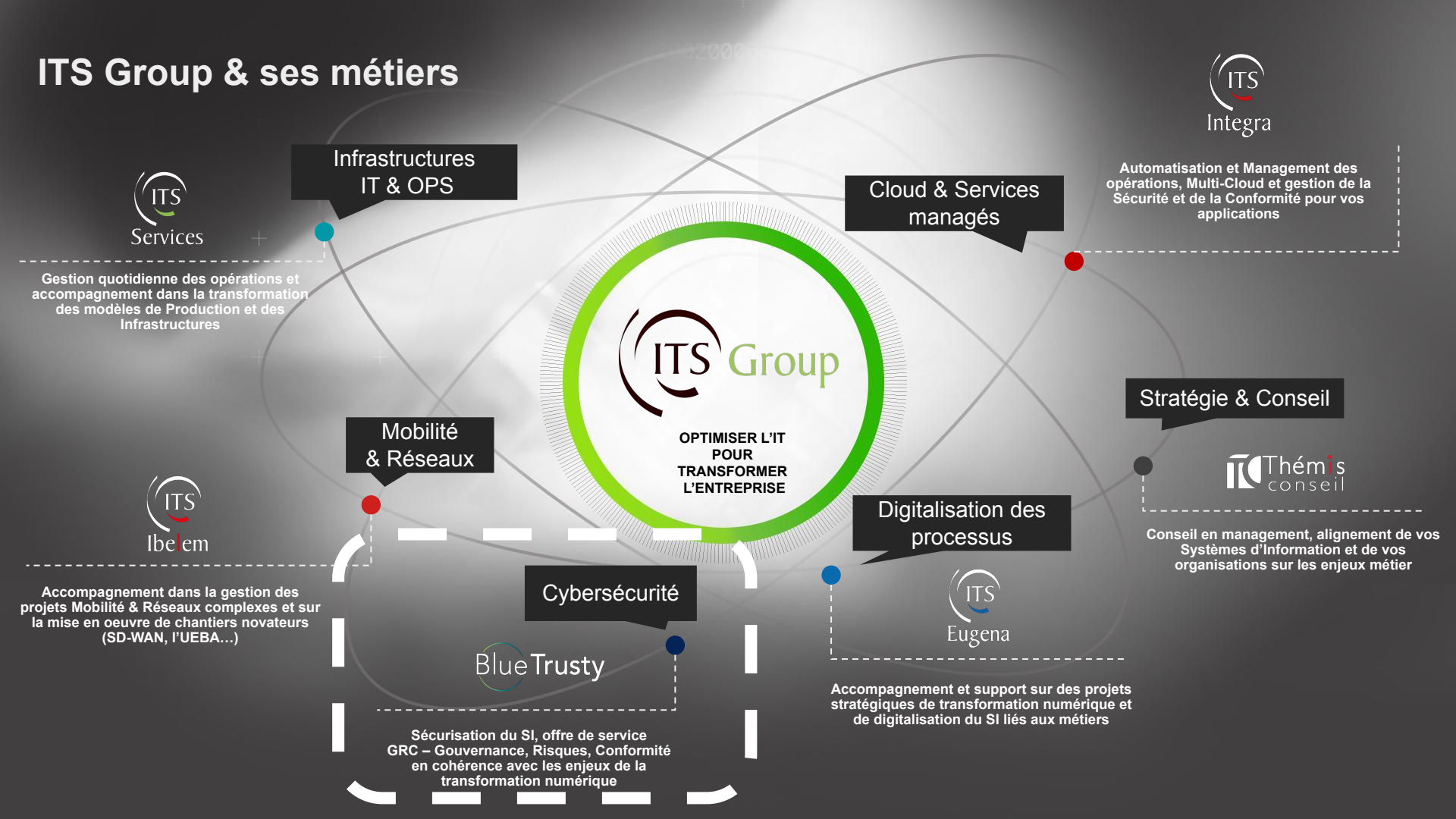

BlueTrusty
Stress-Test
non intrusif
aux ransomwares
Edition 2023
698.11
698.11
879.73
BlueTrusty - Powered by ITS Group

ITS Group & ses métiers



Nos certifications

Qualité

ISO 9001
Système de management par la qualité
SMQ

ITS Services · ITS Integra

Environnement

ISO 14001
Système de management Environnemental
SME

ITS Services · ITS Integra

Sécurité

ISO 27001
Système de management de la Sécurité et de l'Information
SMSI

HDS
Hébergeur de Données de Santé à caractère personnel

ITS Integra · SPHERE

Système de Management Intégré

Nos engagements RSE

Nos reconnaissances

Gaïa INDEX 11ème

ITS Group obtient 71/100 au classement Gaïa-Index 2019

ITS Group classé 11ème sur 74 dans sa catégorie sur les critères Environnementaux, Sociaux et de Gouvernance par l'agence de notation extra-financière Gaïa Rating

GOLD 2019 ecovadis CSR Niveau Gold

EcoVadis attribue à nouveau le niveau Gold à ITS Group pour sa démarche RSE

En 2019, ITS Group a obtenu la note de 67/100 par Ecovadis et fait partie des 5% d'entreprises les mieux notées avec la certification Gold.

THE GLOBAL COMPACT
NOUS SOUTENONS LE PACTE MONDIAL
Depuis 2009

ITS Group ratifie chaque année depuis 2009 les 10 principes du Pacte Mondial

ITS Group renforce sa position d'entreprise responsable et consciente des problématiques sociales et environnementales.

BlueTrusty est un prestataire référencé sur Cybermalveillance.gouv.fr

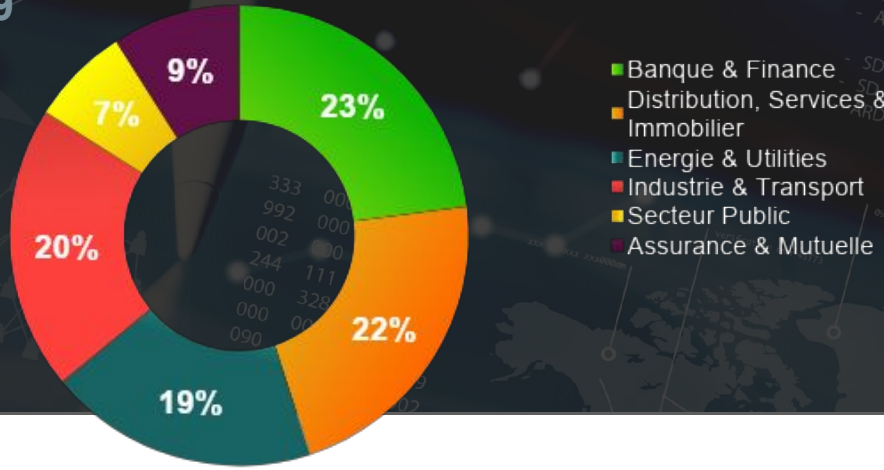
La plateforme Cybermalveillance.gouv.fr met à disposition de la victime une liste de professionnels proches de sa localisation géographique, qui se sont déclarés en mesure d'apporter une assistance technique.

Ces professionnels, dont BLUETRUSTY, sont référencés sur la plateforme après une candidature volontaire de leur part.

Lors de notre candidature, nous nous sommes engagés par la signature d'une charte à respecter de bonnes pratiques commerciales, à respecter la confidentialité des données de nos clients et à remonter à Cybermalveillance.gouv.fr les éléments techniques qui pourront être utiles à une meilleure analyse de la menace.

Une présence sur les principaux secteurs d'activités

Répartition de notre CA en 2019



Ils nous font confiance

Les Ransomwares sont une menace concrète et fréquente pour les organisations en France

No	Victim	Ransomware Gang	Date	Victim Country
2484	ENE TECHNOLOGY, Inc	SynACK	2021-06-16	Taiwan
2485	American Cotton Coop Association	Grief	2021-06-16	USA
2486	Vogel Heating & Cooling	Conti	2021-06-17	USA
2487	Sunsations Inc.	Conti	2021-06-17	USA
2488	Performance Award Center	Marketo	2021-06-17	USA
2489	Contrast Lighting	Conti	2021-06-17	Canada
2490	BRANGEON Groupe	Conti	2021-06-17	France
2491	Ascenz	Conti	2021-06-17	Singapore
2492	Au Forum Du Batiment SAS	Conti	2021-06-17	France
2493	Groupe ISERBA	Conti	2021-06-17	France
2494	Cerfrance Côtes d'Armor	Conti	2021-06-17	France
2495	Voltalia	Conti	2021-06-18	France
2496	Uniware Systems	Conti	2021-06-18	UK
2497	Maître Prunille	Conti	2021-06-18	France
2498	Groupe Traon Industrie Development	Conti	2021-06-18	France
2499	Windmill Health Products	Conti	2021-06-18	USA
2500	Moore Stephens Cape Town	Sodinokibi (REvil)	2021-06-19	South Africa
2501	Lamaziere	Everest	2021-06-20	France
2502	Epsilon Hydraulique	Everest	2021-06-20	France
2503	HAAI GmbH	Sodinokibi (REvil)	2021-06-20	Austria
2504	Always Group	Everest	2021-06-20	France
2505	ASSURANCES ET COURTAGES LYONNAIS	Everest	2021-06-21	France
2506	Alltech France	Everest	2021-06-21	France

Source : DarkTracer

Vous pensez être résilient aux Ransomwares.
Faites le test.

Principe par échantillonnage

80+ points de contrôle

10 thématiques

https://stresstest.bluetrusty.com

BlueTrusty

Principes du stress-test aux ransomwares

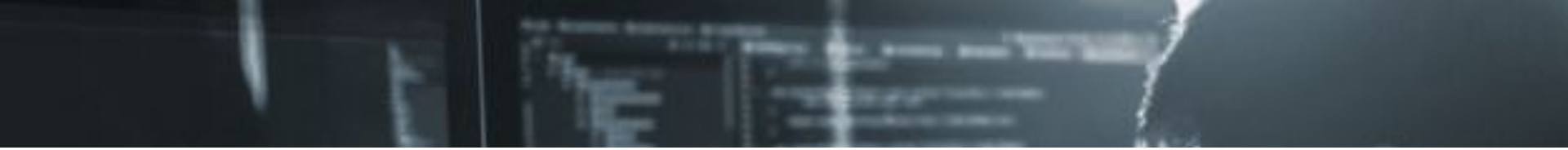
360° : mises à jour logicielles, filtrage de la navigation et du mail, restrictions des droits et des applications, sécurité physique, sauvegarde, fiches réflexe ...

Normatif : dans le temps (évolution de la note au fil des tests) et dans l'espace (permet de comparer des SI hétérogènes).

Actuel : nous intégrons/mettons à jour a minima mensuellement des contrôles suivant les données de *Cyber Threat Intelligence*

Pratique : réalisable à distance, en général, une à deux heures par poste suffisent.

Abordable : prix par couple {poste de travail,compte utilisateur} à distance ou sur site. Nous préconisons de choisir d'analyser 3 postes.



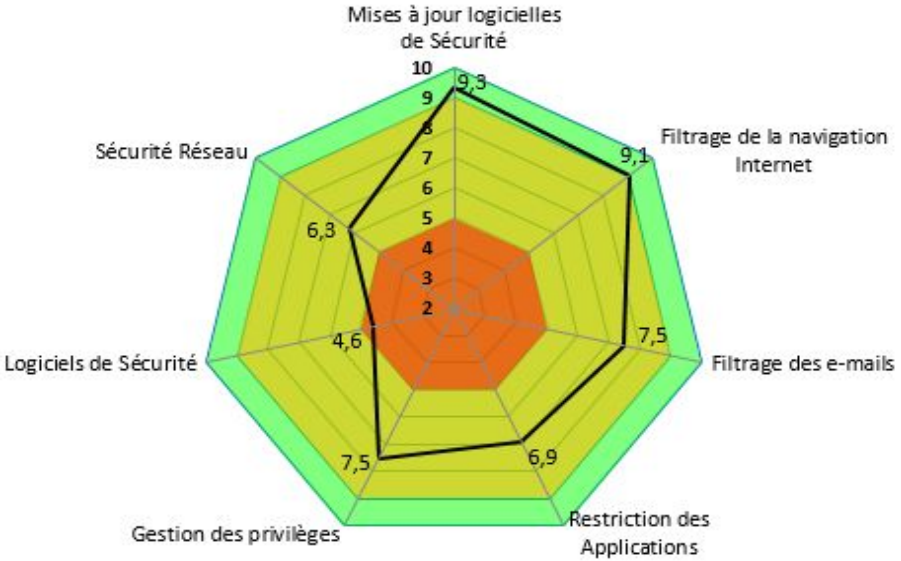
Un Stress Test incluant 10 thématiques, plus de 80* points de contrôle

- Sauvegarde des données
- Mises à jour logicielle
- Cloisonnement réseau
- Sécurité des applications
- Filtrage de contenu des emails et de la navigation web
- Détection des intrusions
- Droits des utilisateurs
- Sensibilisation des utilisateurs
- Réponse à incident de sécurité
- Légal et Assurances

(*) liste mise à jour et enrichie hebdomadairement

CYBERSECURITY AS A SERVICE

Une idée du livrable du stress-test aux ransomwares



BlueTrusty

[StressTest Rapport] X

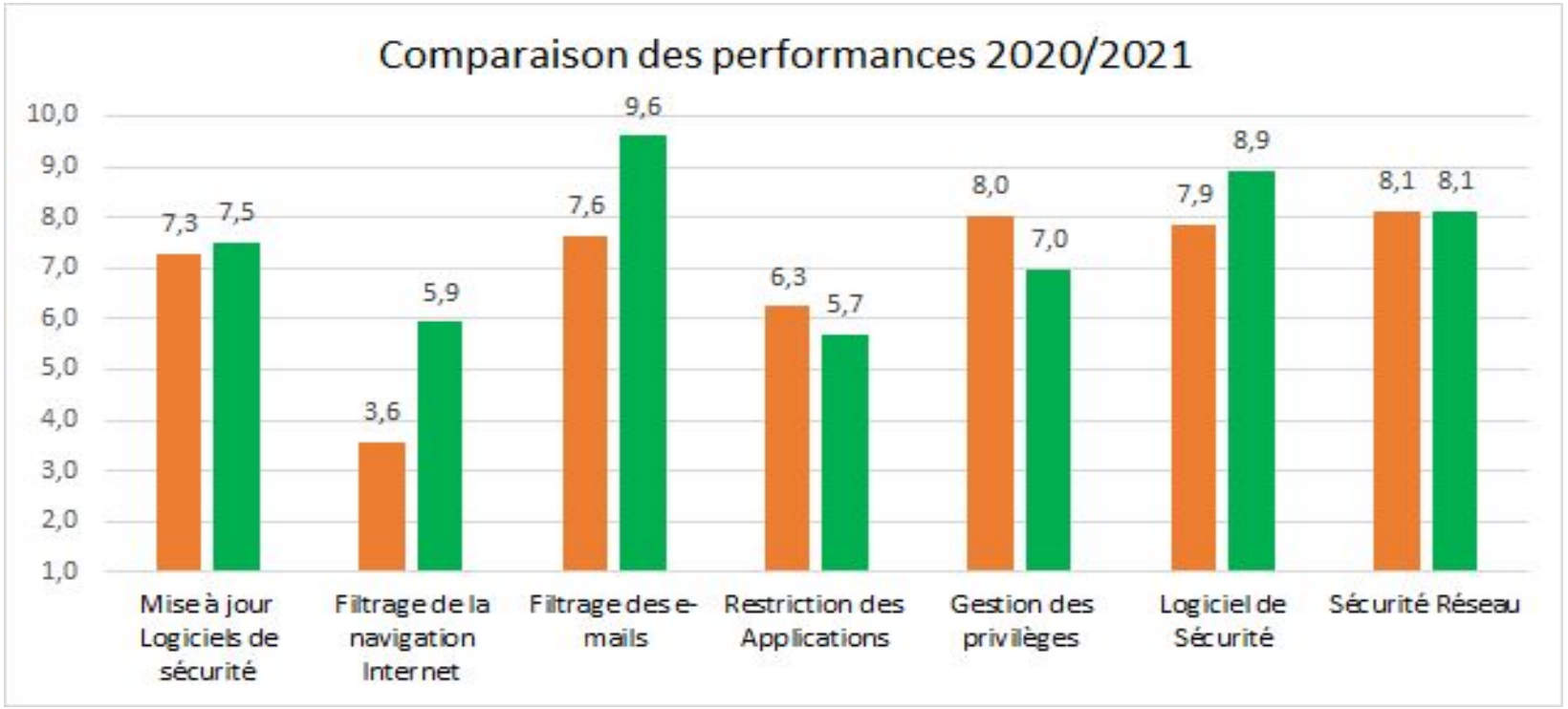
OK | Critique | Risque faible | Risque important | Non Analysé

Compte utilisateur : trustybl
Date :

N	Type	Description	Docs
		Gestion des privilèges	
1	Tech	Vérification des privilèges et des exploits avec **DazzleUp** : Oui (tous les privilèges sont désactivés sauf celui par défaut "SeChangeNotifyPriviledge"	Lien
2	Tech	L'utilisateur n'est pas administrateur local	
3	Tech	Dernière date de changement de mot de passe : 09/03/2021	
4	Tech	Date d'expiration du mot de passe : N/A	Lien
5	Tech	Ce PC est-il un PAW ? : Non	Lien
6	Tech	LAPS installé ? : Non	Lien
7	Tech	WDigest actif ? : Non	Lien
8	Tech	Credential Guard actif ? : Non	Lien
9	Tech	Pas d'affaiblissement de Windows Defender constaté (TA505)	Lien
10	Tech	Pas d'affaiblissement de Windows Defender constaté (CyaX DotNet Packer)	Lien
11	Tech	Statut du CredSSP délégation : Pas de clef (Non)	Lien Lien
12	Tech	Statut du CredSSP cache : Pas de clef (Non)	Lien
13	Tech	Taille max des Journaux d'évènements : 20971520	
14	Tech	Sysmon installé et à jour ? : Non	Lien
15	Tech	Port USB activé ? : Oui	Lien
16	Tech	Ordinateur partagé par de nombreux utilisateurs ? : Non	
17	Tech	Le mode *EnableLUA* (UAC) est activé pour le compte utilisateur: Oui	Lien
18	Tech	Test de Suppression d'une DLL : bloqué	

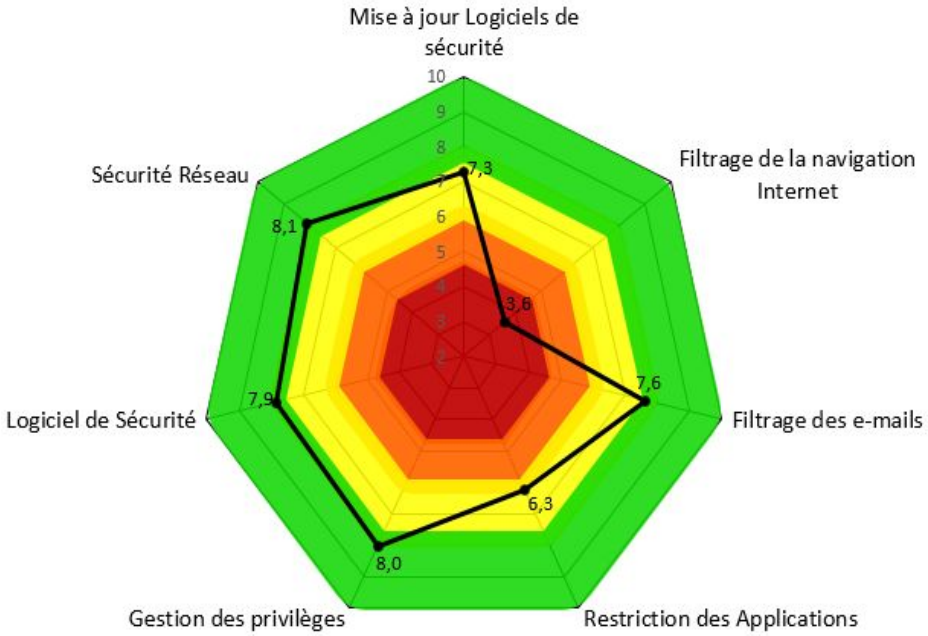
CYBERSECURITY AS A SERVICE

Cas Client : Revue d'évolution du stress-test aux ransomwares (1)

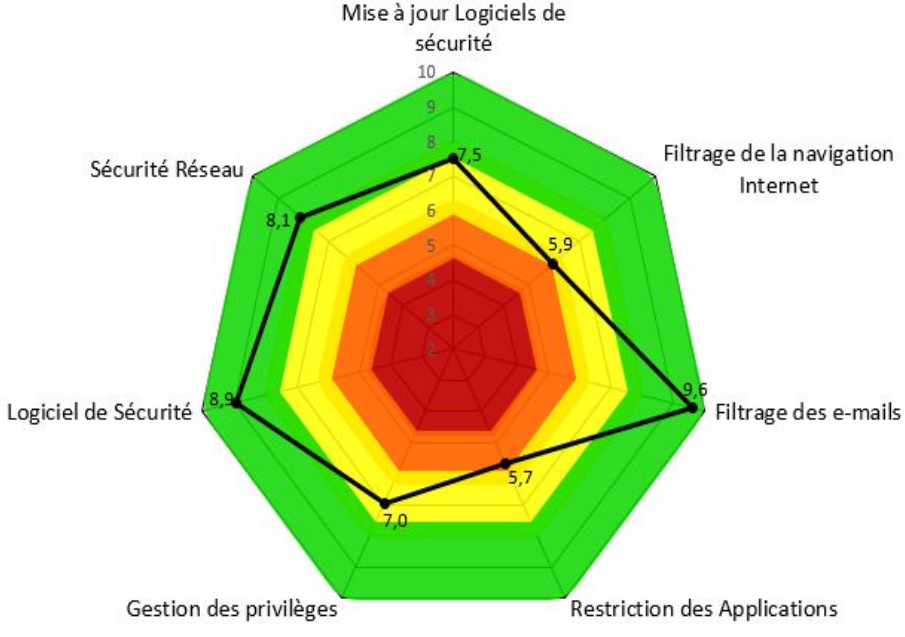


Cas Client : Revue d'évolution du stress-test aux ransomwares (2)

2022



2023



Organisation du projet

Lancement

Lors de cette réunion, suivant vos disponibilités nous fixons la date de collecte et les conditions du stress-test

Collecte

Nous intervenons à distance ou sur site (en option) pour réaliser le stress-test sur un ou plusieurs postes, il faut compter 2H par poste

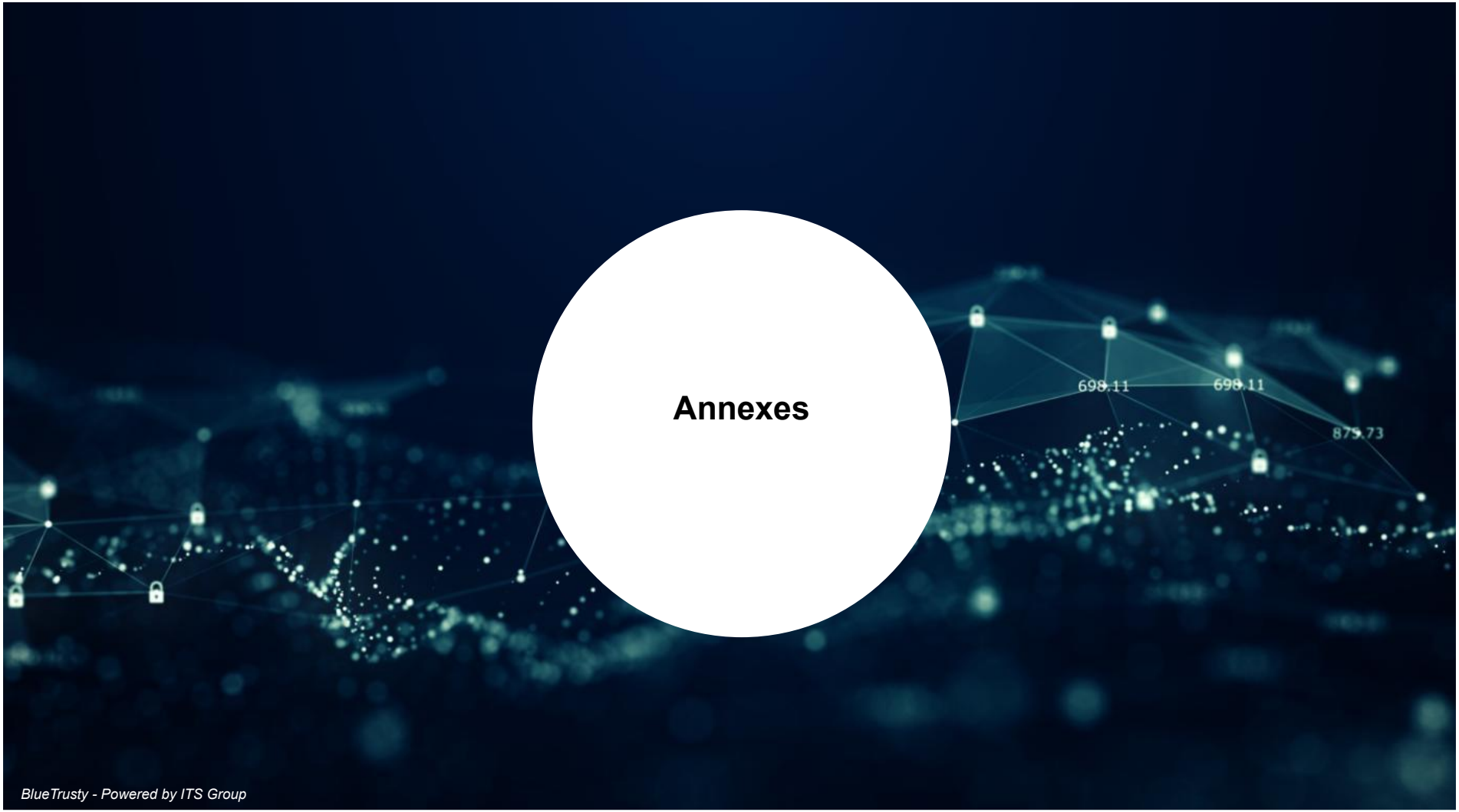
Analyse

En lab, nous analysons le résultat de la collecte, effectuons des recherches complémentaires, et rédigeons les livrables

Restitution

Lors de cette réunion en ligne nous vous présentons les livrables et procédons à un débrief et une discussion avec l'un des nos experts CyberSécurité

CYBERSECURITY AS A SERVICE



Annexes

Options : quelques-unes de nos offres de sécurité opérationnelle complémentaires

Option	Option	Option	Option
SIEM as a Service *Light*	**Gestion des mises à jour de sécurité**	**Surveillance de la vulnérabilité de vos services exposés**	**Campagne de sensibilisation au Phishing**
Stockage 8 GB /mois 14j en ligne Rétention 12 mois Alerte sur *pattern-matching* ou Indicateur de Compromission (IOC)	Veille sur les vulnérabilités Qualification, Application et Suivi des mises à jour logicielles	Recherche de vulnérabilité TCP/IP ou Web suivant le référentiel OWASP Top10	Création d'un mail et d'une pièce jointe ou d'un portail web piégés avec capture de données suivant un scénario réaliste et personnalisé avec l'acquisition d'un nom de domaine sur mesure Restitution détaillé. Conforme RGPD
280 € HT /mois*	**à partir de 15 € HT / PC / mois ***	**80 € HT / IP publique / mois***	**nous contacter**

* dans le cadre d'un contrat de 12 mois.

CYBERSECURITY AS A SERVICE