Tenexa

Cyber-SOC 360°
by Tenexa

Nous proposons une approche complète de la Cyber-Sécurité incluant les aspects préventifs, défensifs (protection), d'actions rapides comme l'analyse forensique et remédiation. La restauration des systèmes en état "sain" pour reprise de la production.

Notre démarche consiste à fournir les solutions et services en adéquation avec chaque client, son contexte, son existant et ses besoins :

- Adaptation au métier, à la criticité et à la taille de chaque client
- Prise en compte de l'existant (outillages déjà en place) : solutions modulaires
- Conception ou adaptation de la totalité du processus de protection et PRI en incluant toutes les composantes techniques, fonctionnelles et organisationnelles
- Accompagnement Client et/ou RSSI en mode partenariat sur le long terme
- Garanties de résultat sur les services fournis (SLAs) : GTI / GTR / RTO / RPO...

POINTS CLÉS :

- Supervision : pour un suivi quotidien des infrastructures et applications
- SIEM/ SOC / XDR : pour une détection et des actions immédiates en cas d'attaque cyber
- BaaS : pour assurer l'externalisation des données et des systèmes
- PRI Cyber : pour assurer une remise en fonctionnement d'une version "validée saine" du système d'information

MOYENS :

- Equipes CDS : Pilotes H24, Ingénieurs, Experts
- Equipes "Field" de remédiation
- SOC / NOC / CERT
- Partenaires technologiques experts, pen testing, formation

Références :

AAADATA · FFHANDBALL · FRANCE GALOP · QUADRILLE · SJB · SANTÉCLAIR · LADURÉE Paris

---

NOTRE MÉTHODOLOGIE S'ARTICULE EN 3 PHASES :

PHASE 1

Préventifs / Suivi :
- Fourniture, mise en oeuvre et paramétrage des solutions techniques nécessaires pour compléter le dispositif en fonction de la cible fonctionnelle
- Suivi quotidien par des spécialistes infra et cyber, y compris h24
- Veille, conseil, assistance (alerte de vulnérabilité, patching, trajectoire)
- Sauvegardes externalisée et managées : conformité 3-2-1, stockage immuable (sanctuarisation des sauvegardes)
- Suivi, testing régulier et évolution du processus de protection et de PRI ainsi que toutes ses composantes
- Pilotage de la prestation sécurité
- Tests d'intrusion et plans d'amélioration continue
- Formation et sensibilisation des utilisateurs

PHASE 2

Remédiation / Gestion de crise :
- Remédiation incident cyber (réseau, serveurs, postes de travail...)
- Analyse forensique suite détection d'incident pour identification de la cause racine

Cyber-SOC 360° by Tenexa

PHASE 3

Restauration / Remise en production :
- Restauration données et systèmes y compris vers cloud public Azure dans le cas d'infrastructures "sources" non-réutilisables (destruction ou compromission)
- Test en bac-à-sable des versions historiques (recherche et validation de version saine du SI)

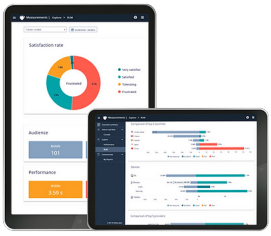
Solutions

Infodis propose des solutions techniques validées, packagées et managées pour venir compléter les systèmes déjà en place dans l'entreprise cliente.

Cyber-SOC 360° by Tenexa

EV Observe supervision technique :

EV Observe est une plateforme de monitoring pour l'infrastructure et les réseaux IT, l'Internet des objets (IoT), le cloud et les applications qui offre aux utilisateurs une expérience proactive et prédictive d'un bout à l'autre de la chaîne de production d'un service numérique. Avec EV Observe, les Directions Informatiques offrent à leurs utilisateurs une expérience du support plus proactive et prédictive. La grande souplesse de l'outil et ses fonctions avancées de Météo des Services permet un suivi synthétique et pertinent du fonctionnement des Infrastructures et d'anticiper les opérations de maintenance ou d'évolution.

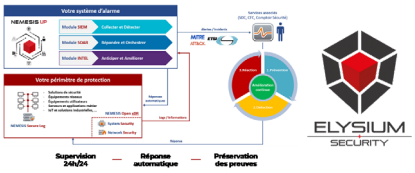


IP Label supervision applicative :

Ekara est une plateforme totalement hybride, capable de superviser 100% des applications existantes et de s'assurer de la disponibilité et de la performance de votre environnement (intranet et internet). Les parcours utilisateurs sont scriptés puis exécutés en permanence pour remonter la performance réelle ressentie par les utilisateurs et/ou valider la conformité du contenu présenté.

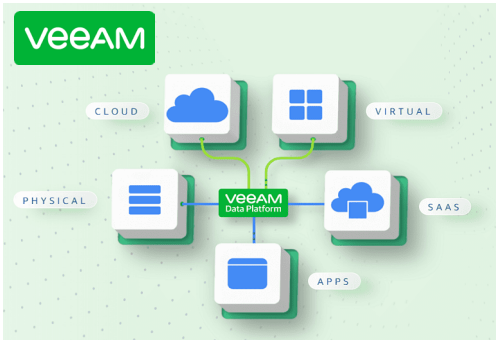
NemesisUP SIEM/xDR :

A l'image d'un système d'alarme, NEMESIS UP analyse en continu tous les événements générés lors de l'utilisation de vos ressources informatiques afin de détecter tout risque pour votre sécurité. Il fournit en un point central l'ensemble des outils utiles aux équipes en charge de la détection et de la réponse à incident et permet ainsi d'optimiser les ressources allouées à votre protection. S'adaptant à tous types d'environnements (IT/OT/CLOUD), NEMESIS UP démocratise l'accès à une protection globale et continue.



Veeam Sauvegarde/PRA :

Solution mondialement reconnue pour fournir une résilience des données grâce à une sauvegarde sécurisée et Solutions de récupération rapides et fiables pour l'ensemble de votre infrastructure IT et Cloud. Infodis IT opère le service pour ses clients et l'intègre pour aller jusqu'à la gestion complète de PRI.



Azure Cloud Public de reprise :

Les plateformes Azure IaaS et Storage sont exploitées par les services de Sauvegarde et PRI Infodis IT. Services cloud hautement sécurisés, disponibles et scalables, cela permet de garantir un stockage et une reprise des services en maîtrisant au mieux les coûts.

Agora Calycé - VMWare VCDA : Cloud Privé de reprise et d'analyse en bac à sable

Experts de l'hébergement sensible et complexe : un prestataire féru de nouvelles technologies, prêt à vous accompagner avec un maximum de proximité et de transparence.

C'est cet ADN qui différencie Agora Calycé : la technologie et de la relation en priorité. Une expertise et une maîtrise des solutions d'hébergement, un engagement pour vous aider à construire les meilleures stratégies, bâtir les bonnes plateformes, réaliser les déploiements.

agoracalycé groupe E'nergys