X-SPIErience Day 2020

SOUVERAINETÉ NUMÉRIQUE

SPIE

cisco Partner

FORTINET

HUAWEI

SPIE, sharing a vision for the future

X-SPIErience Day 2026
SOUVERAINETÉ NUMÉRIQUE

SPIE

Souveraineté numérique au centre : gérer intelligemment et automatiquement les risques liés aux tiers

HUBERT RÉMOND

Team Leader Solution Network Security
SPIE ICS

Pourquoi maintenant ?

82 % des organisations [] considèrent le risque [tiers] comme « **important** » ou « **très important** » [1]

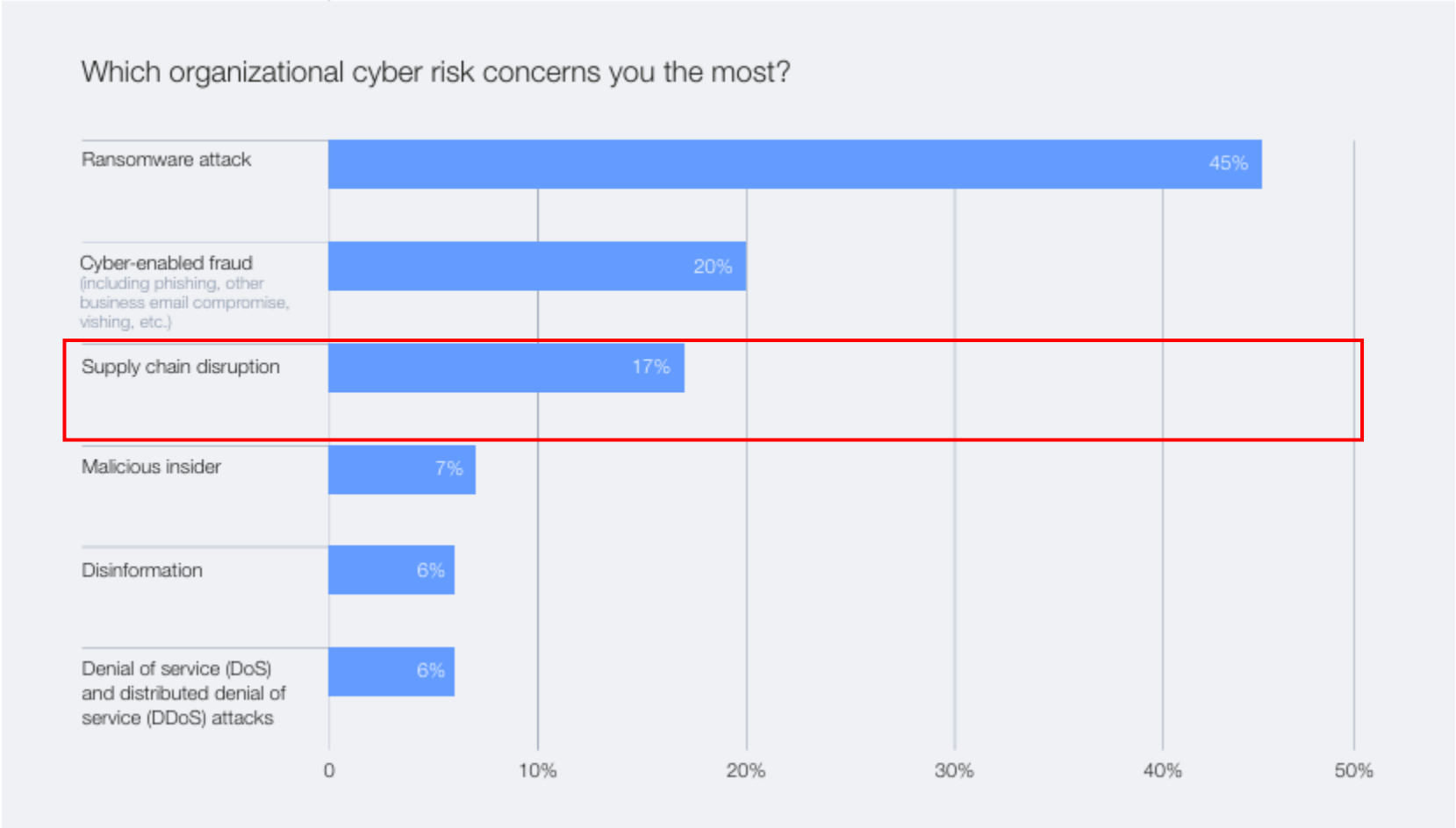
4 % ont une grande confiance que leurs questionnaires [tiers] **correspondent à la réalité du risque** [2]

24 % Incidents de sécurité causés par des tiers en 2024 [2]
266% *d'augmentation depuis 2020*

[1]Source: TPRM Observatory 2025 | Board of cyber
[2]Source: The State of 3rd-Party Risk Management Report 2024 | RiskRecon

Pourquoi maintenant ?

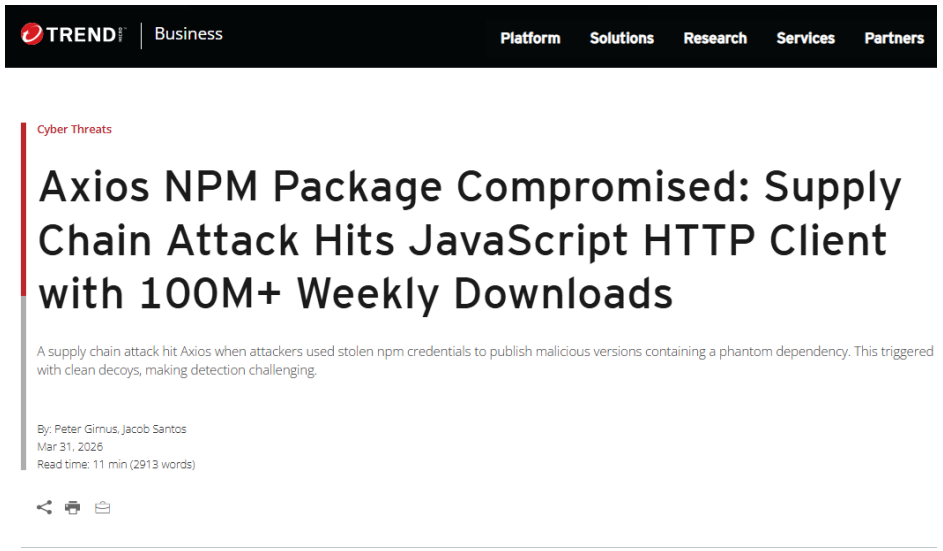
FIGURE 3 **Organizational cyber risks ranked – 2025**



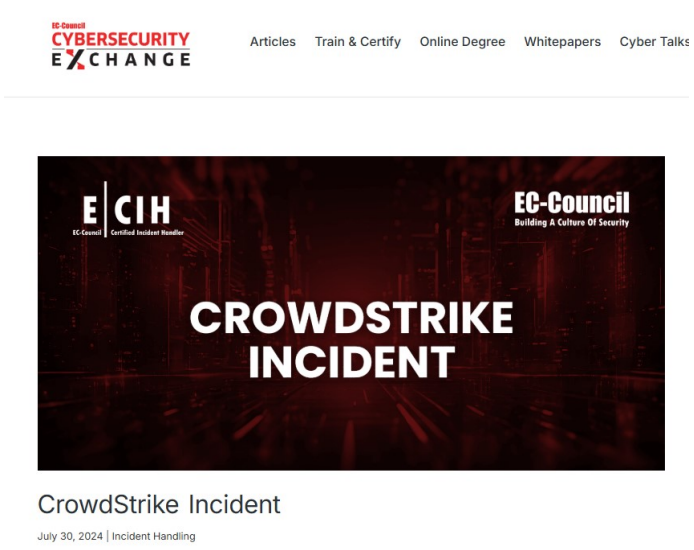
Source: WEF_Global_Cybersecurity_Outlook_2025.pdf

Exemples récents de réalisation du risque lié aux tiers

Fuite de données



Accès non autorisé



Disponibilité

Alignement réglementaire et principaux cadres

finma
Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

NIS2 Network & Information Systems Directive

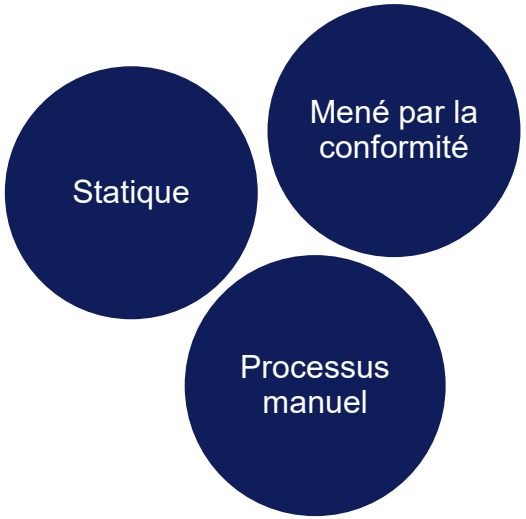
DORA

EU Cyber Resilience Act
For safer & more secure digital products
#DigitalEU #CyberSecEU

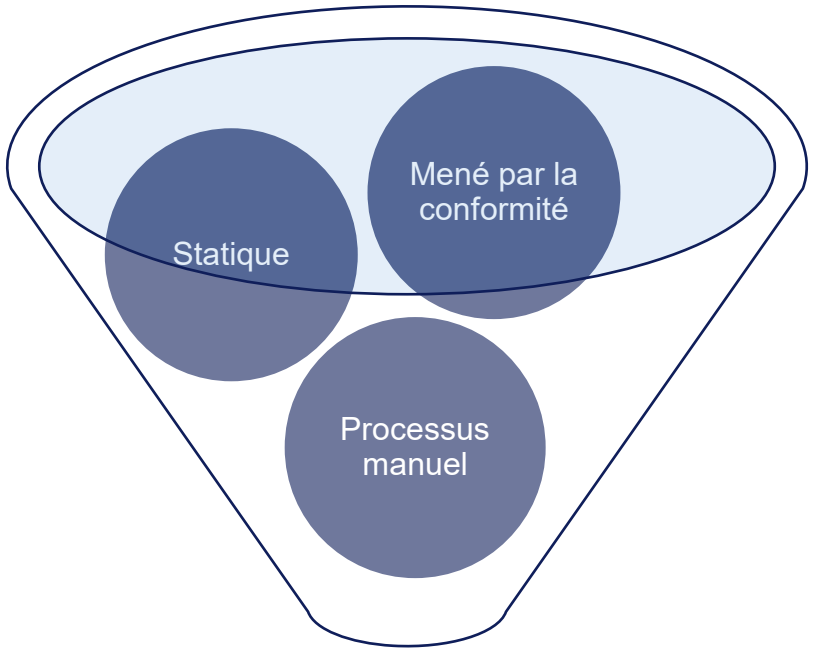
Information Security Management ISO 27001 Certified

NIST Cybersecurity Framework
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
GOVERN

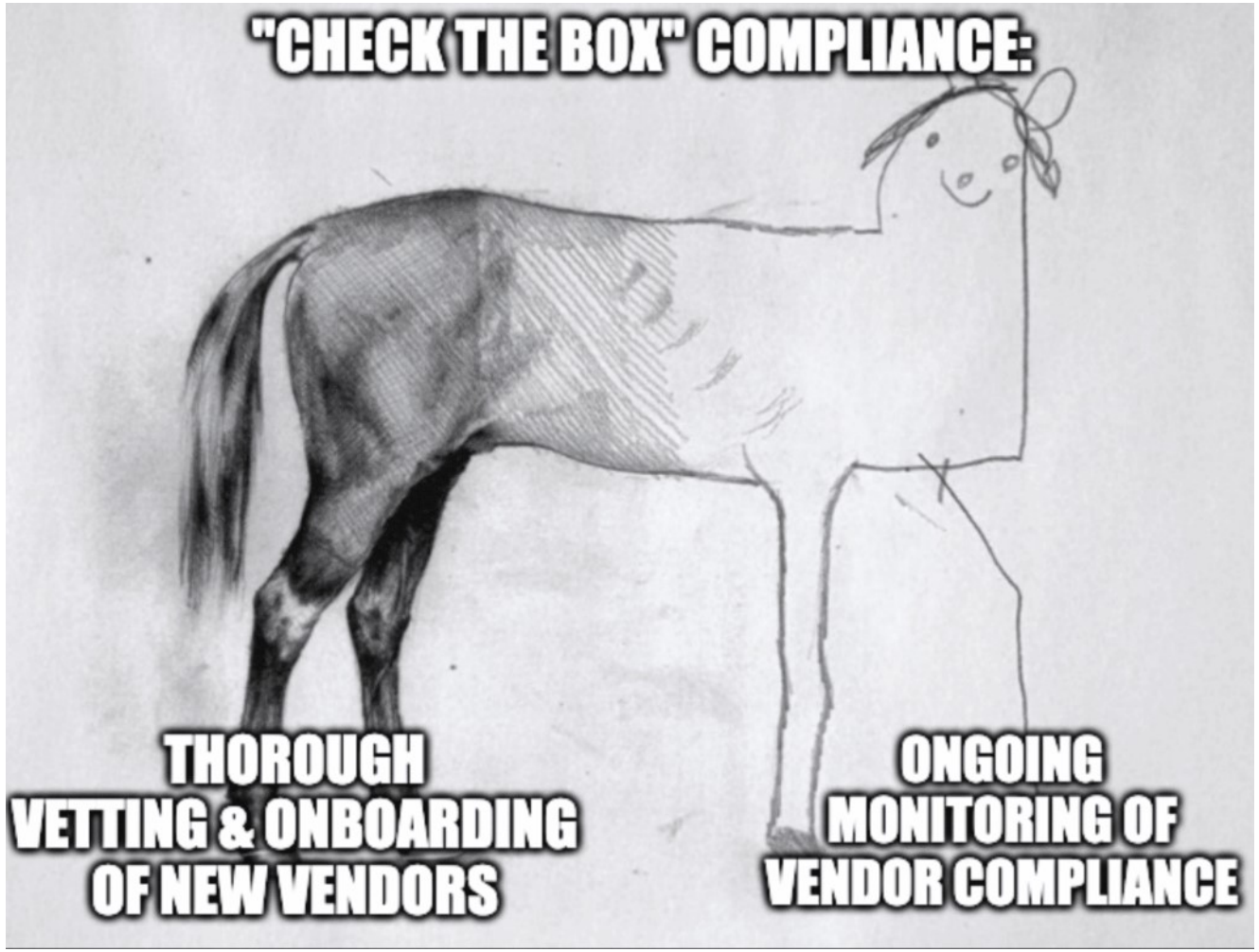
Gestion typique du risque tiers



Gestion typique du risque tiers



ECHEC



Notations automatisés

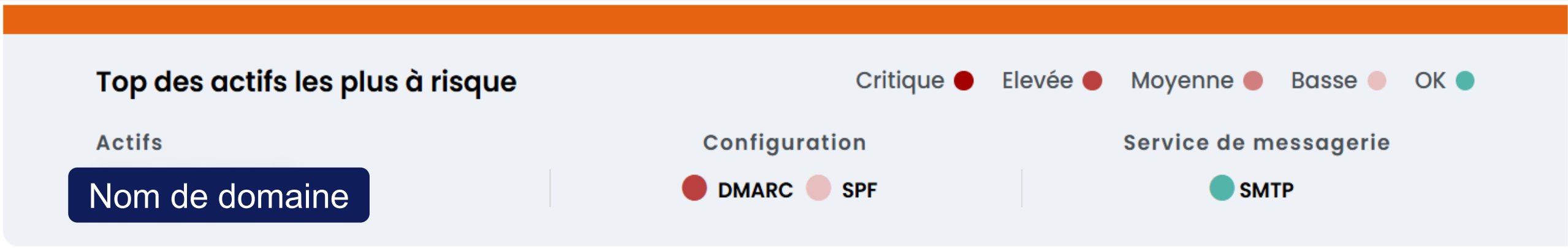
Visibilité **Contrôle** **Agilité**

- Informations publiques

Notations automatisés

Visibilité **Contrôle** **Agilité**

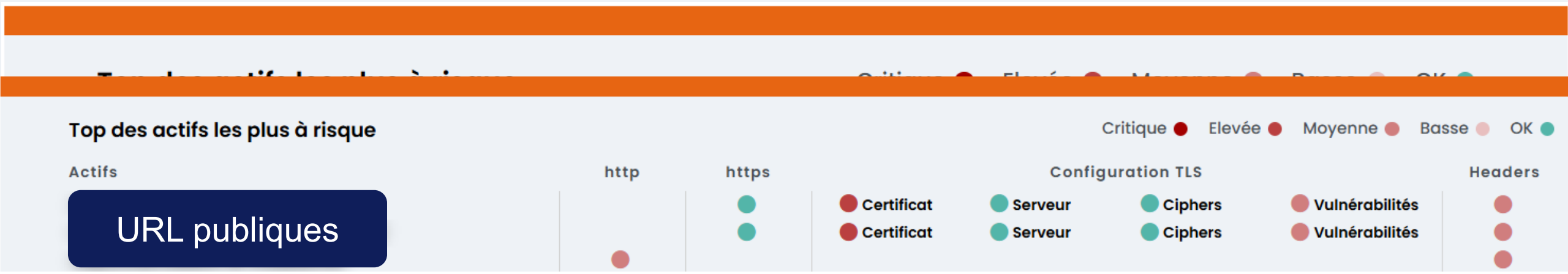
- Informations publiques



Notations automatisés

Visibilité **Contrôle** **Agilité**

- Informations publiques



Notations automatisés

Visibilité **Contrôle** **Agilité**

- Informations publiques

Notations automatisés

Visibilité **Contrôle** **Agilité**

- Informations publiques

Aperçu de la posture de sécurité, automatisée, toujours à jour
10 minutes à installer

Visibilité (risques liés aux Nth-party)

Répartition des fournisseurs

Mon compte | Répartition globale

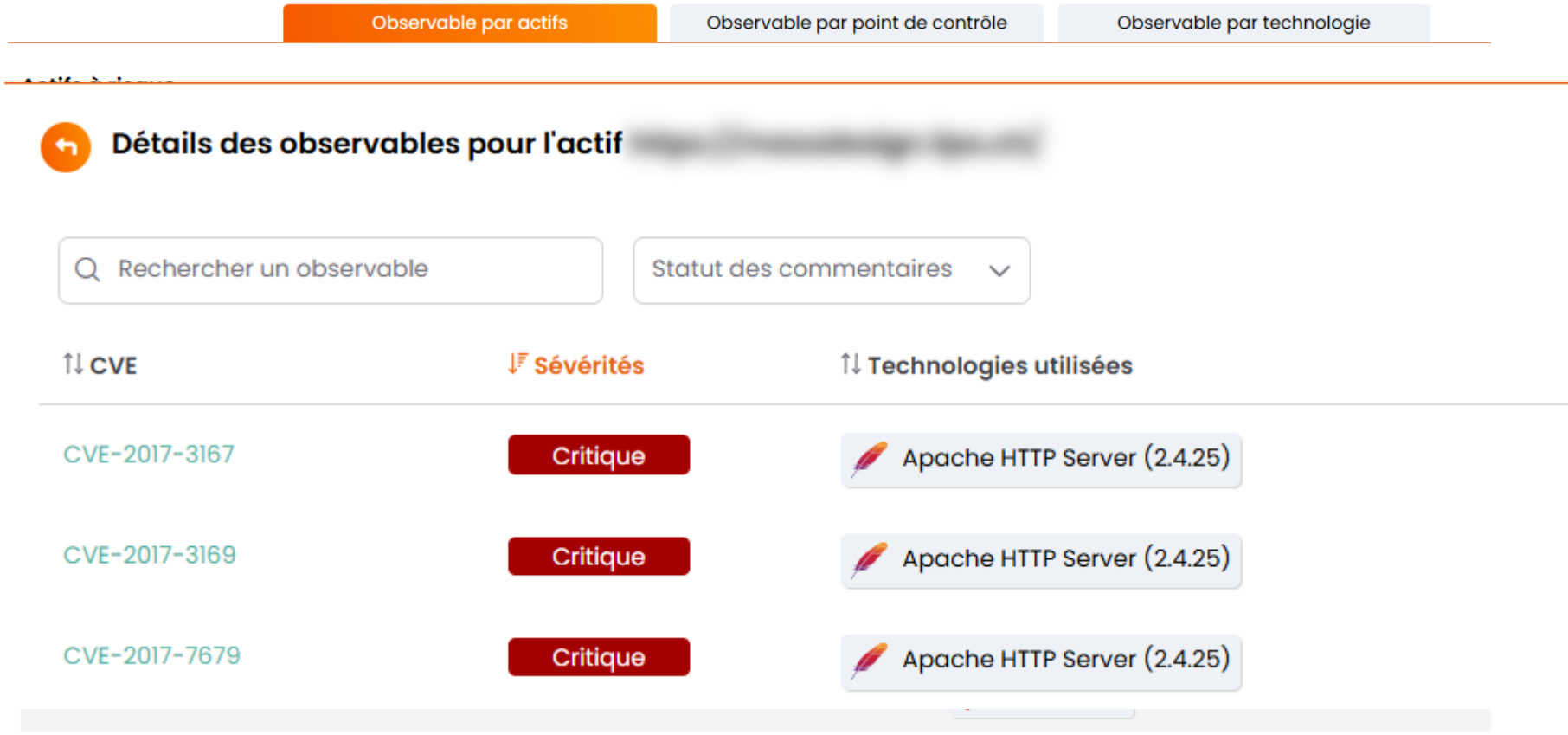
Filtrer sur les fournisseurs majeurs

- 27.8% - Group < 1% : 1&1 Mail & Media GmbH|1a
- 22.3% - Microsoft Corporation
- 11.8% - Amazon.com, Inc.
- 9.5% - Amazon Data Services Northern Virgini
- 8.9% - Group < 5% : Google LLC|OVH SAS
- 8.1% - Group < 2% : A100 Row GmbH|Amazon D
- 6.5% - Group < 4% : Amazon Data Services No
- 5% - Cloudflare, Inc.

- 27.8% - Group < 1% : 1&1 Mail & Media GmbH
- 22.3% - Microsoft Corporation
- 11.8% - Amazon.com, Inc.
- 9.5% - Amazon Data Services Northern Virginia
- 8.9% - Group < 5% : Google LLC
  - OVH SAS
- 8.1% - Group < 2% : A100 Row GmbH
  - Amazon Data Services Ireland Limited
  - GANDI DEDICATED HOSTING SERVERS
  - GANDI SAS
  - Gandi.net
  - Marchand Guillaume
  - Salesforce.com, Inc.

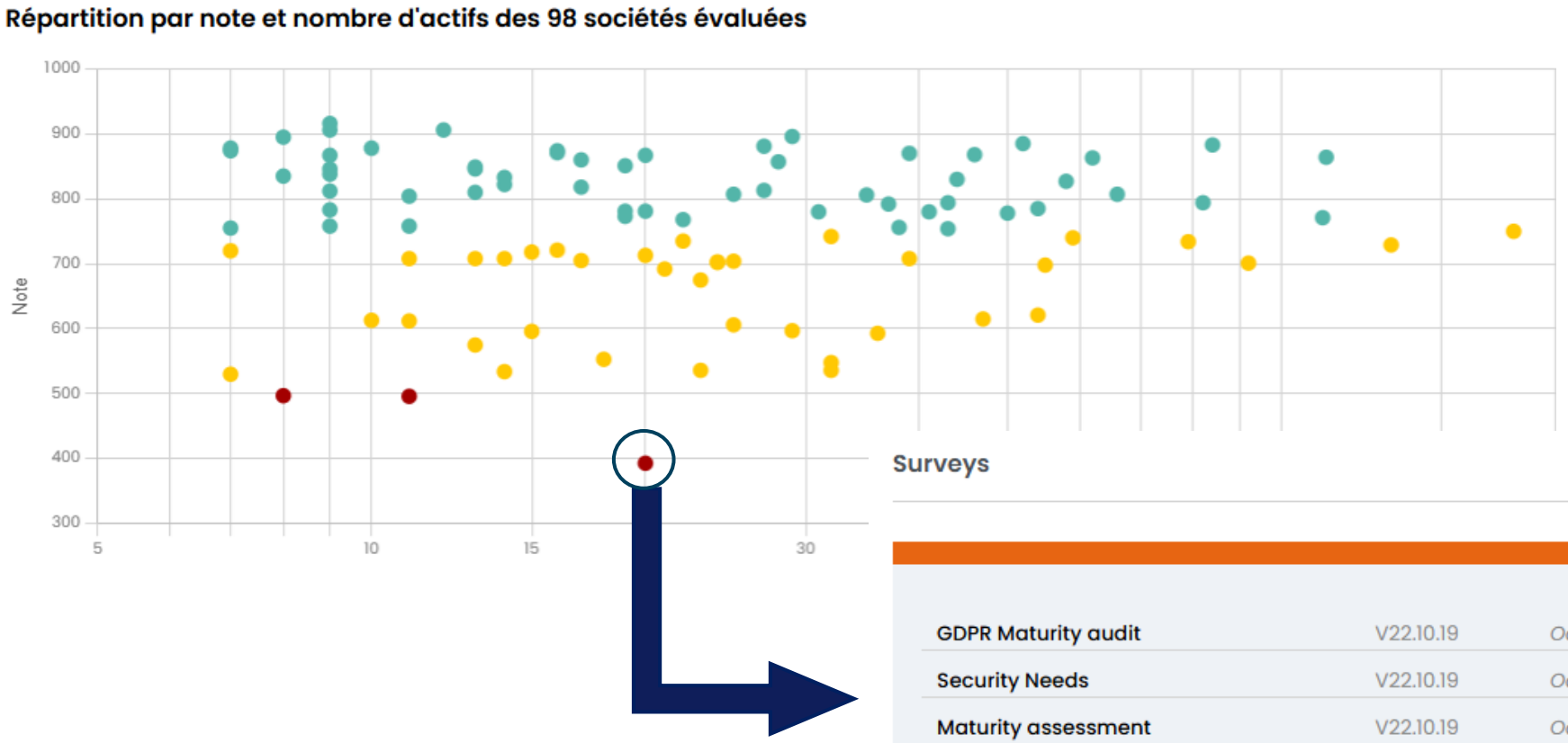
Maturité cyber de vos tiers

Maturité cyber de vos tiers



Maturité cyber de vos tiers

Visibilité, Contrôle, Agilité



Surveys

GDPR Maturity audit	V22.10.19	*Oct 19, 2022*	**In progress**
Security Needs	V22.10.19	*Oct 19, 2022*	**E**
Maturity assessment	V22.10.19	*Oct 19, 2022*	**C**

See more

Étapes concrètes pour une gestion efficace

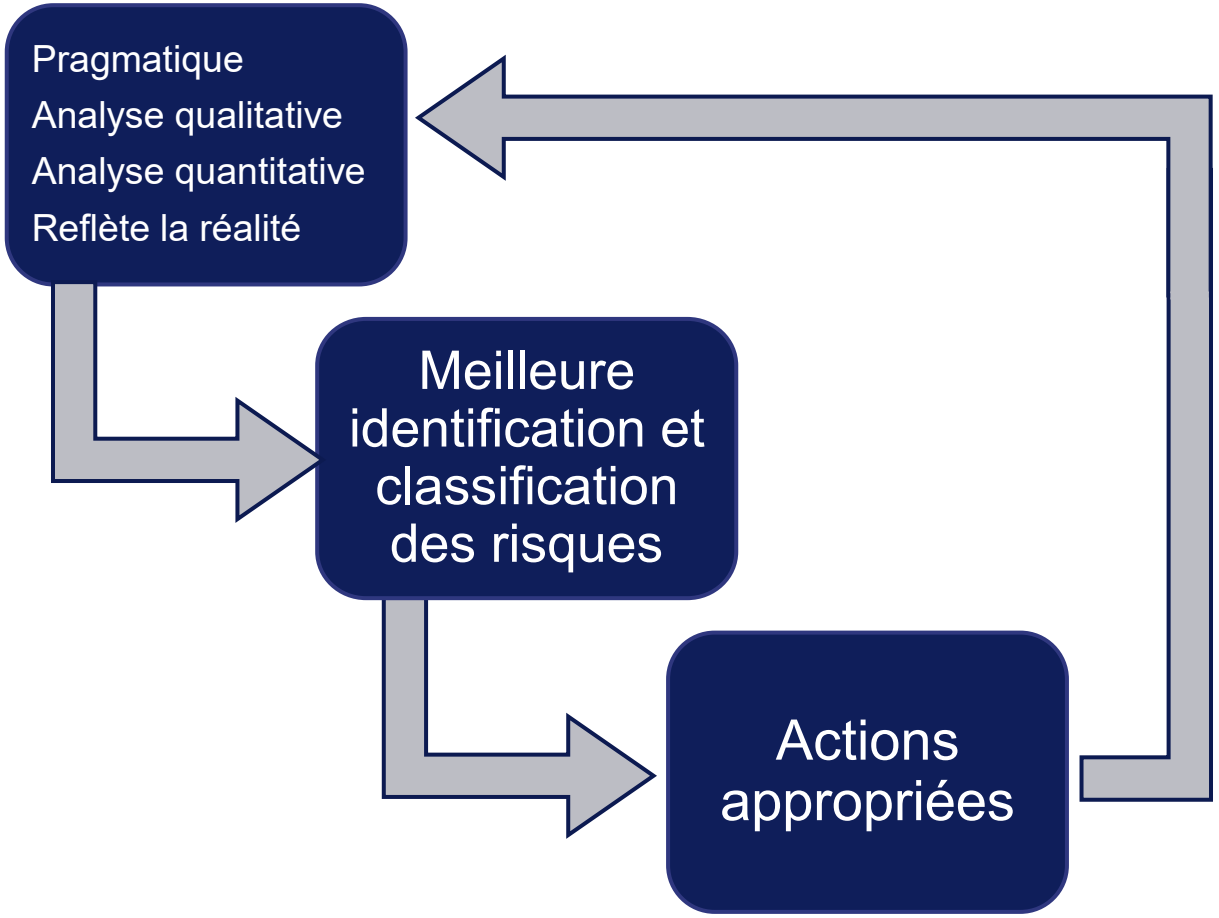
QUESTIONNAIRE SIMPLE

NOTATION AUTOMATISÉE

RÉSULTATS DU DERNIER PENTEST (Y COMPRIS LES ANALYSES)

INDICATEURS DE GESTION DES VULNÉRABILITÉS ET MTTR

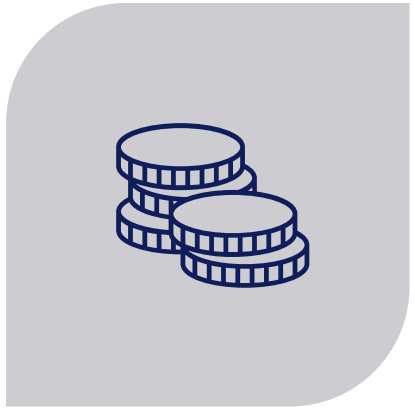
PARCOURS D'UN INCIDENT SPÉCIFIQUE DES 12 DERNIERS MOIS, ROOT CAUSE, CORRECTIONS



Que se passe-t-il si vous attendez ?

EXPOSITION ACCRUE AU RISQUE

AUGMENTATION DU COÛT D'UNE ATTAQUE



NON-CONFORMITÉ À LA RÉGLEMENTATION

COÛT DE L'AMENDE

MAILLON FAIBLE DE VOTRE CHAÎNE D'APPROVISIONNEMENT

COÛT DE REVENUS MANQUANTS

Votre feuille de route pour la souveraineté numérique commence aujourd'hui!

Étape 1 : Augmenter la visibilité de votre écosystème

Commencez petit, concentrez-vous sur les tiers critiques pour l'entreprise (y compris les sous-traitants et les quatrième parties).

Étape 2 : Vérifier la localisation des données et les règles de confidentialité

Privilégiez les tiers qui proposent des options d'hébergement local et sont conformes aux réglementations applicables.

Étape 3 : Évaluation intégrée des tiers à travers les catégories de risques

Sécurité, capacité opérationnelle, santé financière et conformité réglementaire.

Étape 4 : Pratiques d'achats résilientes

Dans la mesure du possible, évitez le « vendor lock-in », privilégiez les standards ouverts et les stratégies de sortie rigoureuses.

Étape 5 : Surveillance continue

Mettre en œuvre des outils automatisés de surveillance en temps réel pour détecter et gérer les risques, garantissant ainsi l'alignement avec les objectifs de souveraineté à long terme.

CONFORMITÉ

CONFIANCE

Votre interlocuteur chez SPIE ICS

« Pour prospérer et survivre, la souveraineté est une nécessité, tout comme la confiance est indispensable. »

spie.ch/cyber

Hubert Rémond

Team Leader Solution Network Security

Tél. +41 79 801 06 47

Mail hubert.remond@spie.com