De l'information au renseignement

9 décembre 2020

Anticiper, détecter et répondre aux menaces cyber et aux incidents de sécurité

Quels outils pour vous protéger des cybermenaces ?

Building a better working world

De l'information au Renseignement : Les intervenants

Olivier PATOLE
Partner EY, Cyber Security,
CTI Service Leader

Hervé GABIREAU
Monnoyeur
Directeur Infrastructure IT

Le paysage de la menace cyber

La digitalisation, l'adoption croissante du cloud et de mobilité étendent la surface numérique des organisations et, en conséquence, à une exposition accrue aux menaces. En parallèle, nous assistons à une professionalisation de la menace au travers d'attaques de plus en plus sophistiquées et contextualisées.

Les tendances actuelles en matière de cyber menaces et de cyber attaques

Phishing, sites malicieux et compromission de messagerie professionnelle

- Les cybercriminels peuvent exploiter l'intérêt suscité par une situation contextuelle pour diffuser des campagnes malveillantes et réaliser des activités de phishing ou créer de faux sites usurpant des institutions gouvernementales.

Extorsion ou vol de données et atteinte à l'image

- Les entreprises peuvent recevoir de nombreuses menaces et être sous pression du fait de la diffusion de l'épidémie.
- Les actions inhabituelles ou les anomalies doivent être considérées comme des signaux faibles et peuvent être gérées comme des menaces.

Rupture dans l'activité dues aux attaques

- Les ransomware exploitant des thèmes liés au Coronavirus peuvent chiffrer les disques durs des postes informatiques et permettre aux pirates d'exiger le versement d'une rançon pour déchiffrer les données.

des membres du conseil d'administration ne sont, au mieux, que peu convaincus que les risques de cybersécurité et les mesures d'atténuation qui leur sont présentés peuvent protéger l'organisation contre les cyberattaques majeures.

01 60% des organisations ont dû faire face à incident majeur au cours des 12 derniers mois

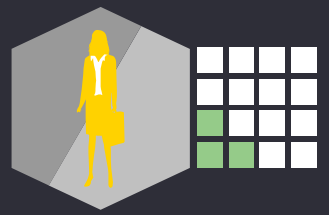
02 70% des attaques sont causées par des ransomware et/ou des logiciels malveillants

03 12% des organisations sont capables de détecter les nouvelles menaces

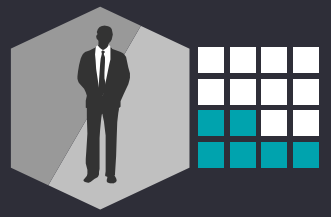
04 Seulement 26% des organisations déclarent que leur SOC a identifié l'intrusion la plus importante au cours des 12 derniers mois

Source: EY's Global Information Security Survey 2020 results

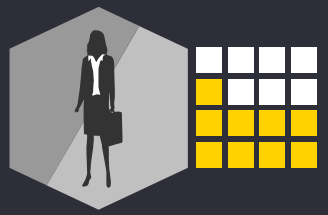
Le paysage de la menace cyber



12% Des entreprises n'ont pas de moyens de détecter les fuites d'informations



35% Des entreprises décrivent leur politique de protection de la donnée comme basique.



57% Des entreprises n'ont pas de programme de renseignement Cyber

La majorité des fuites d'informations se font suite à l'exploitation de vulnérabilités connues.

99% des vulnérabilités exploitées sont connues des professionnels de la sécurité depuis au moins un an.

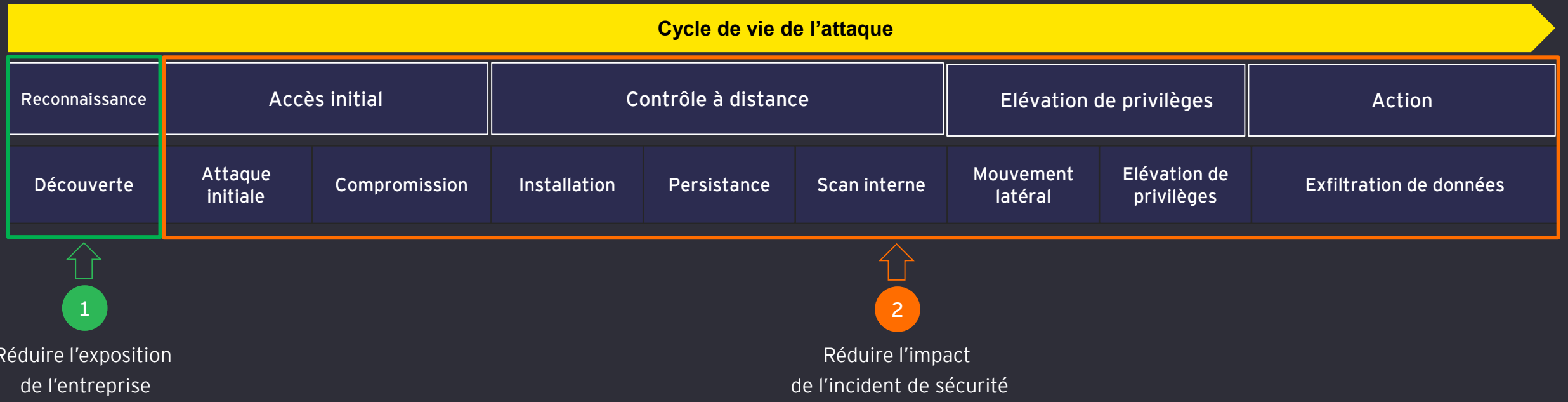
'State of the Threat Landscape 2017', Greg Young, Gartner, 2017 pp. 19, 24; "Is it possible to be predictive in Information Security?", Craig Lawson, Gartner 2017, p. 15

Le besoin de renseignement sur le risque Cyber

Le renseignement est une fonction de recherche d'information utile à la décision pour l'action dans l'incertitude.

Intelligence = Renseignement

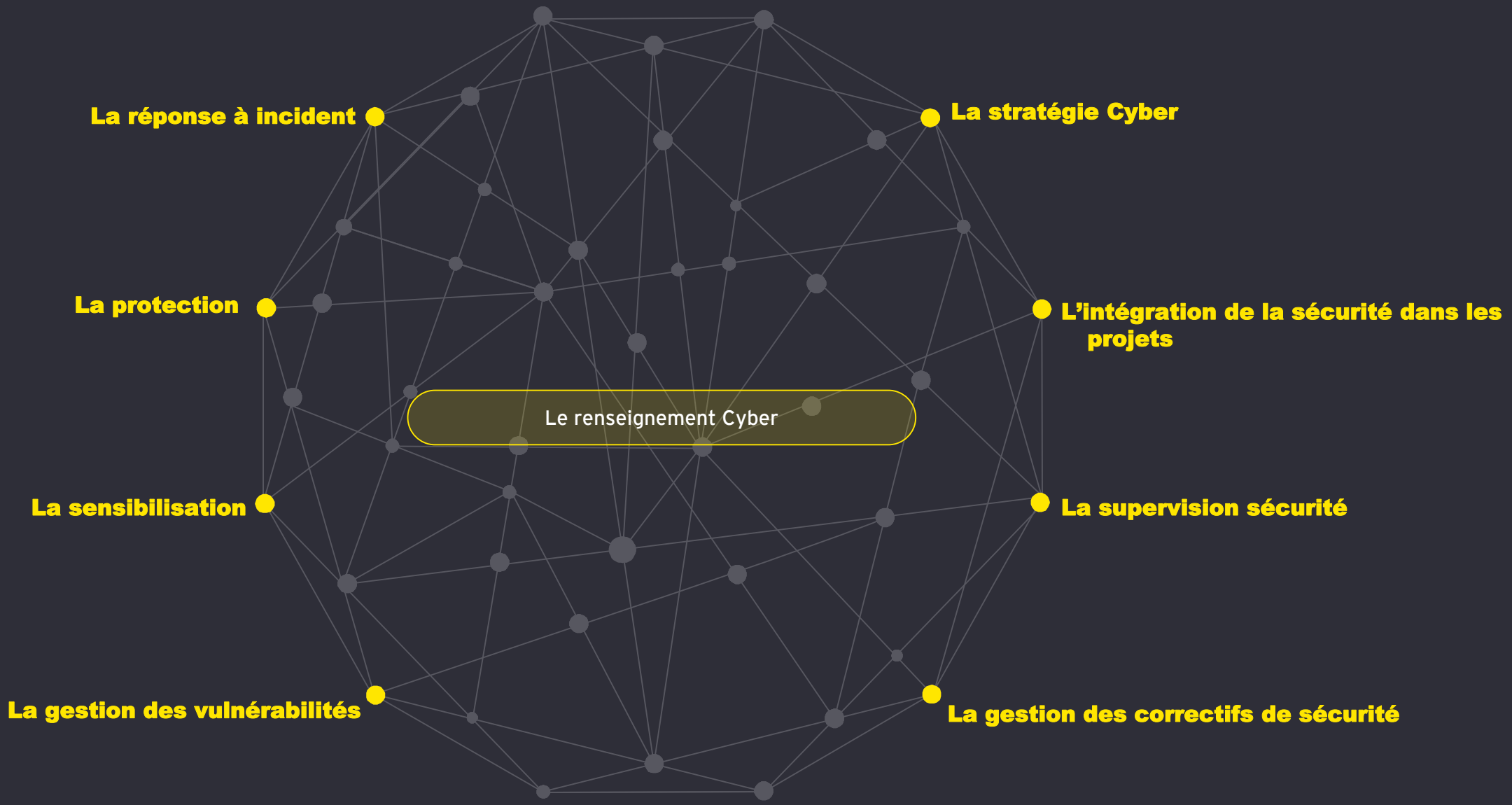
Les apports du renseignement Cyber



Réduire l'exposition de l'entreprise

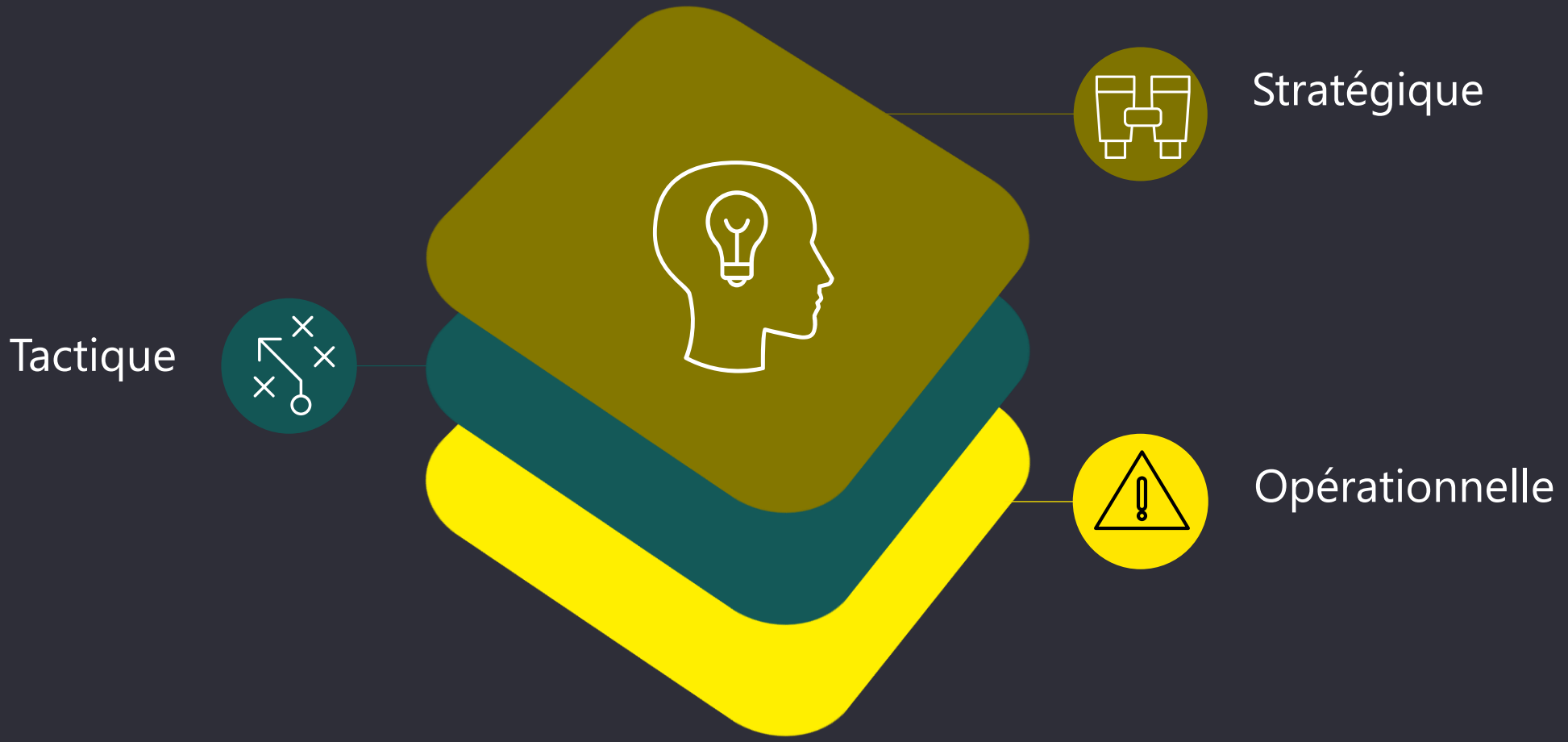
Réduire l'impact de l'incident de sécurité

L'intégration du renseignement Cyber

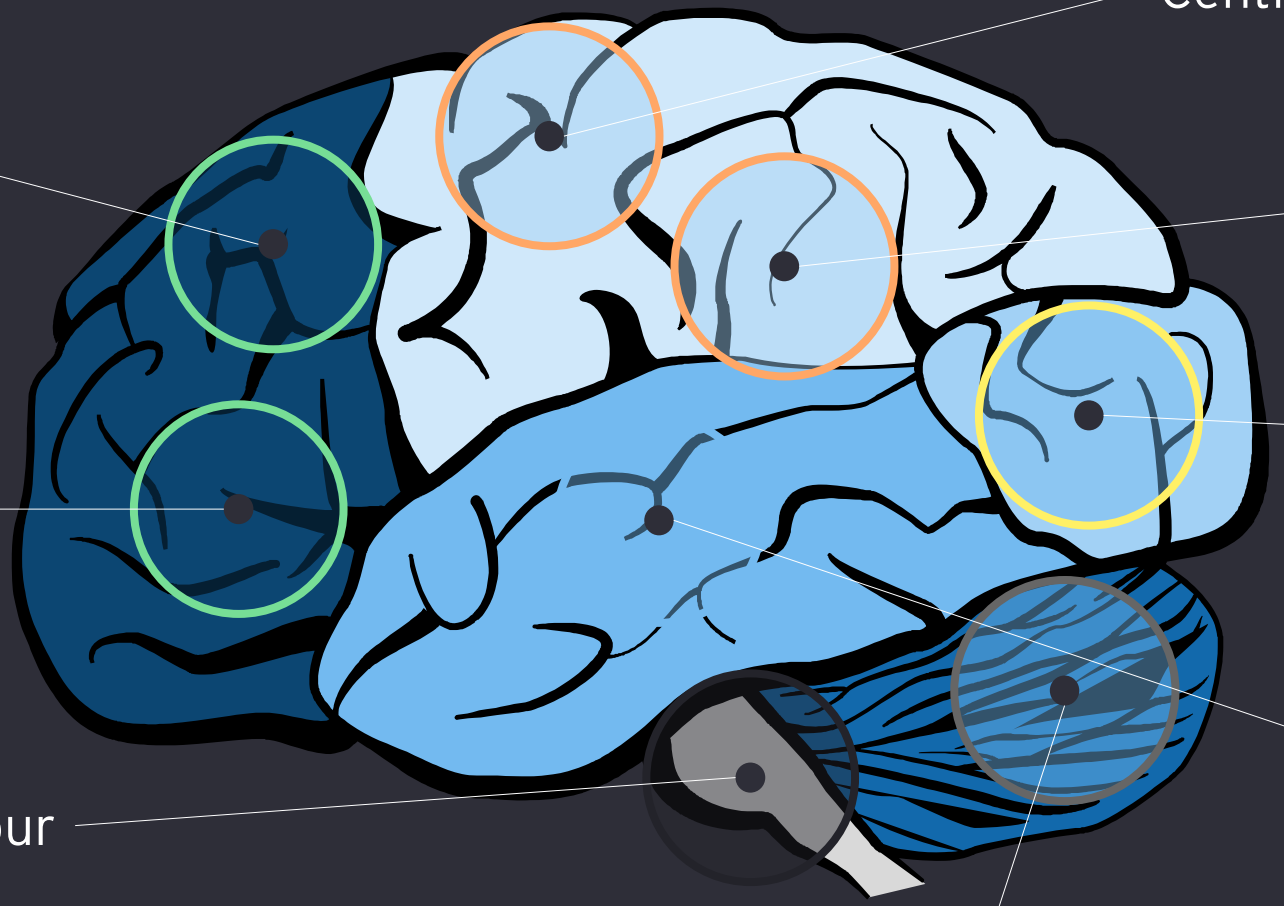


L'intégration du renseignement Cyber

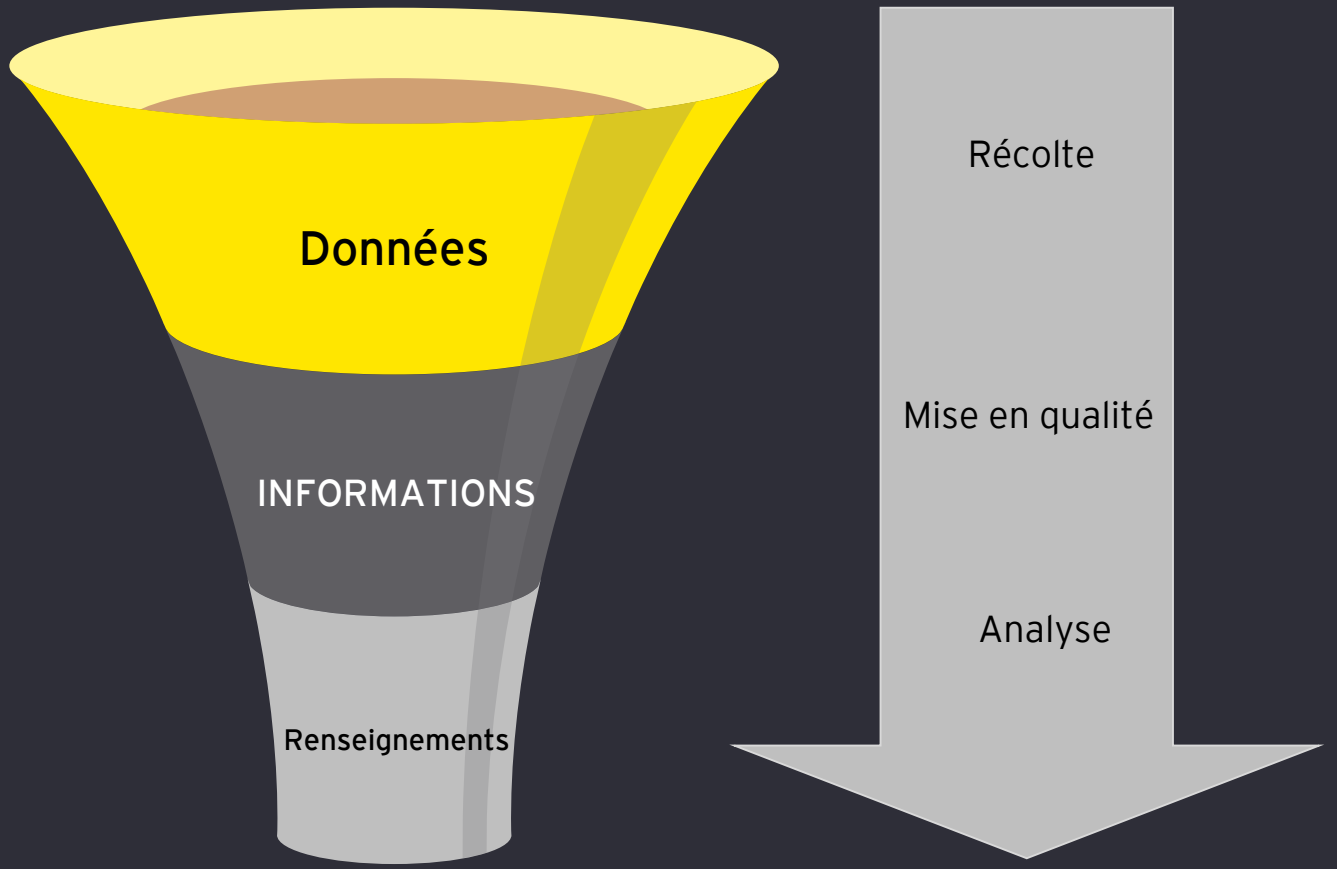
- Les différents niveaux du renseignement Cyber



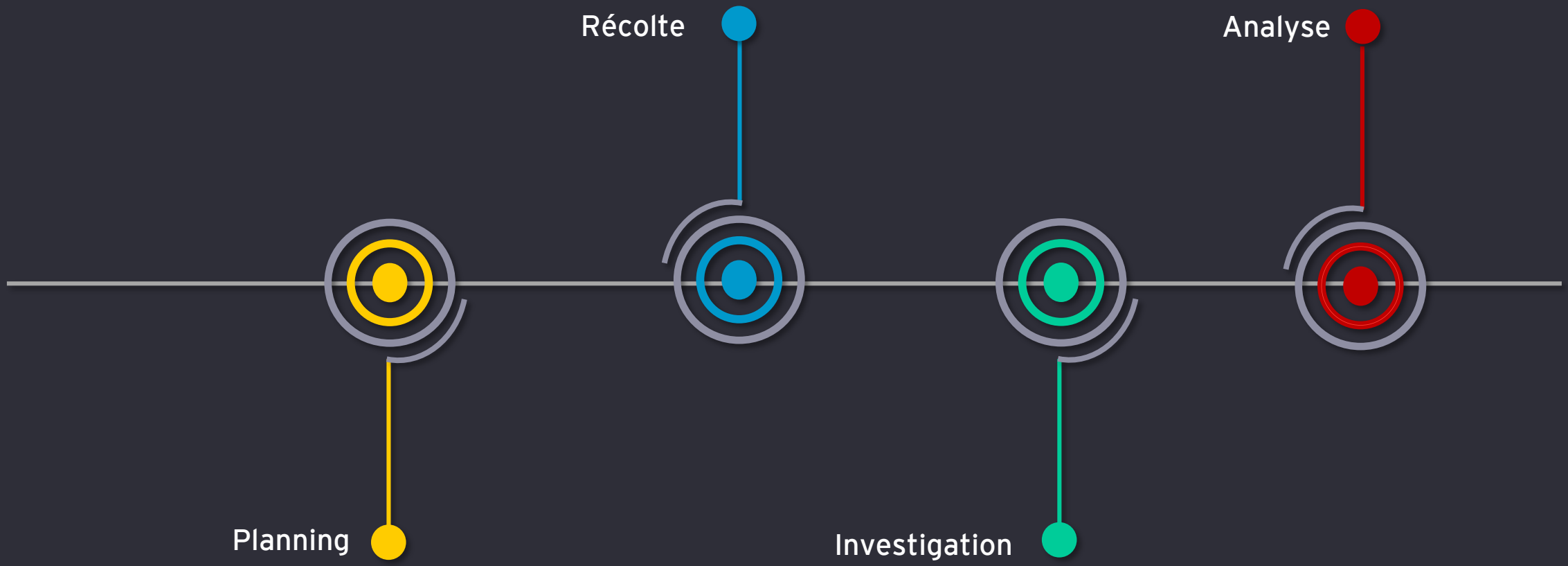
Les enjeux du renseignement Cyber



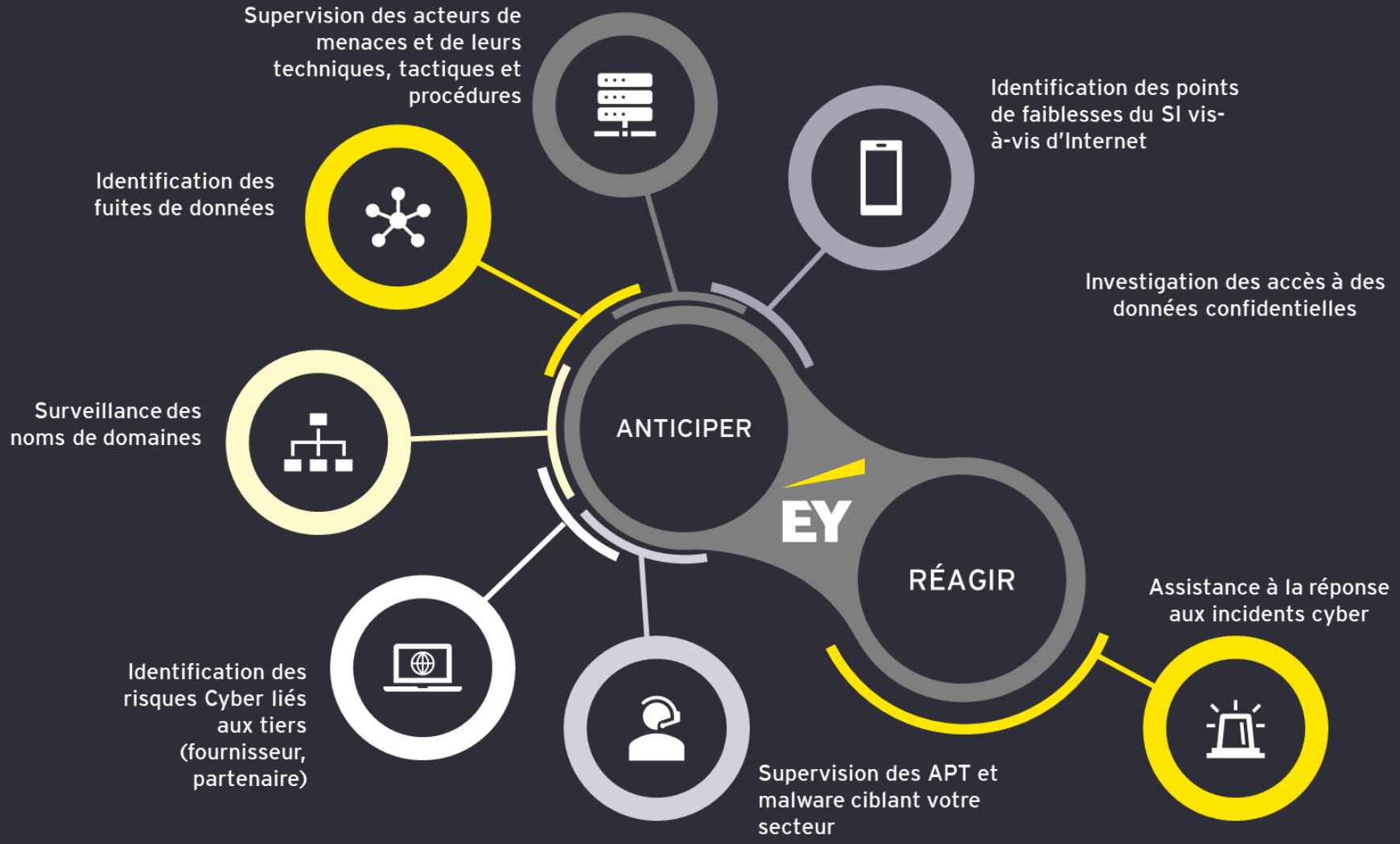
Le processus de transformation de la donnée en renseignement



La gestion du renseignement Cyber



Ce que permet d'obtenir le renseignement Cyber



Service CyberEYe : Retour d'expérience

Hervé GABIREAU
Monnoyeur
Directeur Infrastructure IT

Groupe Monnoyeur

- Une entreprise familiale fondée en 1906
- 6 200 Salariés
- + de 2 Mds € de Chiffre d'affaire en 2019
- Une activité présente dans 15 pays répartis (Europe, Afrique du Nord et Asie)
- 4 pôles d'activité

Service CyberEYe : Retour d'expérience

1 Contexte

2 Objectif

3 CyberEYe

Service CyberEYe : Retour d'expérience

La valeur ajoutée du service

- La veille sécurité
- La qualité de la donnée
- La diversité des sources notamment dark web
- L'expertise des équipes

De l'information au renseignement

Questions ?

De l'information au renseignement : Contact

Olivier PATOLE
Partner EY, Cyber Security,
CTI Service Leader
+33 7 62 02 18 90
olivier.patole@fr.ey.com

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation is available via ey.com/privacy. For more information about our organization, please visit ey.com.

1912-3343095
ED None

ey.com