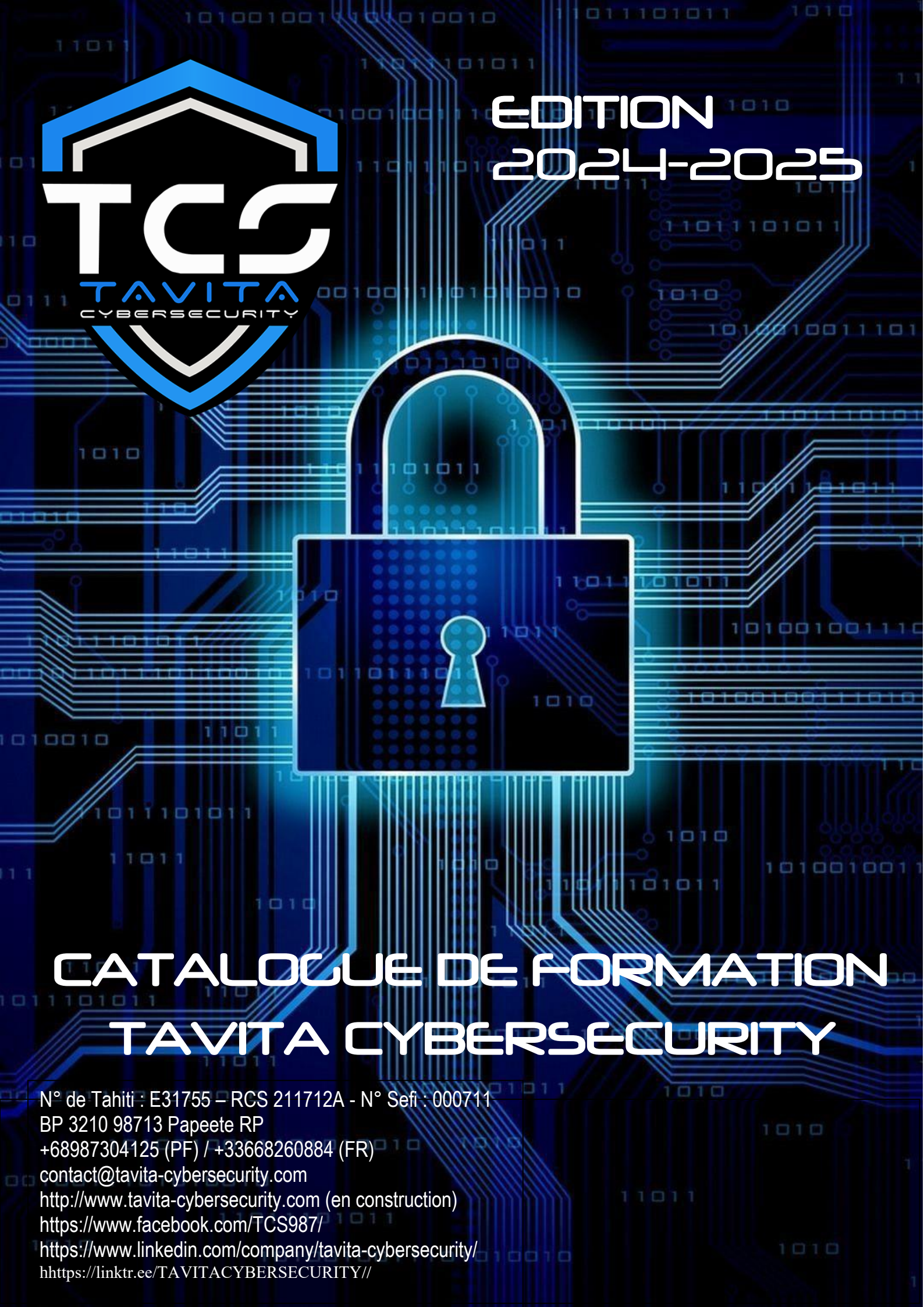

EDITION
2024-2025

CATALOGUE DE FORMATION
TAVITA CYBERSECURITY

N° de Tahiti : E31755 – RCS 211712A - N° Sefi : 000711
BP 3210 98713 Papeete RP
+68987304125 (PF) / +33668260884 (FR)
contact@tavita-cybersecurity.com
http://www.tavita-cybersecurity.com (en construction)
https://www.facebook.com/TCS987/
https://www.linkedin.com/company/tavita-cybersecurity/
hhttps://linktr.ee/TAVITACYBERSECURITY//

« Rester alerte, rester serein : la sécurité informatique se construit avec vous »

**« Qui connaît son ennemi et se connaît lui-même peut livrer cent batailles sans jamais être en péril.
Qui ne connaît pas l'autre mais se connaît lui-même, pour chaque victoire, connaîtra une défaite.
Qui ne connaît ni l'autre ni lui-même perdra inéluctablement toutes les batailles. »**

« Les cyberattaques sont comme des catastrophes naturelles. Il n'y a aucun moyen d'empêcher un ouragan de frapper votre ville, mais vous pouvez certainement vous y préparer »

« La sécurité informatique n'est pas une dépense, mais bien un investissement pour la survie de votre société »

Tavita Cybersecurity ?

La société dont la dénomination sociale : David TOUCHE - N° de TAHITI : E31755/001, est localisée à Papeete et évolue sous le nom commercial « Tavita Cybersecurity » (TCS) ayant le numéro RCS TPI 211712A.

Tavita Cybersecurity a été créée en juillet 2021 par David TOUCHE, ancien des Forces Armées à la retraite depuis septembre 2021, fort de 23 ans d'expérience au sein du ministère des Armées dans le domaine de la sécurité des systèmes d'informations et communications et diplômé d'un Master 2 Architecte système réseau et sécurité.

L'activité principale de Tavita Cybersecurity est de former et d'accompagner les entreprises et organismes dans leur effort de mise en conformité avec la réglementation et les règles de l'art en matière de cybersécurité en s'appuyant sur les préconisations des organismes de référence comme l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), le Center for Internet Security (CIS), le National Institute of Standards and Technology (NIST), des standards comme OWASP TOP10, et des Framework comme MITRE ATTACK, pour ne citer que ceux-là ; mais aussi sur les bonnes pratiques reconnues et appliquées aussi bien dans le domaine civil que militaire.

Son savoir-faire et ses compétences techniques et organisationnelles s'appuient non seulement sur son expérience, mais également sur des certifications reconnues.

À titre d'exemple :

TABLE DES MATIERES

SENSIBILISATION ET INITIATION A LA CYBERSECURITE

MODULE 1 - Notions de base

OBJECTIFS :

- Comprendre les motivations et le besoin de sécurité des systèmes d'information
- Connaitre les définitions de base et la typologie des menaces
- Sensibiliser les utilisateurs et les administrateurs d'un système d'informations aux problématiques de la sécurité informatique

CONTENU :

1. LES ENJEUX DE LA SECURITE DES SI

- Préambule
- Les enjeux
- Pourquoi les pirates s'intéressent aux S.I ?
- La nouvelle économie de la cybercriminalité
- Les impacts sur la vie privée
- Les infrastructures critiques
- Quelques exemples d'attaques

2. LES BESOINS DE SECURITE

- Introduction aux critères DIC
- Besoin de sécurité : « Preuve »
- Différences entre sureté et sécurité
- Exemple d'évaluation DICP
- Mécanisme de sécurité pour atteindre les besoins DICP

3. NOTIONS DE VULNERABILITE, MENACES, ATTAQUE

- Notion de « Vulnérabilité »
- Notion de « Menace »
- Notion d'« Attaque »
- Exemple de vulnérabilité lors de la conception d'une application
- Illustration d'un usage normal de l'application vulnérable
- Illustration de l'exploitation de la vulnérabilité présente dans l'application

4. PANORAMA DE QUELQUES MENACES

- Les sources potentielles de menaces
- Panorama de quelques menaces
- Hameçonnage & ingénierie sociale
- Déroulement d'une attaque avancée
- Violation d'accès non-autorisé
- Fraude interne
- Virus informatique

- Déni de service Distribué (DDoS)
- Illustration d'un réseau de botnets

5. LE DROIT DES T.I.C ET L'ORGANISATION DE LA SECURITE EN FRANCE

- L'organisation de la sécurité en France
- Le contexte juridique
- Le droit des T.I.C.
- La lutte contre la cybercriminalité en France
- Le rôle de la CNIL : La protection des données à caractère personnel

PUBLIC CONCERNE : tout public

PRE-REQUIS : aucun

MOYENS PEDAGOGIQUES :

- Pédagogie par l'expérience fondée sur l'interaction dans le groupe.
- Découverte et/ ou navigation sur les sites de référence.
- Exercices pratiques à partir de mise en situation,

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 : 4h

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**

SENSIBILISATION ET INITIATION A LA CYBERSECURITE

MODULE 2 - Règles d'hygiène informatique

OBJECTIFS :

- Appréhender et adopter les règles d'hygiène de base de la cybersécurité, pour les organisations et les individus

CONTENU :

1. CONNAITRE LE SYSTEME D'INFORMATION

- Identifier les composants du SI
- Inventorier les biens
- Types de réseau
- Interconnexion

2. MAITRISER LE RESEAU

- Sécuriser le réseau interne
- BYOD (Bring Your Own Device)
- Contrôler les échanges internes
- Protéger le réseau interne d'Internet
- Accès distant
- Sécuriser l'administration
- Wifi

3. SECURISER LES TERMINAUX

- Choisir les applications
- Mises à jour logicielles et systèmes
- Antivirus / Antimalware / Antispyware
- Symptômes de présence des codes malicieux
- Protéger les données
- Durcissement de configuration des équipements

4. GERER LES UTILISATEURS

- Attribution de privilèges
- Rôles utilisateur
- Mots de passe
- Autres méthodes d'authentification
- Sensibilisation des utilisateurs

- Spam
- Phishing / Spear phishing / Social engineering
- Réagir en tant que victime

5. SECURISER PHYSIQUEMENT

- Protection physique des locaux
- Imprimantes / Photocopieuses
- Sécuriser les équipements

6. CONTROLER LA SECURITE DU SI

- L'organisation de la sécurité en France
- Contrat/Maintenance/Professional Services
- Surveiller/Superviser
- Incidents de sécurité
- Plans de secours
- Audit

PUBLIC CONCERNE : tout public

PRE-REQUIS : Connaissances de base sur les systèmes d'information (biens, fonctionnement, etc.)

MOYENS PEDAGOGIQUES :

- Pédagogie par l'expérience fondée sur l'interaction dans le groupe.
- Découverte et/ ou navigation sur les sites de référence.
- Exercices pratiques à partir de mise en situation,

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 : 4h

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**

SENSIBILISATION ET INITIATION A LA CYBERSECURITE

MODULE 3 - Les aspects réseau et applicatifs

OBJECTIFS :

- Comprendre les vulnérabilités inhérentes aux mécanismes réseaux et applicatifs couramment utilisés.
- Connaitre le panorama des solutions techniques de sécurité

CONTENU :

1. LA SECURITE DU PROTOCOLE IP

- Préambule
- Exemple d'attaque par réflexion
- Exemples d'écoute de trafic
- Exemple de modification du routage des datagrammes IP
- Sécurisation du protocole IP

2. SECURISATION D'UN RESEAU

- Pare-feu
- Répartiteur de charge
- Anti-virus
- IDS et IPS
- VPN
- Segmentation
- Exemple pratique de sécurisation avec un réseau simple

3. LES BASES DE LA CRYPTOGRAPHIE

- Vocabulaire
- Un peu d'histoire
- Chiffrement symétrique
- Chiffrement asymétrique
- Chiffrement symétrique vs Chiffrement asymétrique
- Signature électronique
- Certificats électroniques
- Jetons cryptographiques

4. LA SECURITE DES APPLICATIONS WEB

- Usurpation d'identité via les cookies
- Injection SQL

PUBLIC CONCERNE : tout public

PRE-REQUIS :

- Connaissances de base sur les systèmes d'information (biens, fonctionnement, etc.)
- Connaissances de base sur le fonctionnement technique des réseaux, des systèmes d'exploitation et des applications

MOYENS PEDAGOGIQUES :

- Pédagogie par l'expérience fondée sur l'interaction dans le groupe.
- Découverte et/ ou navigation sur les sites de référence.
- Exercices pratiques à partir de mise en situation,

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 : 4h

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**

SENSIBILISATION ET INITIATION A LA CYBERSECURITE

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

OBJECTIFS :

- Appréhender les méthodes et normes de prise en compte de la sécurité :
  - de façon globale au sein d'une organisation dont l'activité est supportée par un système d'information
  - de façon plus unitaire au sein des projets, une activité étant gérée en mode projet
- Comprendre et anticiper les difficultés couramment rencontrées dans la gestion de la sécurité dans une organisation
- Présenter les filières métiers de la cybersécurité dans l'environnement d'exercice de leur fonction au sein des organisations

CONTENU :

1. INTEGRER LA SECURITE AU SEIN D'UNE ORGANISATION

- Préambule
- Panorama des normes ISO 2700x
- Système de Management de la Sécurité de l'Information (27001)
- Code de bonnes pratiques pour le management de la sécurité de l'information (27002)
- Gestion des risques (27005)
- Classification des informations
- Gestion des ressources humaines

2. INTEGRER LA SECURITE DANS LES PROJETS

- Préambule
- Sécurité dans l'ensemble du cycle de vie d'un projet
- Sécurité prise en compte en fin de développement
- Approche par l'analyse et le traitement du risque
- Plan d'action SSI

3. DIFFICULTES LIEES A LA PRISE EN COMPTE DE LA SECURITE

- Compréhension insuffisante des enjeux
- Implication nécessaire de la direction
- Difficulté pour faire des choix en toute confiance
- Délicat arbitrage entre commodité et sécurité
- Suivre l'évolution des technologies
- Frontières floues entre sphères professionnelle, publique, et privée

4. METIERS LIES A LA CYBERSECURITY

- Positionnement des métiers au sein des organisations
- Cartographie des métiers et compétence
- Profils et carrières
- Perspectives d'embauche

PUBLIC CONCERNE : tout public

PRE-REQUIS : Connaissances de base sur les systèmes d'information (biens, fonctionnement, etc.)

MOYENS PEDAGOGIQUES :

- Pédagogie par l'expérience fondée sur l'interaction dans le groupe.
- Découverte et/ ou navigation sur les sites de référence.
- Exercices pratiques à partir de mise en situation,

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 : 4h

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**

SENSIBILISATION ET INITIATION A LA CYBERSECURITE

MODULE 5 – Sécurisation Active Directory et ransomwares

OBJECTIFS :

- Comprendre les motivations et le besoin de sécurité des systèmes d'information
- Appréhender la notion de Ransomware et les bonnes pratiques pour se protéger.
- Sensibiliser les administrateurs d'un système d'informations aux bonnes pratiques de sécurisation Active Directory.

CONTENU :

1. LES ENJEUX DE LA SECURITE DES SI

- Les enjeux
- Pourquoi les pirates s'intéressent aux S.I ?
- La nouvelle économie de la cybercriminalité
- Les impacts sur la vie privée
- Quelques exemples d'attaques

2. LES RANSOMWARES

- Qu'est-ce qu'un ransomware ?
- Les vecteurs d'attaque
- Les principaux ransomwares
- Déroulement d'une attaque
- Réaction en cas d'infection
- Comment s'en prévenir ?
- Cas concret : Le ransomware MAKOP

3. SECURISATION ACTIVE DIRECTORY

- Qu'est que Active Directory ?
- Pourquoi protéger Active Directory ?
- Comment protéger AD ?
- Cinétique d'une attaque sur AD

4. BONNES PRATIQUES DANS UN ENVIRONEMENT ACTIVE DIRECTORY

- PKI
- LDAPS
- LAPS
- DNSSEC
- WSUS
- Gestion des ports d'écoute AD
- Corbeille AD
- Gestion des comptes de services (gMSA)
- Mise à niveau des GPO

- Stratégie de mots de passe affinés (PSO)
- Délégation de contrôle
- Sécurisation du protocole RDP
- DFS
- Outil de suivi de la matrice de droits d'accès aux partages
- Procédure de gestions des utilisateurs IN/OUT
- Gestion des mots de passe (Keepass, Dashlane)
- Guides de sécurisation

PUBLIC CONCERNE : Techniciens et administrateurs systèmes ou infrastructure

PRE-REQUIS : Connaissance de base sur Active Directory

MOYENS PEDAGOGIQUES :

- Pédagogie par l'expérience fondée sur l'interaction dans le groupe.
- Découverte et/ ou navigation sur les sites de référence.

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 : 4h

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**

SENSIBILISATION A LA CYBERSECURITE

Pour les acteurs SI

OBJECTIFS :

- Conflit Russie-Ukraine : état de la menace et mesures de vigilance cybersécurité
- Comprendre les motivations et le besoin de sécurité des systèmes d'information face à la situation géopolitique
- Comprendre les enjeux de demain et les tendance
- Connaitre les définitions de base et la typologie des menaces
- Sensibiliser les utilisateurs et les administrateurs d'un système d'informations aux problématiques de la sécurité informatique face aux nouvelles menaces.
- Connaitre les outils de gestion de la cybersécurité au sein de l'entreprise

CONTENU :

1. NOTIONS DE BASE DE LA CYBERSECURITE

- Préambule
- Les enjeux de la cybersécurité
- Les impacts de la cybercriminalité sur la vie privée
- Les impacts de la cybercriminalité sur les infrastructures critiques
- Notions de vulnérabilité
- Notion de menace
- Notions de cyberattaque
- Notion de violation/fuite de données
- Quelques exemples d'attaques

2. PANORAMA DE LA CYBERCRIMINALITE

- Quelques chiffres
- Qu'en est-il sur la Polynésie Française ?
- Typologie de la menace
- Ecosystème du cybercrime
- Organisation des cyber-gangs
- Top 15 des cybermenaces
- L'arnaque au président (FOVI)
- Les données personnelles – la controverse d'un business en pleine expansion

3. FOCUS RANCONGICIEL

- Qu'est-ce qu'un ransomware ?
- Les vecteurs d'attaques
- Mode opératoire
- Impacts
- Doit-on payer la rançon ?

4. RETOUR SUR UNE CYBERATTAQUE SUR UNE ENTREPRISE POLYNESIENNE

- Attaque par ransomware - contexte
- Attaque par ransomware - Déclenchement de la cyberattaque
- Attaque par ransomware – Pourquoi ?
- Attaque par ransomware – Que s'est-il passé ?
- Attaque par ransomware - Conséquences
- Attaque par ransomware – Erreurs commises
- Attaque par ransomware – Investigations forensiques
- Attaque par ransomware – Retour au calme (PCA/PRA)

5. QUE FAIRE EN CAS DE CYBERATTAQUE ?

- Premiers réflexes
- Piloter la crise
- Sortir de la crise

6. LES BONNES PRATIQUES D'HYGIENE INFORMATIQUE

- Gestion des mots de passe
- Gestion des identités
- Sécurisation des réseaux Wifi
- Politique de mise à jour
- Gestion des accès
- Gestion des appareils mobiles
- Sécurité des communications
- Gestion des sauvegardes
- Sécurisation des accès distants
- La cyber assurance

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

- Intégrer la sécurité au sein de la sécurité
- Panorama des normes ISO 27K
- Intégrer la sécurité dans les projets
- Difficultés liées à la prise en compte de la sécurité
- Le système de management de la sécurité des SI (SMSI)

PUBLIC CONCERNE : Tout professionnel occupant la fonction de DSI, de RSSI, de chef de projet, d'administrateur système et réseau, ou de techniciens voués participer la mise en conformité CYBER ou acteur de la gouvernance SSI de leur entreprise.

PRE-REQUIS : Avoir des notions en matière de cybersécurité ou personnel souhaitant acquérir les bonnes pratiques d'hygiène informatique pour faire face aux nouveaux enjeux.

MOYENS PEDAGOGIQUES :

- Pédagogie par l'expérience fondée sur l'interaction dans le groupe.
- Découverte et/ ou navigation sur les sites de référence.

EVALUATION & ATTESTATION :

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

MODALITES PRATIQUES :

Durée de la formation : 4h

Lieu de formation : INTER / INTRA (à définir)

Support de formation remis à l'issue

Tarifs : Demander un devis (tarif de groupe possible)

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

SENSIBILISATION A LA CYBERSECURITE

Tout public

OBJECTIFS :

- Connaitre les définitions de base et la typologie des menaces
- Sensibiliser les utilisateurs d'un système d'informations aux problématiques de la sécurité informatique face aux nouvelles menaces.
- Acquérir les bonnes pratiques d'hygiène informatique pour limiter le risque cyber

CONTENU :

1. NOTIONS DE BASE DE LA CYBERSECURITE

- Préambule
- Qu'est-ce-que la cybersécurité et sécurité informatique (différence) ?
- Les enjeux de la cybersécurité
- Notions de cyberespace
- Notion de vulnérabilité
- Notion de menace
- Qu'est-ce-qu'un hacker ?
- Notion de violation/fuite de données
- Les virus et malwares
- Les différents types de cyberattaque
- Le phishing – hameçonnage
- Quelques exemples de cyberattaques et ses conséquences
- Focus sur les ransomwares (rançongiciels)

2. PANORAMA DE LA CYBERCRIMINALITE

- Qu'en est-il sur la Polynésie Française ?
- Quelques chiffres en France
- Typologie de la menace
- Ecosystème du cybercrime
- Organisation des cyber-gangs
- Les données personnelles – la controverse d'un business en pleine expansion

3. QUE FAIRE EN CAS DE CYBERATTAQUE/ESCROQUERIE ?

- Premiers réflexes

4. LES BONNES PRATIQUES DU SALARIE POUR LIMITER LE CYBERISQUE

- Les règles de base
- La gestion des mots de passe
- Sécurité de son adresse électronique
- Gestion sécurisée des courriels professionnels
- Aide à la suppression des traces sur internet
- L'authentification multi facteur (MFA)

- Les objets connectés (IoT)
- Sécurité lors des déplacements professionnels
- Liens utiles – déclaration incident
- Conclusion

PUBLIC CONCERNE : Tout public, pour les salariés et collaborateur amenés à utiliser l'outil informatique.

PRE-REQUIS : Aucun

MOYENS PEDAGOGIQUES :

- Pédagogie par l'expérience fondée sur l'interaction dans le groupe.
- Découverte et/ ou navigation sur les sites de référence.

EVALUATION & ATTESTATION :

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

MODALITES PRATIQUES :

Durée de la formation : 4h

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 WINDOWS SERVER 2019/2022

Administation

OBJECTIFS :

- Appréhender les nouveautés de Windows Serveur 2019
- Installer Windows Serveur 2019 dans ses différentes déclinaisons
- Utiliser Windows Admin Center
- Installer et déployer Active Directory
- Mettre en œuvre ReFS

CONTENU :

1. ARCHITECTURE ET INSTALLATION

- Introduction à Windows Server 2019.
- Panorama des nouveautés.
- Les nouveautés de l'interface Windows Server 2019.
- Les modes d'installation de Windows Server 2019.
- Installation de Windows Server 2019.

2. OUTILS D'ADMINISTRATION ET CONFIGURATION

- Administrer votre environnement avec le gestionnaire de serveur.
- Déploiement et utilisation du Windows Admin Center (WAC).
- Présentation et utilisation des modules Windows System Insights.
- Les adhérences et interconnexions Azure.
- Les nouveautés de RDS.

3. ACTIVE DIRECTORY

- Les silos et stratégies d'authentification.
- La gestion des objets en PowerShell.
- Les prérequis à l'installation.
- L'installation de l'Active Directory.
- Les nouvelles interfaces de gestion des objets.
- Le centre de gestion d'administration Active Directory (ADAC).
- Les comptes de services administrés.
- La gestion des accès privilégiés (PAM).

4. DISQUES ET SYSTEMES DE FICHIERS

- Storage Migration Services.
- Le système de fichiers ReFS (Resilient File System).
- Configurer les espaces de stockage dans Windows Server 2019.
- Windows Defender Malware Protection.
- La sécurité des fichiers et des dossiers.

5. OPTIMISATION, PERFORMANCE ET DEPANNAGE

- Windows Defender Advanced Threat Protection.
- Les moniteurs de performances.
- Les outils de récupération.
- Les sauvegardes et restaurations du système.

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

PRE-REQUIS : Bonnes connaissances de la gestion de postes Windows (10, 8 ou 7) en réseau.

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**

MICROSOFT WINDOWS SERVER 2019/2022

Initiation à l'administration de Active Directory

OBJECTIFS :

- Appréhender l'administration de Windows Serveur 2019/2022
- Installer et déployer Active Directory

CONTENU :

1. ARCHITECTURE ET INSTALLATION

- Introduction à Windows Server
- Installation de Windows Server 2019/2022.

2. ACTIVE DIRECTORY

- Les prérequis à l'installation.
- L'installation de l'Active Directory.
- Le centre de gestion d'administration Active Directory (ADAC).

3. COMPTES UTILISATEURS ET GROUPES

- Administrer votre AD
- Comptes et groupes locaux, profils utilisateurs
- Les stratégies de groupe
- Le principe de fonctionnement
- Le magasin central
- Les héritages, blocages et filtrages
- Création des objets avec PowerShell

4. INFRASTRUCTURE ET SERVICES RESEAUX

- La création des zones et d'enregistrement DNS
- Joindre un ordinateur au domaine

5. SECURITE ACTIVE DIRECTORY

- Stratégie de mot de passe (PSO)
- Activation et gestion de la corbeille AD
- Journalisation
- Gestion et mise à niveau des stratégies de groupe
- Mise en œuvre de LAPS
- Mise en œuvre de rôles sur Server Core
- Paramétrage du pare-feu avec fonctionnalités avancées
- Quelques GPO de durcissement contre les attaques AD

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

PRE-REQUIS : Bonnes connaissances sur 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 sous forme de travaux pratiques

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 WINDOWS SERVER 2019/2022

Installation, configuration et administration avancée

OBJECTIFS :

- Installer Windows server 2019 ou mettre à niveau une version précédente infrastructure Connaître les différentes options disponibles pour la gestion du stockage et identifier la solution la plus adaptée à vos besoins
- Installer et configurer le système de virtualisation Hyper-V
- Savoir planifier, créer et gérer un cluster de basculement
- Comprendre comment sécuriser l'infrastructure
- Apprendre à utiliser Windows Server 2019 comme plate-forme applicative

CONTENU :

1. INTRODUCTION

- Préparation et installation des différents modes GUI, CORE, Nano Server
- Modèles d'activation de Windows Server
- Panorama des nouveautés
- Les nouveautés de l'interface Windows Server 2019
- L'installation
- Les rôles en session locale ou distante

2. DISQUES, PARTAGES ET SYSTEME DE FICHIERS

- Le système de fichiers ReFS (Resilient File System)
- La disponibilité du système de fichier
- Configurer les espaces de stockage dans Windows Server 2019
- Vue d'ensemble du contrôle d'accès dynamique (DAC)
- L'espace disques dynamiques
- Windows Defender Malware Protection
- La sécurité des fichiers et des dossiers
- Storage Migration Services
- La protection de données
- Rappel sur les fondamentaux de la sécurité NTFS, ReFS
- Mise en place d'EFS, limites d'EFS
- BitLocker : cryptage du disque et stockage de la clé de cryptage
- Le contrôle d'accès dynamique
- Vue d'ensemble du DAC et des revendications
- Principes des règles, stratégies d'accès centralisés
- Le gestionnaire de ressources FSRM, les autorisations
- Bonnes pratiques

3. COMPTES UTILISATEURS ET GROUPES

- Administrer votre AD avec Windows Admin Center
- Présentation d'Active Directory, ADAC
- Comptes et groupes locaux, profils utilisateurs
- Création des objets avec PowerShell
- Les stratégies de groupe
- Le principe de fonctionnement
- Le magasin central
- Le filtrage WMI
- Les héritages, blocages et filtrages
- Azure Active Directory
- Configuration de l'application et l'accès aux ressources avec Azure AD
- L'extension sur site de domaine Active Directory pour Azure
- Outils disponibles (AD Connect, FIM...)

4. MICROSOFT ET HYPER-V 2019

- Failover Clustering
- Hyper-V Replica

5. CLUSTERING ET HAUTE DISPONIBILITE

- Les nouveautés en haute disponibilité et clusters
- Sauvegarde et restauration Windows Server 2019

6. INFRASTRUCTURE ET SERVICES RESEAUX

- DNS, DHCP et DHCP Failover
- Mise en oeuvre de l'IPAM
- DHCP et DHCP Failover, DNS et DNS Secure
- Les serveurs et les protocoles IPv4
- Le gestionnaire d'adresse IP
- Gestion du réseau avec PowerShell
- La création des zones et d'enregistrement DNS avec PowerShell
- Optimisation de la bande passante avec le NIC Teaming

7. PLATE-FORME D'APPLICATIONS

- Les nouveautés applicatives
- Les conteneurs et leurs améliorations
- Bonnes pratiques

PUBLIC CONCERNE : Toute personne disposant de compétences Windows Server intéressée par la mise en œuvre de la version 2019 et 2022

PRE-REQUIS : Avoir une expérience en administration Windows Server.

Avoir suivi la formation Windows Server 2019/2022 – Initiation et découverte des services essentiels

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 WINDOWS SERVER 2019/2022

Mise en œuvre et gestion avancée des services active directory

OBJECTIFS :

- Installer et configurer des contrôleurs de domaine
- Implémenter Active Directory dans des environnements complexes
- Implémenter des stratégies de groupe
- Déployer des autorités de certification Active Directory
- Synchroniser Azure Active Directory avec votre Active Directory sur site
- Surveiller, dépanner et établir le service de continuité pour les services AD

CONTENU :

1. INSTALLER ET CONFIGURER DES CONTROLEURS DE DOMAINE

- Vue d'ensemble d'Active Directory
- Vue d'ensemble des contrôleurs de domaine
- Déployer des contrôleurs de domaine
- Déployer Windows Admin Center

2. GESTION DES OBJETS ACTIVE DIRCTORY

- Gérer les comptes utilisateurs
- Gérer les groupes dans Active Directory
- Gérer les objets ordinateurs dans Active Directory
- Utiliser Windows PowerShell pour administrer Active Directory
- Implémenter et gérer les Unités d'Organisation

3. ADMINISTRATION AVANCEE D'UNE INFRASTRUCTURE ACTIVE DIRECTORY

- Vue d'ensemble de déploiements avancés d'infrastructure Active Directory
- Déployer Active Directory dans un environnement distribué
- Configurer des relations d'approbation Active Directory

4. MISE EN ŒUVRE DES SITES AD DS ET DE LA REPLICATION

- Présentation de la réplication AD DS
- Configurer des sites AD DS
- Configuration et surveillance de la réplication AD DS

5. MISE EN ŒUVRE DE L'INFRASTRUCTURE DE STRATEGIE DE GROUPE

- Introduction aux stratégies de groupe
- Mettre en œuvre et administrer les stratégies de groupe
- Gérer l'étendue et le traitement des stratégies de groupe

- Dépanner des stratégies de groupe

6. GERER LES PARAMETRES UTILISATEURS AVEC LES STRATEGIES DE GROUPE

- Mettre en œuvre les modèles d'administration
- Configurer les redirections de dossiers, les installations de logiciels et les scripts
- Configurer les préférences de stratégie de groupe Configurer le Branch Cache dans Windows Server 2019

7. SECURISATION DES SERVICES DE DOMAINES ACTIVE DIRECTORY

- Sécuriser les contrôleurs de domaine
- Sécuriser les comptes utilisateurs
- Audit des authentifications
- Configurer des comptes de services managés

8. DEPLOIEMENT ET GESTION DES SERVICES DE CERTIFICATS ACTIVE DIRECTORY

- Déployer AD CS
- Administrer AD CS
- Dépannage et maintenance d'AD CS

9. DEPLOIEMENT ET GESTION DES CERTIFICATS

- Déployer et gérer les modèles de certificats
- Gérer le déploiement des certificats, la révocation et la récupération
- Utiliser les certificats dans un environnement de travail
- Mettre en œuvre et gérer les cartes à puce

10. MISE EN ŒUVRE DE LA SYNCHRONISATION AD ET AZURE AD

- Planifier et préparer la synchronisation d'annuaires
- Implémenter la synchronisation d'annuaire en utilisant Azure AD Connect
- Gérer les identités avec la synchronisation d'annuaire

11. SURVEILLANCE, GESTION ET RECUPERATION DE ACTIVE DIRECTORY DOMAIN SERVICES

- Surveiller AD DS
- Gérer la base de données AD DS
- Sauvegarde et restauration AD DS

PUBLIC CONCERNE : Administrateurs Active Directory souhaitant mettre à jour leurs connaissances sur les services de domaine Active Directory. Administrateurs souhaitant mettre en œuvre une infrastructure Active Directory dans un environnement d'entreprise.

PRE-REQUIS : Connaissances de base des services de domaine Active Directory

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 : 3 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 WINDOWS SERVER 2019/2022

Sécuriser votre infrastructure active directory

OBJECTIFS :

- Acquérir des connaissances et compétences pour concevoir et configurer une infrastructure sécurisée sous Windows Server 2019/2022.
- Connaître les principales méthodes de sécurisation d'un parc Windows Server
- Connaitre les bonnes pratiques de durcissement de la sécurité du moment.

CONTENU :

1. LA SECURITE DANS SON ENSEMBLE

- Les différents types et niveaux de vulnérabilité
- Les différents types de risques
- Les impacts de l'approche sécurité dans un système information
- Nécessité de durcissement
- Les techniques de persistance AD

2. MISE EN PLACE D'UNE PKI (Public Key Infrastructure)

- Présentation et déploiement d'une PKI
- Configuration et suivi d'une PKI avec AD CS (Active Directory Certificate Services)
- Modèle de certificats
- Configuration de la révocation (OCSP)
- Sécurisation HTTPS d'un serveur Web
- Activation de LDAPS

3. SECURISATION D'ACTIVE DIRECTORY (AD)

- Stratégie d'authentification via ADAC
- Mise en place et configuration RODC (Read Only Domain Controller)
- Stratégie de mot de passe (PSO)
- Activation et gestion de la corbeille AD
- Activation DNSSEC
- Journalisation
- Gestion et mise à niveau des stratégies de groupe
- Mise en œuvre de LAPS
- Mise en œuvre de rôles sur Server Core et Server Nano
- Utilisation des outils d'analyse tels que Security Assessment

4. SECURISATION DU SERVEUR DE FICHIERS – PROTECTION CONTRE LES RANSOMWARES

- La méthode AGDLP
- Configuration des notifications

- Configuration du groupe d'extension de fichiers
- Configuration du modèle de filtre des fichiers
- Configuration du contrôle d'accès dynamique (DAC)
- Activer l'énumération basée sur l'accès EBA

5. SECURISATION DE L'ARCHITECTURE

- Configuration et mise en œuvre de BitLocker au niveau du parc et stratégies de récupération
- Mise en place d'EFS (Encrypting File System) et récupérations
- Paramétrage du pare-feu avec fonctionnalités avancées

6. DURCISSEMENT D'ACTIVE DIRECTORY

- Configuration Net Session Enumeration (BloodHound – Block Netcase)
- Configuration SSL v3 pour les contrôleurs de domaine
- Configuration LLMNR (Local Link Multicast Name Resolution)
- Configuration NTLMv1 et LM (Durcissement Kerberoasting)
- Configuration PrintNightmare
- Sécurisation service Spooler d'impression pour les serveurs
- SMBv2
- Audit sur le pare-feu Windows
- Configuration du cycle de rafraichissement des GPO
- Configuration priorité à IPv4
- Sécuriser PowerShell
- Restriction accès Internet pour un serveur
- BitLocker via la puce TPM
- Installation et application des stratégies :
    - SCM - Pass the hash (LSA protection) + Audit
    - MSS Legacy
    - MS Guide
- Restreindre l'énumération AD (SAM-R)
- Credential Guard
- Device Guard
- Déploiement de Microsoft Security Compliance Toolkit 1.0

7. SECURISATION DE L'ADMINISTRATION DU DOMAINE

- Architecture N-Tier
- Durcissement du service d'identité, gestions des silos
- WinRM (Windows Remote Management)
- WMI (Windows Management Instrumentation)
- RDP (administrateur restreint) - Changement de port
- Sécurité des services et comptes de services managés (MSA)
- Réduction de la surface d'attaque (désactivation des ports inutiles)
- Analyse des protocoles actifs sur le domaine (Netstat et Wireshark)
- Mise en œuvre de PowerShell Just Enough Administration (JEA),

8. APPLICATIONS DES CORRECTIFS DE SECURITE

- Configuration d'un serveur de mises à jour
- Stratégie de déploiement des mises à jour
- Gestion des rapports
- Maintenance et optimisation

PUBLIC CONCERNE : Toutes les personnes impliquées dans la sécurité du système d'information

PRE-REQUIS : Avoir une expérience en administration Windows Server

MOYENS PEDAGOGIQUES :

- Pédagogie par l'expérience fondée sur l'interaction dans le groupe.
- Guides de sécurisation (ANSSI, CIS, Microsoft Security Compliance Toolkit, etc…)
- Navigation sur les sites de référence
- Exercices pratiques à partir de mise en situation,

INTERVENANT(S) : Consultant en cybersécurité

EVALUATION & ATTESTATION :

- Une évaluation de la formation est faite à chaud par le participant tout au long 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 WINDOWS SERVER 2019/2022

Hyper-V Installation, stockage et virtualisation

OBJECTIFS :

- Cette formation permet d'acquérir les compétences et connaissance nécessaires pour gérer le stockage et la virtualisation avec Windows Server 2016 2019 ou 2022 et comprendre les scénarios, les besoins et le stockage disponibles et applicables

CONTENU :

1. INTRODUCTION

- Virtualisation : historique et intérêts
- Types de virtualisation, hyperviseurs
- Architecture globale de Windows Server 2019
- Windows Server Hyper-V Core et Nano Core
- Hyper V : concepts, OS invités pris en charge, gestion des licences

2. CONFIGURATION DU STOCKAGE LOCAL

- Gérer les disques dans Windows Server 2019
- Gérer les volumes dans Windows Server 2019

3. MISE EN ŒUVRE DES ESPACES DE STOCKAGE ET DE LA DEDUPLICATIONS DE DONNEES

- Mettre en œuvre des espaces de stockage
- Gérer les espaces de stockage
- Mettre en œuvre la déduplication de données

4. INSTALLATION ET CONFIGURATION DE HYPER-V ET DES MACHINES VIRTUELLES

- Prérequis matériels et logiciels pour l'installation d'Hyper-V
- Vue d'ensemble de Hyper-V
- Installer Hyper-V
- Configurer le stockage sur les serveurs hôtes Hyper-V
- Configurer le réseau sur les serveurs hôtes Hyper-V
- Configurer les machines virtuelles Hyper-V
- Gérer les machines virtuelles Hyper-V

5. DEPLOIEMENT ET GESTION DE WINDOWS SERVER ET DE CONTENEURS HYPER-V

- Vue d'ensemble des conteneurs dans Windows Server 2019
- Déployer Windows Server et les conteneurs Hyper-V
- Installer, configurer et gérer les conteneurs

6. VUE D'ENSEMBLE DE LA HAUTE DISPONIBILITE ET DE LA RECUPERATION D'URGENCE

- Définir les niveaux de la disponibilité
- Planifier la haute disponibilité et les solutions de récupération d'urgence avec les machines virtuelles Hyper-V
- Sauvegarder et restaurer Windows Server 2019 et les données avec Windows Server Backup
- Haute Disponibilité avec le clustering de basculement dans Windows Server 2019
- Mise en œuvre de la réplication entre 2 hôtes

7. MISE EN ŒUVRE ET GESTION DES CLUSTERS DE BASCULEMENT

- Planifier la mise en place d'un cluster
- Créer et configurer un nouveau cluster
- Maintenir un cluster
- Dépanner un cluster
- Mettre en œuvre la haute disponibilité d'un site avec un cluster étendu

8. MISE EN ŒUVRE DU CLUSTER DE BASCULEMENT POUR LES MACHINES VIRTUELLES HYPER-V

- Vue d'ensemble de l'intégration de Hyper-V dans Windows Server 2019 avec le cluster
- Mettre en œuvre et maintenir les machines virtuelles Hyper-V sur les clusters
- Fonctionnalités clés pour les machines virtuelles dans un environnement de cluster

9. MISE EN ŒUVRE DE LA REPARTITION DE CHARGES RESEAU

- Vue d'ensemble des clusters NLB
- Configurer un cluster NLB
- Planifier la mise en œuvre NLB

10. POWERSHELL POUR HYPER-V

- Présentation de powershell
- Voir les scripts pour Hyper-V

PUBLIC CONCERNE : Cette formation s'adresse aux administrateurs Windows Server et aux professionnels IT

PRE-REQUIS : Avoir une bonne expérience en administration Windows Server 2012

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 : 3 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 WINDOWS SERVER 2019/2022

Mise en œuvre du service de certificats

OBJECTIFS :

- Améliorer la sécurité dans une infrastructure Active Directory
- Déployer une autorité de certification, générer des certificats et mettre en œuvre une authentification forte par certificat X509

CONTENU :

1. INTRODUCTION AU CHIFFREMENT – LA CRYPOGRAPHIE

- Chiffrement symétrique
- Principaux algorithmes à clé symétrique
- Chiffrement asymétrique
- Exemple simplifié d'usage de la confidentialité en HTTPS
- Fonction de hachage
- Signature numérique
- Attaque "Man in the middle"
- Signature électronique et authentification.

2. INTRODUCTION AUX SYSTEMES D'INFRASTRUCTURE A CLES PUBLIQUES

- Vue d'ensemble des PKI
- Le certificat X.509
- L'Autorité de Certification
- Autorité d'enregistrement (RA).
- Le protocole LDAPS
- La liste de révocation
- Les bonnes pratiques et les bonnes typologies
- Règles et recommandations générales des clés

3. MISE EN ŒUVRE D'UNE PKI

- Gérer une PKI dans une infrastructure complexe
- Configurer un template de certificat
- Configurer "Certificate Enrollment"
- Archiver et récupérer un certificat
- Génération de certificats utilisateurs et serveurs
- Configuration entre deux organisations
- Déploiement de carte à puce
- Intégrer la PKI
- Services SSL
- Scripts Powershell de l'entreprise
- Technologies VPN de l'entreprise
- Technologies IPsec de l'entreprise
- Protocole de vérification en ligne de certificats (OCSP)

- Système EFS et agents de recouvrement
- Principe du stockage chiffré
- La délégation de confiance

PUBLIC CONCERNE : Techniciens et administrateurs systèmes ou infrastructure

PRE-REQUIS : Bonnes connaissances de l'administration de Windows server

MOYENS PEDAGOGIQUES:

- Pédagogie par l'expérience fondée sur l'interaction dans le groupe.
- Guides de sécurisation (ANSSI, CIS, etc…)
- 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 WINDOWS SERVER 2019/2022

Configuration et gestion du service de mise à jour WSUS

OBJECTIFS :

- Appréhendez la gestion de la distribution de logiciels et les mises à jour avec WSUS 5.0 sous systèmes Windows Server 2019 et 2022.
- Grace à ce stage, Vous apprendrez à installer et configurer WSUS, effectuer les tâches d'administration courantes, planifier les mises à jour et appliquer les corrections de sécurité.

CONTENU :

1. ARCHITECTURE ET INSTALLATION

- Les mises à jour Microsoft.
- Vue globale du projet de déploiement.
- La mise en place de WSUS 4.0 au sein du projet.
- Les types d'installation complète ou console.
- Le service Windows Server Update Services (WSUS).
- La base de données interne et distante SQL.

2. MAITRISER L'ADMINISTRATION DE BASE

- La gestion de l'administration WSUS 4.0.
- La console d'administration, la connexion.
- La configuration des équipements réseau.
- Les commandes WSUSUTIL, WUAUCLT.
- Interaction avec Active Directory.
- Stratégies de groupes pour Windows Update.
- Le mode autonome, le mode serveur déconnecté.

3. METTRE EN PLACE LA SECURITE

- Mise en place du serveur WSUS Réplica et WSUS autonome.
- La sécurité du transfert de métadonnées.
- La sauvegarde et la restauration.
- Paramétrage du protocole SSL entre le serveur et les clients WSUS.
- L'approbation des correctifs, ses rapports associés.
- Création, exportation du certificat racine de l'autorité de certification pour les clients.

4. METTRE EN ŒUVRE LE DEPLOIEMENT

- Mise en place des serveurs WSUS Maître (Master).
- Groupes d'ordinateurs sur le serveur maître.
- Paramétrage de la synchronisation du serveur MASTER-WSUS.
- Procédure d'exportation de la base de données WSUS pour/et sur site déconnecté.

- Le déploiement des clients WSUS via regedit ou GPO.
- System Center Configuration Manager 2012 R2 et WSUS 4.0
- La désinstallation du produit WSUS 4.0.

5. UTILISER LES FONCTIONS DE REPORTING

- La génération des rapports WSUS 4.0.
- Les rapports de mises à jour et d'ordinateurs.
- Le groupe Rapporteurs.

PUBLIC CONCERNE : Administrateurs et ingénieurs systèmes.

PRE-REQUIS : Connaissances de base de l'administration d'un server 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**

MICROSOFT WINDOWS SERVER 2019/2022

Mise en œuvre et administration d'un serveur Exchange 2016/2019

OBJECTIFS :

- Décrire Déployer et gérer Exchange Server 2016/2019 ;
- Créer et gérer les destinataires Exchange Server 2016/2019 ;
- Utiliser Exchange Management Shell pour la gestion des destinataires et des serveurs ;
- Configurer la connectivité des clients ;
- Implémenter et gérer une solution de haute disponibilité ;
- Mettre en œuvre la sauvegarde et une solution de reprise après sinistre ;
- Configurer les options de transport de messages ;
- Configurer les options de sécurité des messages ;
- Mettre en œuvre des déploiements Exchange Online ;
- Surveiller et dépanner Exchange Server 2016/2019

CONTENU :

1. DEPLOIEMENT

- Vue d'ensemble d'Exchange Server 2016/2019
- Pré requis et options de déploiement pour Exchange Server 2016/2019

2. GESTION DU SERVEUR

- Gérer Exchange Server 2016/2019
- Vue d'ensemble du serveur de boîtes aux lettres Exchange 2016/2019
- Configurer les serveurs de boîtes aux lettres

3. GESTION DES OBJETS DESTINATAIRES

- Vue d'ensemble des destinataires Exchange 2016/2019
- Gérer les destinataires Exchange Server
- Configurer les listes et les stratégies d'adresses

4. GESTION DU SERVEUR ET DES OBJETS DESTINATAIRES EN UTILISANT EXCHANGE MANAGEMENT SHELL

- Vue d'ensemble d'Exchange Management Shell
- Gérer Exchange Server 2016/2019 en utilisant Exchange Management Shell
- Gérer Exchange Server 2016/2019 en utilisant des scripts Exchange Management Shell

5. MISE EN ŒUVRE DE LA CONNECTIVITE POUR LES CLIENTS

- Configurer les services d'accès client d'Exchange Server 2016/2019
- Gérer les services clients
- Connectivité client et publication des services Exchange Server 2016/2019

- Configurer Outlook sur le web
- Configurer la messagerie mobile sur Exchange Server 2016/2019

6. GESTION DE LA HAUTE DISPONIBILITE DANS EXCHANGE SERVER

- Haute disponibilité dans Exchange Server 2016/2019
- Configurer des bases de données de boîtes aux lettres hautement disponibles
- Configurer des services d'accès client hautement disponibles

7. IMPLEMENTATION D'UNE SOLUTION DE RECUPERATION D'URGENCE POUR EXCHANGE

- Implémenter la sauvegarde d'Exchange Server 2016/2019
- Implémenter la restauration d'Exchange Server 2016/2019

8. CONFIGURATION ET GESTION DU TRANSFORT DES MESSAGES

- Vue d'ensemble du transport des messages
- Configurer le transport des messages
- Gérer les règles de transport

9. CONFIGURATION DE LA PROTECTION ANTIVIRUS, ANTI-SPAM ET LOGICIELS MALVEILLANTS

- Déployer et gérer un serveur Edge Transport pour sécuriser les messages
- Implémenter une solution antivirus pour Exchange Server 2016/2019
- Implémenter une solution anti-spam pour Exchange Server 2016/2019

10. IMPLEMENTATION ET GESTION D'UN DEPLOIEMENT MICROSOFT EXCHANGE ONLINE

- Vue d'ensemble d'Exchange Online et d'Office 365
- Gérer Exchange Online
- Implémenter une migration vers Exchange Online

11. ANALYSE ET DEPANNAGE DE MICROSOFT EXCHANGE SERVER

- Analyser Exchange Server 2016/2019
- Dépanner Exchange Server 2016/2019

12. SECURISATION ET MAINTENANCE D'EXCHANGE SERVER

- Sécuriser Exchange Server 2016/2019 avec le contrôle d'accès basé sur les rôles
- Configurer la journalisation d'audit
- Maintenance d'Exchange Server 2016/2019

13. SUPERVISION D'EXCHANGE SERVER

- Analyse de files d'attente d'envoi de message
- Mise en place des compteurs de performance
- Mise en place d'outils de stress
- Analyse de la résistance au stress.

PUBLIC CONCERNE : Toute personne disposant de compétences Windows Server intéressée par la mise en œuvre d'un service de messagerie Exchange 2016 ou 2019

PRE-REQUIS : Avoir une expérience en administration Windows Server 2012 ou 2016

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**

MICROSOFT WINDOWS SERVER 2019/2022

Initiation et découverte des services essentiels

OBJECTIFS :

- Apprendre à installer et à administrer Windows Server 2019
- Gérer les utilisateurs
- Découvrir NTFS
- Configurer une imprimante réseau
- Gérer la sécurité de Windows Server
- Protéger et surveiller son serveur
- Installer et configurer Terminal Server

CONTENU :

1. INSTALLER WINDOWS SERVER 2019

- Préparation de l'installation
- Installation de Windows 2022 Server, Windows 2022 Core

2. UTILISER LE DASHBOARD ET LE WINDOWS ADMIN CENTER

- Présentation et utilisation
- Gestion de grappes de serveurs
- Prise en charge des serveurs virtuels
- Administrer les serveurs avec l'interface graphique et Core
- L'installation des rôles et des fonctionnalités (locale et à distance)

3. GERER DES COMPTES D'UTILISATEURS

- Présentation des comptes d'utilisateurs
- Éléments requis pour les nouveaux comptes d'utilisateurs
- Création d'un compte d'utilisateur
- Définition de critères pour les mots de passe
- Définition de propriétés pour les mots de passe
- Personnalisation de paramètres utilisateur à l'aide de profils
- Gestion des données utilisateur en créant des répertoires de base

4. CONFIGURER LES ACCES AUX RESSOURCES A L'AIDE DE GROUPES

- Présentation des groupes
- Élaboration d'une politique de création des groupes de sécurité
- Utilisation des groupes prédéfinis

5. GERER LE STOCKAGE

- Types de stockages sur disque disponibles dans Windows Server (NTFS et ReFS)
- Partitionnement d'un lecteur de base
- Création de volumes sur un lecteur dynamique
- Les pools de stockage pour simplifier la gestion du stockage
- Exécution de tâches courantes pour gérer des disques
- Gestion unifiée à distance pour les services de fichiers et pool de stockage

6. CONFIGURER L'ACCES RESEAU AUX RESSOURCES DISQUE

- Description des dossiers partagés
- Création de dossiers partagés
- Combinaison d'autorisations NTFS et de dossiers partagés : SMB, NFS, iSCSI
- Configuration de dossiers partagés à l'aide du système DFS
- Utilisation du gestionnaire de ressources du serveur de fichiers FSRM
- Configurer les espaces de stockage dans Windows Server 2019
- Configurer le Branch Cache dans Windows Server 2019

7. CONFIGURER DES PERIPHERIQUES D'IMPRESSION

- Présentation de l'impression dans Windows Server
- Ajout d'une imprimante
- Configuration d'une imprimante réseau
- Particularité du serveur d'impression Windows 2019

8. DECOUVRIR LA SECURITE DANS WINDOWS SERVER

- Stratégies de sécurité Windows Server
- Implémentation de stratégies de sécurité sur les Objets
- Gestion des ACL et du DAC
- Audit de l'accès aux ressources système
- Sécurisation des partitions avec Bitlocker
- Atelier : Mise en place d'une stratégie de sécurité

9. SECURISER LES RESEAUX

- Configurations réseaux
- Outils classiques de sécurité réseau
- Mettre en œuvre une politique d'audit
- Configuration du pare-feu Windows avec sécurité avancée : règles de trafic entrant et sortant

10. SURVEILLER ET OPTIMISER LES PERFORMANCES DANS WINDOWS SERVER

- Surveillance des ressources système
- Surveillance des journaux d'événements

- Optimisation des performances

11. CONFIGURER LE SERVICE DHCP

- Installation, paramétrage et gestion d'un serveur DHCP
- Sécurisation de DHCP
- Les commandes Powershell pour DHCP
- Diagnostiquer et dépanner des problèmes DHCP
- Mettre en œuvre de la gestion d'adresse IP (IPAM)
- Atelier : Installation, paramétrages et tests d'un serveur DHCP

12. GERER LES SERVICES DE RESOLUTION DE NOMS

- Rappel sur le fonctionnement de DNS
- Nouvelles fonctionnalités de DNS sous Windows 2019
- La haute disponibilité pour le service DNS
- Outils de dépannage et de diagnostics

13. INSTALLER ET CONFIGURER DES SERVICES RDS

- Présentation des Remote Desktop Services
- Planification de l'installation
- Configuration d'un serveur Hôte de session
- Installation d'une ferme RDS avec un Broker de connexion
- Installation du Gestionnaire de licences
- Utilisation de Remote App et de l'accès Web
- Installation d'applications sur un serveur RDS
- Administrer le système avec PowerShell

PUBLIC CONCERNE : Toute personne disposant de compétences Windows Server intéressée par la mise en œuvre de la version 2019 et 2022

PRE-REQUIS : Avoir une expérience en administration Windows Server

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 : 5 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 WINDOWS 10/11

Sécurité dans une infrastructure active directory

OBJECTIFS :

- Améliorer la sécurité des données dans une infrastructure Active Directory
- Cette formation vous apprendra à optimiser les performances de Windows 10 et vous permettra de maîtriser les techniques et outils destinés à assurer un bon niveau de sécurité

CONTENU :

1. INTRODUCTION

- La sécurité sous Windows 10
- L'évolution des systèmes d'information et leur ouverture sur le monde
- Les menaces courantes pesant sur les systèmes d'information
- Les menaces récentes
- Chronologie et évolutions majeures des systèmes d'exploitation Windows

2. LES ATTAQUES – L'AUTHENTIFICATION

- Les attaques
- Gestion de l'authentification
- Mise en application de LAPS
- Mise en application d'une PSO

3. STRATEGIES ET MODELES DE SECURITE

- Recommandations de sécurité pour Active Directory (bonnes pratiques)
- Les modèles d'administration.
- Les paramètres d'environnement de l'utilisateur.
- Installer et configurer des applications.
- Gestion des Apps du Windows Store.
- Paramètres de configuration du navigateur Internet.
- Configuration du contrôle de compte utilisateur (UAC)
- Gestion des ACL

4. LA PROTECTION DES CONNEXIONS RESEAUX

- La sécurité dans un contexte domaine Windows.
- Le pare-feu de Windows 10 et ses fonctions avancées.
- Le Network Access Protection (NAP).
- Administrer les PC à distance avec DirectAccess.
- Découvrir Windows to go.

5. LES DONNEES – LA SECURITE APPLICATIVE

- Les données
- Mise en application de EFS
- Mise en application de Bitlocker
- Mise en application de Applocker
- Mise en application de Device Guard
- Mise en application de Credential Guard
- Les apports de Windows Anniversary Update

6. LES SAUVEGARDES ET POINTS DE RESTAURATION

- La protection du système.
- Gérer et automatiser les sauvegardes.
- Les clichés instantanés et les Volume Shadow Copies

7. LES OUTILS D'ANALYSE

- L'analyseur de performances et de stabilité. Les rapports d'erreurs.
- Diagnostiquer la mémoire.
- Le kit de déploiement et d'évaluation Windows.
- Les outils : Windows 10 Performance Toolkit (WPT).
- Autonomie de la batterie et consommation d'énergie.

PUBLIC CONCERNE : Techniciens et administrateurs systèmes ou infrastructure

PRE-REQUIS : Bonnes connaissances de l'administration de Windows 10

MOYENS PEDAGOGIQUES :

- Pédagogie par l'expérience fondée sur l'interaction dans le groupe.
- Guides de sécurisation (ANSSI, CIS, etc…)
- Exercices pratiques à partir de mise en situation,

INTERVENANT(S) : Consultant en cybersécurité

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**

GESTION DE PARC INFORMATIQUE
Installation et administration de Microsoft Endpoint Configuration Manager (SCCM) 2303

OBJECTIFS :

- Installer et configurer System Center Configuration Manager CB
- Déployer les systèmes d'exploitation
- Déployer des packages et des applications
- Déployer et gérer les mises à jour logicielles
- Gérer les requêtes, les inventaires et les rapports
- Sauvegarder et restaurer le site

CONTENU :

1. PLANIFICATION ET DEPLOIEMENT D'UN SITE PRIMAIRE

- Dimensionnement de l'infrastructure.
- Installation du site primaire.
- Configuration de la hiérarchie.
- Vue d'ensemble des services Cloud.

2. GESTION DES CLIENTS

- Les méthodes de déploiement du client.
- Préparation du site primaire au déploiement push.
- L'applet Configuration Manager et le Centre Logiciel.
- Vue d'ensemble des logs côté client.

3. INVENTAIRE, REQUETES, REGROUPEMENTS

- Le process d'inventaire sur les clients et les logs associés.
- Vue d'ensemble des requêtes.
- Vue d'ensemble des regroupements et des règles d'adhésion.

4. TELEDISTRIBUTION D'APPLICATIONS

- Création de packages et d'applications.
- Vue d'ensemble de la distribution.
- Les déploiements et l'affinité utilisateurs.
- Les logs côté serveur et clients.
- Les stratégies de gestion d'applications

5. TELEDISTRIBUTION DES MISES A JOUR LOGICIELLES

- Les mises à jour logicielles (CB, CBB et LTSB) pour Windows 10.
- Les plans de maintenance Windows 10.

- Mise en œuvre de WSUS 4.0.
- Les règles de déploiement automatique.
- Etude des logs côté clients et serveurs.

6. DEPLOIEMENT DE SYSTEMES D'EXPLOITATION

- Configuration des packages de pilotes, des images de démarrage et de systèmes d'exploitation.
- Les séquences de tâches.
- Supervision des déploiements.

7. REPORTING, MAINTENANCE DE SITE ET SECURITE

- Configuration des SQL Server Reporting Services.
- Déploiement du point de reporting et des rapports.
- Configuration de la sécurité.
- Vue d'ensemble des tâches de maintenance.
- Dépannage et récupération d'un site.

PUBLIC CONCERNE : Toute personne disposant de compétences Windows Server intéressée par la mise en œuvre d'un service de gestion de parc informatique avec SCCM 2016 ou 2019

PRE-REQUIS : Très bonnes connaissances de l'environnement Windows Server et Clients.

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**

GESTION DE PARC INFORMATIQUE

WAPT Entrerprise - Maintenez à jour votre parc informatique

OBJECTIFS :

À la fin de la formation, le stagiaire disposera des **outils, des connaissances et des méthodes** nécessaires pour **utiliser les différentes fonctionnalités de WAPT** et **créer des paquets de déploiement** et configuration de logiciels.
Ainsi, les objectifs opérationnels de la formation WAPT sont donc d'**acquérir les outils et méthodes indispensables** pour :

- Utiliser correctement WAPT au quotidien.
- Déployer des paquets WAPT.
- Créer et maintenir les paquets WAPT.
- Utiliser les fonctionnalités de la version Enterprise.

CONTENU :

1. INSTALLER SON ENVIRONNEMENT WAPT

- Préparer son serveur WAPT
  - *Suivre les préconisations de dimensionnement*
  - *Configurer correctement le système (nom, IP, prérequis logiciels)*
- Installer son serveur WAPT sur CentOS / Debian / Windows
  - *Configurer les dépôts*
  - *Exécuter le Post-conf*
- Installer la console et générer les certificats
  - *Installer la console*
  - *Générer le certificat administrateur*
  - *Prendre en main la console WAPT*
  - *Configurer la console*
- Générer l'agent WAPT puis le déployer
  - *Comprendre les options de base*
  - *Déployer manuellement et GPO*
- Utiliser l'agent WAPT
  - *Configurer le fichier wapt-get.ini*
  - *Utiliser l'agent WAPT en ligne de commande*

2. DECOUVRIR ET UTILISER LES FONCTIONS DE WAPT ENTERPRISE

- Mettre en place WAPT WUA
- Déployer le WAPT Self-Service
- Utiliser le reporting
- Configurer les dépôts secondaires
- Mettre en place l'authentification AD de la console

- Paramétrer l'authentification Kerberos des agents
- Configurer l'authentification par certificat client des agents
- Utiliser l'API WAPT
- Déploiement de Windows 10

3. DEVELOPPER SES PROPRES PAQUETS WAPT

- Créer des paquets simples
  - *À partir d'un MSI*
  - *À partir d'un EXE*
- Créer des paquets personnalisés
  - *Lister les paquets voulu par le client*

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

PRE-REQUIS : Connaissances de base d'administration 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 sera remise à la fin de la formation

MODALITES PRATIQUES :

Durée de la formation : 2 jours

Lieu de formation : INTER / INTRA (à définir)

Tarifs : Demander un devis

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

VMWARE VSPHERE 6.X/7.X/8.X

Installation, configuration et administration

OBJECTIFS :

- Installer et configurer les différents composants VMware vSphere
- Configurer et gérer le réseau virtuel
- Configurer, gérer et optimiser le stockage
- Sécuriser l'accès à l'infrastructure VMware

CONTENU :

1. LA VIRTUALISATION

- Présentation de VMware vSphere, les licences.
- Marché et enjeux de la virtualisation.
- Cloud computing.

2. HYPERVISEURS, CLIENT ET VCENTER

- Architecture, Management Node et Platform Services Controller.
- Hyperviseur et vCenter Server, déploiement de l'Appliance photon OS.
- Clients vSphere Flash et Html5.
- Conversion de serveur et VMware Converter Standalone.

3. GESTION DU RESEAU VIRTUEL

- Fonctionnalités du réseau virtuel.
- Configurations réseau : switchs locaux/distribués, sécurité, gestion du trafic et du teaming.

4. CONFIGURER ET GERER LE RESEAU VIRTUEL

- Gestion du stockage virtuel
- Stockage SAN Fibre Channel, SAN iSCSI, NFS, volumes virtuels.
- Datastores : création et gestion.

5. ADMINISTRATION DES MACHINES VIRTUELLES (VM)

- Les VMware Tools.
- Créations de VM, clones, templates, snapshots.
- Migration à chaud et à froid, volumes RDM.
- Gestion du matériel virtuel, Thin Provisionning, VMDirectPath, vSphere Replication.

6. INSTALLATION ET CONFIGURATION DE HYPER-V ET DES MACHINES VIRTUELLES

- Gestion d'un cluster VMware High Availability (HA), Distributed Resource Scheduler (DRS).
- Optimisation de l'utilisation des CPU, de la mémoire.
- Persistance des données.

7. MONITORING ET SECURITE DE L'INFRASTRUCTURE VIRTUELLE

- Alarmes par défaut et personnalisées.
- Sécurisation des accès : rôles et permissions.
- Gestion des mises à jour (VMware Update Manager).

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 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

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**

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 :

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
- Les 7 couches OSI, intérêts
- OSI en pratique

3. 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

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.

Travaux pratiques

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

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
- 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.

6. 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**