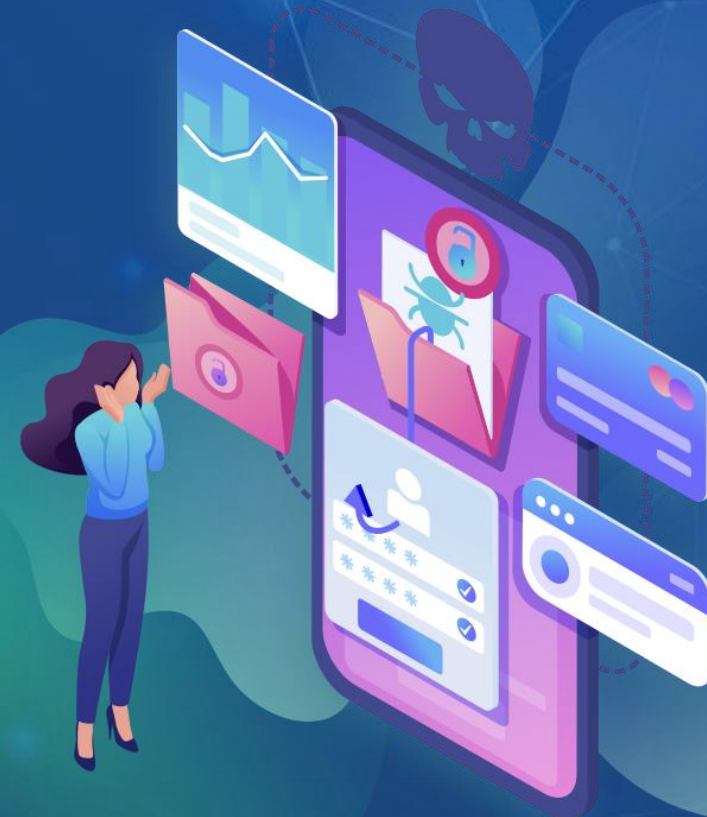


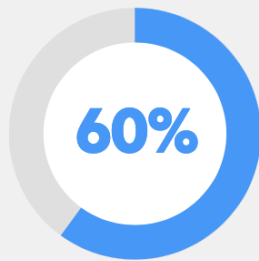
*Pourquoi avez-vous besoin
d'un SOC 24/7 ?*

**Notre offre SOC
WithSecure SÉRÉNITÉ**

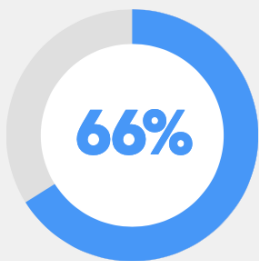


Le constat

**DANS LE CAS DES PME,
60 % DES DÉCISIONNAIRES NE DISPOSENT
D'AUCUNE STRATÉGIE POUR PRÉVENIR OU
RÉPONDRE À UNE CYBER ATTAQUE**



**66% CONSIDÈRENT QUE LEUR
ENTREPRISE N'EST PAS SUSCEPTIBLE
D'ÊTRE VISÉE PAR UNE ATTAQUE**



68 % des entreprises ont détecté au moins une cyber attaque et 49 % ont été ciblées à plusieurs reprises au cours des 12 derniers mois.

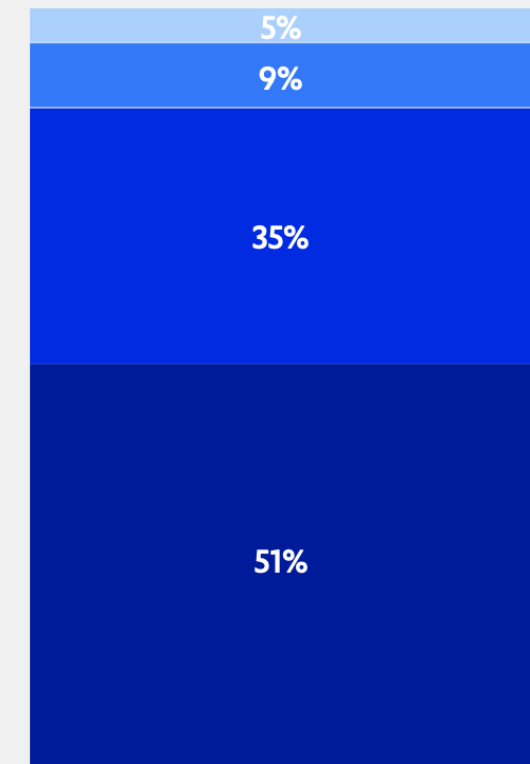
étude de marché 2020 menée par F-Secure

- Une cyber attaque peut être suffisamment élevée pour conduire une entreprise à la faillite.
- Impact dévastateur de la paralysie de l'activité, de la perte de confiance des clients, de la fuite de données...

Les Menaces

- Croissance exponentielle des surfaces d'attaque liée au télétravail
- Les SPAMS représentent 51 % des tentatives d'infection en 2020
- 35 % des malwares introduits via des téléchargements manuels (outils de visio, port RDP ouvert)
- Kit d'exploits (virus, backdoor) utilisant les failles de sécurité représentent 10%
- Augmentation des ransomwares (emails malveillants) visant les entreprises

MÉTHODES DE DIFFUSION DES MALWARES



- E-mails
- Installation manuelle / Charge utile secondaire
- Kit d'exploit / Exploitation de logiciels / Publicité malveillante / Téléchargement Drive-by
- Cracks de logiciels / Packs logiciels

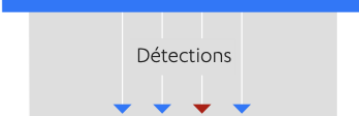
Comment se protéger



1 Sondes sur les postes de travail, serveurs, terminaux mobiles



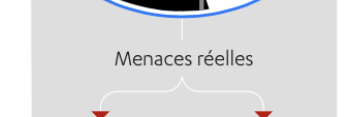
2 EPP & EDR collectent les données pour examiner les évènements suspects des activités.



3 Le SOC reçoit une liste filtrée d'alertes sur son tableau de bord



4 Une fois les menaces isolées du réseau, le SOC mènent des actions de réponses

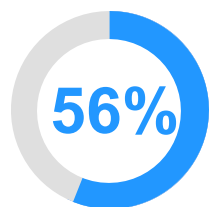


“ En faisant appel à notre SOC, vous serez en capacité de détecter les cyber attaques à un stade précoce, avant qu'elles ne nuisent à votre activité.

Et si on vous disait que **30 % de votre parc** n'était pas protégé

Que **seul 40 % de vos postes sont à jour** et que plus d'un ordinateur sur trois a une mise à jour de sécurité critique manquante

Êtes-vous prêt à prendre ce **risque** ?



56% des violations de données passent inaperçues durant plusieurs mois



Il faut aux entreprises 280 jours en moyenne pour repérer et contenir une violation de données

(Source : Ponemon Cost of a Data Breach Report 2020)

Complétez votre **protection** !

Pack SÉRÉNITÉ
WithSecure EPP/EDR



Optez pour notre solution tout en un **infogérée** par nos équipes



Principales fonctionnalités :

EPP :

- ✓ Protection et détection
- ✓ Mise à jour de sécurité
- ✓ Protection trafic Web
- ✓ Antimalware
- ✓ Contrôle des connexions

EDR : (+ fonctionnalités EPP)

- ✓ Analyse comportementale
- ✓ Remédiation
- ✓ Isolation des postes infectés
- ✓ Détection avancée



Service 100% managé

Supervision 24h/24 par notre Centre de Services

Détection et prévention des risques

Remédiation sur incidents

Mise à jour de sécurité

Contact en cas de failles de sécurité

Expertise de notre SOC

Reporting personnalisé



Pack SÉRÉNITÉ

WithSecure Element

(licence + service managé)

Prix mensuel

Pack SÉRÉNITÉ EPP & EDR :

17€ / poste de travail

25€ / serveur

Pack SÉRÉNITÉ EPP :

13 € / poste de travail

17 € / serveur

15€ / mobiles

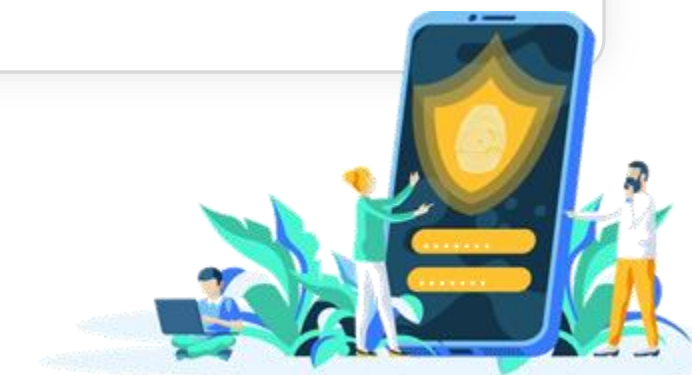
Contactez nous :



0825 745 692

06 17 78 11 96

soc@reelit.fr



Nos gestes techniques

SOC 24/7/365 (Astreinte en HNO)

- Ajout / Modification / Suppression licence poste de travail
- Ajout / Modification / Suppression licence serveur

SOC

Inclus

- Mise à jour logicielle
- Installation patch de sécurité (critique)

Inclus

- Mise en isolation du réseau
- Remise sur le réseau

Inclus

- Suppression de l'appareil (liste de blocage ou définitif)

Inclus

- Remédiation (suppression fichiers, MBR, Registry ...)

Inclus dans EDR

Merci pour votre attention !



Nous contacter
soc@reelit.fr

0 825 745 692 / 06 17 78 11 96