FORMATION CISSP

Mise à jour du programme (CBK) et de l'examen CISSP

(Entrée en vigueur à compter du 15 avril 2024)

Structure du CBK CISSP et pondération 02

L'examen CISSP 03

Domaine 1 : Sécurité et gestion des risques 04

Domaine 2 : Sécurité des actifs 06

Domaine 3 : Architecture et Ingénierie de la Sécurité 07

Domaine 4 : Sécurité des réseaux et des communications 13

Domaine 5 : Gestion des identités et des accès (IAM) 17

Domaine 6 : Evaluation et tests de sécurité 19

Domaine 7 : Opérations de sécurité 21

Domaine 8 : La sécurité dans le développement des logiciels 22

Structure du CBK CISSP et pondération

A compter du 15 avril 2024, un nouveau programme d'étude du CISSP (CBK) ainsi qu'une nouvelle version de l'examen entreront en vigueur.

Concernant le CBK il y a très peu de modifications. Les 8 domaines restent inchangés et seule la pondération est quelque peu modifiée. Le domaine n°1 qui était déjà le plus important des 8 domaines gagne un point de pondération (16%) alors que le domaine n°8 passe de 11% à 10%.

Le tableau ci-dessous résume l'importance des différents domaines et indique en rouge les 2 changements applicables à compter du 15 avril 2024.

	Domaines du CBK CISSP	2021	2024
1	**Sécurité et gestion des risques** (Security and Risk Management)	15%	16%
2	**Sécurité des actifs** (Asset Security)	10%	10%
3	**Architecture et ingénierie de sécurité** (Security Architecture and Engineering)	13%	13%
4	**Sécurité des communications et des réseaux** (Communication and Network Security)	13%	13%
5	**Gestion des identités et des accès (IAM)** (Identity and Access Management)	13%	13%
6	**Evaluation et test de la sécurité** (Security Assessment and Testing)	12%	12%
7	**Opérations de sécurité** (Security Operations)	13%	13%
8	**Sécurité dans le développement logiciel** (Software Development Security)	11%	10%

L'examen CISSP

Depuis le 1er juin 2022, l'(ISC)2 avait introduit 25 questions de pré-test supplémentaires dans l'examen. A partir du 15 avril 2024, on revient à la situation précédente comme le résume le tableau ci-dessous. On notera que l'examen n'est plus disponible en français depuis 2022. Au-delà de l'anglais, sachez qu'il est également possible de passer l'examen CISSP dans 5 autres langues : Allemand, Espagnol, Japonais, Coréen et Chinois.

Examen CISSP	avant le 01/06/2022	du 01/06/2022 au 14/04/2024	à partir du 15/04/2024
Nombre de questions	100 - 150	125 - 175	100 - 150
Nombre de questions de pré-test (beta)	25	50	25
Durée (max)	3 h	4 h	3 h
Temps moyen par question	72 sec.	82 sec.	72 sec.
Score nécessaire	700 / 1000	700 / 1000	700 / 1000
Langue	Anglais / Français	Anglais	Anglais
Type d'examen	CAT / linéaire	CAT	CAT

Légende du document

En rouge : les nouveautés du CBK 2024

En bleu : les explications de VERISAFE

Domaine 1 : Sécurité et gestion des risques

1.2 Comprendre et appliquer les concepts de sécurité

- Les 5 piliers de la sécurité de l'information (confidentialité, intégrité, disponibilité, authenticité et non-répudiation)

→ Il s'agit ici d'une simple reformulation des principes de sécurité. Dans le programme précédent, on parlait de triade CID (confidentialité, intégrité et disponibilité) mais d'autres concepts comme l'authenticité et la non-répudiation étaient également abordés. Désormais, on parle des 5 piliers de la sécurité de l'information pour englober les 5 éléments.

1.3 Evaluer et appliquer les principes de gouvernance de la sécurité

- Référentiels de sécurité (ex : ISO, NIST, COBIT, SABSA, PCI, FedRAMP)

→ Introduction d'un nouveau référentiel : SABSA (Sherwood Applied Business Security Architecture)

SABSA est une méthodologie permettant de développer des architectures de sécurité basées sur les risques et les opportunités commerciales.

Bien que protégée par le droit d'auteur, SABSA n'est pas un produit commercial mais une méthodologie ouverte. Elle comprend tout une série de frameworks, modèles, méthodes et processus et notamment :

- Un framework pour l'ingénierie des exigences commerciales (profilage des attributs)
- Un framework pour la gestion des risques et des opportunités
- Un framework pour la conception d'architecture orientée services de sécurité
- Un framework pour la gouvernance
- Un framework pour le domaine de la sécurité
- Un framework pour la gestion des services de sécurité et de la performance

La méthodologie SABSA est développée et maintenue par l'Institut SABSA. Elle est aujourd'hui utilisée par des professionnels qui l'utilisent dans environ 50 pays à travers le monde.

1.7 Identifier, analyser, évaluer, prioriser et mettre en œuvre les exigences de continuité d'activité

- Dépendances externes

→ Il s'agit ici de bien comprendre qu'un plan de continuité doit prendre en compte des éléments extérieurs à l'organisme : fournisseurs ISP/télécoms, prestataires de services informatiques, fournisseurs

de services Cloud, prestataires de transport/logistique, entités réglementaires et juridiques, institutions financières, clients, partenaires, installations ou services partagés.

Il convient également de prendre en compte le contexte géopolitique ainsi que d'éventuels facteurs environnementaux.

1.9 Comprendre et appliquer les concepts de gestion des risques

- Traitement des risques (ex : cyberassurance)

→ Le programme mentionne ici explicitement la possibilité de faire appel à une cyberassurance pour traiter les risques cyber.

Selon les options de traitement de risque proposés par l'(ISC)[2], la cyberassurance correspond à l'option transfert du risque (risk transfer). Par exemple, une entreprise pourra souscrire à une assurance cyber pour mitiger les impacts d'une crise ransomware. L'assurance comprendra tout un ensemble de prestations d'assistance : gestion de crise, communication, remédiation, … Certaines assurances pourront également prendre en compte tout ou partie de la rançon demandée par les cybercriminels.

Attention pour info dans la norme ISO 27005 dédiée à la gestion des risques, l'ISO a abandonné en 2008 l'option « risk transfer » par « risk sharing ». En effet, même si l'assurance permet de diminuer l'impact d'une crise cyber, le terme de partage du risque reste beaucoup plus approprié car l'ensemble des conséquences d'une crise cyber ne peut être transféré à une assurance (sanctions pénales, impact d'image, perte ultérieure de clients, etc…)

1.12 Etablir et maintenir un programme de sensibilisation, d'éducation et de formation à la sécurité

- Revues périodiques des contenus pour intégrer les technologies et tendances émergentes (ex : crypto-monnaies, intelligence artificielle (IA), blockchain)

→ Le programme précise désormais que les revues périodiques des programmes de formation/sensibilisation doivent intégrer les nouvelles technologies et tendances avec comme exemple les crypto-monnaies, l'intelligence artificielle et la Blockchain.

Les crypto-monnaies ne sont pas véritablement nouvelles en 2024 puisque la première d'entre-elles (bitcoin) est apparue en 2009. Il est cependant important d'en parler lors des sessions de sensibilisation pour indiquer le rôles qu'elles jouent dans la cybercriminalité.

La Blockchain est la technologie sous-jacente sur laquelle s'appuie la plupart des crypto-monnaies. Il peut également être intéressant de montrer en formation quelles sont les autres usages potentiels de la blockchain et notamment en matière de sécurité.

L'IA n'est pas non plus une nouvelle technologie mais l'arrivée de l'IA générative avec chatGPT en novembre 2022 a incontestablement changé la donne en matière de cybersécurité mais également de cybercriminalité. Tout programme de sensibilisation doit effectivement expliquer pourquoi les cybercriminels seront de plus en plus performants grâce à l'IA (phishing sophistiqué, deep fake audio/vidéo, etc...)

Domaine 2 : Sécurité des actifs



Aucune modification dans le domaine n°2 du CBK

Domaine 3 : Architecture et Ingénierie de la Sécurité

3.1 Rechercher, mettre en œuvre et gérer des processus d'ingénierie en utilisant les principes de conception sécurisée

- Approche Keep It Simple and Small

→ L'(ISC)^2 ajoute le terme « small » pour rappeler que lourdeur et complexité sont bien souvent l'ennemi de la sécurité.

Voici quelques exemples d'application du concept KISS (Keep It Simple and Small) en matière de cybersécurité :

- Optimiser le code en essayant de minimiser sa taille.
- Mettre en œuvre des solutions modulaires qui peuvent être gérées et mises à jour individuellement.
- Réduire la surface d'attaque en supprimant les fonctionnalités ou composants inutiles d'un système.
- Utiliser des micro-services ou d'autres modèles architecturaux qui favorisent des composants légers et indépendants.

Exemple d'application du concept de micro-segmentation :
La micro-segmentation utilise les technologies de virtualisation réseau pour créer des zones de sécurité très granulaires au sein des Data Centers et des déploiements dans le Cloud afin d'isoler les charges de travail. La micro-segmentation limite la capacité d'un assaillant à se déplacer latéralement au sein de l'infrastructure même s'il a infiltré les défenses au niveau d'un périmètre (réduction des déplacements Est/Ouest).

3.1 Rechercher, mettre en œuvre et gérer des processus d'ingénierie en utilisant les principes de conception sécurisée

- SASE (Secure Access Service Edge)

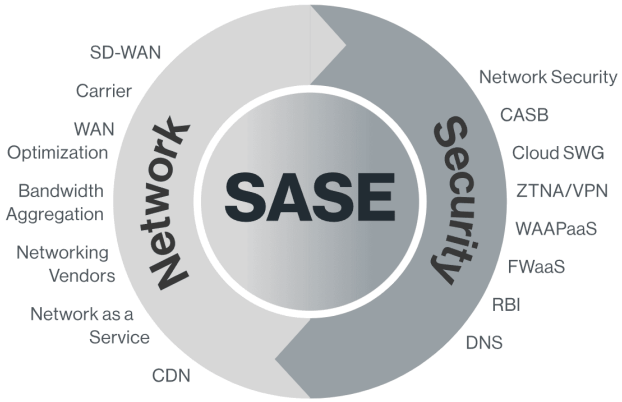
→ SASE se prononce « sassi »

SASE (que l'on prononce sassi) est un modèle d'architecture basé sur le cloud. Le SASE est une combinaison de services réseaux (SD-WAN, CDN, optimisation WAN, agrégation de bande passante,..) et de services de sécurité (CASB, SWG, ZTNA, FWaaS, RBI,...).

Le terme « SASE » a été inventé par le Gartner en 2019. Le cabinet américain est parti du constat suivant :

- Les utilisateurs ne sont plus toujours dans le réseau d'entreprise (Cloud, mobilité, télétravail, …)
- Les solutions pour optimiser et sécuriser l'accès aux applications et aux données ne peuvent plus être basées sur des appliances matérielles conventionnelles déployées dans les datacenters des entreprises

Le principal apport du SASE est de fournir un accès sécurisé quel que soit l'endroit où se trouvent les utilisateurs, les données, les applications ou les appareils.



Qui sont les fournisseurs de solutions SASE ? Il existe à ce jour quelques rares « pure players » comme par exemple Cato Networks. On retrouve bien sûr des acteurs du réseau (Cisco, Versa Networks,…) ou de la sécurité (Palo Alto, Fortinet, Zscaler, …). Et il ne fait aucun doute que demain, les leaders du IaaS comme Amazon, Microsoft ou Google se positionneront sur ce marché.

3.5 Évaluer et atténuer les vulnérabilités dans les architectures et éléments de solution de sécurité

- Technologie opérationnelle (OT) et systèmes de contrôle industriel (ICS)

→ L'(ISC)^2 introduit la notion d'OT (Operational Technology) dans le programme du CISSP. L'OT englobe l'ensemble des logiciels et matériels nécessaires au fonctionnement des équipements industriels. Les systèmes OT sont souvent utilisés dans des infrastructures critiques telles que les réseaux électriques, les installations de traitement de l'eau et les usines de fabrication.

Quelle est la différence entre IT et OT ? L'OT concerne le contrôle des équipements industriels alors que l'IT (la technologie de l'information) se concentre sur le traitement et l'échange d'informations.

Attention à ne pas confondre OT et ICS. L'ICS (Industrial Control System) est un système de contrôle industriel utilisé dans l'OT. Un ICS est donc un composant de l'OT. Il existe plusieurs types de système de contrôle utilisés dans les environnements industriels comme par exemple les systèmes de contrôle et d'acquisition de données (SCADA), les systèmes de contrôle distribués (DCS) ou encore les contrôleurs logiques programmables (PLC).

La sécurisation d'un réseau industriel est un vaste sujet mais qui reprend la plupart des principes fondamentaux de sécurité de l'IT. On notera que dans l'IT, on cherche principalement à assurer la sécurité du système d'information d'un organisme alors que dans l'OT on cherche assurer la sûreté de fonctionnement des équipements industriels et la sécurité des biens et des personnes.

Pour ceux qui souhaitent approfondir le sujet, nous vous recommandons les 3 ressources suivantes :

- NIST : Guide to Operational Technology (OT) Security
  - https://www.nist.gov/news-events/news/2023/09/nist-publishes-guide-operational-technology-ot-security
- ANSSI : Guide sur la sécurité des systèmes industriels
  - https://cyber.gouv.fr/publications/lanssi-publie-un-guide-sur-la-cybersecurite-des-systemes-industriels
- CLUSIF : Cybersécurité des systèmes industriels

- https://clusif.fr/wp-content/uploads/2021/09/20210303-Guide-cyberse%CC%81curite%CC%81-des-systemes-industriels.pdf

---

3.6 Identifier et choisir des solutions cryptographiques

- Infrastructure à Clé Publique (PKI) et distribution quantique des clés (QKD)

→ Nous avons vu dans le module CIS-07 de la formation qu'il sera peut-être possible dans le futur d'attaquer la cryptographie asymétrique via un ordinateur quantique. On sait en effet que l'algorithme de Peter Shor (1994) pourra résoudre le problème du logarithme discret (Diffie-Hellman) ou celui de la factorisation (RSA) dès qu'un ordinateur quantique suffisamment puissant sera opérationnel (environ 20 millions de qubits).

Pour anticiper ce problème, le NIST a lancé un concours pour sélectionner des algorithmes dits «quantum-resistant». On parle alors de cryptographie post-quantique (PQC - Post Quantum Cryptography). En 2017, 69 algorithmes ont été retenus par le NIST, puis 26 dans une 2ème sélection en 2019 pour aboutir à une sélection finale de 4 algorithmes en juillet 2022 (CRYSTALS-Kyber, CRYSTALS-Dilithium, Sphincs+ et FALCON).

En août 2024, le NIST a officiellement publié les trois premières normes de chiffrement post-quantique.

Norme FIPS 203 (ML-KEM) : Basée sur l'algorithme CRYSTALS-Kyber, rebaptisé ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism) elle est destinée à être la principale norme de chiffrement asymétrique. Parmi ses avantages, on trouve des clés de chiffrement relativement petites que deux parties peuvent s'échanger facilement ainsi qu'une grande rapidité d'exécution.

Norme FIPS 204 (ML-DSA) : Elle utilise l'algorithme CRYSTALS-Dilithium, rebaptisé ML-DSA (Module-Lattice-Based Digital Signature Algorithm). Elle est destinée à être la norme principale pour effectuer des signatures numériques.

Norme FIPS 205 (SHL-DSA) : Elle utilise l'algorithme Sphincs+, rebaptisé SLH-DSA (Stateless Hash-Based Digital Signature Algorithm). Elle est également destinée à effectuer des signatures numériques mais en utilisant une approche mathématique totalement différente de celle de ML-DSA. L'algorithme SHL-DSA constitue ainsi une solution de secours en cas de découverte d'une vulnérabilité sur l'algorithme ML-DSA.

Quant à FALCON, le 4ème algorithme retenu par le NIST en 2022, il sera nommé FN-DSA et fera l'objet d'un normalisation ultérieure sous la référence FIPS 206. L'algorithme FN-DSA est encore un algorithme de signature numérique. Il utilise la transformation de Fourier rapide sur les réseaux euclidiens de type NTRU pour FFT (fast-Fourier transform) over NTRU-Lattice-Based Digital Signature Algorithm.

Une autre approche pour se prémunir d'une attaque par un ordinateur quantique lors de l'échange de clé est d'utiliser une distribution quantique de clé alias QKD (Quantum Key Distribution).

La distribution quantique de clé utilise les principes de la mécanique quantique. QKD exploite le comportement des particules quantiques (photons), pour envoyer des informations. Dans un système QKD, l'émetteur génère une clé et la transmet sous forme d'une série de photons polarisés. Le destinataire reçoit une chaîne de bits quantiques (qubits) qu'il peut transformer en une clé secrète classique (exemple un nombre de 256 bits) qui peut être utilisée pour chiffrer et déchiffrer les messages (avec un algorithme symétrique comme AES).

Une propriété intéressante de la mécanique quantique est que toute mesure d'un système quantique le perturbe, entrainant de facto des modifications de l'état des qubits transmis. Par conséquent, si un hacker tente d'intercepter les photons transmis, il modifiera inévitablement l'état de certains d'entre eux. L'émetteur et le destinataire ne seront pas en mesure d'échanger par un chiffrement symétrique des informations puisque la clé est différente et ils détecteront en même temps la tentative d'écoute clandestine.

Plusieurs protocoles permettant une distribution de clés quantiques ont été développés pour améliorer la sécurité, l'efficacité, ou pour fonctionner dans différents contextes. Chaque protocoles utilise de manière unique les principes de la mécanique quantique pour sécuriser la distribution de clés cryptographiques, chacun avec ses avantages, inconvénients, et domaines d'application spécifiques. Le choix du protocole dépend souvent du contexte d'application, de la distance de communication, des ressources disponibles, et des exigences de sécurité.

Voici une liste des principaux protocoles de QKD :

- BB84 : C'est le premier protocole d'échange de clé quantique proposé en 1984 par Charles Bennett et Gilles Brassard. Il repose sur l'envoi de photons polarisés selon quatre orientations possibles, et sa sécurité est basée sur les principes de la mécanique quantique, notamment le fait que la mesure d'un système quantique peut le perturber.

- E91 (Ekert Protocol) : Proposé par Artur Ekert en 1991, ce protocole repose sur l'utilisation des paires de photons intriqués et des inégalités de Bell pour garantir la sécurité de l'échange de clés. Contrairement à BB84, qui repose sur la polarisation des photons, E91 utilise les corrélations quantiques entre les paires de photons pour détecter toute écoute éventuelle.

- B92 : Proposé par Charles Bennett en 1992, ce protocole est une simplification du BB84. Il n'utilise que deux états quantiques non orthogonaux au lieu de quatre ce qui réduit les besoins en termes de préparation et de mesure des états quantiques mais rend le protocole plus sensible aux erreurs et aux attaques.

- SSP (Six-State Protocol) : A l'inverse de B92, SSP est une version plus sophistiquée de BB84 qui utilise six états de polarisation des photons au lieu de quatre. En ajoutant deux orientations supplémentaires, le SSP améliore la sécurité contre certaines attaques en augmentant le taux d'erreur détectable pour un espion qui tenterait d'intercepter et de mesurer les photons.

- Continuous-Variable QKD (distribution de clés quantiques à variables continues) : Contrairement aux protocoles mentionnés précédemment, qui utilisent des photons individuels et leurs propriétés de particule, les protocoles à variables continues exploitent les ondes lumineuses et leurs aspects ondulatoires pour coder l'information. Ces protocoles peuvent utiliser des techniques de modulation et de mesure des champs lumineux, comme la modulation d'amplitude ou de phase, pour l'échange de clés.

- SARG04 : Proposé par Scarani, Acin, Ribordy, et Gisin en 2004, ce protocole est une variante du BB84 visant à améliorer la sécurité contre certaines attaques spécifiques. Il utilise une technique de

codage différente pour les états quantiques, ce qui rend plus difficile pour un hacker éventuel d'obtenir des informations sur la clé.

- MDI-QKD (Measurement-Device-Independent QKD) : Ce protocole a été proposé pour éliminer les faiblesses liées à la sécurité des dispositifs de mesure dans les protocoles QKD traditionnels. En MDI-QKD, aucune des parties ne mesure directement les états quantiques. Au lieu de cela, elles envoient des photons à une station de mesure centrale qui effectue une mesure de Bell. Ce protocole augmente la sécurité en rendant l'échange insensible aux attaques visant les détecteurs.

- TF-QKD (Twin-Field QKD) : Proposé pour augmenter la portée des communications sécurisées par QKD, le TF-QKD utilise des champs lumineux faibles ou des photons uniques émis simultanément par les deux parties vers une station intermédiaire qui effectue une mesure interférométrique. Ce protocole promet des taux de transmission de clés sécurisées sur des distances beaucoup plus longues que ce qui est possible avec les protocoles QKD traditionnels.

Il existe encore bien d'autres protocoles comme DPS (Differential Phase Shift) ou COW (Coherent One Way). Cette liste illustre la diversité des approches en cryptographie quantique, chacun exploitant de manière unique les propriétés de la mécanique quantique pour sécuriser la communication.

Si d'un point de vue théorique, la distribution quantique de clé peut sembler idéale, elle souffre cependant de 4 principales limitations.

1. La QKD n'est qu'une réponse partielle aux problèmes soulevés par la cryptanalyse quantique. En effet, la QKD ne fournit pas de moyen d'authentifier la source de transmission des photons. Par conséquent, elle ne peut pas être utilisée pour des opérations de signature numérique mais uniquement à des fins de confidentialité.
2. La QKD nécessite des équipements spéciaux (fibres optiques dédiées ou gestion physique des émetteurs). Elle est particulièrement difficile à intégrer dans les architectures actuelles car elle ne peut pas être mise en œuvre via un simple logiciel ou un service réseau.
3. Les réseaux QKD nécessitent souvent l'utilisation de relais de confiance, entraînant ainsi des coûts supplémentaires pour leur installation sécurisée et un risque accru de menaces internes.
4. La QKD augmente sensiblement le risque de déni de service. En effet, il suffit à un attaquant d'effectuer des écoutes passives systématiques pour empêcher l'échange de clés valides.

En conclusion, l'approche du NIST avec la cryptographie résistante au quantique (PQC) est une solution plus complète (confidentialité et signature), moins couteuse et plus facile à installer et à maintenir que la distribution quantique de clé.

---

10 Gérer le cycle de vie d'un système d'information

- Besoins et exigences des parties prenantes
- Analyse des besoins
- Conception de l'architecture
- Développement / mise en œuvre
- Intégration
- Vérification et validation
- Transition / déploiement

- Opérations et maintenance / maintien opérationnel
- Retrait / cession

→ Dans ce module n°3, l'(ISC)^2 introduit un nouveau chapitre qui concerne la gestion du cycle de vie d'un système d'information. Le nouveau programme du CISSP, précise les 9 phases du processus global depuis la conception initiale d'un SI jusqu'à son retrait éventuel.

- Besoins et exigences des parties prenantes : Cette phase identifie et rassemble les besoins, attentes et exigences spécifiques de toutes les personnes et entités impliquées ou affectées par le système.
- Analyse des exigences : une analyse approfondie des exigences recueillies pour comprendre, clarifier et détailler les objectifs du système.
- Conception de l'architecture : l'architecture du système décrit sa structure, ses composants et ses relations.
- Développement/Mise en œuvre : création de l'architecture du SI et développement des applications.
- Intégration : validation de l'ensemble des différentes parties du système qui doivent fonctionner comme un système monolithique et de manière transparente y compris si elles ont été conçues ou développées par des tiers.
- Vérification et validation : vérifier que le système répond aux exigences initiales et fonctionne correctement.
- Transition/déploiement : déploiement du système dans l'environnement de production pour une utilisation effective.
- Opérations et maintenance/maintenance : gestion continue du système, y compris les mises à jour, les correctifs et autres modifications nécessaires pour assurer son bon fonctionnement.
- Retrait/élimination : fin éventuelle de l'utilisation du système, ce qui peut impliquer la migration des données, l'archivage ou la mise hors service du système en toute sécurité.

Domaine 4 : Sécurité des réseaux et des communications

4.1 Appliquer les principes de conception sécurisée dans les architectures réseaux

- Protocoles convergents (ex : Fiber Channel Over Ethernet (FCoE), Voice over Internet Protocol (VoIP), iSCSI, InfiniBand over Ethernet, Compute Express Link)

→ l'(ISC)^2 introduit 2 nouveaux types de protocoles convergents : InfiniBand over Ethernet et Compute Express Link. On rappelle tout d'abord que les protocoles convergents sont des protocoles qui fonctionnent sur TCP/IP. Ils sont donc particulièrement faciles à intégrer dans l'architecture réseau des entreprises.

InfiniBand over Ethernet est un protocole réseau qui permet un accès direct à la mémoire à distance (Remote Direct Memory Access - RDMA) via Ethernet. RDMA permet d'accéder directement à la mémoire d'un serveur (local ou distant) sans impliquer l'unité centrale. Dans un datacenter, cela permet d'obtenir une très grande passante et une faible latence tout en diminuant la consommation CPU des systèmes.

Compute Express Link (CXL) est une norme ouverte pour les connexions à très haute vitesse entre un CPU et un périphérique ou entre un CPU et la mémoire vive (RAM) d'un serveur. CXL est basé sur le protocole PCI Express (PCIe).

4.1 Appliquer les principes de conception sécurisée dans les architectures réseaux

- Architecture de transport (ex : topologie, plan de données/de contrôle/de gestion, cut-through/store-and-forward)

→ Dans cette section l'(ISC)^2 introduit de nouveaux concepts d'architecture de transport.

Le plan de gestion (management plane) permet de gérer les configurations réseaux, de surveiller le fonctionnement des réseaux et de gérer la sécurité. Exemples de protocoles utilisés dans le plan de gestion : SNMP (Simple Network Management Protocol) ou encore NETCONF (Network Configuration Protocol).

Le plan de contrôle (controle plan) sert à la gestion et au fonctionnement des protocoles de routage. Exemples de protocoles utilisés dans le plan de contrôle : STP (Spanning Tree Protocol), OSPF (Open Shortest Path First) ou encore BGP (Border Gateway Protocol).

Enfin le plan de données est responsable de l'acheminement des paquets de données selon les directives fixés par le plan de contrôle.

2 types de commutation (switch) sont également mentionnés dans le programme :

Cut-through : le commutateur prend des décisions de transfert dès qu'il reçoit le début d'une trame. C'est l'option à choisir lorsque que l'on souhaite obtenir une latence ultra-faible.

Store-and-forward : le commutateur met en mémoire tampon l'intégralité de la trame avant de prendre la décision de transfert. Ce mode est à privilégier lorsque l'on veut privilégier la fiabilité des transmissions plutôt que la latence.

4.1 Appliquer les principes de conception sécurisée dans les architectures réseaux

- Mesures de performances (ex : bande passante, latence, gigue, débit, rapport signal/bruit)

→ Les mesures de performance permettent de mesurer les performances, l'efficacité et la qualité des réseaux.

Bande passante (Bandwidth) : c'est la capacité maximale d'un canal réseau à transmettre des données. Elle indique le taux de transfert de données maximum théorique.

Débit (Throughput) : c'est le débit de transfert de données réel atteint dans la pratique. Il prend en compte divers paramètres comme la latence, la perte de paquets ou la congestion du réseau.

Latence (Latency) : Lors d'une transmission de paquet, la latence indique le délai entre l'envoi d'un paquet et son arrivée à destination. Elle est inversement proportionnelle au débit du réseau. Lors de la gestion d'un paquet par un routeur ou un switch, elle indique le délai entre la réception d'un paquet et sa retransmission sur le réseau. Le temps de réponse global d'un réseau se calcule en additionnant les différences latences de transmission et de gestion par les équipements (routeurs, switch, firewall, etc…).

Jitter : il traduit la variation de la latence. Le jitter affecte la qualité de service (QoS) pour les applications en temps réel.

Rapport signal sur bruit (Signal-to-noise ratio - SNR) : c'est la mesure de la qualité d'un signal par rapport au bruit de fond. Il est notamment utilisé pour mesurer la qualité des communications sans fil. Plus le SNR est élevé, meilleure est la qualité du signal.

4.1 Appliquer les principes de conception sécurisée dans les architectures réseaux

- Flux réseaux (ex : nord-sud, est-ouest)

→ Un flux réseau Nord-Sud (North-South) caractérise un trafic réseau entre le réseau interne d'une entreprise et le réseau public internet (entrant ou sortant).

Un flux réseau Est-Ouest (East-West) caractérise le trafic au sein du réseau interne d'une entreprise. Les données se déplacent alors latéralement au sein du réseau. Lorsqu'il s'agit de la progression d'un attaquant au sein du SI d'un entreprise, on parle de mouvement latéral.

4.1 Appliquer les principes de conception sécurisée dans les architectures réseaux

- Segmentation physique (ex : in-band, out-of-band, air-gapped)

→ Dans la conception d'une architecture réseau sécurisée, on peut mettre en œuvre de la segmentation physique ou logique.

On parle par exemple d'administration « out-of-band » lorsqu'on dispose d'une interface réseau physique dédiée à l'administration d'un équipement et que les autres interfaces physiques servent aux transferts de données et donc au fonctionnement de l'équipement. Il y a donc une séparation physique entre le réseau d'administration et le réseau d'utilisation du système.

Par opposition on pourrait avoir sur cet équipement une seule interface physique et faire de l'administration « in-band ». Dans ce cas le transfert des données et les opérations d'administration utilise la même interface physique. Dans ce cas, l'usage de sous-réseaux (subnets) ou de réseaux virtuels (VLANs) permettra d'assurer qu'aucun utilisateur du système ne puisse accéder aux fonctions d'administration. Il s'agit ici d'une segmentation logique des réseaux.

On parle de réseau « air-gap » lorsque tout le réseau est physiquement isolé de tout autre réseau. Aucun lien filaire ou non-filaire ne doit exister avec un autre réseau. L'isolation complète de type air-gap est généralement utilisée pour assurer la sécurité de réseaux ultra-sensibles (réseaux gouvernementaux, réseaux industriels, secteur militaire ou nucléaire).

4.1 Appliquer les principes de conception sécurisée dans les architectures réseaux

- Réseaux périphériques (Edge Networks, ex : ingress/egress, peering)

→ La notion de « Edge networks » (réseaux en périphérie ou réseaux de bordure) fait référence à une infrastructure de réseau et de calcul située en périphérie de réseau, c'est-à-dire plus proche des sources de données ou des utilisateurs finaux. On parle alors de « Edge computing ».

L'objectif principal est de réduire la latence et d'améliorer les performances en traitant les données au plus près de l'endroit où elles sont générées plutôt que de les envoyer dans des centres de données distants pour le traitement.

Une architecture réseau basée sur du Edge computing apporte les avantages suivants :

- Réduction de la latence : En traitant les données près de la source, cela permet des temps de réponse beaucoup plus rapides. C'est un élément fondamental pour certains types d'application comme le streaming, la réalité augmentée, les véhicules autonomes et plus généralement pour toute application des décisions en temps réel.
- Optimisation de la bande passante : En traitant les données localement, seulement les informations pertinentes ou agrégées sont envoyées sur des réseaux distants, réduisant ainsi le besoin en bande passante et les coûts associés.
- Amélioration de la sécurité et respect de la vie privée : Le traitement de proximité peut également aider à améliorer la sécurité et la confidentialité car moins de données sensibles sont transmises sur le réseau à des système tiers.
- Meilleure fiabilité : En décentralisant le traitement et le stockage des données, le edge computing offre une plus grande résilience en cas de panne de réseau ou de perturbation, puisque les dispositifs peuvent continuer à fonctionner localement.

Les termes de Ingress/Egress ou de Peering font partie du vocabulaire du Edge computing.
Ingress/Egress (entrée/Sortie) : ce sont les points d'entrée ou de sortie dans un réseau en périphérie.

Le « Peering » quant à lui consiste à interconnecter directement entre deux systèmes situés dans les Edge networks sans passer par un hub central. Cela permet de réduire la latence et évite les goulots d'étranglement (bottleneck).

4.1 Appliquer les principes de conception sécurisée dans les architectures réseaux

- Cloud privé virtuel (VPC)

Un Cloud Privé Virtuel ou VPC (Virtual Private Cloud), est un service de cloud computing qui offre aux entreprises la possibilité de créer une infrastructure IT totalement dédiée et isolée au sein de l'infrastructure du fournisseur. Par défaut et pour des raisons de sécurité, un VPC est isolé du réseau Internet et donc non-accessible via Internet. Bien entendu, si une connexion à Internet est nécessaire, il est toujours possible de l'autoriser via par exemple chez AWS une IGW (Internet Gateway).

Selon le fournisseur Cloud, l'acronyme pour désigner un cloud privé virtuel pourra être différent. Ainsi dans AWS (Amazon) et GCP (Google), on parlera de VPC (Virtual Private Cloud) alors que dans Azure (Microsoft) c'est le terme de VNET (Virtual NETwork) qui sera utilisé.

Les 3 principaux avantages d'un cloud privé virtuel sont les suivants :

- Isolation et Sécurité : Ils fournissent un environnement réseau isolé, permettant aux utilisateurs de contrôler leur espace de réseau virtuel, y compris la sélection des plages d'adresses IP, la création de sous-réseaux, et la configuration des tables de routage et des réseaux privés virtuels (VPN).

- Contrôle d'Accès : On peut configurer des listes de contrôle d'accès (ACL) et des groupes de sécurité pour contrôler l'accès aux instances et aux applications dans leur VPC. Cela permet une gestion fine des permissions d'accès, augmentant ainsi la sécurité des données et des applications.

- Connectivité Hybride : Les VPC peuvent être connectés à des réseaux d'entreprise via des connexions VPN ou des liaisons dédiées (exemple pour Amazon avec AWS Direct Connect). Cela permet une extension transparente du data center de l'entreprise au cloud afin de créer un environnement de cloud hybride.

Domaine 5 : Gestion des identités et des accès (IAM)

5.2 Concevoir une politique d'identification et d'authentification des personnes, des appareils et des services

- Authentification, autorisation et traçabilité (AAA) (ex : authentification multi-facteurs (MFA), authentification sans mot de passe)

→ Ce n'était pas dans le programme du CBK d'avril 2021, mais nous avions déjà abordé dans la formation, la notion de passwordless à savoir l'authentification utilisateur sans mot de passe. Pour cela nous avons présenté le standard UAF (Universal Authentication Framework) de la FIDO Alliance qui est un mécanisme d'authentification par challenge/response basé sur la cryptographie asymétrique. Retenez qu'aujourd'hui UAF porte le nom de passkey et qu'en plus de la FIDO Alliance, il est promu par 3 grands acteurs de l'IT : Apple, Google et Microsoft. Ainsi avec les passkeys, il est possible de stocker de manière sécurisé les clés privées des utilisateurs dans Android, Windows, iOS et iPadOS et de s'authentifier sur diverses application ou services en ligne qui supporte ce standard (WhatsApp, Amazon, Paypal,…).

Les principaux avantages des passkeys sont les suivants :

- Plus de mots de passe à retenir. Il n'y a plus la nécessité d'utiliser un gestionnaire de mot de passe.
- Plus de mots de passe à changer. Même si les changements réguliers et systématiques n'étaient plus considérés comme une bonne pratique, il n'y a plus de mots de passe, il n'y a donc plus la nécessité de les changer régulièrement.
- Excellente protection contre le phishing. Il n'est pas possible pour un attaquant de récupérer un mot de passe via un site frauduleux. La seule chose transmise est un challenge chiffré avec une clé privée. La clé privée n'est jamais transmise sur le réseau donc non violable par une opération de phishing.
- Plus de risque en cas de compromission d'un site. En effet, si un site est compromis, seules les clés publiques des utilisateurs seront divulguées ce qui n'entraîne aucun risque pour les utilisateurs. Bien entendu si sur un site l'utilisateur a provisionné une passkey mais également aussi un password (mot de passe), il lui faudra impérativement changer son mot de passe en cas de compromission de ce service en ligne.

Sachez également qu'il est également possible de s'authentifier sans mot de passe dans l'environnement Microsoft (Windows 10 & 11) avec Windows Hello (pour les particuliers) et Windows Hello for Business (pour les entreprises). La technologie Hello de Microsoft s'appuie sur le standard FIDO2 et elle est tout à fait similaire aux passkeys mais reste limitée aux environnements Microsoft.

5.4 Mettre en œuvre et gérer les mécanismes d'autorisation

- Application des politiques d'accès (ex : Policy Enforcement Point (PEP) et Policy Decision Point (PDP))

→ PEP et PDP n'étaient pas explicitement mentionnés dans le programme du CBK d'avril 2021, mais nous les avions déjà abordés dans la formation (module CIS-14) lorsque nous avions présenté XACML (eXtensible Access Control Markup Language).

Pour rappel, un PDP (Point de décision de la politique) est l'entité dans laquelle les décisions d'accès sont prises conformément aux politiques d'accès définies. Un PEP (Point d'application des politiques) est l'entité qui autorise ou refuse les accès sur la base des décisions du PDP. En d'autres termes, le PDP juge de la validité des demandes d'accès alors que le PEP applique effectivement la décision du PDP.

5.5 Gérer le cycle de vie du provisionnement des identités et des accès

- Gestion des comptes de services

→ Qu'est-ce qu'un compte de services (service account) ?

Lorsqu'un logiciel est installé sur un système, il peut nécessiter certains privilèges pour s'exécuter et accéder à d'autres ressources (systèmes, données). Pour cela, on crée un compte de service pour cette application qui lui permettra de fonctionner correctement sans aucune intervention humaine. Les comptes de services sont très utilisés pour lancer des applications comme des bases de données ou encore des solutions de sécurité (antimalware, EDR,…).

On notera que dans le Cloud, un concept similaire existe pour des charges de travail (VM, container, serverless). Il permet de leur fournir une identité pour leur permettre d'accéder à des ressources (données, applications, …). Tous les fournisseurs de service IaaS proposent ce type de service avec une appellation différente : managed identity dans Microsoft Azure, service role dans Amazon AWS ou encore service account identity dans Google GCP.

La gestion des comptes de service est cruciale, car ces comptes disposent souvent de privilèges élevés pour effectuer des tâches spécifiques, ce qui en fait des cibles potentielles pour les acteurs malveillants.

Une bonne gestion de leur cycle de vie ainsi que l'application du principe du moindre privilège sont très importants afin de s'assurer que les applications/services fonctionnent correctement sans pour autant poser de risques inutiles à l'environnement de production.

5.6 Mettre en œuvre des systèmes d'authentification

- ~~OpenID Connect (OIDC) / Open Authorization (Oauth)~~
- ~~Security Assertion Markup Language (SAML)~~
- ~~Kerberos~~
- ~~Remote Authentication Dial-In User Service (RADIUS) / Terminal Access Controller Access Control System Plus (TACACS+)~~

→ Attention, il n'y a plus de détail sous forme de puces dans le CBK mais on peut penser que le programme reste identique et que tous ces sujets (OIDC, Oauth, SAML, Kerberos et TACACS+) peuvent encore faire l'objet d'une question lors de l'examen.

Domaine 6 : Evaluation et tests de sécurité

6.1 Concevoir et valider des stratégies d'évaluation, de test et d'audit

- Selon l'emplacement (sur site, dans le cloud, en hybride)

6.5 Conduire ou faciliter des audits de sécurité

- Selon l'emplacement (sur site, dans le cloud, en hybride)

→ L'emplacement des systèmes et des données joue un rôle important en matière d'évaluation, de test et d'audit.

Emplacement sur site (on-premise) :

- Audit : Les auditeurs peuvent avoir un accès physique au matériel, aux périphériques réseau et aux centres de données à des fins d'inspection, de révision de configuration et de tests.

- Contrôle et visibilité : L'entreprise conserve le contrôle total de son infrastructure, ce qui permet aux auditeurs d'avoir une visibilité globale et directe des configurations de sécurité.

- Périmètre : Les audits peuvent se concentrer sur l'infrastructure informatique traditionnelle, y compris la sécurité du réseau, les systèmes d'exploitation, les protections physiques, etc.

Emplacement dans le Cloud :
Dans ce cas, les audits sur site ne sont pas en général autorisés pour des raisons de sécurité, de confidentialité et de gestion opérationnelle.

Voici les principaux facteurs qui justifient ces restrictions :

- La sécurité : Les datacenters hébergent des infrastructures critiques non seulement pour un client, mais pour des centaines, voire des milliers d'autres. Permettre l'accès physique ou même un audit détaillé par les clients pourrait exposer le datacenter à des risques de sécurité, y compris un vol potentiel de données.

- La confidentialité : Les fournisseurs de cloud hébergent les données et les applications de nombreux clients simultanément, souvent dans un environnement mutualisé. Un audit par un client pourrait potentiellement compromettre la confidentialité des données d'autres clients, surtout si des informations sensibles ou des configurations spécifiques sont révélées pendant l'audit.

- L'intégrité des opérations : Les datacenters sont des environnements hautement contrôlés et optimisés pour assurer la performance, la disponibilité, et la sécurité des services hébergés. L'introduction d'auditeurs externes dans ces espaces peut perturber les opérations normales, entraîner des risques de panne ou affecter la qualité du service pour tous les clients.

- La conformité règlementaire : Les fournisseurs de cloud sont souvent soumis à des réglementations strictes concernant la protection des données, la sécurité de l'information, et

d'autres standards sectoriels. Ils suivent des procédures d'audit internes et externes avec des entités accréditées pour garantir leur conformité. Les audits client pourraient interférer avec ces processus et potentiellement mettre en péril la conformité du fournisseur.

Pour surmonter ces défis tout en offrant une certaine forme de transparence et de confiance aux clients, les fournisseurs de services cloud adoptent plusieurs approches :

- Rapports d'audit tiers : Les fournisseurs de cloud s'engagent souvent avec des auditeurs tiers pour réaliser des audits réguliers de leurs datacenters et pratiques de sécurité. L'évaluation de la sécurité du service Cloud se fait alors avec une approche conformité. Il s'agit de vérifier le respect de normes de sécurité spécifiques au cloud (ISO 27001 avec DdA qui intègre l'ISO 27017 ou l'ISO 27018, SOC1/2 type1/2, FedRAMP,…). Les certifications (exemple ISO 27001) ou rapport (exemple SOC3) issus de ces audits sont ensuite partagés avec les clients pour démontrer la conformité et la sécurité sans exposer directement les installations à des audits externes.

- Transparence accrue : Certains fournisseurs offrent une transparence via des dashboards de sécurité, des mises à jour régulières sur leurs pratiques de sécurité ou des réponses détaillées à des questionnaires de sécurité comme celui proposé par la CSA (Cloud Controls Matrix).

- Visites virtuelles : Afin d'offrir de la visibilité sans impacter la sécurité, certains fournisseurs proposent des visites virtuelles de leurs datacenters, permettant aux clients de voir les installations sans y accéder physiquement.

Ces mesures visent à équilibrer la nécessité pour les clients de comprendre et de faire confiance à l'infrastructure qui supporte leurs opérations tout en protégeant l'intégrité, la sécurité, et la confidentialité des datacenters.

Concernant l'audit d'un cloud hybride, il faut bien comprendre que le terme hybride signifie que plusieurs modes de déploiement sont utilisés (typiquement cloud privé + cloud public). Les audits seront assujettis aux mêmes contraintes selon le périmètre à auditer. Par exemple, s'il faut auditer un Cloud hybride (privé on-premise / public chez AWS), on pourra auditer la partie privé comme on audite toute installation sur site mais les auditeurs ne pourront pas auditer « in-situ » les infrastructures en raison des limitations évoquées précédemment.

Domaine 7 : Opérations de sécurité

7.12 Tester les Plans de Reprise après Sinistre (DRP)

- Communications (ex : parties prenantes, résultats des tests, régulateurs)

→ Dans ce domaine, très peu de changement. L'(ISC)2 rajoute une section communications concernant les tests des plans de reprise après sinistre.

Notifier les parties prenantes : il convient d'informer toutes les parties prenantes concernées (direction, DSI, utilisateurs finaux, fournisseurs tiers…) des modalités du test DRP (dates, périmètre, …). Cela permet de les informer des éventuelles perturbations mais également de pouvoir les engager dans la procédure afin de bien comprendre le rôle et les responsabilités de chacun.

Communiquer sur les résultats : Cela permet d'informer les parties concernées de la progression du test DRP et des résultats obtenus. Les parties prenantes peuvent interagir avec les personnes en charge des tests afin de vérifier que les résultats obtenus sont conformes à leurs attentes et d'inclure éventuellement des mises à jour du plan actuellement testées afin de palier à certaines insuffisances.

Communiquer avec les régulateurs : si l'organisme opère dans un secteur réglementé, il peut être nécessaire d'informer les organismes de réglementation du test DRP, en particulier s'il existe des exigences de conformité spécifiques liées à la reprise après sinistre. En Europe, certains règlements imposent des tests de continuité/reprise d'activité comme par exemple DORA pour le secteur financier.

Communication externe et média : si le test DRP peut avoir un impact sur les clients ou le public, prévoir une stratégie de communication afin bien identifier leurs attentes et de répondre à leurs préoccupations.

On notera que lors de sinistres de grande ampleur (exemple ransomware), l'ensemble des moyens de communication peuvent être anéantis. Le plan devra alors prévoir un système de communication alternatif, non impactable par les sinistres potentiels (serveurs de mail de secours, postes/téléphones de remplacement, …). Ce système de communication d'urgence devra également faire l'objet de tests réguliers.

Domaine 8 : La sécurité dans le développement des logiciels

8.1 Comprendre et intégrer la sécurité dans le Cycle de Vie du Développement Logiciel (SDLC)

- Méthodologies de développement (ex : Agile, Waterfall, DevOps, DevSecOps, Scaled Agile Framework -SAFe)

→ SAFe propose une approche structurée permettant aux grandes organisations d'adopter des pratiques agiles d'une manière plus adaptée à leur taille et à leur complexité. En effet, La plupart des méthodes agile comme Scrum ou Kanban sont bien adaptées aux équipes individuelles et aux petites organisations mais pas aux projets très complexes et à grande échelle. SAFe n'a pas vocation de remplacer Agile mais plutôt d'ajouter les couches nécessaires pour faire fonctionner Agile dans un contexte à grande échelle.

8.2 Identifier et appliquer les contrôles de sécurité dans les écosystèmes de développement logiciel

- Tests de sécurité des applications (ex : Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), software composition analysis, Interactive Application Security Testing (IAST))

→ Dans cette section, l'(ISC)2 introduit la notion de « software composition analysis » et de Interactive Application Security Testing (IAST).

L'analyse de la composition logicielle (en anglais Software Composition Analysis - SCA) est une pratique dans le domaine de la cybersécurité et du développement logiciel qui consiste à analyser automatiquement les composants logiciels tiers, notamment les bibliothèques et les frameworks open source, utilisés dans un projet de logiciel. L'objectif est d'identifier et de gérer les risques de sécurité, les licences incompatibles et les vulnérabilités potentielles qui pourraient affecter l'application.

Le Software Composition Analysis couvre les aspects suivants :

- Identification de composants tiers : L'outil SCA scanne le code source, les fichiers binaires ou les dépendances déclarées dans les gestionnaires de paquets pour identifier tous les composants logiciels tiers utilisés dans le projet. Cette étape permet de créer un inventaire précis des bibliothèques externes intégrées au logiciel.

- Analyse de sécurité : Elle consiste à comparer les composants identifiés contre des bases de données de vulnérabilités connues, comme la NVD (National Vulnerability Database) ou d'autres sources de renseignements sur les menaces. L'outil SCA peut ainsi détecter les vulnérabilités connues dans les composants utilisés et fournir des recommandations pour leur mitigation, telles que la mise à jour vers une version plus sécurisée du composant.

- Gestion des licences : L'outil SCA examine les licences des composants logiciels tiers pour s'assurer qu'elles sont compatibles avec les politiques de licence du projet. Cette analyse aide à éviter les risques légaux et de conformité liés à l'utilisation inappropriée de logiciels sous licence.

- Remédiation et conformité : à partir des résultats de l'analyse, le SCA aide les équipes de développement à prendre des décisions éclairées sur la manière de gérer les risques identifiés, que ce soit par la mise à jour, la substitution ou la suppression de composants vulnérables ou non conformes. Le SCA peut également intégrer des politiques de sécurité et de conformité pour automatiser une partie de la gouvernance des composants logiciels tiers.

En conclusion on eut dire que les outils de Software Composition Analysis sont essentiels dans la boîte à outils de gestion moderne de la sécurité des applications. Ils offrent une bonne visibilité sur les composants logiciels tiers qui pourraient introduire des risques dans les applications.

Enfin et pour finir la notion de IAST (Interactive Application Security Testing) n'était pas au programme du CBK d'avril 2021, mais nous l'avions déjà abordé dans notre formation. Consultez le module CIS-20 pour plus d'information sur les tests interactifs de sécurité des applications.