

The main title "X-SPIERience Day" is in white, with "X-SPIE" in a larger font. To the left is a circular graphic of circuit traces. To the right is the year "2020" in a stylized font, with "20" in white and "20" in yellow. Below the title is the subtitle "SOVERAINETÉ NUMÉRIQUE" in yellow.

X-SPIERience Day

SOVERAINETÉ NUMÉRIQUE



FORTINET





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 %

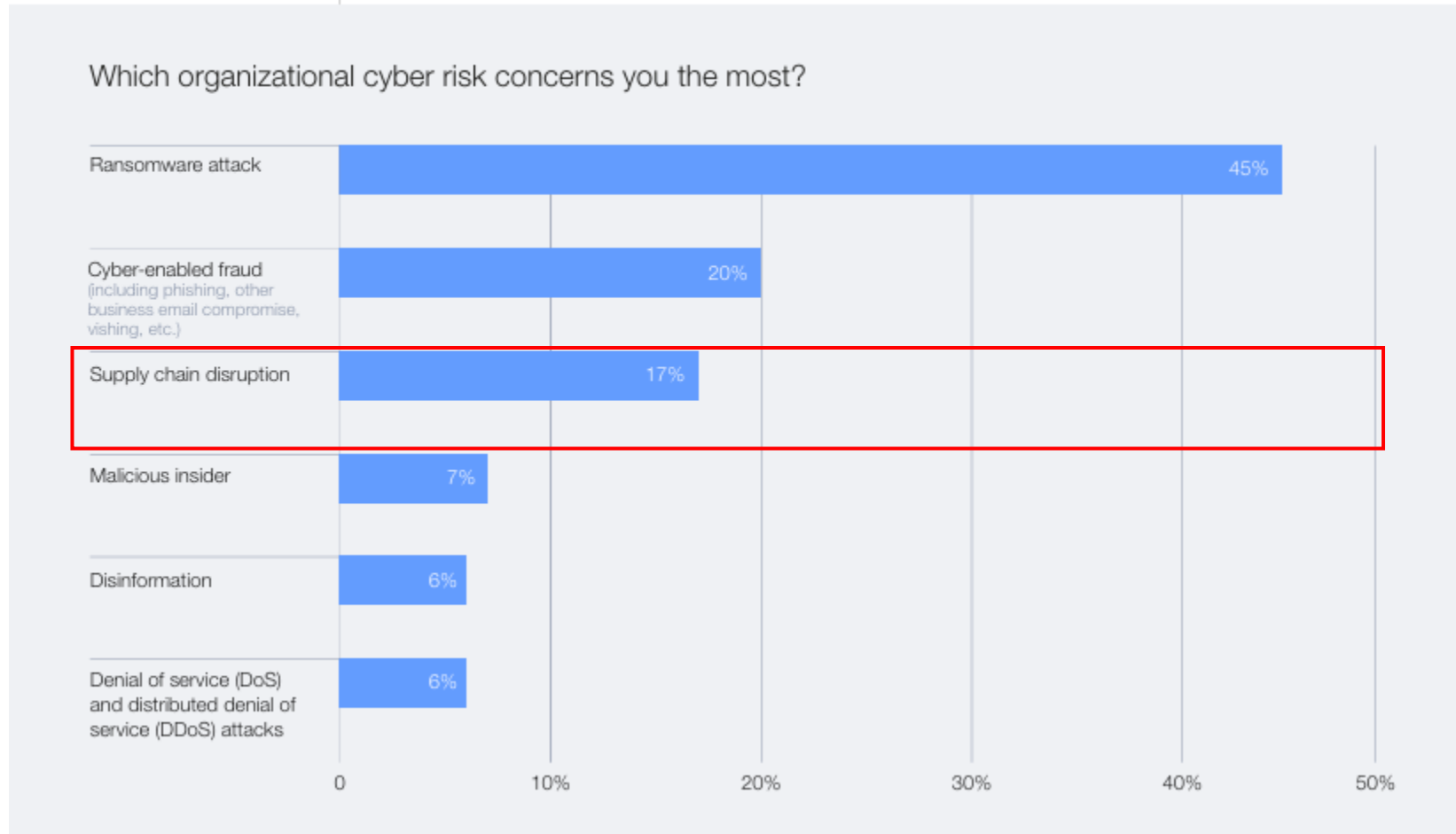
Incidents de sécurité causés par des tiers en 2024 ²
266% d'augmentation depuis 2020

¹Source: TPRM Observatory 2025 | Board of cyber

²Source: The State of 3rd-Party Risk Management Report 2024 | RiskRecon

Pourquoi maintenant ?

FIGURE 3 | Organizational cyber risks ranked – 2025



Exemples récents de réalisation du risque lié aux tiers



Plus de 16 000 fichiers ont été volés à la Confédération, aux cantons et à des polices dans l'attaque contre Xplain

Après le piratage du prestataire informatique Xplain, l'Office fédéral de la cybersécurité a publié jeudi un rapport chiffrant l'ampleur des dégâts. Des fichiers contenant des mots de passe sont concernés

Fuite de données



Cyber Threats

Axios NPM Package Compromised: Supply Chain Attack Hits JavaScript HTTP Client with 100M+ Weekly Downloads

A supply chain attack hit Axios when attackers used stolen npm credentials to publish malicious versions containing a phantom dependency. This triggered with clean decoys, making detection challenging.

By: Peter Girnus, Jacob Santos
Mar 31, 2026
Read time: 11 min (2913 words)



Accès non autorisé



CrowdStrike Incident

July 30, 2024 | Incident Handling

Disponibilité

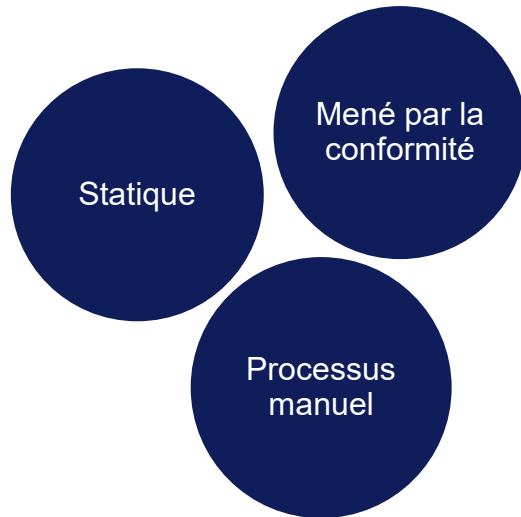
Alignement réglementaire et principaux cadres



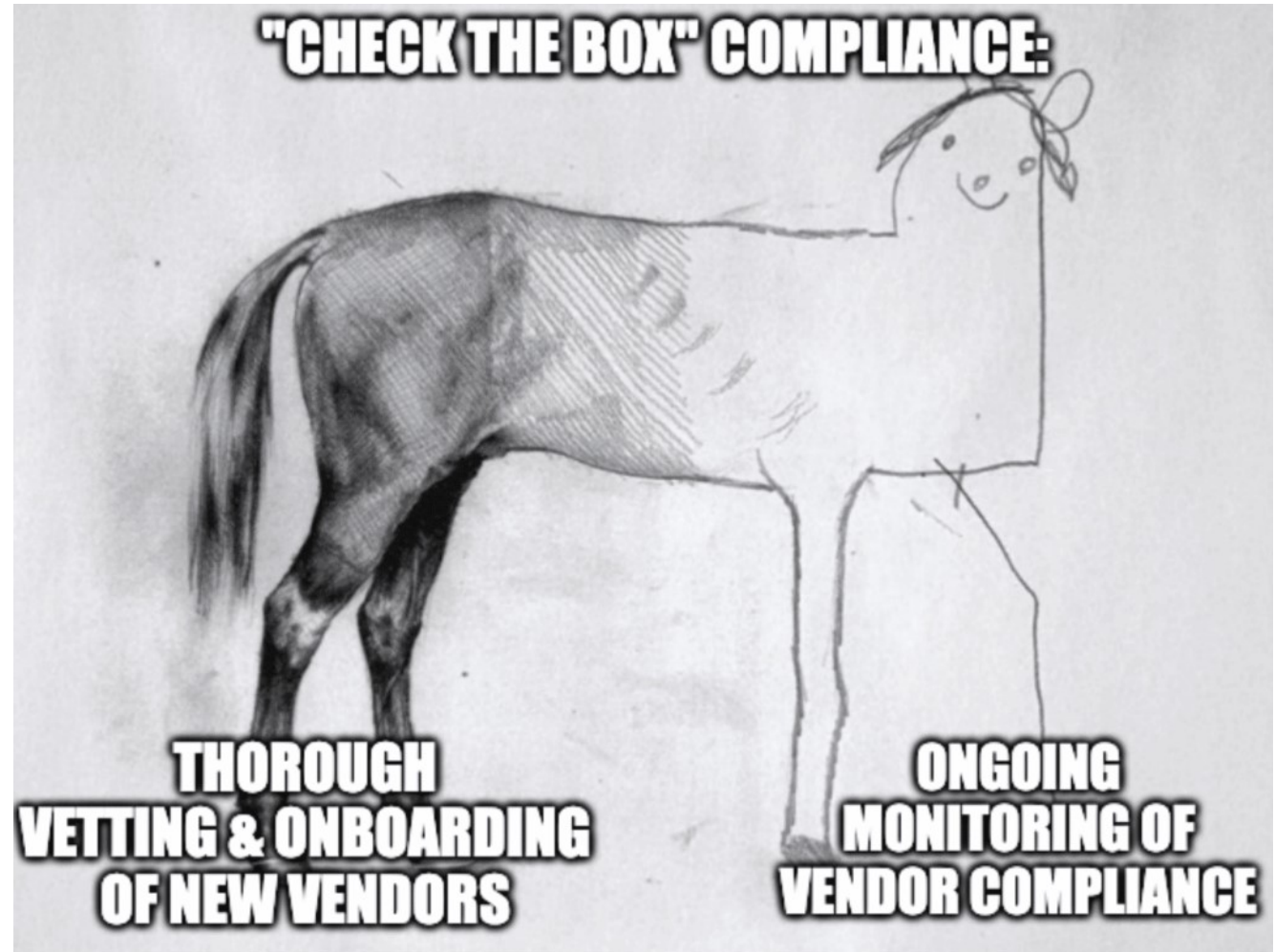
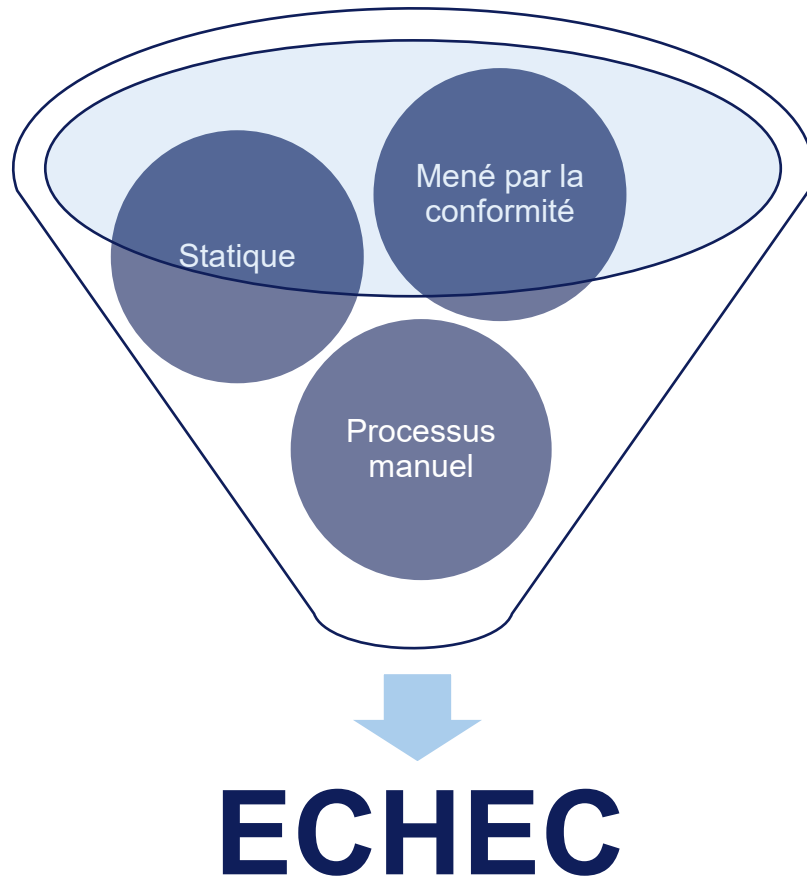
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra



Gestion typique du risque tiers



Gestion typique du risque tiers



Notations automatisés



Visibilité



Contrôle



Agilité

- Informations publiques

Top des actifs les plus à risque

Critique ● Elevée ● Moyenne ● Basse ●

Actifs

1er parent

Ports ouverts / Interfaces d'administration

@ IP
Publique

● 111/TCP(sunrpc) ● 3306/TCP(mysql) ● 111/UDP(sunrpc) ● 22/TCP(ssh) ⓘ

Notations automatisés



Visibilité



Contrôle



Agilité

- Informations publiques

Top des actifs les plus à risque

Critique ● Elevée ● Moyenne ● Basse ● OK ●

Actifs

Configuration

Service de messagerie

Nom de domaine

● DMARC ● SPF

● SMTP

Notations automatisés



Visibilité

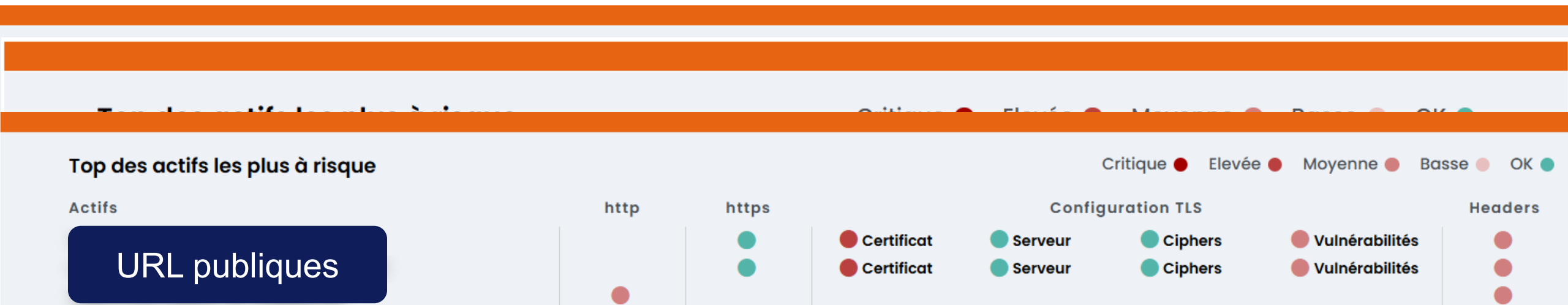


Contrôle



Agilité

- Informations publiques



Notations automatisés



Visibilité

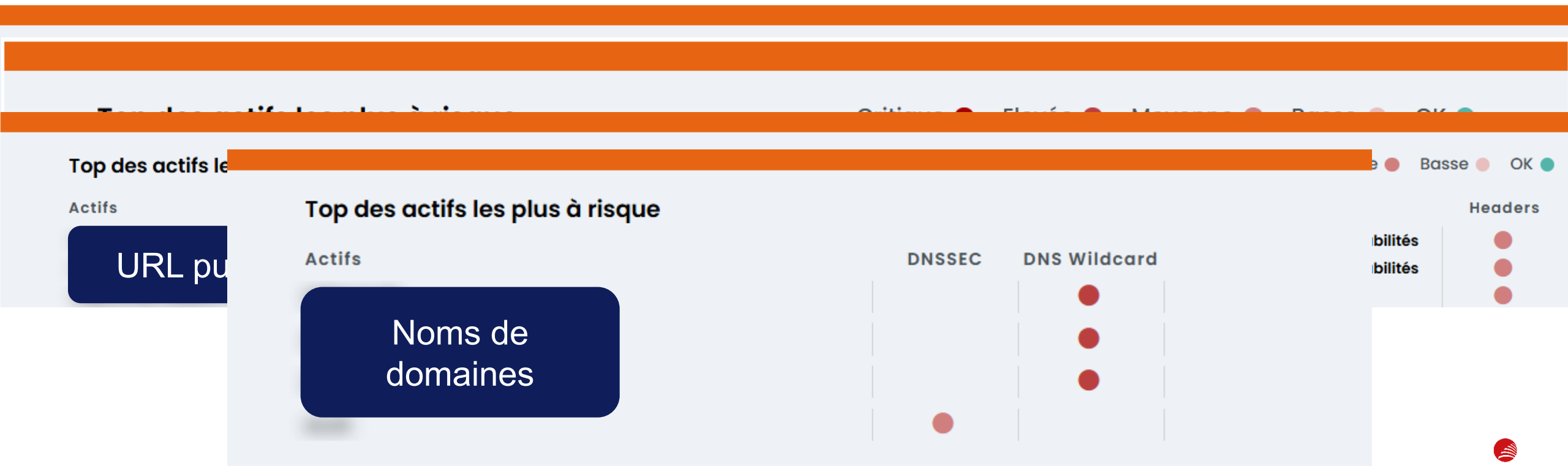


Contrôle



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 i



Maturité cyber de vos tiers

Vulnérabilités ⓘ

NOTE ⓘ

E

Actifs évalués **6**

Actifs à risque **1**

Site web publique

Voir plus

Observable par actifs | Observable par point de contrôle | Observable par technologie

Actifs à risque

Rechercher un actif

↑↓ Actifs | ↓ Sévérités | ↑↓ Nombre | ↑↓ Technologies utilisées

Site web publique

11 16 27 0

54

- Bootstrap
- Cart Functionality
- Font Awesome
- HSTS
- Joomla (1.5 ≤ 1.5.26)
- jQuery (3.7.1)
- jQuery UI (1.13.2)
- jsDelivr
- Leaflet (1.3.0)
- Livefyre (1.3.0)
- Lodash (4.17.5)
- metisMenu (1.4.0)
- Modernizr (2.8.3)
- Moment.js (2.30.1)
- Nginx
- OWL Carousel
- parallax.js
- PHP (8.3.30)
- RSS
- TomTom Maps

Maturité cyber de vos tiers

Vulnérabilités

NOTE

E

Actifs évalués 6

Actifs à risque 1

Site web publique

Voir plus

Observable par actifs | Observable par point de contrôle | Observable par technologie

Détails des observables pour l'actif

Rechercher un observable | Statut des commentaires

↑↓ CVE	↓ Sévérités	↑↓ Technologies utilisées
CVE-2017-3167	Critique	Apache HTTP Server (2.4.25)
CVE-2017-3169	Critique	Apache HTTP Server (2.4.25)
CVE-2017-7679	Critique	Apache HTTP Server (2.4.25)

Maturité cyber de vos tiers

Vulnérabilités

NOTE

E

Actifs évalués 6

Actifs à risque 1

Site web publique

Voir plus

Observable par actifs

Détails des observables pour l'actif

Rechercher un observable

Statut d

↑↓ CVE

↓ Sévérités

CVE-2017-3167	Critique
CVE-2017-3169	Critique
CVE-2017-7679	Critique

Performances de mise à jour

NOTE

E

Actifs évalués 6

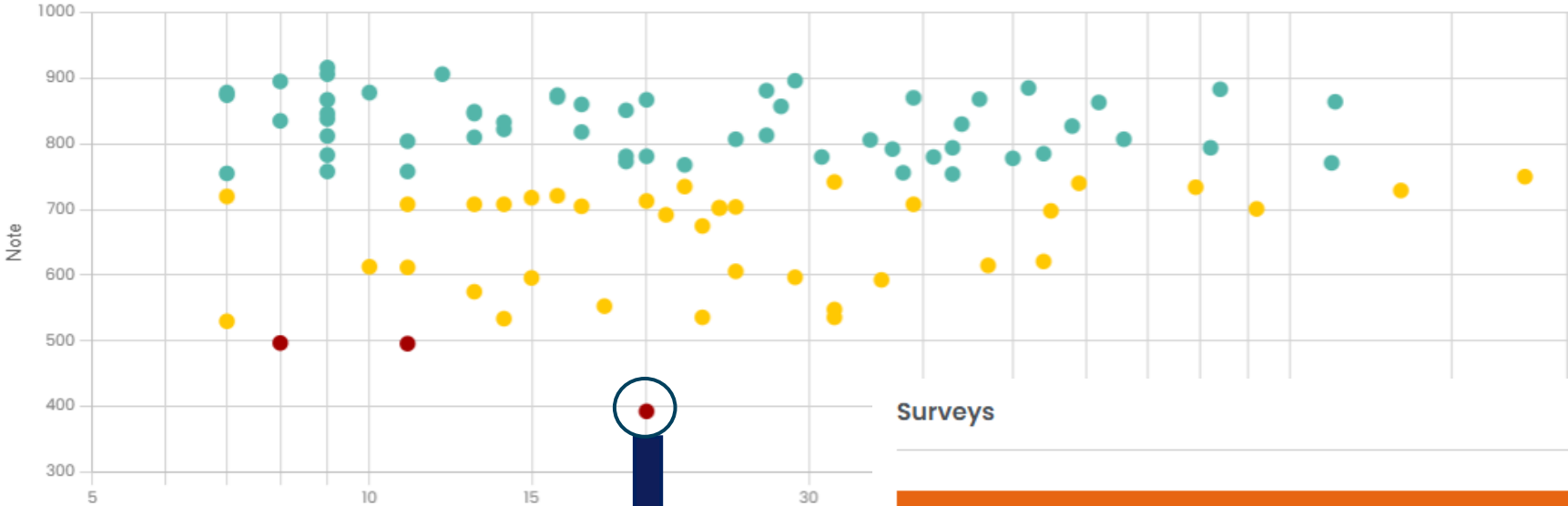
Délais de remédiation

Sévérité	Constaté	Cible	Nombre de CVE
Critique	521 jour(s)	≤ 5 jour(s)	63
Elevée	568 jour(s)	≤ 15 jour(s)	102
Moyenne	569 jour(s)	≤ 30 jour(s)	78
Basse	564 jour(s)	≤ 90 jour(s)	5

Voir plus

Visibilité, Contrôle, Agilité

Répartition par note et nombre d'actifs des 98 sociétés évaluées



Surveys

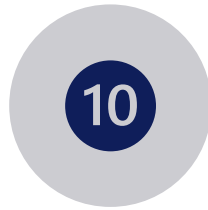
GDPR Maturity audit	V22.10.19	Oct 19, 2022	In progress
Security Needs	V22.10.19	Oct 19, 2022	E ^②
Maturity assessment	V22.10.19	Oct 19, 2022	C ^②

[See more](#)

Étapes concrètes pour une gestion efficace



QUESTIONNAIRE
SIMPLE



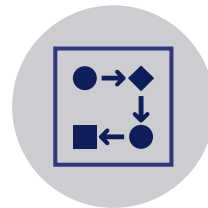
NOTATION
AUTOMATISÉE



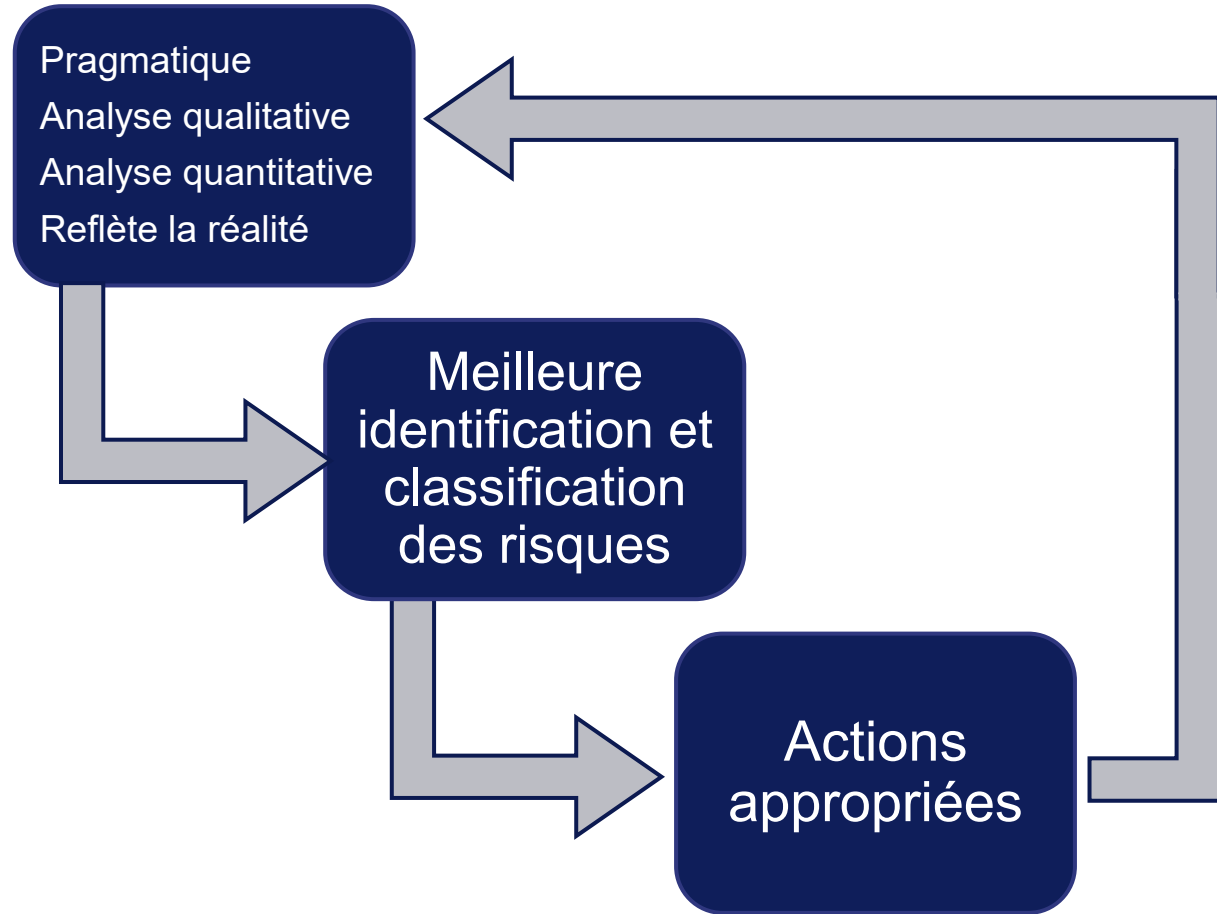
RÉSULTATS DU
DERNIER PENTEST (Y
COMPRIS LES
ANALYSES)



INDICATEURS DE
GESTION DES
VULNÉRABILITÉS ET
MTTR



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

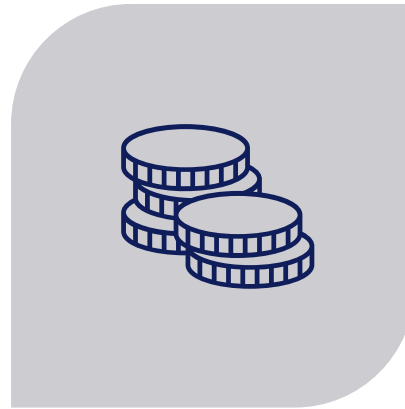


Que se passe-t-il si vous attendez ?



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. »

Hubert Rémond

Team Leader Solution Network Security

Tél. +41 79 801 06 47

Mail hubert.remond@spie.com

spie.ch/cyber

