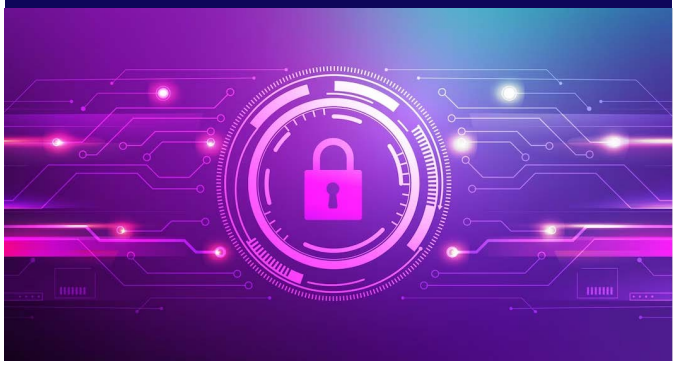
Cyber-SOC 360° by infodis



Nous proposons une approche complète de la Cyber-Sécurité incluant les aspects préventifs, défensifs (protection), d'actions rapides comme l'analyse forensique et la 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 :

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 infodis

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)