENU :

8. INTRODUCTION

- Qu'est-ce qu'un réseau ?
- Les éléments d'un réseau (équipements finaux, intermédiaires, les médias réseau)
- Les besoins des utilisateurs (communiquer sur site, entre sites distants, avec l'extérieur).
- Les différents types de réseaux (LAN, WAN, WLAN, etc…)
- Les grands enjeux des réseaux

9. LE MODELE OSI

- OSI, vue d'ensemble
- Les 7 couches OSI, intérêts
- OSI en pratique

10. LES FONDAMENTAUX DU RESEAU

- L'introduction à TCP/IP
- Les classes IPv4
- Les fondamentaux des LANs Ethernet
- Les fondamentaux de l'adressage et du routage IPv4
- La notation CIDR
- Les réseaux privés
- Le NAT
- Plusieurs débits de 10 Mo à plusieurs Go (10/100 base T/Gigabit Ethernet)
- Introduction aux réseaux sans fil (802.11x)
- Le protocole IP. L'adressage et la configuration
- Principes des protocoles TCP et UDP
- La notion de port
- Le modèle client/serveur
- Les commandes utiles (ARP, IPCONFIG, PING, NETSTAT, TRACERT)

Travaux pratiques :

- Calcul des adresses de sous-réseaux
- Mise en réseau de postes clients
- Les commandes

11. LES DIFFERENTS EQUIPEMENTS

- Les ponts et commutateurs (switch).
- Les routeurs, rôles et intérêt.
- Point d'accès Wifi
- Les types de raccordements
- Concept de passerelle.

Travaux pratiques

- Mise en réseau de postes clients – intérêt du switch
- Configuration d'une passerelle sur un poste client
- Configuration d'un routeur

12. LES PRINCIPAUX SERVICES ET PROTOCOLES DE HAUT NIVEAU

- Le serveur de nom DNS. Rôles et intérêt
- Notions de domaine : principes de fonctionnement
- Le serveur DHCP
- Partager des ressources via FTP et NTFS
- Les protocoles de messagerie SMTP, POP3 et IMAP4
- Le http, https, ftp, telnet, SSH
- La voix sur IP, introduction au protocole SIP

Travaux pratiques

- Exemple d'utilisation de FTP entre les postes de travail et le serveur FTP.
- Création d'un partage NTFS
- Capture et analyse des trames et paquets (Wireshark)
- Intégration des postes de travail en tant que client DNS et DHCP.

13. INTRODUCTION A LA SECURITE ET A L'ADMINISTRATION DES RESEAUX

- Notions fondamentales de la sécurité informatique.
- Les risques et les menaces.
- Le firewall et le VPN. Principes.
- Les sauvegardes (Backups)
- Le cloud computing
- Le stockage NAS/SAN
- Pourquoi l'administration est-elle indispensable ?
- L'utilité des logs

Travaux pratiques

- Configuration d'une règle de pare-feu
- Test de bon fonctionnement de la règle.

PUBLIC CONCERNE : Tout informaticien étant amené à installer et paramétrer un réseau local en environnement TCP/IP.

PRE-REQUIS : Aucun

MOYENS PEDAGOGIQUES :

- Pédagogie par l'expérience fondée sur l'interaction dans le groupe.
- Exercices pratiques à partir de mise en situation

EVALUATION & ATTESTATION :

- L'attestation de formation sera remise à la fin de la formation

MODALITES PRATIQUES :

Durée de la formation : 4 jours

Lieu de formation : INTER / INTRA (à définir)

Support de formation remis à l'issue

Tarifs : Demander un devis

Contact : David TOUCHE au 87 30 41 25 ou **contact@tavita-cybersecurity.com**