RAPPORT GENERAL – M 6105 X 18

Publié par l'EXERA, Décembre 2018

Index de classification : 50

Résultats du dépouillement des réponses des adhérents Exera au sondage 2018 « Cybersécurité des systèmes industriels »

AUTEUR : COMMISSION TECHNIQUE « CYBERSÉCURITÉ DES SYSTÈMES INDUSTRIELS » - CT CSI

DIFFUSION

Le présent rapport a été établi pour l'usage interne des membres de l'EXERA. Son contenu – complet ou partiel - ne doit pas être diffusé à des personnes qui ne font pas partie du personnel employé par un membre de l'EXERA sans l'autorisation expresse de l'EXERA.

MEMBRES DE L'EXERA - 2018

ADISSEO
AÉROPORTS DE PARIS
AIR LIQUIDE
AIRBUS GROUP
ANTARGAZ FINAGAZ
ARIANE GROUP
ARLANXEO ELASTOMERES FRANCE
AXENS
CETIAT
DGA
EDF
ENGIE
GRTgaz
INERIS
INRS
IRA
LNE
LUBRIZOL FRANCE
LYONDELLBASELL
NANTES MÉTROPOLE
NAVAL GROUP
ORANO
PETROINEOS FRANCE
RATP
RUBIS
TOTAL
VARO REFINERY CRESSIER SA

Dans le cadre de ses travaux, la Commission Technique « Cybersécurité des Systèmes industriels » de l'Exera a souhaité procéder à un sondage en ligne des membres de l'Exera sur le thème de la cybersécurité des systèmes industriels.

Trois objectifs étaient poursuivis au travers de ce sondage :

- Évaluer le degré de conscience du danger « Cyber » chez les adhérents de l'Exera et leur niveau d'information,
- Partager aux fins de parangonnage éventuel les dispositions prises pour gérer la menace « Cyber » et mettre en œuvre des contre-mesures,
- Mesurer la sensibilité des adhérents aux thématiques futures dans le domaine de la cybersécurité.

Le sondage a été élaboré sous la forme d'une liste d'une vingtaine de questions fermées, établies pour certaines en collaboration avec la société Sentryo. Les votants disposaient toutefois de la possibilité de laisser des commentaires pour quelques questions.

Mis en ligne le 9 juillet 2018, le sondage a fait l'objet d'une annonce sur le site de l'Exera et d'un message électronique adressé à l'ensemble des personnels des adhérents de l'Exera présents à cette date dans l'annuaire électronique de l'Exera, soit environ 820 personnes.

Seule condition mise à l'accès au sondage, être inscrit à l'espace du site www.exera.com réservé aux adhérents de l'Exera, soit 190 inscrits sur un total de 820 personnels figurant dans l'annuaire.

Il a été clôturé le 14 septembre suivant, et le présent rapport expose les résultats issus du dépouillement sous forme de fiches. Les résultats sont fournis sous forme anonymisée.

Chacune des questions posées donne lieu à une fiche comportant :

- L'intitulé complet de la question ;
- Le nombre de votants ;
- L'origine des votants qui indique les entreprises des votants, avec, pour chacune d'elles, le nombre de votants ;
- Le nombre de choix ouverts aux votants ;
- L'intitulé des réponses proposées aux votants, avec le nombre de suffrages recueillis ;
- Et, lorsque cela a été jugé utile, un graphique permettant de visualiser les résultats ;
- Les éventuels commentaires laissés, avec l'indication de l'entreprise d'appartenance du votant.

Bien entendu, le nombre de votants, une vingtaine tout au plus, ne constitue pas un échantillon statistiquement représentatif des entreprises desquels ils relèvent. De même, les votants ne sont pas responsables de la cybersécurité au sein de leurs entreprises, et leurs réponses ne reflètent pas l'avis de leurs entreprises pour autant que ces dernières se soient exprimées.

Toutefois, les positions occupées par les votants au sein de leurs entreprises, tous en lien avec les problèmes de cybersécurité, conférent au sondage un intérêt certain.

S'agissant des entreprises adhérentes de l'Exera desquelles les votants relèvent, elles sont au nombre de douze. Il s'agit de :

- ADP, anciennement Aéroports de Paris, avec un votant,
- DGA avec deux votants et SSF avec, également, deux votants, organismes relevant du ministère des armées,
- EDF avec un représentant,
- INERIS avec un représentant,
- INRS avec un représentant,
- Naval Group avec un représentant,
- Orano, anciennement Areva, avec quatre représentants,
- Petroineos avec deux représentants,
- RATP avec un représentant,
- Rubis avec un représentant,
- Total avec un représentant.

Le nombre de réponses varie d'une question à l'autre, les votants étant totalement libres de répondre ou pas à chacune des questions. Comme l'on pouvait s'y attendre, le nombre de votant est plus faible pour les questions sensibles en matière de confidentialité des sujets abordés.

- Nombre maximum de votants : 18
- Nombre minimum de votants : 10
- Moyenne arithmétique de votants : 14
- Nombre moyen pondéré de votants : 14,9

On constate que le nombre moyen pondéré de votants est plus élevée que la moyenne simple.

L'interprétation des résultats est laissée à la libre appréciation du lecteur.

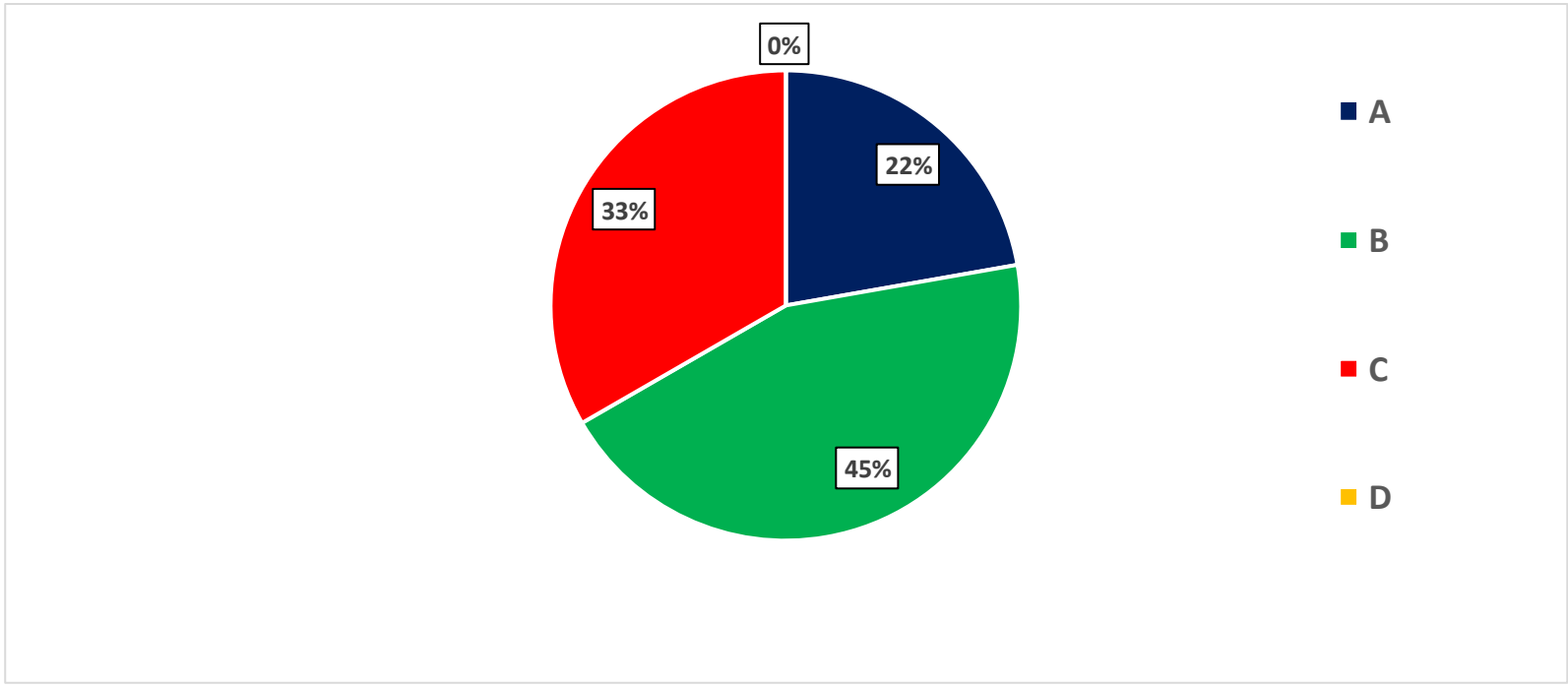
PROFILS DES VOTANTS AU REGARD DE LA CYBERSÉCURITÉ

Question 0 - Vous et la cybersécurité...

Nombre de votants : 18
Origine des votants : ADP (1), DGA (2), EDF (1), INERIS (1), INRS (1), Naval Group (1), Orano (4), Petroineos (2), RATP (1), Rubis (1), SSF (2), Total (1)
Réponse unique par votant

Réponses **Nombre de réponses :** 18

A	Vous travaillez au sein d'un service en charge d'assurer la cybersécurité des réseaux OT	4
B	Vous travaillez au sein d'un service exploitant un ou plusieurs réseaux OT, ou en charge de leur maintenance	8
C	Vous n'êtes dans aucune des situations précédentes, mas vous vous sentez concerné par le sondage...	6
D	Vous ne vous sentez pas concerné par le sondage...	0



CONSCIENCE DU DANGER CYBER ET NIVEAU D'INFORMATION

Question 1 - Avez-vous déjà entendu parler de cyber-attaques ciblant un site industriel ?

Nombre de votants : 18
Origine des votants : ADP (1), DGA (2), EDF (1), INERIS (1), INRS (1), Naval Group (1), Orano (4), Petroineos (2), RATP (1), Rubis (1), SSF (2), Total (1)
Réponse unique par votant

Réponses

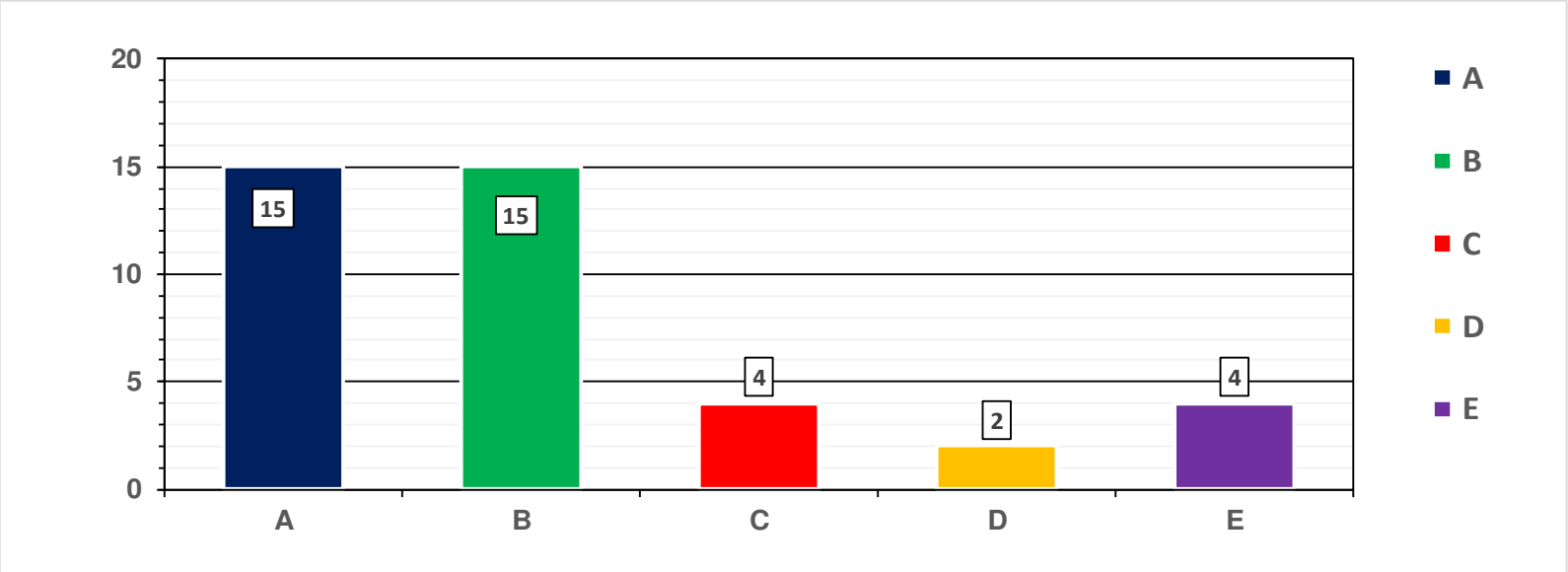
Oui	**18**	**100%**
Non	**0**	**0%**

Question 1-1- Si vous avez répondu par l'affirmative à la question précédente, connaissez-vous les cyber-attaques sur sites industriels suivantes ?

Nombre de votants : 18
Origine des votants : ADP (1), DGA (2), EDF (1), INERIS (1), INRS (1), Naval Group (1), Orano (4), Petroineos (2), RATP (1), Rubis (1), SSF (2), Total (1)
Plusieurs réponses possibles pour chaque votant

Réponses **Nombre de réponses :** 40

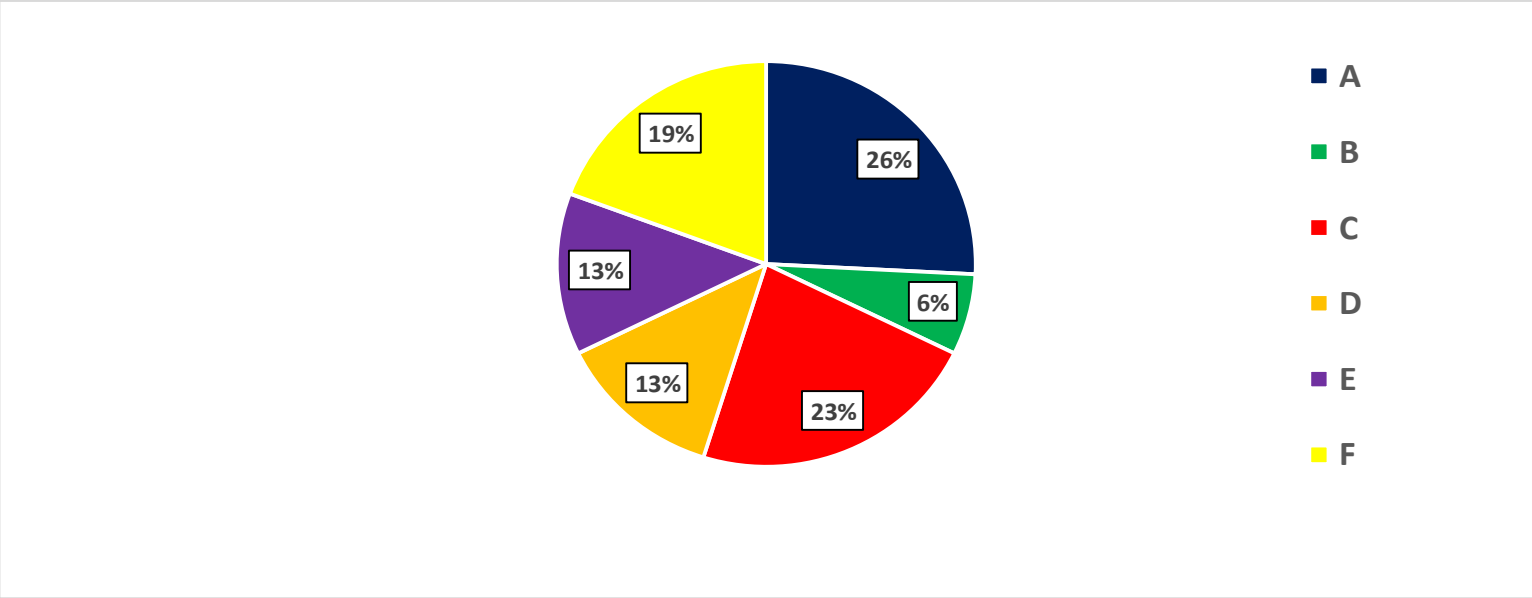
A	Attaque de réseaux de distribution électrique en Ukraine en 2015 et 2016	15
B	Attaque d'une usine iranienne d'enrichissement d'uranium en 2011	15
C	Attaque d'une aciérie allemande en 2014	4
D	Attaques d'usines de traitement des eaux "Kemuri Water Company" en 2015	2
E	Autres	4



Question 2 - Si vous avez répondu affirmativement à la question 1, par quel(s) canal(aux) avez-vous entendu parler de ces attaques ?

Nombre de votants : 18
Origine des votants : ADP (1), DGA (2), EDF (1), INERIS (1), INRS (1), Naval Group (1), Orano (4), Petroineos (2), RATP (1), Rubis (1), SSF (2), Total (1)
Au plus 2 réponses possibles par votant

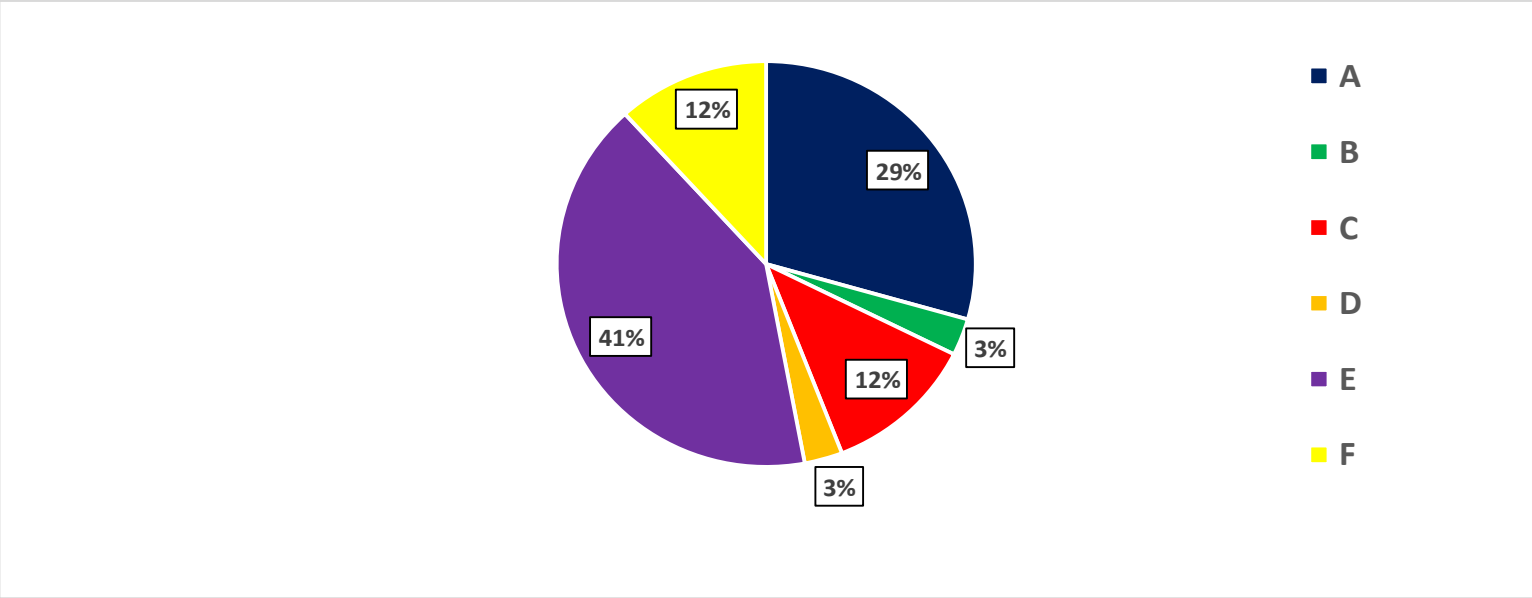
Réponses		Nombre de réponses :	31
A	Conférences		8
B	Presse spécialisée dans l'IT		2
C	Presse/média généraliste		7
D	Bouche à oreille		4
E	Presse spécialisée dans l'industrie		4
F	Voie interne (service en charge de la cybersécurité au sein de votre entreprise)		6



Question 3 - Si vous avez répondu affirmativement à la question 1, par quel(s) canal(aux) avez-vous entendu parler de ces attaques ?

Nombre de votants : 18
Origine des votants : ADP (1), DGA (2), EDF (1), INERIS (1), INRS (1), Naval Group (1), Orano (4), Petroineos (2), RATP (1), Rubis (1), SSF (2), Total (1)
Au plus deux réponses possibles par votant

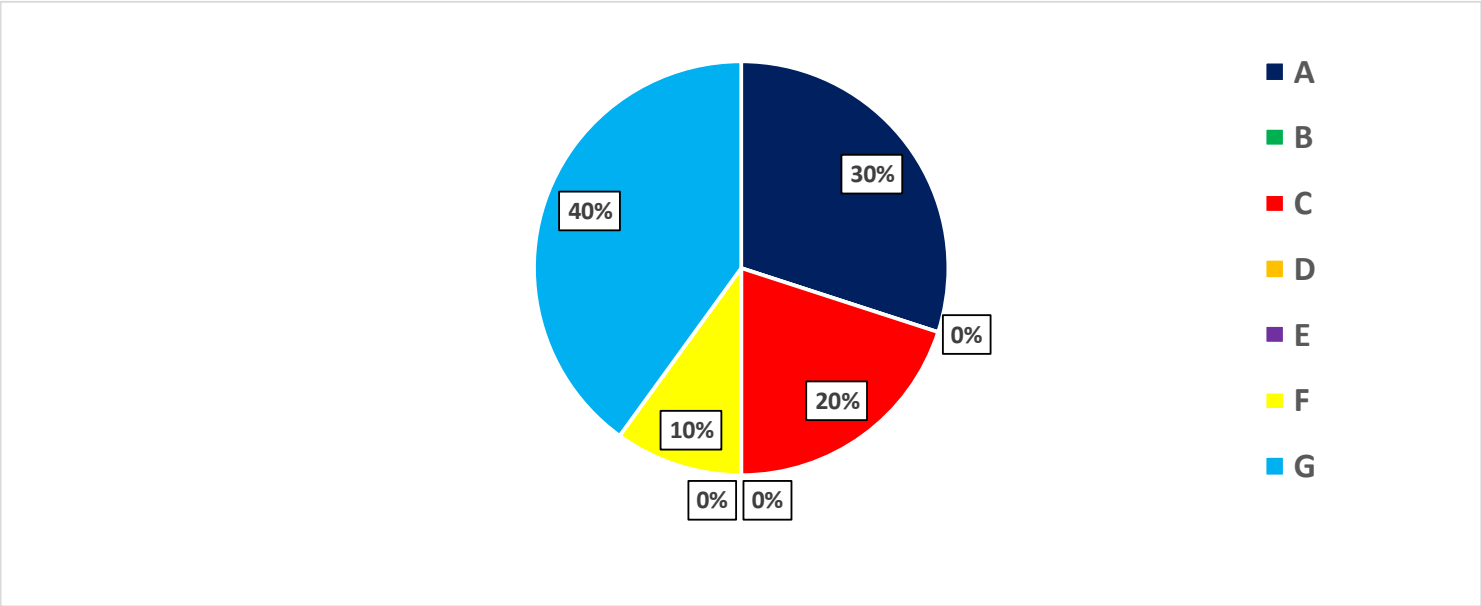
Réponses		Nombre de réponses :	34
A	ANSSI (France)		10
B	ICS-CERT (Etats-Unis)		1
C	ANSSI/CERT-FR (France)		4
D	SANS Institute		1
E	Voie interne (service en charge de la cybersécurité au sein de votre entreprise)		14
F	Autre(s)		4



Question 4 - Votre entreprise est-elle membre d'un ou plusieurs des organismes suivants ?

Nombre de votants : 10
Origine des votants : ADP (1), DGA (2), INERIS (1), INRS (1), Orano (2), RATP (1), SSF (2), Total (1)
Plusieurs réponses possibles pour chaque votant

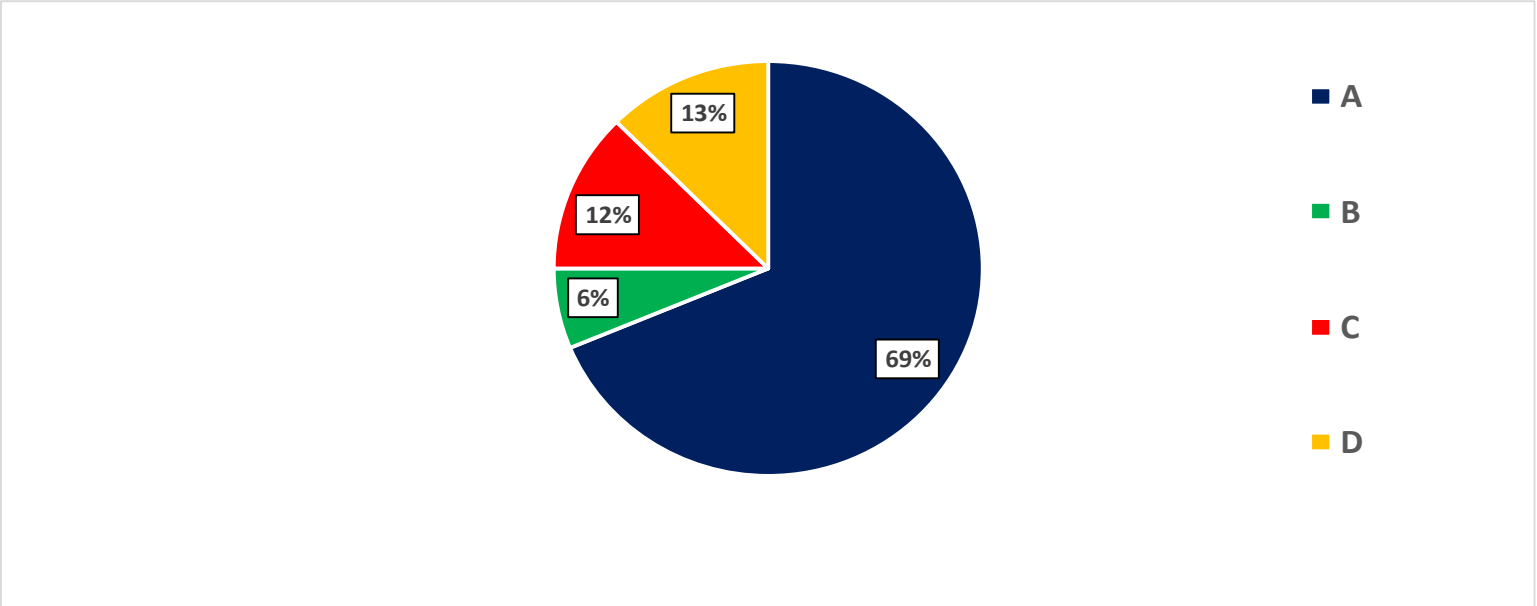
Réponses		Nombre de réponses :	10
A	Club Automation		3
B	CLUSIR		0
C	ISA		2
D	Gimelec		0
E	Cercle européen de la sécurité et des systèmes d'information		0
F	CLUSIF		1
G	Autre(s)		4



Question 5 - Votre entreprise est-elle soumise à une réglementation applicable à la cybersécurité des systèmes industriels ?

Nombre de votants : 16
Origine des votants : ADP (1), DGA (2), INERIS (1), INRS (1), Orano (3), RATP (1), SSF (2), Total (1)
Réponse unique par votant

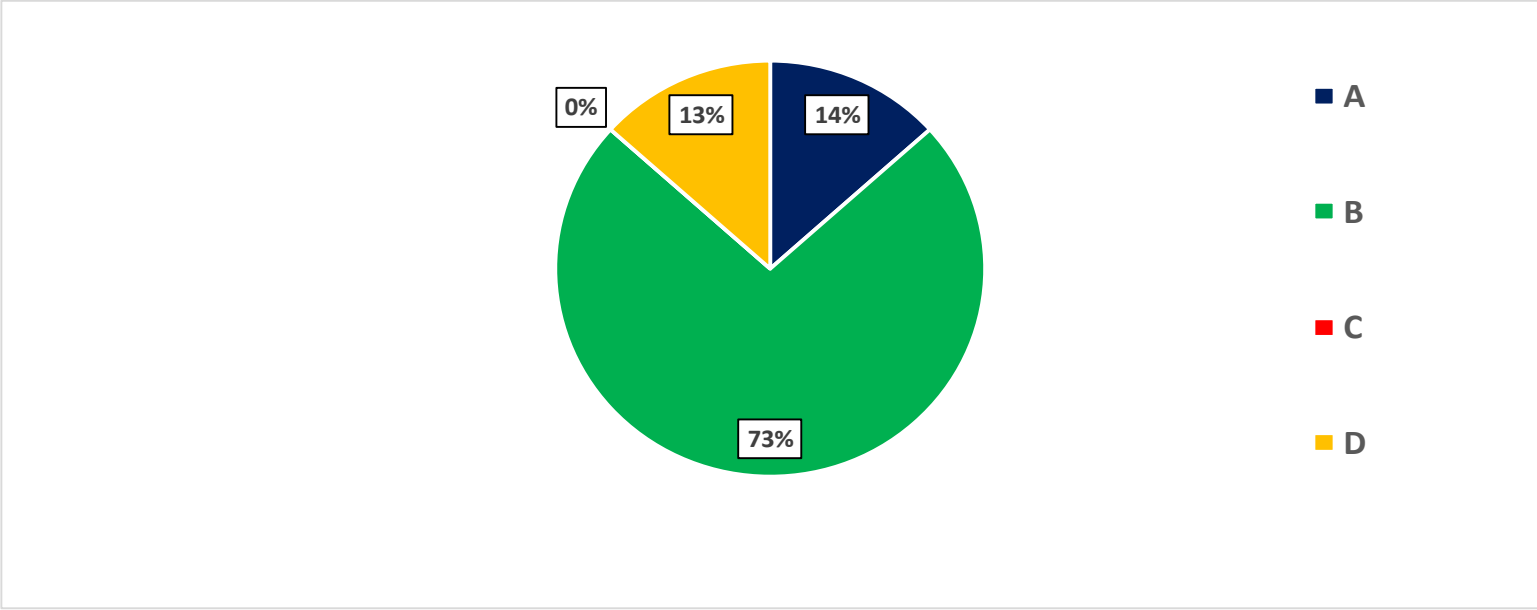
Réponses		Nombre de réponses :	16
A	Oui		11
B	Non		1
C	Je ne souhaite pas ou ne suis pas autorisé à répondre à cette question		2
D	Je ne sais pas		2



Question 5-1 - Si vous avez répondu par l'affirmative à la question précédente, merci d'indiquer la ou les réglementations applicables.

Nombre de votants : 11
Origine des votants : ADP (1), DGA (2), INERIS (1), INRS (1), Orano (3), RATP (1), SSF (2), Total (1)
Plusieurs réponses possibles pour chaque votant

Réponses		Nombre de réponses :	15	
A	Directive européenne NIS		2	
B	Législation et réglementation françaises		11	
C	Réglementation américaine		0	
D	Autre(s)		2	--> DGA et SSF : Réglementation propre au MINARM

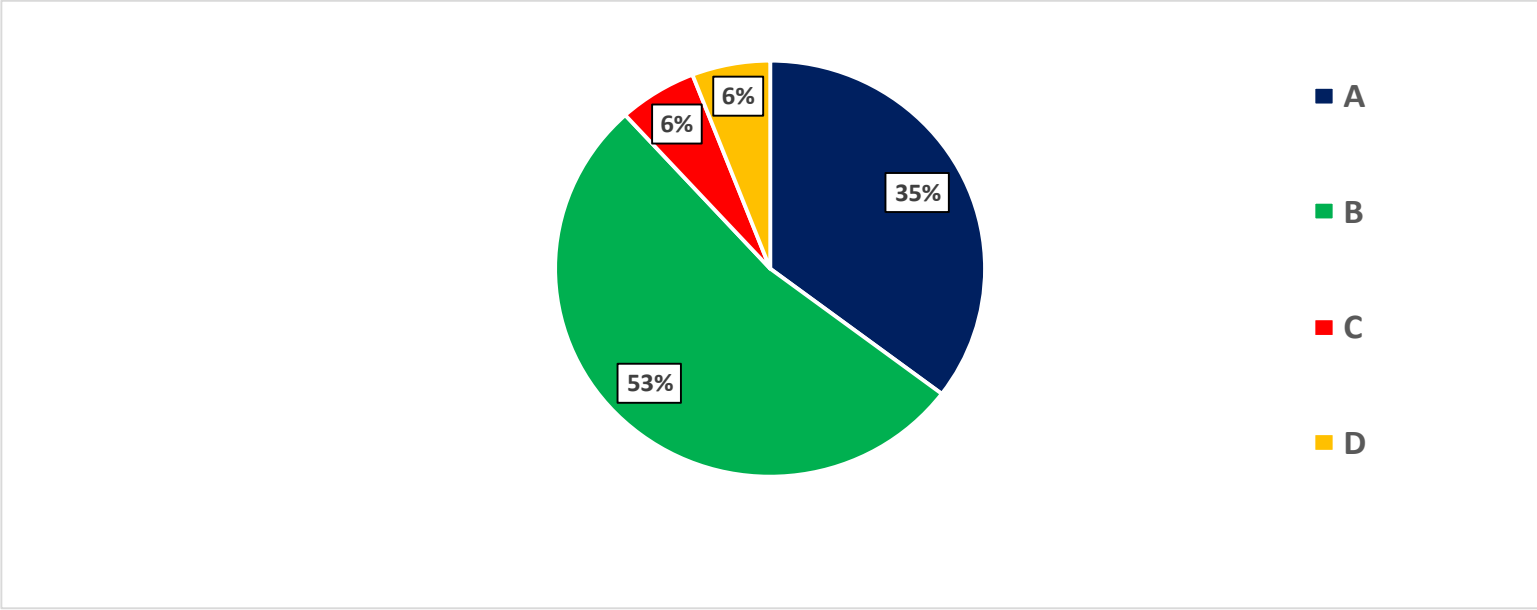


GESTION DE LA MENACE - MISE EN ŒUVRE DE CONTRE-MESURES

Question 6 - Quel est, selon vous, le niveau de menace sur la cybersécurité des systèmes industriels de votre entreprise ?

Nombre de votants : 17
Origine des votants : ADP (1), DGA (2), EDF (1), INRS (1), INERIS (1), Orano (4), SSF (2), Petroineos (2), RATP (1), Rubis (1), Total (1)
Réponse unique par votant

Réponses		Nombre de réponses : 17
A	Elevé (risques avérés avec impacts potentiels graves)	6
B	Moyen (risques réels avec impacts gênants mais gérables)	9
C	Bas (risques acceptables sans mesure de sécurité supplémentaire)	1
D	Inexistant (risques quasi-inexistants et impacts quasi-insignifiants)	1

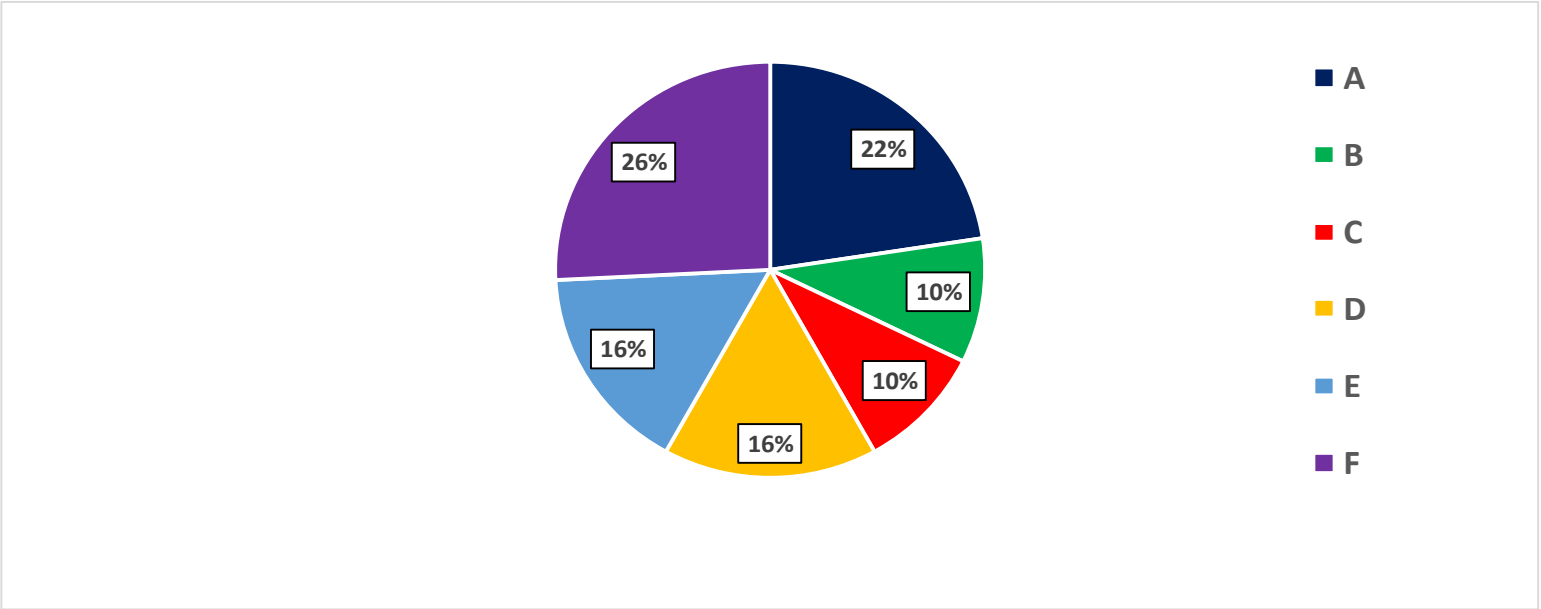


Question 7 - Parmi les réponses suivantes, quelles sont, selon vous, les deux sources de cyber-attaque les plus probables ?

Nombre de votants : 16
Origine des votants : ADP (1), DGA (2), EDF (1), INRS (1), INERIS (1), Orano (3), SSF (2), Petroineos (2), RATP (1), Rubis (1), Total (1)
Au plus deux réponses possibles par votant

Réponses **Nombre de réponses :** 31

A	Origine interne non intentionnelle	7
B	Origine interne intentionnelle	3
C	Origine externe non intentionnelle : fournisseurs, prestataires, sous-traitants	3
D	Origine externe intentionnelle : individus isolés tels que hackers amateurs et/ou professionnels	5
E	Origine externe intentionnelle : organisations criminelles	5
F	Origine externe intentionnelle : organisations actionnées par un ou plusieurs Etats	8

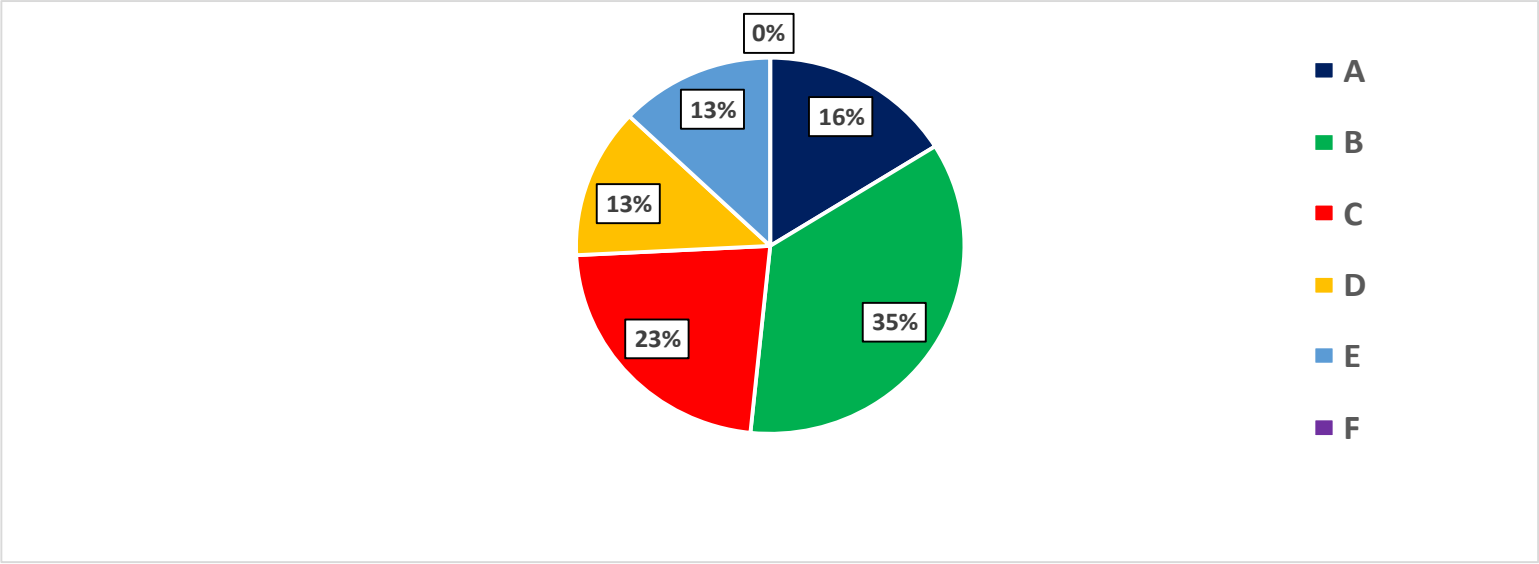


Question 8 - Parmi les réponses suivantes, quels sont, selon vous, les deux chemins d'attaque les plus probables ?

Nombre de votants : 16
Origine des votants : ADP (1), DGA (2), EDF (1), INRS (1), INERIS (1), Orano (3), SSF (2), Petroineos (2), RATP (1), Rubis (1), Total (1)
Au plus deux réponses possibles par votant

Réponses **Nombre de réponses :** 31

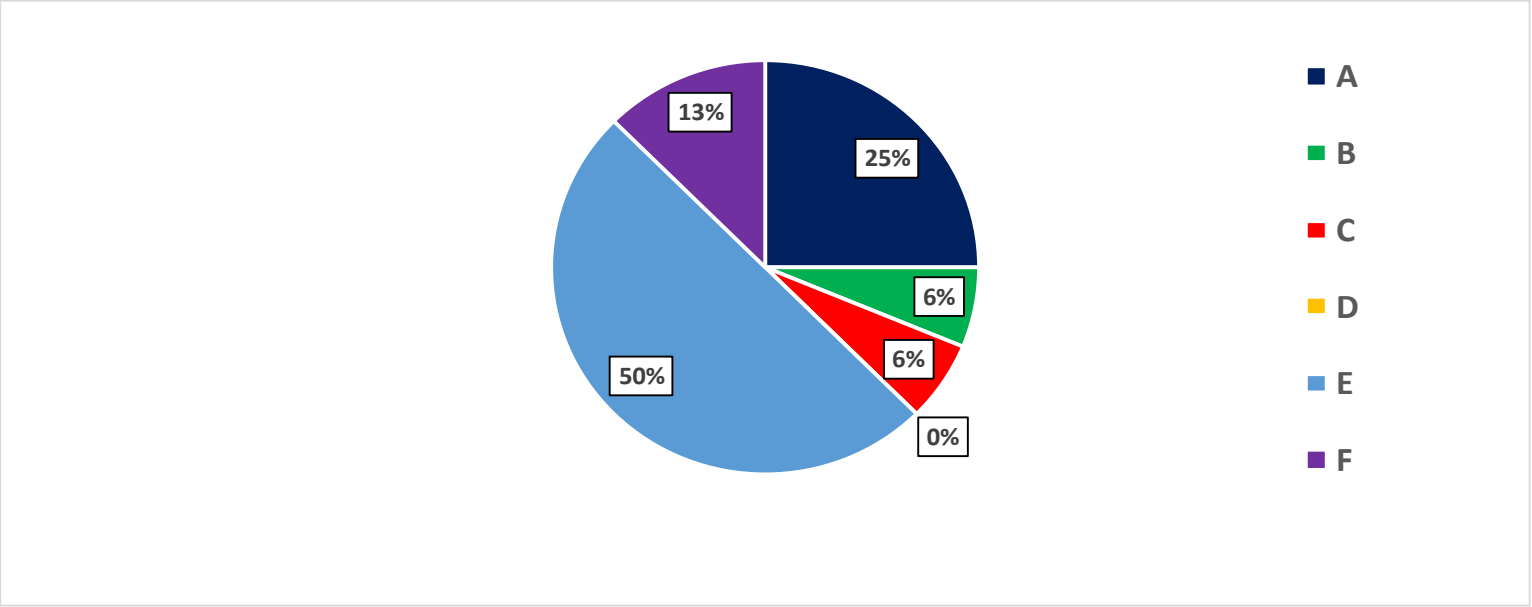
A	Passerelle entre réseau(x) IT et réseau OT	5
B	Hameçonnage (Phishing) par envoi par messagerie de pièces jointes contenant un virus	11
C	Maliciel (Malware) ciblé, contenant un virus conçu sur mesure, via clé USB ou PC portable	7
D	Maliciel (Malware) non ciblé, contenant un virus répandu, via clé USB ou PC portable	4
E	Connection via le Web	4
F	Autre(s)	0



Question 9 - Vos réseaux IT ou OT ont-ils déjà été infectés ou pénétrés ?

Nombre de votants : 16
Origine des votants : ADP (1), DGA (2), EDF (1), INRS (1), INERIS (1), Orano (3), Petroineos (2), RATP (1), Rubis (1), SSF (2), Total (1)
Une seule réponse possible par votant

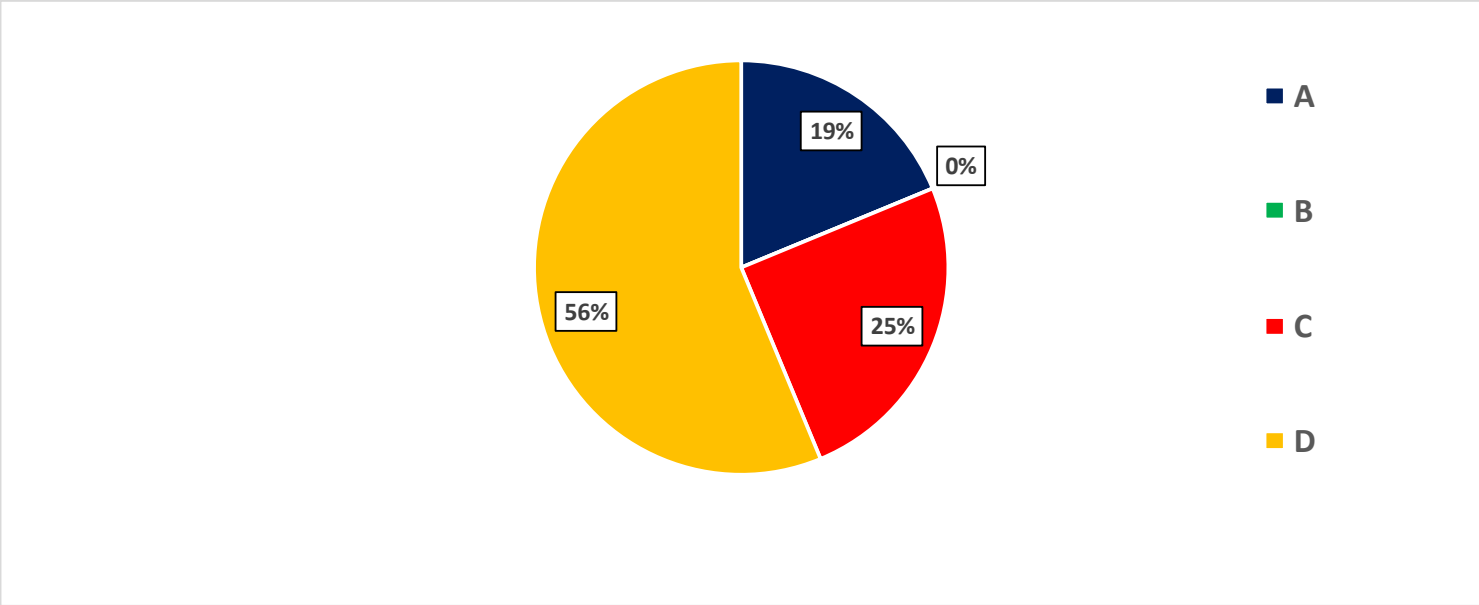
Réponses		Nombre de réponses : 16
A	Oui, avec preuve(s) avérée(s)	4
B	Oui, mais sans preuve avérée	1
C	Non, mais sans certitude	1
D	Non, de manière certaine	0
E	Je ne souhaite pas ou ne suis pas autorisé à répondre à cette question	8
F	Je ne sais pas	2



Question 10 - Sentez-vous une accélération du rythme des attaques ?

Nombre de votants : 16
Origine des votants : ADP (1), DGA (2), EDF (1), INRS (1), INERIS (1), Orano (3), SSF (2), Petroineos (2), RATP (1), Rubis (1), Total (1)
Une seule réponse possible par votant

Réponses		Nombre de réponses :	16
A	Oui, depuis pas mal de temps		3
B	Oui, récente		0
C	Non		4
D	Pas d'avis		9



Question 11 - Rencontrez-vous des difficultés pour la mise en place de mesures de cybersécurité au sein de votre entreprise ?

Nombre de votants : 16
Origine des votants : ADP (1), DGA (2), EDF (1), INERIS (1), INRS (1), Petroineos (1), Orano (4), RATP (1), Rubis (1), SSF (2), Total (1)
Réponse unique

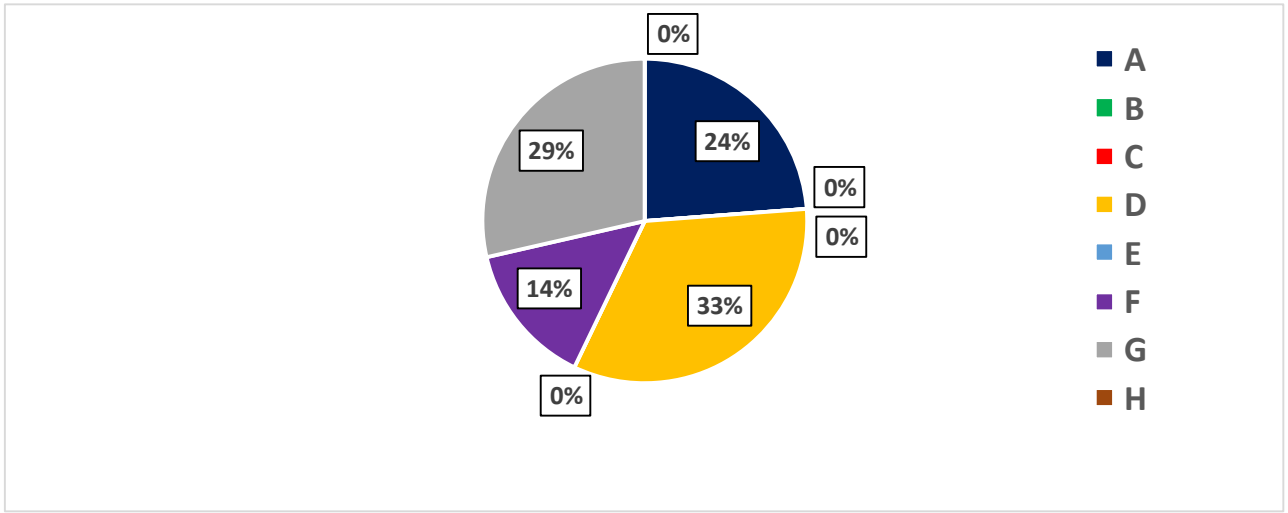
Réponses

Oui	**9**	**56%**
Non	**7**	**44%**

Question 11-1 - Si vous avez répondu par l'affirmative à la question précédente, merci de caractériser les difficultés rencontrées.

Nombre de votants : 10
Origine des votants : ADP (1), DGA (1), Orano (4), SSF (1), Petroineos (2), Rubis (1)
Au plus trois réponses possibles par votant

Réponses		Nombre de réponses :	21
A	Contraintes budgétaires		5
B	Motivation des dirigeants inexistante ou faible		0
C	Faiblesse connaissance - voire méconnaissance - des personnels en charge des OT		0
D	Complexité et durée de mise en oeuvre		7
E	Absence d'audit initial		0
F	Difficultés d'organisation IT/OT		3
G	Fréquence trop élevée des diffusions de correctifs de sécurité		6
H	Autre(s)		0



Question 12 - Quelles mesures d'ordre organisationnel ont déjà été mises en place pour améliorer la cybersécurité des OT au sein de votre entreprise ?

Nombre de votants : 15

Origine des votants : ADP (1), DGA (2), EDF(1), INERIS (1), INRS (1), Orano (4), Petroineos (1), RATP (1), Rubis (1), SSF (2), Total (1)

Plusieurs réponses possibles pour chaque votant

Réponses	Nombre de réponses : 94	
A - Mise en place de bonnes pratiques, et suivi de leur application	13	14%
B - Programme de sensibilisation du personnel	13	14%
C - Programme de formation et de certification	4	4%
D - Conduite d'un ou plusieurs audits de cybersécurité d'ordre technique et organisationnel	9	10%
E - Formalisation d'une politique de cybersécurité et nomination d'un responsable chargé de sa mise en œuvre	10	11%
F - Mise en place d'exigences contractuelles auprès des intervenants extérieurs (fournisseurs et prestataires)	10	11%
G - Déploiement d'outils de surveillance des réseaux OT pour la détection d'anomalies	7	7%
H - Déploiement d'outils de surveillance des réseaux OT pour la détection d'intrusions	6	6%
I - Recrutement de personnels qualifiés en cybersécurité ou externalisation dans la durée	7	7%
J - Déploiement d'outils de surveillance des communications sans fil	0	0%
K - Mise en place d'une gestion des identités et des accès sur les SI et OT	6	6%
L - Segmentation des SI industriels	9	10%
M - Autre(s)	0	0%

Question 13 - Quelles sont les mesures d'ordre organisationnel dont le déploiement est prévu à court terme (12 à 18 mois) ?

Nombre de votants : 13
Origine des votants : ADP (1), DGA (2), EDF(1), INERIS (1), Orano (2), Petroineos (1), RATP (1), Rubis (1), SSF (2), Total (1)
Plusieurs réponses possibles pour chaque votant

Réponses	Nombre de réponses : 32	
A - Mise en place de bonnes pratiques, et suivi de leur application	2	6%
B - Programme de sensibilisation du personnel	2	6%
C - Programme de formation et de certification	1	3%
D - Conduite d'un ou plusieurs audits de cybersécurité d'ordre technique et organisationnel	2	6%
E - Formalisation d'une politique de cybersécurité et nomination d'un responsable chargé de sa mise en œuvre	4	13%
F - Mise en place d'exigences contractuelles auprès des intervenants extérieurs (fournisseurs et prestataires)	3	9%
G - Déploiement d'outils de surveillance des réseaux OT pour la détection d'anomalies	5	16%
H - Déploiement d'outils de surveillance des réseaux OT pour la détection d'intrusions	3	9%
I - Recrutement de personnels qualifiés en cybersécurité ou externalisation dans la durée	3	9%
J - Déploiement d'outils de surveillance des communications sans fil	0	0%
K - Mise en place d'une gestion des identités et des accès sur les SI et OT	2	6%
L - Segmentation des SI industriels	1	3%
M - Autre(s)	4	13%

Question 14 - Quels sont les outils et méthodes d'ordre technique déjà mises en oeuvre dans votre entreprise ?

Nombre de votants : 15
Origine des votants : ADP (1), DGA (2), EDF(1), INRS (1), Orano (4), Petroineos (1), RATP (1), Rubis (1), SSF (2), Total (1)
Plusieurs réponses possibles pour chaque votant

Réponses	Nombre de réponses : 70	
A - Strict contrôle d'accès physique aux locaux et aux infrastructures des réseaux	12	17%
B - Contrôle d'accès logique	8	11%
C - Segmentation stricte des réseaux OT (Zonages et conduits)	9	13%
D - Logiciels Antivirus	10	14%
E - Mise en oeuvre de solutions de cartographie et d'inventaire OT	6	9%
F - Déploiement effectif des correctifs de sécurité	9	13%
G - Surveillance des journaux	5	7%
H - Mise en place de sondes de détection d'intrusion	3	4%
I - Mise en oeuvre de scanners de vulnérabilité	3	4%
J - Contrôle d'intégrité (liste blanche)	3	4%
K - Autre(s)	2	3%

Question 15 - Quels sont les outils et méthodes d'ordre technique dont le déploiement est prévu à court terme (12 à 18 mois) dans votre entreprise ?

Nombre de votants : 15
Origine des votants : ADP (1), DGA (2), EDF(1), INRS (1), Orano (4), Petroineos (1), RATP (1), Rubis (1), SSF (2), Total (1)
Plusieurs réponses possibles pour chaque votant

Réponses	Nombre de réponses : 70	
A - Strict contrôle d'accès physique aux locaux et aux infrastructures des réseaux	12	17%
B - Contrôle d'accès logique	8	11%
C - Segmentation stricte des réseaux OT (Zonages et conduits)	9	13%
D - Logiciels Antivirus	10	14%
E - Mise en oeuvre de solutions de cartographie et d'inventaire OT	6	9%
F - Déploiement effectif des correctifs de sécurité	9	13%
G - Surveillance des journaux	5	7%
H - Mise en place de sondes de détection d'intrusion	3	4%
I - Mise en oeuvre de scanners de vulnérabilité	3	4%
J - Contrôle d'intégrité (liste blanche)	3	4%
K - Autre(s)	2	3%

Question 16 - Quels sont selon vous les trois composants des réseaux OT les plus à risques ?

Nombre de votants : 14
Origine des votants : ADP (1), DGA (2), EDF(1), INRS (1), Orano (4), Petroineos (1), Rubis (1), SSF (2), Total (1)
Au plus trois réponses possibles par votant

Réponses **Nombre de réponses :** 35

A	Les applications de supervision	5	14%
B	Les applications d'historisation/consultation	1	3%
C	Les applications de maintenance	6	17%
D	Les applications de développement/programmation	2	6%
E	Les réseaux de communication filaires	3	9%
F	Les réseaux sans fil	7	20%
G	Les automates et contrôleurs	4	11%
H	Les passerelles et/ou Remote Terminal Units	0	0%
I	Les systèmes d'exploitation commerciaux	7	20%
J	Les systèmes d'exploitation propriétaires	0	0%
K	Autre(s)	0	0%
L	Je ne souhaite pas ou ne suis pas autorisé à répondre à cette question	1	3%

Question 17 - Êtes-vous concerné par la sécurisation de réseaux anciens ?

Nombre de votants : 12
Origine des votants : DGA (2), EDF (1), INRS (1), Petroineos (1), Orano (3), Rubis (1), SSF (2), Total (1)
Réponse unique

Réponses

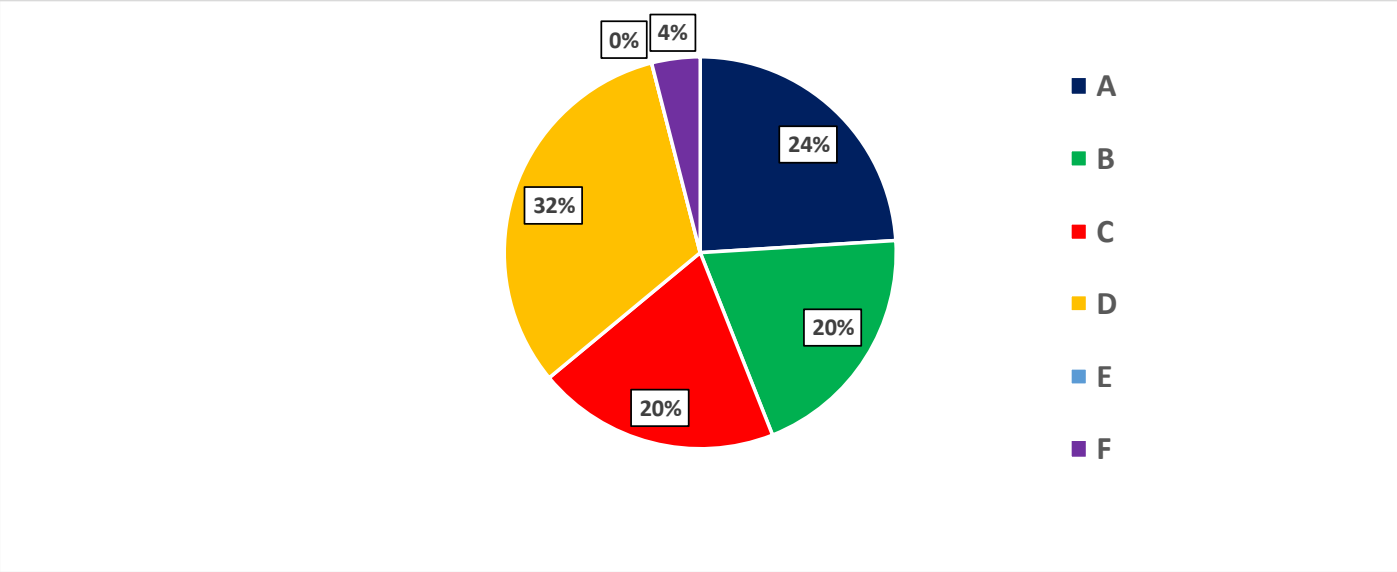
Oui	**8**	**67%**
Non	**4**	**33%**

QUESTIONS PROSPECTIVES...

Question 18 - Quels sont, selon vous, les outils et/ou méthodes les plus prometteurs pour assurer la cybersécurité des systèmes industriels ?

Nombre de votants : 12
Origine des votants : ADP (1), DGA (1), EDF(1), INRS (1), Orano (3), Petroineos (1), Rubis (1), SSF (2), Total (1)
Au plus trois réponses possibles par votant

Réponses		Nombre de réponses :	25		
A	Intelligence artificielle		6		
B	Virtualisation		5		
C	Vitrification des systèmes		5		
D	Mise en place de SOC		8		
E	Développement de logiciels propriétaires		0		
F	Autre(s)		1	--> SSF	Formation aux bons usages et à la connaissance des risques Cyber



Question 19 - La cybersécurité constitue-t-elle un enjeu important pour les projets "Usine du futur" ou "Usine 4.0" ?

Nombre de votants : 12
Origine des votants : ADP (1), DGA (2), EDF(1), Orano (3), Petroineos (1), Rubis (1), SSF (2), Total (1)
Réponse unique

Réponses **Nombre de réponses :** 12

A	Oui	12	100%
B	Non	0	0%
C	Pas d'avis sur la question	0	0%

Commentaires :

ADP L'utilisation massive, pour l'industrie 4.0, de technologies sans fil et des objets connectés (IIOT), aujourd'hui pas toujours bien sécurisées, risque à la fois d'augmenter la surface d'attaque et les points d'entrées des systèmes industriels.

DGA Lorsqu'il y a des enjeux économiques, concurrentiels, de défense, ou autres, l'ouverture d'un système requiert d'évaluer les risques découlant de cette ouverture.
Les risques associés à la cybersécurité sont donc tout naturellement à prendre en compte comme l'une des composantes dans les analyses de risques de tout système ouvert de type "Usine 4.0".
En revanche, l'enjeu fort est l'équilibre à conserver entre les différents risques à maîtriser :
il ne faudrait pas, pour maîtriser la cybersécurité, prendre des mesures extrêmes qui seraient incompatibles avec les autres caractéristiques attendues telles que disponibilité, fiabilité, efficacité/performances.

SSF La cyber insécurité est une contrainte additionnelle désormais incontournable.
La défense contre cette menace participe évidement d'un rapport commun à tous les acteurs de la chaîne industrielle mais pas seulement. L'importance qu'il convient de lui donner est à la mesure de la vulnérabilité de chacun vis-à-vis de ses systèmes et de son environnement.

4 Cité d'Hauteville | 75010 Paris | France
Tél. : +33 1 53 32 80 08 | Web site : www.exera.com