



Orange
Cyberdefense

Securing the new digital enterprise



Guillaume Chabas

Expert Cybersécurité



Contexte et Enjeux

\$ 3,5m par an

représente le coût d'une faille de sécurité dans une organisation

Plus de 3 entreprises sur 4

gèrent des transactions en ligne et/ou proposent des services online à leurs clients/usagers

1 loi par an

depuis 10 ans
LPM, RGS, RGPD/GDPR
Règlementation sur la protection des données personnelles (4% du CA)

Le risque cyber est protéiforme et touche tous les secteurs

La transformation digitale multiplie les fenêtres d'attaque

La cybercriminalité s'industrialise

La pression réglementaire se poursuit

70% des utilisateurs

sont équipés d'au moins trois devices différents pour se connecter au SI

100 %

des entreprises touchées au moins une fois.

Pression

des compagnies d'assurances et des agences de notation financière.

Démonstration



L'ambition



Protéger les nouveaux process numériques

Dès lors que les nouveaux process numériques, les métiers et savoir-faire de demain seront sécurisés, ils deviendront un axe de progrès, d'innovation et de développement stratégique des entreprises.



Cibler les actifs à protéger

Le risque 0 n'existe pas. Il faut que l'entreprise/l'organisme se concentre sur la protection des actifs sensibles et limite l'impact des incidents qui ne pourront être évités.



Fournir une réponse holistique

Hier à la recherche ponctuelle d'un expert dans un domaine spécifique de la sécurité, l'entreprise demande aujourd'hui un partenaire capable de l'accompagner sur toutes les dimensions de sécurité.

Protéger vos essentiels

Nous concevons, opérons et surveillons les systèmes de défense qui protègent vos actifs critiques.



Vos processus
métiers, industriels
et leur disponibilité



Vos données
économiques
& financières



Vos données personnelles
& professionnelles
(clients & collaborateurs)



Votre propriété
intellectuelle



Votre
réputation



Identifier vos essentiels
(risques, menaces, vulnérabilités)

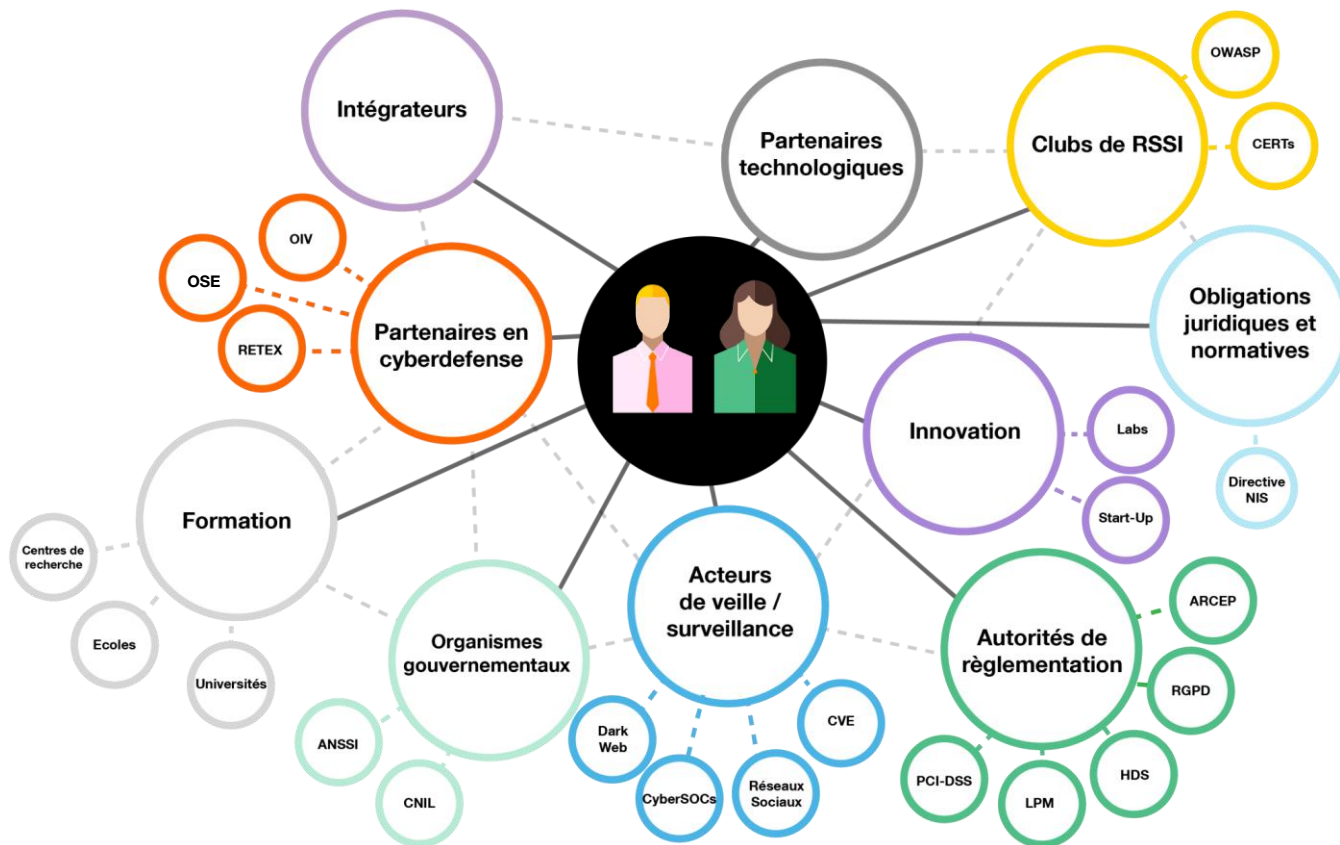


Déployer l'éco système
de défense



Adapter à vos modèles
économiques et votre stratégie

Impossible de lutter seuls



Orange Cyberdefense : l'entité d'Orange **dédiée** **à la sécurité** des entreprises



Nous accompagnons tout type et taille
d'entreprises et d'organisations :
banque, transport, santé, secteur
public, industrie...



30

années d'expérience en
sécurisation
d'infrastructures sensibles



+ 1 200 experts Orange
Cyberdefense,



dont + de 300 situés à Rennes
et Nantes

Une approche 360°



Identifier

Identifier vos expositions face aux risques, avoir une bonne vision de vos intérêts et priorités. Prévenir, former et sensibiliser.

Protéger

Protéger vos actifs critiques au travers d'un arbitrage sur les choix de solutions techniques et le budget à associer.

Détecter

Surveiller, détecter et analyser les événements de sécurité.

Réagir

Intervenir en cas de crise avérée et réagir à l'incident : le comprendre, le contenir et y remédier.

Anticiper

Connaître et anticiper les menaces émergentes, pouvoir les caractériser et anticiper leur évolution.



Identifier vos expositions face aux risques, avoir une bonne vision de vos intérêts et priorités. Prévenir, former et sensibiliser.

Etre conseillé pour orienter mon action et mes moyens sur les sujets prioritaires



Conseil

Tester mon système d'information sur ses faiblesses



Tests d'intrusion

Mettre mes systèmes en conformité avec la réglementation applicable à mon secteur



Audit et conformité

Eprouver la sécurité de mes systèmes d'information les plus critiques



Scans de vulnérabilité

Former mon personnel aux meilleures pratiques et les entraîner à réagir en cas d'attaques



Formation et sensibilisation



Protéger vos actifs critiques au travers d'un arbitrage sur les choix de solutions techniques et le budget à associer.

Etre accompagné dans le choix des mes solutions

Protéger les accès à mon système d'information

Protéger mes données et mes applications dans le Cloud

Protéger mes réseaux, ma messagerie

Garantir la confidentialité des données personnelles

Protéger les identités et les droits d'accès de mes collaborateurs

Sécuriser / chiffrer ma flotte et mes communications mobile



Conseil



Protection du Web et du réseau



Protection des données et des applicatifs



Gestion des identités et des accès



Sécurité des terminaux mobile



**Surveiller, détecter
et analyser les
événements de
sécurité.**

**Etre accompagné sur toutes mes activités de
détection**

**Surveiller mon système d'information
en continu
Pouvoir détecter les comportements
inhabituels**

**Détecter les nouveaux comportements
(familles de malwares, attaques, ...)**

**Lever les doutes et avoir un correspondant
fiable en support**



**Conseil stratégique,
audit de maturité,
mesure d'efficacité**



24/7 CyberSOC



Lab d'épidémiologie



Analystes



Intervenir en cas de crise avérée et réagir à l'incident : le comprendre, le contenir et y remédier.

Etre accompagné dans le suivi des plans d'action, orienter mes priorités d'actions

Pouvoir qualifier grâce à l'aide d'experts immédiatement disponibles, l'ampleur et la nature de l'attaque

Etre accompagné à la reconstruction de mon système d'information

Etre aidé dans la gestion de la crise par des équipes multi-disciplinaires (IT, juridiques, Communication ...)

Pouvoir tirer les enseignements de mes crises



Conseil



Réponse à incidents en 24/7 C-SIRT



Information légale (digital Forensics)



Cyber résilience



Connaître et anticiper les menaces émergentes, pouvoir les caractériser et anticiper leur évolution.

Connaître les dernières vulnérabilités de mon système d'information.

Connaître les menaces émergentes qui pèsent sur mon secteur d'activité.

Savoir si des attaques sont en préparation (Hacktivisme)

Savoir si mes données ne sont pas en circulation sur Internet (Dark Web, forums ...)

Connaître la réputation des mes VIP

Connaître le niveau de sécurité et la confiance à accorder à certains éditeurs/hébergeurs



Bulletins de veille et de Threat Intelligence

Surveillance technique des sites web et réputation IP



Cyber surveillance

▶ **Veille en recherche de contenu ciblé**

▶ **Surveillance de la fraude**



Veille juridique et réglementaire

Merci

