Cyber4U

Le 1er Centre de Cybersécurité Pour Tous
ETI - Filiales Grands Groupes - Sous-Traitants

Retrouvez toute la liberté d'entreprendre !

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

FRANCE RELANCE

PLAYFRANCE
Numérique, industrie stratégique

CAMPUS CYBER
ASSOCIÉ

PROFESSIONNEL RÉFÉRENCÉ
CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

www.cyber4u.fr

L’offre de Sécurité Managée MSSP

Le constat Cyber4U

- On estime à 94 jours, le délai moyen de détection d'une attaque sur une entreprise européenne.
- Les entreprises ont empilé des solutions de protection sécurité et doivent maintenant être capables de détecter en flux continu les attaques informatiques.
- Le renfort par un MSSP est une nécessité pour les ETI qui souhaitent pérenniser leur relation avec les grands groupes et leur position dans les secteurs sensibles*.

* OIV – LPM – HDS (Santé)

Les services du MSSP C4U

Le service MSSP C4U recouvre trois cas d'utilisation :

- La Supervision SOC, de base et avancée, des outils de la sécurité
- La Détection avancée des menaces : l'alerte en temps réel, l'analyse et la création de rapports sur les activités à risque.
- Le Maintien en Condition de Sécurité (MCS) des outils de la cybersécurité

La valeur ajoutée de l'offre MSSP C4U

- **Le SOC C4U** est idéal pour les Entreprise de Taille Intermédiaire et pour les filiales des grands groupes recherchant un renfort AGILE à moindre coût.
- **Le SOC C4U** répond au besoin d'administration des outils par des spécialistes Cyber pour éviter **« l'abandon de l'administration sécurisé ».**
- **Le SOC C4U** répond idéalement **à la surcharge du RSSI** par les alertes non qualifiées et des incidents de « bas niveau ».

Détecter les attaques et gérer vos outils de sécurité

Volet Surveillance

✔ **Gérer les alertes & attaques**
Le SOC est aux avants postes pour détecter, lever le doute, le tuning de nouvelles alertes et contribuer au plan de remédiation

✔ **Détecter les comportements d'administration à risque**
Les mauvaises pratiques : partage de compte, mots de passe inchangés, utilisation illégitime de comptes à très hauts privilèges.

✔ **Détecter les logiciels à risque**
Des logiciels installés sans droit administrateur exfiltrent des données.

✔ **Détecter les modifications systèmes**
Détecter les changements systèmes, les suppressions de logs, les violations des règles de sécurité.

Volet Protection

✔ **Déployer les outils de sécurité**
La couverture d'agents de surveillance et de protection actifs est contrôlée sur l'ensemble du parc informatique.

- Agent SOC/SIEM4U
- Antivirus (Ws/Linux)
- Virtual Patching
- Web Application Firewall
- Détection de vulnérabilité
- Stations blanches,…

✔ **Administrer les outils de sécurité**
SOC, WAF, IPS, anti-malware,… pour un maintien en condition de sécurité.

✔ **Sécuriser les données du SOC**
Gérer les accès, sécuriser l'infrastructure et des données, maintenir en condition de sécurité.

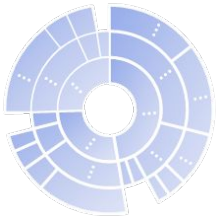
✔ **Intégrer de nouvelles sources**
FW, Proxy, WAF, AV, Tiers 0, VIP/VOP…

Volet Pilotage

✔ **Gérer la traçabilité des alertes**
La liste des alertes et du résultat de l'instruction avec un traçabilité des constats et justifications.

✔ **Mettre à jour la documentation**
Une dizaine de documents depuis la liste des alertes au dossier de sécurisation.

✔ **Mettre à jour le Dashbord sécurité**
Rendre compte de l'activité sécurité opérationnelle.



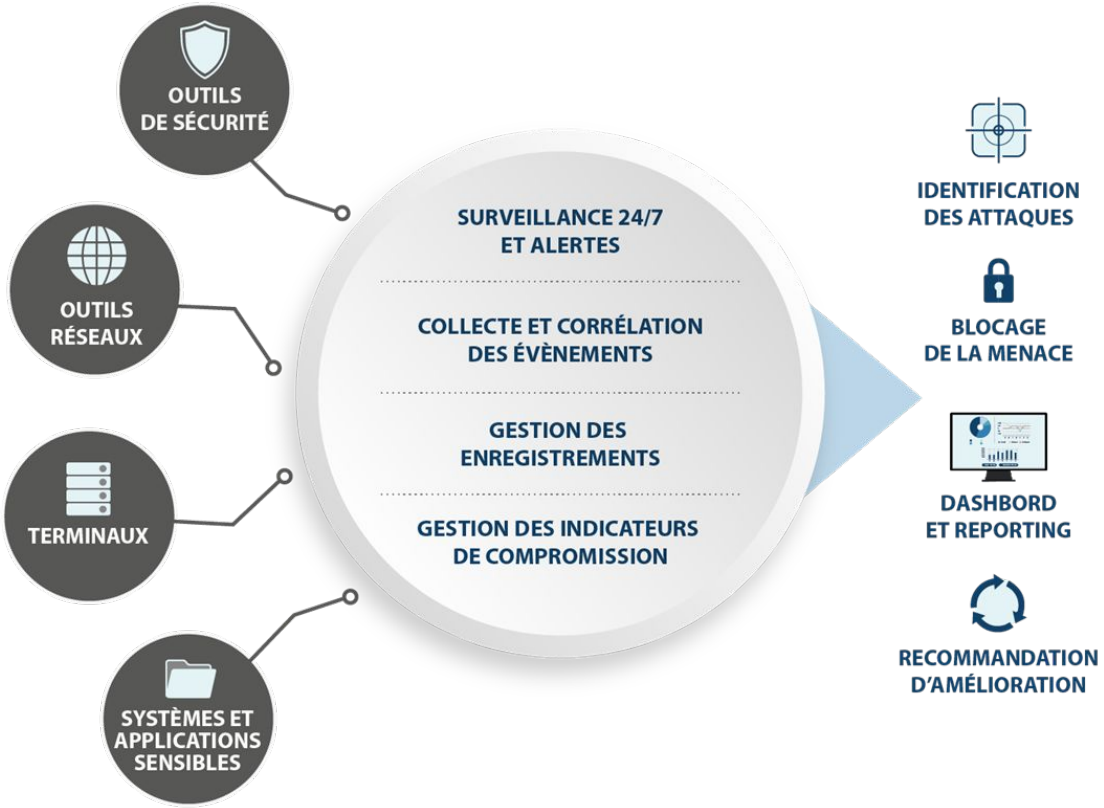
Les livrables MSSP C4U

Les Dashbords et les livrables

- ✔ Inventaire des attaques, des risques et recommandations associées
- ✔ Inventaire des comportements d'administration à risque et recommandations associées
- ✔ Inventaire des logiciels à risque et recommandations associées
- ✔ Inventaire des modifications systèmes à risque et recommandations associées

- ✔ Taux de couverture et des protection des actifs par les outils de sécurité
- ✔ Rapport de MCS des outils de sécurité
- ✔ Dossier de sécurité des données du SOC
- ✔ Rapports d'intégration des nouvelles sources à superviser

- ✔ Dashboard sécurité opérationnelle
- ✔ Journal des alertes
- ✔ Organisation du SOC et engagements de services
- ✔ Procédure d'escalade et gestion des attaques
- ✔ Messages à destination du RSSI



La console MSSP C4U

Une console de supervision simple pour une efficacité maximale

VIP&VOP attaqués

Causes racines à traiter suite aux incidents détectés (vulnérabilité,…)

Origines des attaques
& Régions sous contrôle

Nb incidents détectés, ouverts & clôturés

Taux de couverture des outils sécurité

Cartographie métier (sensibilité des territoires)

Le service MSSP C4U

Un service d'assistance en mode managé de niveau L1, L2 et L3.

L1	Supervision des évènements et détection Paramétrage de sécurité
L2	Soutien à la qualification des incidents Assistance à l'instruction en lien avec le client
L3	Forensic, Recherche des preuves, MCS, Archivage règlementaire

Expériences clients

Des retours d'expérience clients qui nous confortent dans notre stratégie de développement

Notre réseau d'expertise

Nom	Description
EXPERT CYBER	Label sécurité numérique
CIMA	Cybermalveillance.gouv.fr
ANSSI	Agence Nationale des Systèmes d'Information
OWASP	Open Web Application Security Projet
ISO	International Organization for Standardization
CNIL	Commission nationale de l'informatique et des libertés
NIST	National Institute of Standards and Technology
RGPD	Règlement général sur la protection des données
MITRE ATTACK	Adversarial Tactics, Techniques, and Common Knowledge
CESIN	Club des Experts de la Sécurité de l'Information et du Numérique
AFCDP	Association Française des Correspondants à la protection des DCP

Contact :

www.cyber4U.fr

06 11 92 23 97
Commercial@cyber4U.fr