

# 6 RAISONS D'ADOPTER UN SECURITY OPERATIONS CENTER (SOC)

## 1/ Des menaces qui explosent et se complexifient

Les cyberattaques ont augmenté en France de

# 50%



# 52%

 des entreprises françaises ont été piratées

## 2/ Un manque de visibilité sur les incidents



# 66%

des entreprises ont été compromises pendant des mois ou plus, avant de s'en rendre compte

# 220 jours

c'est le temps moyen avant de détecter une compromission réussie.



## 3/ Un manque de moyens



# 50%

des RSSI pensent qu'il n'est pas simple de déterminer l'étendue d'une brèche, de la contenir et d'y remédier après une attaque !



# 35%

des postes ouverts en cybersécurité ne sont pas pourvus.

# 80 jours

Il faut 80 jours pour contenir une compromission après sa détection.



## 4/ Une fausse idée de la cyber-fraude



3/4 des décideurs pensent que l'augmentation des cyber-fraudes n'a pas excédé 25% sur l'année 2015...

considèrent le risque de subir une cyber-attaque comme faible...



...pourtant elle est supérieure à 50%

...En fait 52% des organisations ont déjà subi des attaques.

## 5/ Des nouvelles contraintes réglementaires

### LPM

Loi de Programmation Militaire

En vigueur depuis le 1er juillet 2016

Elle impose aux OIV (Opérateurs d'Importance Vitale)

- De mettre en oeuvre SOC
- De signaler immédiatement aux autorités tout incident de sécurité

Amende maximale encourue : **370 K€**



### GDPR

General Data Protection Regulation

En vigueur au 25 mai 2018 en UE

Règlement européen s'appliquant à toute entreprise qui collecte, traite et stocke des données personnelles. Il impose:

- De mettre en oeuvre un système de sécurité et gouvernance de ces données
- De déclarer toute brèche de sécurité dans les 72h

Amende maximale encourue : **20 M€**



## 6/ De graves dommages business

# 3,4 millions d'euros



C'est le coût moyen d'une brèche informatique en France



# 70%

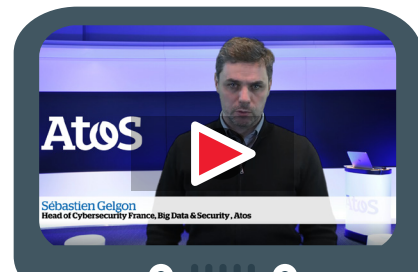
des entreprises ne sont pas certaines de pouvoir se relever après une attaque

## Anticiper en passant de la réaction à la démarche proactive d'un SOC ( Security Operation Center)



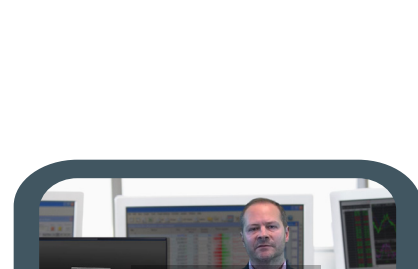
### Le SOC Atos en partenariat avec RSA c'est :

**Une expertise et une réponse adaptées** grâce à une stratégie « Follow the Sun » basée sur un réseau mondial de SOC's, plus de 200 analystes et la proximité immédiate d'équipes CSIRT (Computer Security Incident Response team).



**Des Process éprouvés de cybersécurité**, par exemple dans le cadre de grands événements sportifs mondiaux.

**Des technologies Advanced SOC, telles que RSA Netwitness Suite** la plate-forme de détection et réponse aux menaces. Elle collecte, gère, opère des analyses Big data & comportementales de toute l'activité sécurité (Logs, flux et paquets réseaux, Endpoints, cloud, ... ) et stoppe en temps réel les menaces les plus complexes.



# Atos

# RSA

## Sources

- ANSSI, Agence nationale de sécurité des systèmes d'information
- Etude du cabinet Denjean & Associés en partenariat avec Gan Assurances
- RSA Cybersecurity Poverty Index 2016 - Annexe EMEA
- Verizon breach report 2014
- Ponemon Institute, 2016 France Cost of Data Breach Study
- Data protection index, EMC 2016