koesio
Corporate IT

CYBER**RÉSILIENCE**

METTRE EN PLACE SON **BOUCLIER NUMÉRIQUE** AVEC NOTRE SOLUTION DE **REPRISE D'ACTIVITÉ**

EN PARTENARIAT AVEC vmware by Broadcom

koesio
Corporate IT

VOS **EXPERTS** DU JOUR

DAVID **PIROCCHI**
DIRECTEUR **TECHNIQUE**
KOESIO CORPORATE IT

JEAN-PHILIPPE **LASSERRE**
RESPONSABLE **AVANT-VENTE**
KOESIO CORPORATE IT

MARC **BOURGEOIS**
SR **CLOUD PROVIDER** MANAGER
VMWARE

GILLES **HEDREUX**
CLOUD **SERVICE PROVIDER**
VMWARE

SOMMAIRE

koesio
Corporate IT

Terminologie

- **ANSSI** : Agence nationale de la sécurité des systèmes d'informations - Instance Française de la Sécurité du Numérique.
- **Cybercriminalité** : désigne l'ensemble des moyens, et/ou des comportements d'attaques, et/ou de menaces, appliqués au domaine du numérique.
- **BKP :** Backup, solution de sauvegarde des données
- **DRP :** Disaster Recovery Plan, Solution permettant de palier à une perte de l'environnement de production et BCP.
- **Iso27001 à 27005** : Normes ISO dédiées à la sécurité du numérique permettant notamment de mettre en œuvre un SMSI (ISO27001 système de management de la sécurité informatique) , et de suivre des processus réguliers d'audit des SI.
- **IT** : Information Technology, désigne les solutions déployées dans le périmètre des technologies de l'information.
- **RPO** : (Recovery Point Objective) désigne la durée maximale d'enregistrement des données qu'il est acceptable de perdre lors d'une avarie. Cette durée varie de zéro à quelques heures.
- **RTO :** (Recovery Time Objective) spécifie le délai maximum toléré avant de reprendre son activité. Ce délai varie de zéro seconde à plusieurs heures.
- **ROI** : Return on Investment, retour sur investissement
- **IaaS** : Infrastructure as a service, désigne le principe de disposer de serveurs virtuels/physiques hébergés en cloud public/privé.
- **SaaS** : Software/Storage as a service, désigne le principe de disposer d'applications ou de volumes disques hébergés en cloud public.
- **DRraS** : Disaster Recovery as a Service, est une stratégie visant à protéger l'entreprise en cas d'interruption de son activité
- **BaaS** : Backup as a Service, est une solution managée d'externalisation de la sauvegarde des données.
- **PCA :** Plan de continuité d'activité (pour toutes activités confondues de l'entreprise).
- **PCAI :** Plan de continuité d'activité restreint au domaine informatique.
- **PRA** : Plan de reprise d'activité (pour toutes activités confondues ou spécifiques de l'entreprise).
- **PRAI** : Plan de reprise d'activité restreint au domaine informatique.
- **PSI :** Plan de secours informatique.

koesio Corporate IT

DISASTER RECOVERY
/
ENJEUX

koesio
Corporate IT

DISASTER RECOVERY | CONTEXTE

RISQUES ET MENACES

DÉVELOPPEMENT DES **USAGES** = ÉCOSYSTÈME DE + EN + OUVERT

DÉPENDANCE CROISSANTE À L'INFORMATIQUE

DÉPENDANCE DU SI/IT SUR LES FLUX MÉTIERS

23% V.A. (GARTNER FR 2022 – PME <250)

DATA = INFORMATION CENTRALE AUX **MÉTIERS**

COMPLEXITÉ TECHNOLOGIQUE

NORMES DE CONFORMITÉ ET RÉGLEMENTATIONS

DISASTER RECOVERY | OBJECTIFS

- MINIMISER LE TEMPS D'ARRÊT
- PROTÉGER LES DONNÉES CRITIQUES
- MAINTENIR LA CONFIANCE DES CLIENTS
- GARANTIR LA CONTINUITÉ DES OPÉRATIONS
- RÉDUIRE LES PERTES FINANCIÈRES
- RÉTABLIR LA PRODUCTIVITÉ
- ÉVALUER ET AMÉLIORER CONTINUELLEMENT

koesio Corporate IT

DISASTER RECOVERY | QUELQUES CHIFFRES

3 STATISTIQUES (Ilcbuddy oct. 2023)

- **43 %** des entreprises ne reprennent jamais leur activité après un événement majeur de perte de données
- **93 %** des entreprises qui n'ont pas pu récupérer leurs données dans les dix jours suivant le drame ont dû déclarer faillite dans l'année
- **96 %** des entreprises qui disposent d'une solution de reprise après sinistre sont en mesure de reprendre complètement leurs activités après une perte de données catastrophique

STATISTIQUES CYBERCRIMINALITÉ

- #1 E.U. ; #2 Chine ; **#3 Cybercriminalité** (devant les marchés de la drogue et du sexe cumulés)
- 10,5 $Billion (Prévisionnel 2025 +40% Vs 2021)

koesio Corporate IT

DISASTER RECOVERY | RANSONaaS - UN ÉCOSYSTÈME QUI S'EST PROFESSIONNALISÉ

ANALYSE DE LA RENTABILITÉ DU CYBERCRIME – CAMPAGNE D'ATTAQUE SUR 20 CIBLES

COÛTS

1 – Constitution de l'infrastructure d'attaque
- Hébergement sécurisé **~900 $**
- VPN (anonymat) **~120 $**
- 20 accès piratés à des entreprises **60 000 $**

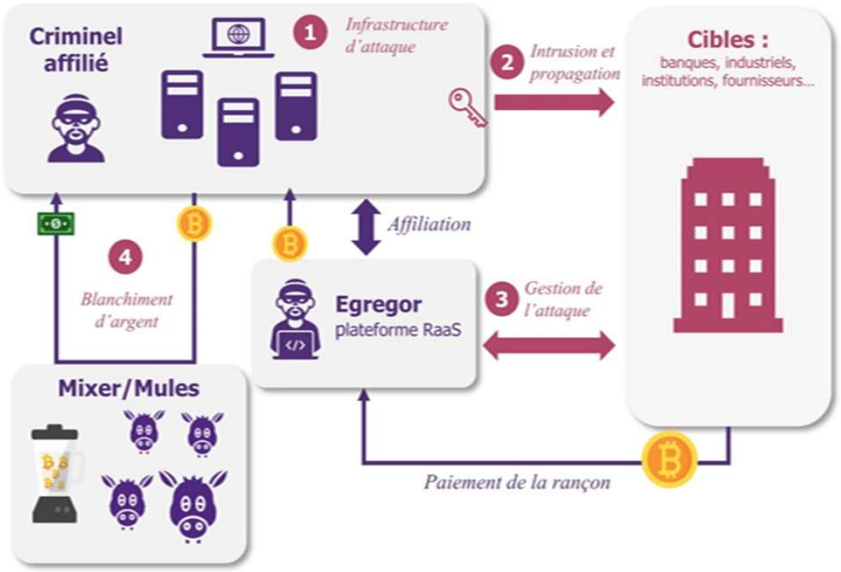
2 – Intrusion dans les systèmes et propagation
- Ressources humaines* et outils de propagation (type Cobalt Strike)

3 – Gestion de l'attaque
- Ressources humaines* et commission pour le RaaS **30 % des gains**

4 – Blanchiment d'argent
- Anonymat des Bitcoins **0.5 % des gains**
- Blanchiment et conversion en monnaie réelle **50 % des gains**

***Ressources humaines**
3 x 3 mois (500 $/j)
90 000 $

Coût total
151 020 $



GAINS

Cibles piratées
20

Rançons demandées entre
1.5 M$ et 2.5 M$

% des acteurs payant la rançon
entre **6** et **10 %**

Montant rançon négocié entre
- 15 % à **- 20 %**

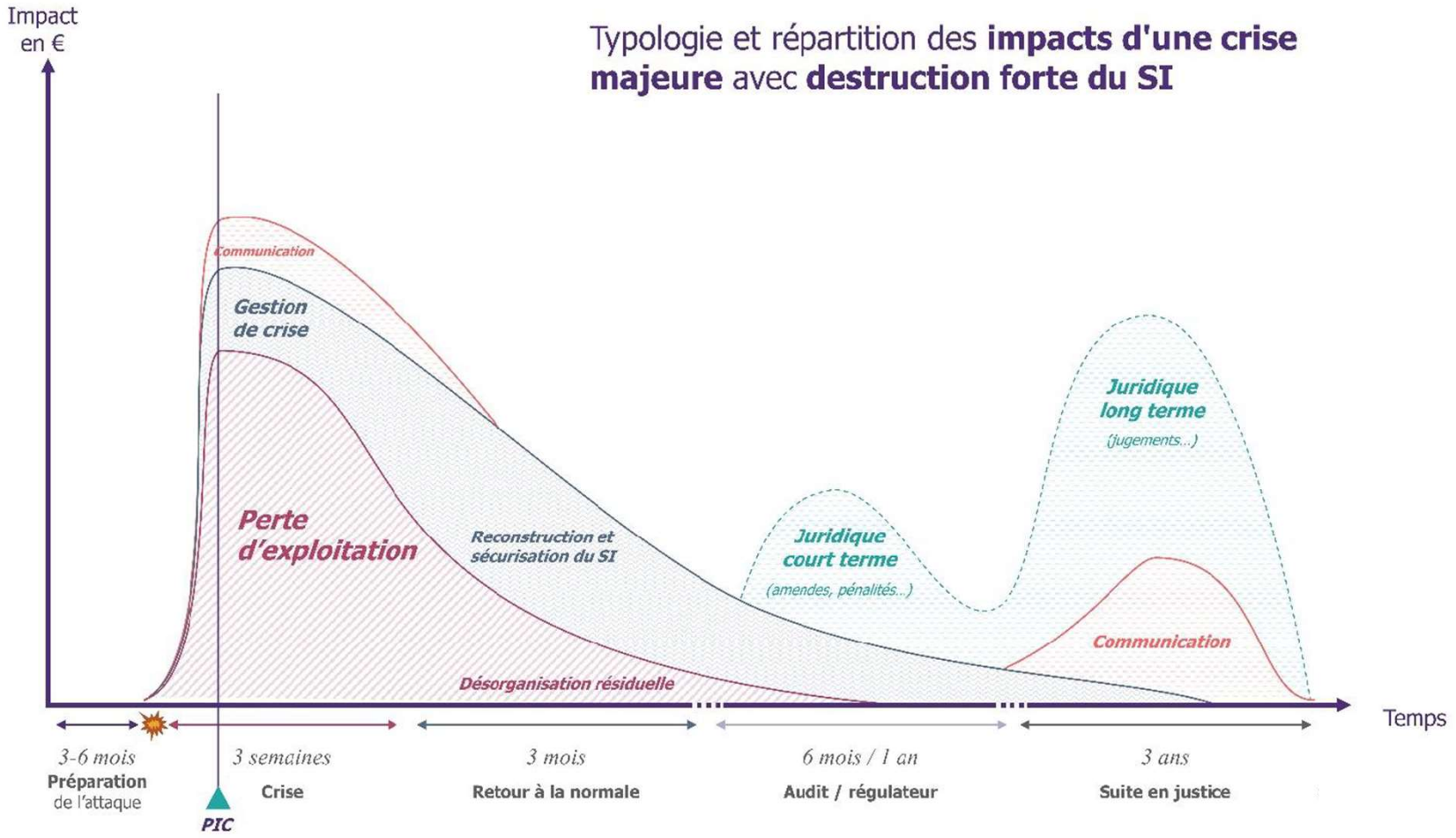
Gain total brut entre
1.4 M$** et **4.3 M$
(avant paiement plateforme RaaS et blanchiment)

GAIN NET (APRÈS BLANCHIMENT) : ENTRE 500 K$ ET 1,5$ | **ROI ENTRE 232% ET 880%**

Source Sénat.fr / https://www.senat.fr/rap/r20-678/r20-678_mono.html

koesio Corporate IT

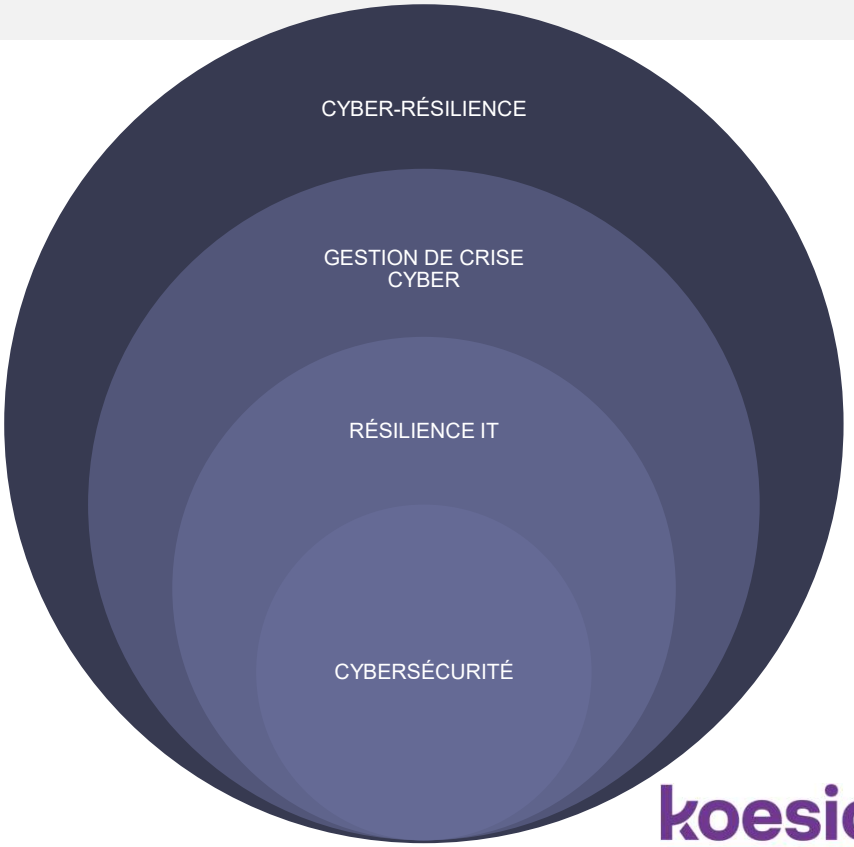
DISASTER RECOVERY | GESTION DE LA CRISE



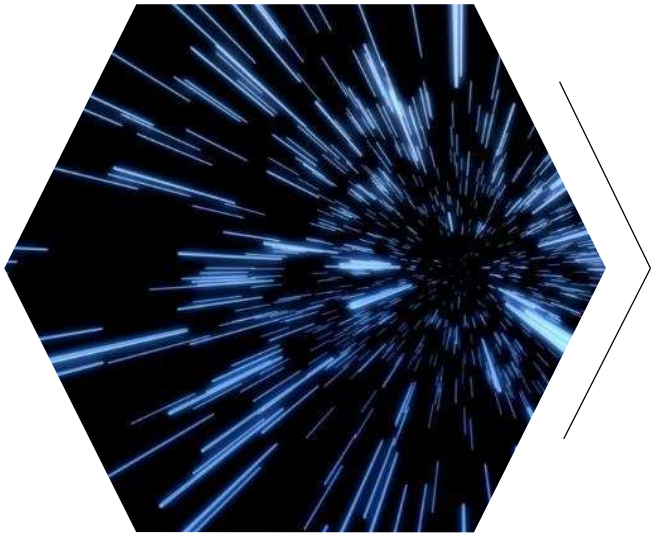
CONCLUSION D.R.P. | CYBER-RÉSILIENCE & COMPLIANCE

L'**objectif ultime** à atteindre par toute **Entreprise soucieuse de la Sécurité de son Système d'Information** est :

➢ L'adoption d'une **posture cyber-résiliente**



DISASTER RECOVERY | ENJEUX DE PROXIMITÉ SERVICES IT



INDISPENSABLE D'ASSOCIER

DES NIVEAUX DE SERVICES OPÉRATIONNELS DE PROXIMITÉ

POUR PRÉVENIR ET RÉAGIR RAPIDEMENT

ANALYSE RISQUE

PROCÉDURE DE GESTION DE CRISE

TEST ANNUEL

GESTION DE CRISE ET DE REMÉDIATION

koesio Corporate IT

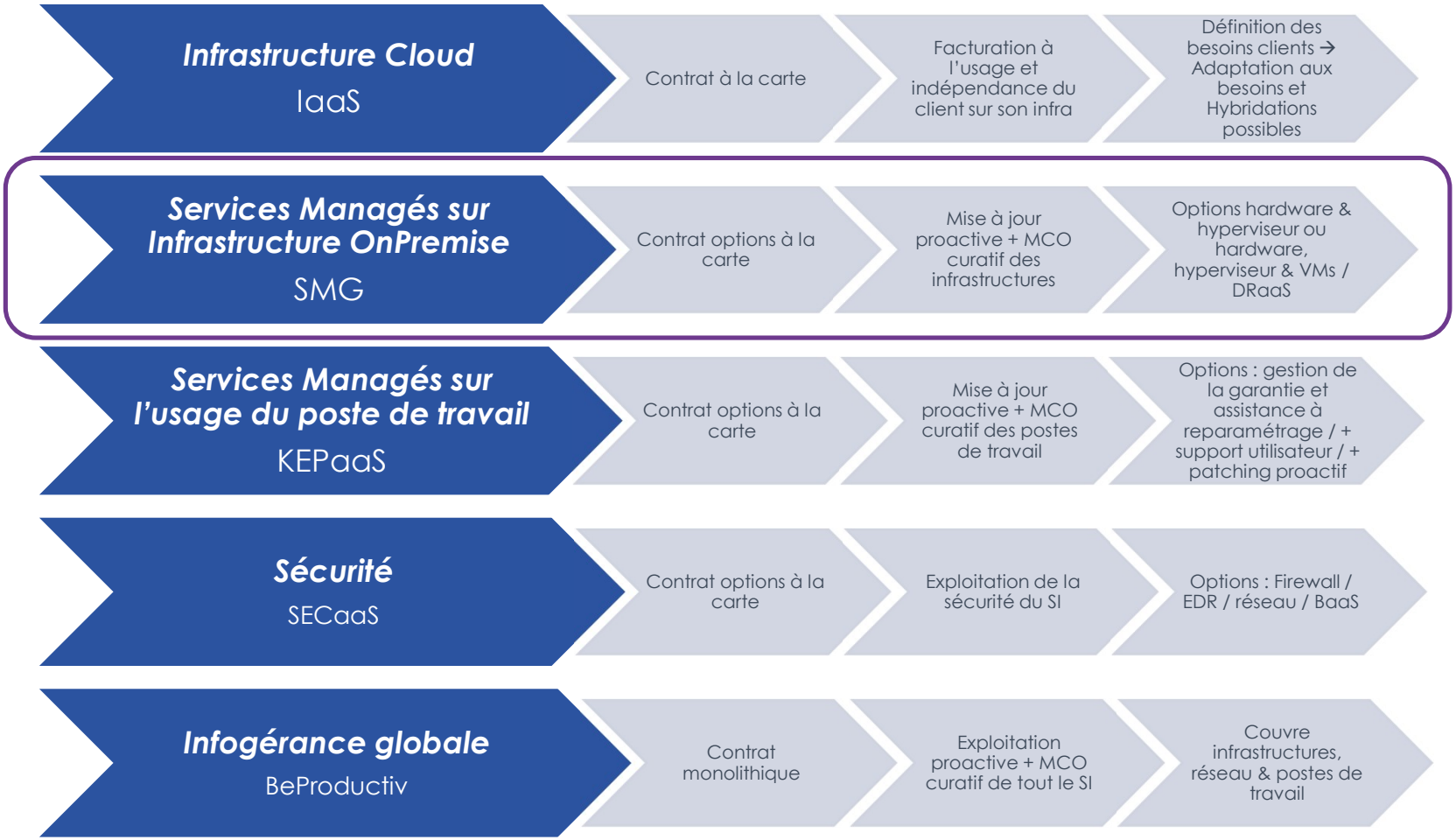
CyberRésilience
/
Les Solutions koesio Corporate IT

SOLUTIONS MATRICIELLES | NIVEAUX DE RÉSILIENCE

SOLUTIONS / NIVEAUX DE RÉSILIENCE	**CLUSTER** ON-PREMISE + IAAS	**BKP** ON-PREMISE	**DRP** ON-PREMISE	**DRAAS** DRP AS A SERVICE	**BKP IMMUABLE** ON-PREMISE	**BAAS** BKP IMMUABLE AS A SERVICE	**BKP EXTERNALISÉ OUT-OF-BAND**	**CONSULTING & EXPERTISES**
DISPONIBILITÉ	X	X	X	X				
CONTINUITÉ	X	X						
REPRISE D'ACTIVITÉ			X	X				X
REPRISE SUR RESTAURATION					X	X	X	X
KOESIO	X	X	X	X	X	X	X	X
RTO	SEC.	0-5 sec.	10 – 30 mn	30 mn <=> 4 hr	12 hr <=> 24 hr	24 hr <=> 72 hr	24 hr <=> 72 hr	12 hr <=> 24 hr
RPO	SEC.	0-5 sec.	1 hr	30 mn <=> 4 hr	<= 24 hr	<= 24 hr	24 hr <=> 72 hr	

koesio Corporate IT

| CATALOGUE DES SERVICES



Disaster Recovery Plan
/
Focus Solution Cyber-résilience
koesio Corporate IT BaaS - DRaaS

| OPÉRATEUR CLOUD

- Savoir-faire +13 années d'expérience Cloud
- Nos x6 DCs (certifications ISO 27001, HDS, Tier IV…)
- Nos moyens opérationnels
- Un catalogue d'offres et de contrats
- Pourquoi un DRP en mode Service ?

NOTRE RÉSEAU DE COMPÉTENCES

LES CERTIFICATIONS

ISO 27001 · ISO 9001:2015 · ISO 14001 · ISO 22301 · ISO 50001 · OHSAS 18001 · PCI DSS COMPLIANT · ISAE 3402 · HDS 123456 · EXPERT CYBER

koesio Corporate IT

DRAAS | DISASTER RECOVERY AS A SERVICE

- ✓ POUR TOUTE ENTREPRISE AYANT BESOIN D'UN **PLAN DE REPRISE D'INFRASTRUCTURE**
- ✓ POUR SE **PROTÉGER** AVEC LE PAIEMENT D'UN SERVICE
- ✓ POUR **PAYER À L'USAGE** EN CAS DE DÉCLENCHEMENT
- ✓ POUR PROFITER DE LA **PERFORMANCE ET DE LA SOUPLESSE** DU CLOUD

SITE DE L'ENTREPRISE

Télétravail

Utilisateurs

Dirigeant DSI

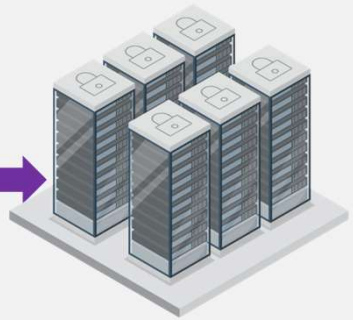
Fournisseurs

Clients

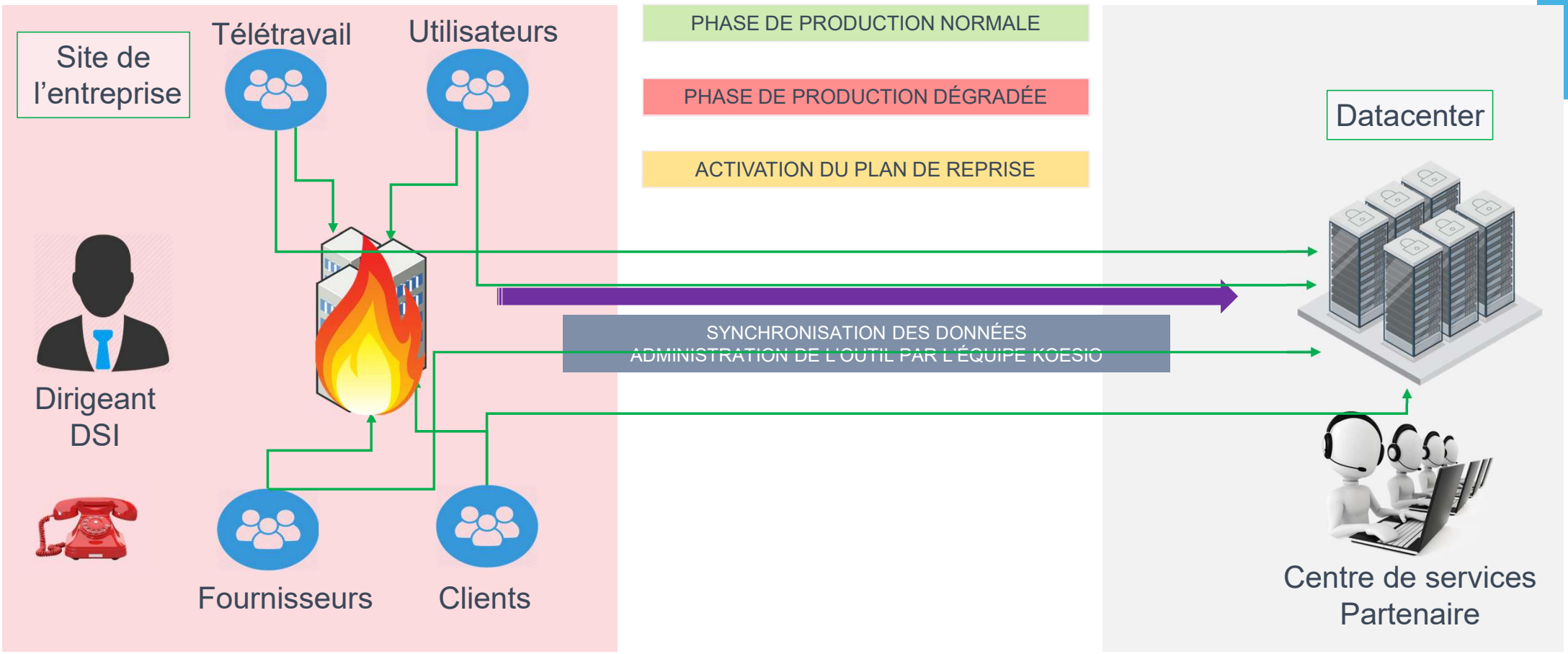
PHASE DE PRODUCTION NORMALE

SYNCHRONISATION DES DONNÉES
ADMINISTRATION DE L'OUTIL PAR L'ÉQUIPE KOESIO

DATACENTER



Centre de services Partenaire


Site de l'entreprise
Télétravail
Utilisateurs
PHASE DE PRODUCTION NORMALE
PHASE DE PRODUCTION DÉGRADÉE
ACTIVATION DU PLAN DE REPRISE
Datacenter
SYNCHRONISATION DES DONNÉES
ADMINISTRATION DE L'OUTIL PAR L'ÉQUIPE KOESIO
Dirigeant
DSI
Fournisseurs
Clients
Centre de services
Partenaire

DRaaS | RPO

L'OFFRE DRAAS KOESIO PERMET UN D'ATTEINDRE LES RECOVERY POINT OBJECTIVE SUIVANTS :

- ✓ RPO 1 : 30 MIN (Offre Bronze)
- ✓ RPO 2 : 2H (Offre Silver)
- ✓ RPO 3 : 4H (Offre Gold)

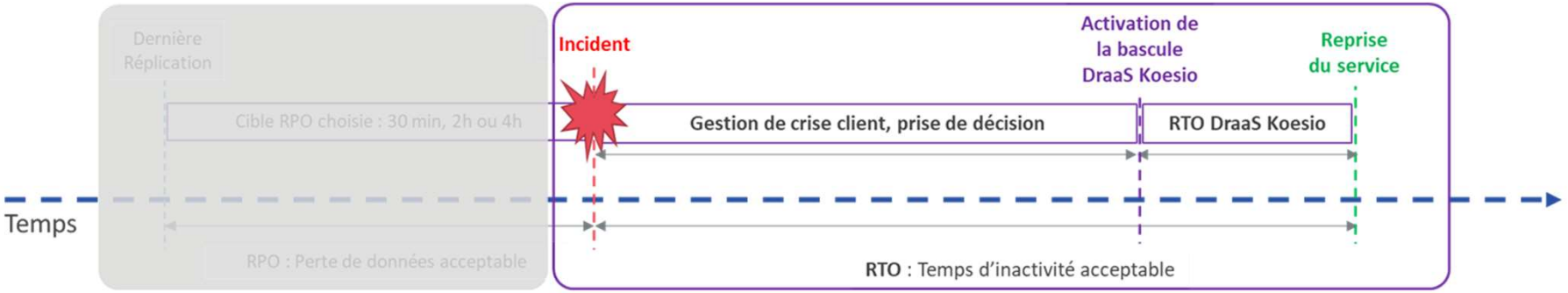
KOESIO S'ENGAGE SUR LES CIBLES RPO CONFIGURÉES

LE **RPO** EST PARAMÉTRÉ AU NIVEAU DES JOBS DE RÉPLICATION,

AVEC UNE GRANULARITÉ À LA VM.

CHAQUE CIBLE DISPOSE DE SON TEMPS MAXIMUM DE REPRISE : 30MIN, 2H, 4H selon l'offre sélectionnée

DRAAS | RTO



L'OFFRE DRAAS KOESIO PERMET UN RTO TECHNIQUE RAPIDE, D'UNE HEURE ENVIRON

- ✓ RTO DÉMARRE APRÈS LA PRISE DE DÉCISION « D'APPUYER SUR LE BOUTON »
- ✓ CE RTO EST DÉPENDANT DU PÉRIMÈTRE

KOESIO NE S'ENGAGE PAS SUR LE RTO

Extrait du livre blanc : décrit la phase de gestion de crise et de prise de décision

Phase	Description des phases	Temporalité
Phase 1	Réception de l'alerte	t
	Analyse de l'alerte	t + 30min
	Déclenchement de la cellule de crise	t + 2h
	Mobilisation des ressources client en cellule de crise	t + 2h30
	- Personnels habilités à déclencher le PRI	
	- Personnels Supports	
Phase 2	Appel KOESIO Corp IT pour déclenchement du PRI	t + 3h
	Mobilisation des ressources client & KOESIO Corp IT	t + 3h10
	Exposé du problème avec KOESIO Corp IT	t + 3h20
	Validation de la décision de la bascule sur le plan de PRI	t + 3h30

koesio Corporate IT

DRAAS | LE LIVRE BLANC KOESIO

TABLE DES MATIERES

DÉFINITION DU PRI

- ✓ SERVICES CRITIQUES ?
- ✓ RTO/RPO ACCEPTABLES ?
- ✓ PROCÉDURES DE BASCULE ET DE GESTION DE CRISE TECHNIQUE

EXPLOITATION

- ✓ TESTS RÉGULIERS
- ✓ ECHANGES SUR LES ÉVOLUTIONS
- ✓ COMPATIBILITÉ INFRASTRUCTURE

koesio
Corporate IT

Disaster Recovery
/
CAS Client

koesio
Corporate IT

ReTex | Crise Client Cloud récent

CONTEXTE	Client de Koesio CIT ayant une infrastructure **Hybride OnPremise** et **Cloud** Koesio Offre **DRaaS** sur l'infrastructure OnPremise → **18 VM** concernées Externalisation des **backups** OnPremise sur le Cloud Koesio → **26 VM** concernées Les VM dans le IaaS sont **sauvegardées** dans un autre Datacenter de Koesio
ATTAQUE	Cryptolock sur l'ensemble de l'infrastructure
RÉSOLUTION	1 – Démarrage de la solution de PRI suivant le livre blanc DRaaS en récupérant la rétention la plus proche de l'attaque pour analyse 2 – Mise en place d'une infrastructure IaaS globale pour redémarrer l'infrastructure (indisponibilité des matériels préalablement attaqués 3 – Démarrage en « bac à sable » et analyse EDR. Pas d'attaque détectée 4 – Pendant cette analyse, récupération des backups VCC pour restauration dans le IaaS 5 – Remise en service de l'infrastructure
ACCOMPAGNEMENT	DRaaS : Redémarrage **1h** après décision client Mise en place du IaaS : **1h** Restauration VCC : dépendant du débit. Dans notre cas : **1 journée** Analyse des 26 VM : **3 jours** (Analyse EDR et rapports) Remise en service globale avec 100% de l'activité : **5 jours**
A RETENIR	Importance d'avoir un plan de reprise testé Ne pas mettre tous les œufs dans le même panier Accompagnent des équipes Koesio en services managés (SOC, CdS, Plateforme, experts…) Transparence des échanges avec le client / confiance Et surtout : Respect de la discrétion demandée

koesio Corporate IT

Disaster Recovery
/
Le Mot de vmware by Broadcom

koesio
Corporate IT

MERCI !

koesio.com

EN PARTENARIAT AVEC vmware by Broadcom

AVEZ-VOUS DES QUESTIONS ?

koesio
Corporate IT