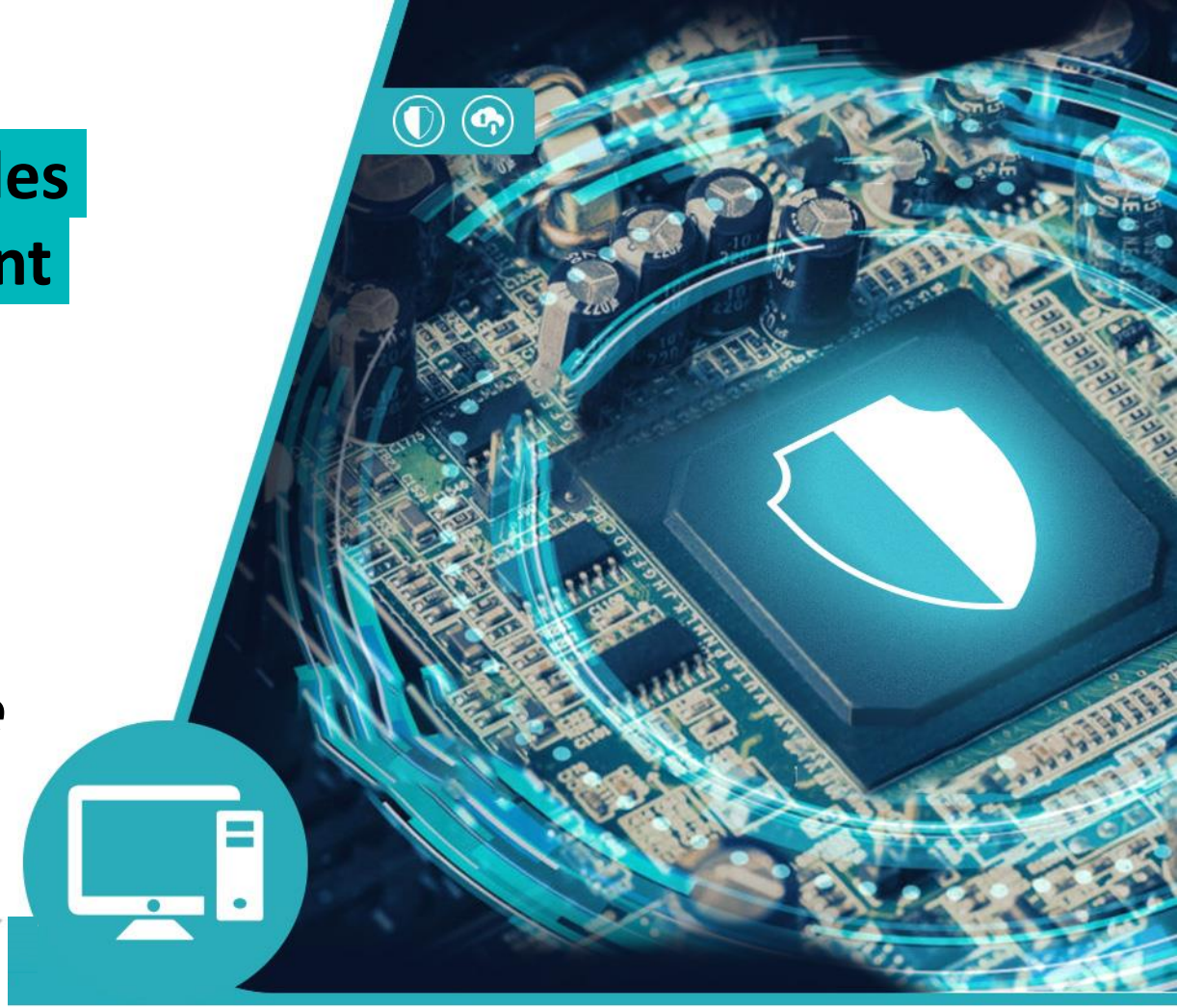
Comment détecter les menaces et comment réagir ? »



Incident Response

Décembre 2023

EVOLINK Security

Sylvain Porchet

sylvain.porchet@evolink.ch
security@evolink.ch

EVOLINK Thinking Solutions Together

Selon une étude menée par Vmware, Kroll, Red Canary et Wakefield Research, en 2021 :

seulement **49% des entreprises déclarent se sentir équipées** en termes **d'outils** de **personnel** ou **d'expertise** pour **détecter** ou **répondre** à une cybermenace.

L'*incident response* fait référence à l'ensemble des **actions planifiées** et des **mesures** prises pour répondre efficacement à un incident de sécurité.

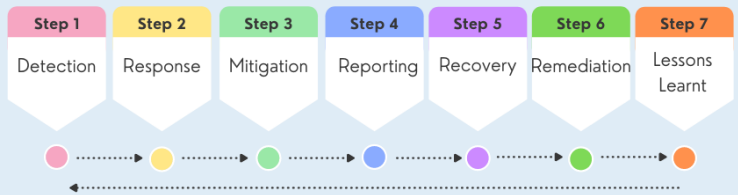
L'objectif est de **minimiser** les dommages et de **rétablir** au plus vite l'intégrité et la sécurité du système affecté.

Un incident de sécurité :

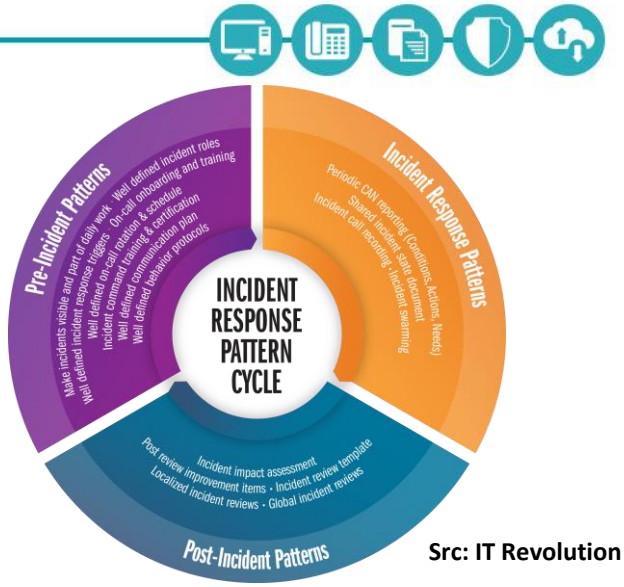
Élément ou une activité qui **compromet** **l'intégrité**, la **confidentialité** ou la **disponibilité** des données, des systèmes informatiques ou des réseaux.

p. ex.: violations de données, attaques de logiciels malveillants, tentatives d'accès non autorisé, failles de sécurité, perte/vol de matériel, etc.

Management de l'IR, plusieurs écoles



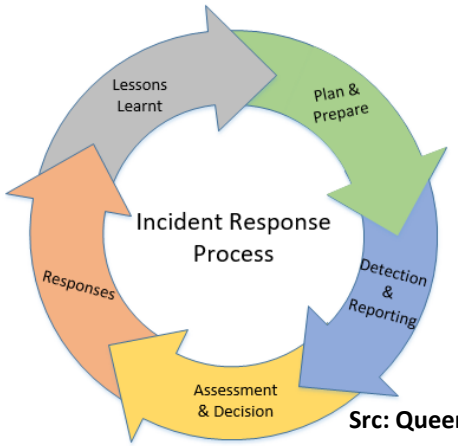
Src: Incident Management Steps for CISSP, Krishna Murthi B



Src: IT Revolution

Src: Antares Netlogix

Src: certstation



Src: Queensland Government

EVOLINK Thinking Solutions Together

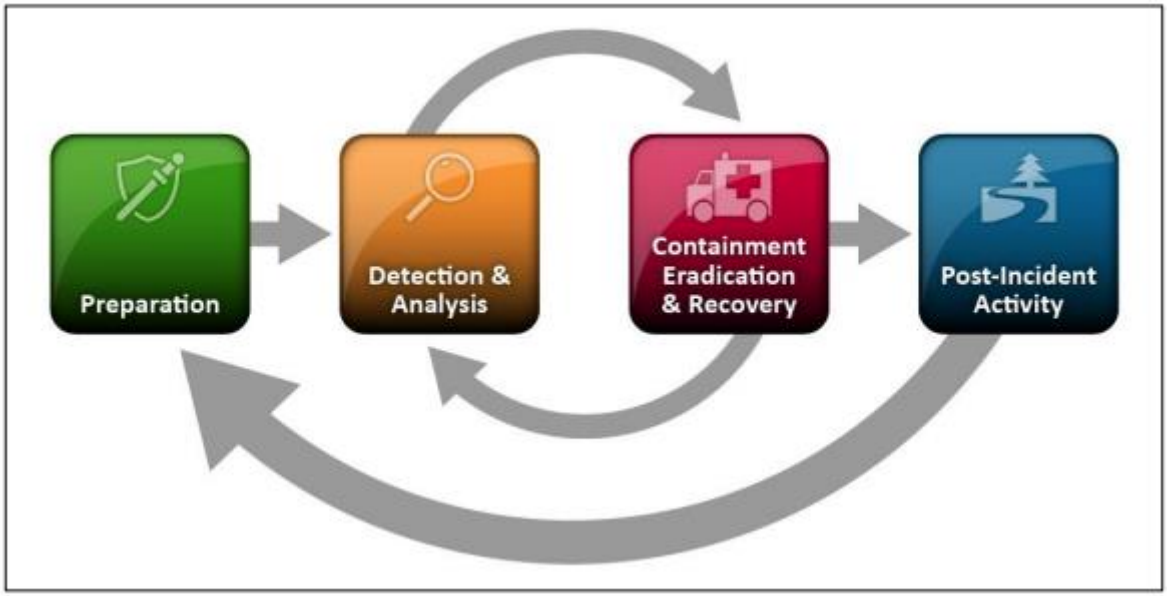
NIST	SANS
+	+
Complet	Pratique
Formel	Concis
Accents sur aspects :	*Accents sur aspects :*
Organisationnels	Opérationnels
De gestion	Tactiques
Techniques	
Infosec	Cybersec

Bien qu'il y ait des différences de portée, de point de vue, de vocabulaire, de segmentation, etc. NIST et SANS partagent certains éléments communs :

1. **Nécessité d'une préparation**
2. ***La détection***
3. ***Le confinement***
4. ***L'éradication***
5. L'apprentissage à tirer des incidents

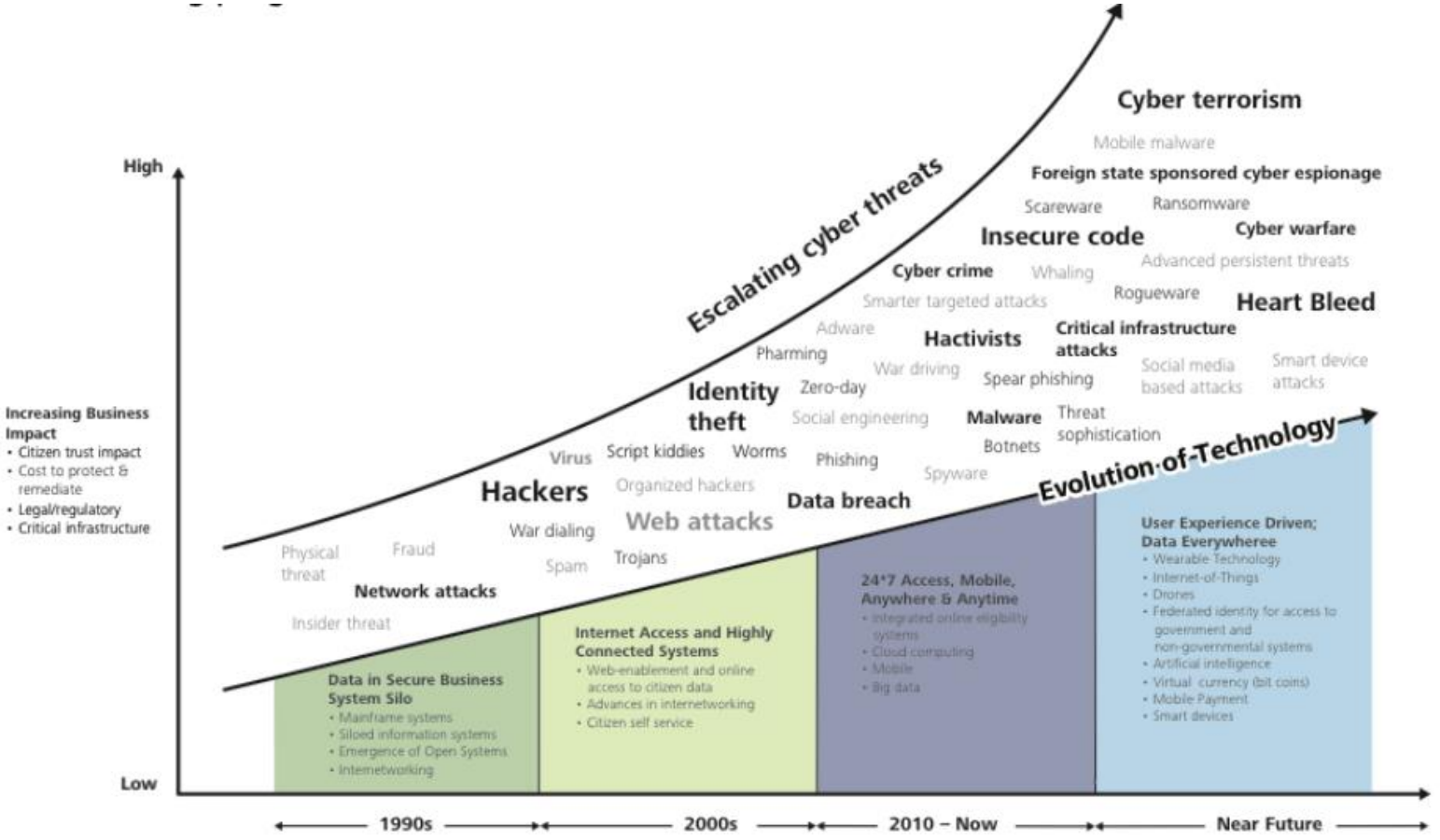
NIST	SANS
1. **Préparation**	1. **Préparation**
2. Détection et analyse	2. Identification
3. **Confinement, éradication et reprise**	3. **Confinement**
4. Activité après incident	4. **Éradication**
	5. **Reprise**
	6. Enseignements tirés

NIST IR lifecycle



Source: Computer Security Incident Handling Guide, NIST, SP 800-61 r2

Face à l'augmentation des menaces, on est tenté de se ruer sur des technologies.



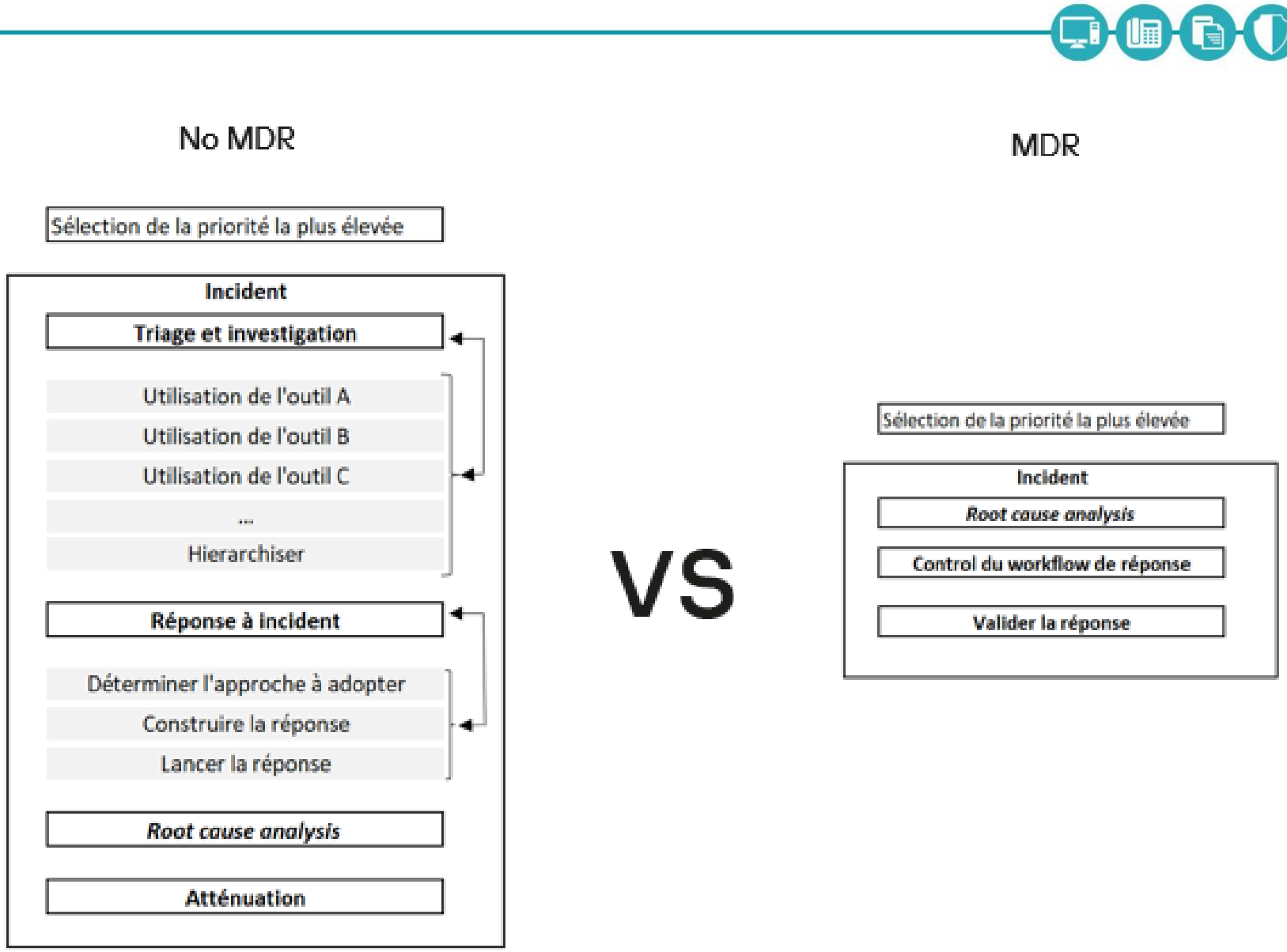
Reproduced from the 2014 Deloitte-NASCIO Cybersecurity Study
"State governments at risk: Time to move forward"

C’est bien, mais c’est aussi un piège.

La technologie qui s’exprime sous forme **d’outils** ou de **jeux d’outils** permet de palier, principalement aux problèmes de :

1. manque de compétences
2. manque de réactivité
3. manque de disponibilité

En effectuant(notamment, mais non exclusivement, grâce au *machine learning* et à l’IA) une multitude de tâches qu’il aurait fallu traiter manuellement auparavant.


No MDR
Sélection de la priorité la plus élevée
Incident
Triage et investigation
Utilisation de l'outil A
Utilisation de l'outil B
Utilisation de l'outil C
...
Hierarchiser
Réponse à incident
Déterminer l'approche à adopter
Construire la réponse
Lancer la réponse
Root cause analysis
Atténuation
VS
MDR
Sélection de la priorité la plus élevée
Incident
Root cause analysis
Control du workflow de réponse
Valider la réponse

Il est nécessaire de prendre du recul et de sortir de la vision **purement technique** pour aborder la problématique dans son ensemble.

Il faut adopter une vision tactique qui permettra de définir une PSSI (politique de sécurité des systèmes informatiques).

Cette PSSI devra notamment inclure :

Une **stratégie de détection des menaces**

un **CSIRP** qui sera le cadre **NON FIGÉ** qui permettra l'appréhension globale de la réponse avec ses aspects techniques et organisationnels.

Qu’est-ce qu’un CSIRP ?

C’est un **document procédural** qui **définit** ce qui **doit être fait**, par **qui** (rôles et responsabilités), en cas d’**incident de sécurité** impactant le fonctionnement de l’entreprise.

Il englobe la **préparation** (qui englobe la **prévention**) et la **rétroanalyse**.

La rétroanalyse viendra sans cesse nourrir la préparation

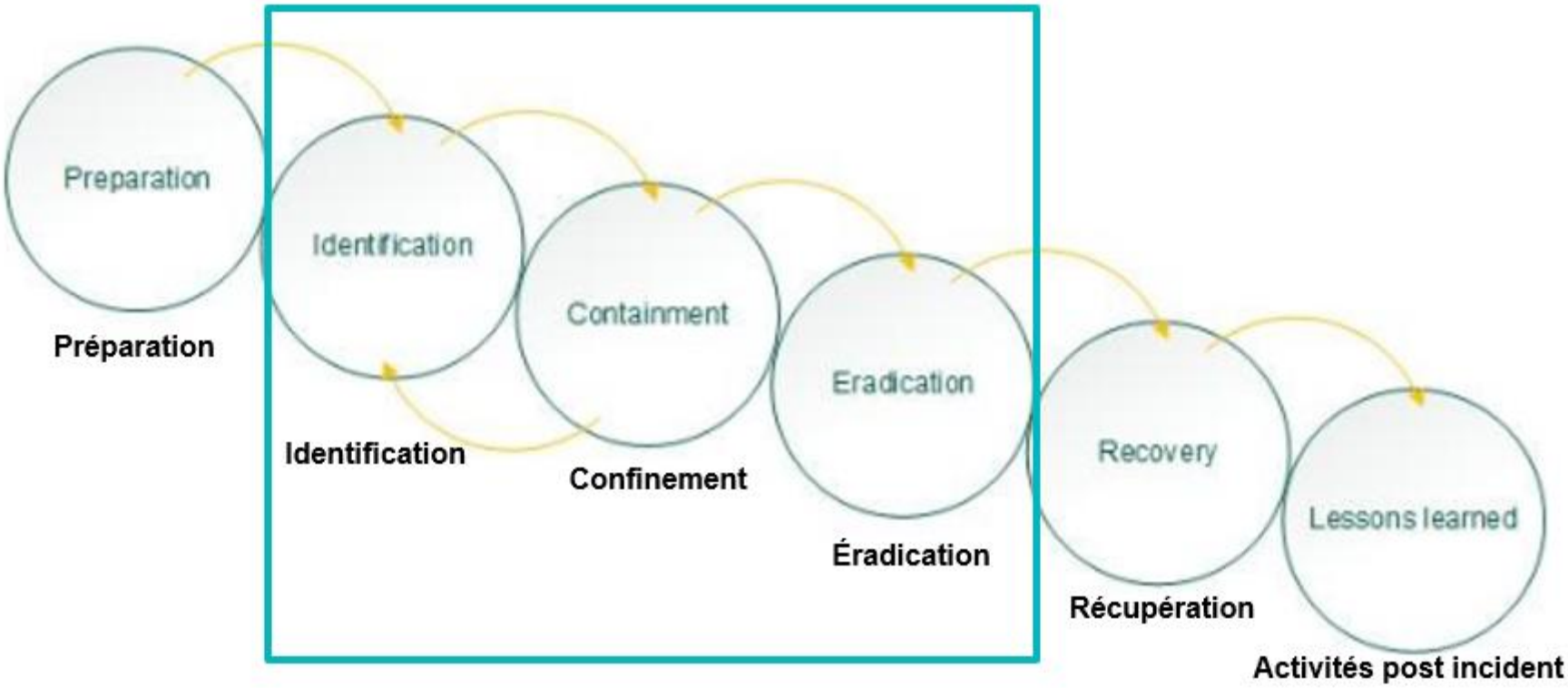
…

Le CSIRP sera la formalisation de l'ensemble des aspects **techniques**, **organisationnels**, **communicationnels** et **humains** et leur engagement méthodique face à un incident.

La difficulté dans la conception de ce dernier réside dans le fait de le proportionner aux risques effectifs et aux coûts que ces derniers peuvent avoir.

Remarque:
Cette difficulté est la même que celle rencontrée dans l'élaboration d'un PCA et d'un PRA.
Le point de départ devrait également être une analyse de risques.

Les 6 phases d'un CSIRP

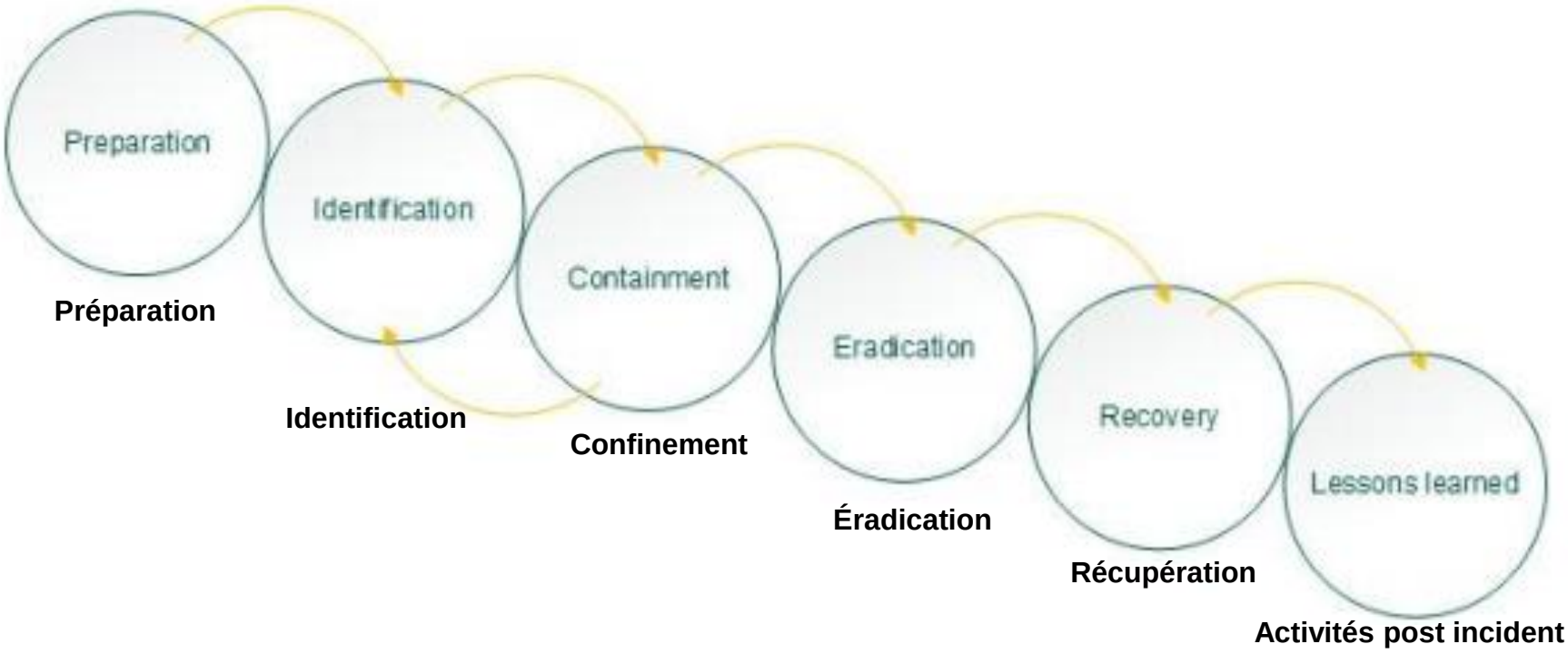


|← Avant impact|

|→ Après impact |

source: Incident response guide, Kaspersky

Les 6 phases d’un CSIRP



|🡐 Avant impact| **|🡒 Après impact |**

source: Incident response guide, Kaspersky

- Il faut **prévoir** sa *toolbox* **AVANT** le jour du malheur !

Au minimum !

1. Un outil de gestion de crise non adhérent aux SI

   Il devra permettre
   - La communication
   - Le partage de données (procédures, etc.)
   - La prise de données

Sharekey

Code:
EVOLINK@CH

2. Des Outils d'analyses

3. Des outils de sauvegarde (et les **documents** et **tests** qui vont avec).

4. Des outils de détection (et de réponse), à minima, EDR, MDR; XDR, MXDR, etc.

Q&R

Bonus special membres **Clusis**

Les 6 phases d'un CSIRP*

1. Préparation
2. Identification
3. Confinement
4. Éradication
5. Récupération
6. Activités post incident / leçons apprises

**Approche « basée SANS »*

1. Préparation

1. Préparation

La plus importante, car elle pose les fondements du reste du plan.

Techniquement, vous devez **toujours être en phase de préparation** : vous devez être prêt à faire face à tout nouvel incident, et maintenir votre plan constamment à jour et opérationnel.

Les éléments clés devant être inclus dans la phase de préparation sont les suivants :

1. S'assurer que tous vos **employés** sont **correctement formés** à la sécurité des données et à la réponse aux cybermenaces et aux urgences.

2. **Réaliser une évaluation des risques** pour hiérarchiser les problèmes de sécurité, identifier les actifs les plus sensibles et les incidents de sécurité les plus critiques sur lesquels votre équipe doit se concentrer.

3. Organisez régulièrement des **formations** et des **exercices** afin que chacun soit prêt à agir de manière appropriée en cas d'incident.

4. Attribuez les **rôles** et **responsabilités** appropriés à votre équipe chargée des incidents de cybersécurité et assurez-vous qu'elle a accès aux systèmes et outils nécessaires.

5. Clarifiez les **processus** et les **lignes de communication** en cas d'incident. (Qui doit être contacté, et quand ? /!\ L'absence de communications claires et établies en cas d'urgence peut entraîner beaucoup de désordre et d'inefficacité.

6. Assurez-vous que tous les aspects de votre plan (formation, exécution, ressources, etc.) sont approuvés, financés et mis en œuvre, etc.) et disponible à l'avance. En bref, votre plan est-il opérationnel ?

Questions à se poser pour le contrôle de la préparation.

1. Tout le monde a-t-il été **formé** aux politiques et procédures de sécurité nécessaires ?

2. Votre plan de sécurité a-t-il été validé par la direction ?
   Est-il à jour et dispose-t-il des **ressources nécessaires** ?

3. Tous les membres de l'équipe de réponse aux incidents connaissent-ils leur rôle et leur plan d'action ?

4. Chacun a-t-il participé à des **exercices de simulation** ? Sont-ils prêts à intervenir ?

2. Identification

Cette phase du plan est déclenchée lorsqu'un incident vient de se produire et qu'il faut le **diagnostiquer** et **décider** des mesures à prendre.

Votre équipe doit être en mesure de détecter efficacement le **type** et la **gravité** de la menace et de **déterminer la réponse à apporter**

*Il existe **deux types** de signes indiquant que vos systèmes de sécurité font l'objet d'une attaque :*

les **précurseurs** (détectés avant qu'une attaque ne se produise) ou les **indicateurs** (détectés pendant ou après une attaque).

- Un exemple de précurseur serait un nombre élevé de tentatives de connexion infructueuses, suggérant qu'un attaquant tente de pénétrer votre réseau en devinant un nom d'utilisateur et un mot de passe.

- Un exemple d'indicateur serait un logiciel antivirus vous avertissant qu’un collaborateur a cliqué sur le lien d'un logiciel malveillant et que son ordinateur est infecté.

Cette phase comprend également la **documentation** : votre équipe doit enregistrer tout ce qui se passe, y compris la nature de l'incident, les preuves et les actions entreprises pour y répondre. Cela sera utile dans la phase des activités post-incident, au tribunal et face à l'auteur de l'attaque.

Cette phase doit également comprendre la **notification** : Il s'agit de s'assurer que toutes les parties concernées (forces de l'ordre, agences fédérales, autorités locales, clients, actionnaires et entreprises touchées, etc.) soient informées qu’une attaque a eu lieu.

Information en temps utile = rester dans la légalité de protéger votre réputation et de réduire votre responsabilité à long terme.

Votre plan doit comporter des **instructions claires sur les personnes à notifier** et les **étapes** de la **procédure de notification,** ainsi que les émetteurs de notifications.

Questions à se poser dans cette phase:

1. Quand et où l'incident a-t-il commencé ?
2. Qui l'a découvert et comment ?
3. Quelle est l'étendue de la compromission ?
4. Quels sont les domaines touchés ?
5. Les activités de l'entreprise sont-elles affectées ? De quelle manière ?

3. Confinement

Lors d’un incident, on peut être tenté de supprimer tous les éléments contaminés dès que possible afin d'éliminer la menace.

➔ Cela supprimerait toutes les preuves qui peuvent être utilisées dans les audits post-incident, et qui seront précieuses pour aider à déterminer comment la violation a commencé et comment empêcher qu'elle ne se reproduise.

Il est préférable **d'endiguer la violation** en **déconnectant** les appareils concernés d'Internet et du réseau, afin d'éviter d'autres dommages l’exfiltration de données.

Il est également conseillé de disposer d'un système de sauvegarde **redondant** et **déconnecté** **(WORM)** afin de rétablir les opérations et de ne pas perdre définitivement les données compromises.

Le confinement peut prendre deux formes :

- Confinement à court terme :
  Solutions temporaires telles que l'isolement du segment de réseau affecté, la mise hors service de tout serveur compromis et la redirection du trafic vers des serveurs de sauvegarde.

- Confinement à long terme :
  Poursuite des opérations à l'aide de solutions temporaires tout en reconstruisant des systèmes propres, en se préparant à les remettre en ligne au cours de la phase de récupération.

Au cours de cette phase, vous pouvez également :

1. mettre à jour et patcher vos systèmes
2. vérifier les protocoles d'accès à distance
3. modifier toutes les informations d'identification d'accès au système
4. renforcer vos mots de passe

Au cours de cette phase, vous pouvez également :

1. Mettre à jour et patcher vos systèmes
2. Vérifier les protocoles d'accès à distance
3. Modifier toutes les informations d'identification d'accès au système
4. Renforcer vos mots de passe

Un certain nombre de facteurs doivent être pris en considération lors du choix d'une procédure de confinement.

Le NIST les énumère comme suit :

1. **Dommages** potentiels et **vol** de ressources
2. Nécessité de **préserver** les preuves
3. **Disponibilité** des services (par exemple, connectivité du réseau, services fournis à des parties externes)
4. **Temps et ressources** nécessaires à la mise en œuvre de la stratégie
5. **Efficacité** de la stratégie (par exemple, confinement partiel, confinement total)
6. **Durée de la solution** (par exemple, une solution de contournement d'urgence à supprimer en quatre heures, une solution de contournement temporaire à supprimer en deux semaines, une solution permanente).

Questions à se poser lors de la phase de confinement :

1. Que faites-vous pour contenir la brèche à court et à long terme ?
2. Avez-vous mis en quarantaine toutes les zones touchées ?
3. Quelles sont les sauvegardes en place ?
4. Toutes les références d'accès ont-elles été modifiées et renforcées ?
5. Avez-vous appliqué tous les derniers correctifs et mises à jour de sécurité ?

4. Éradication

Les étapes exactes de la phase d'éradication dépendent du type d'attaque.

Par exemple, vous pouvez supprimer les logiciels malveillants, désactiver les comptes compromis, combler les failles du réseau, etc.

Fondamentalement, l'éradication **consiste à trouver la cause première de l'attaque et à s'en débarrasser** !

L'éradication doit être complète.

Si la moindre trace de logiciel malveillant ou de zone affectée subsiste dans vos systèmes, vous risquez de souffrir de la compromission de vos données et d'accroître votre responsabilité.

Il est essentiel de disposer d'un solide CSIRP pour cette phase, car le respect de ses instructions garantira que vos procédures d'éradication et de sécurité sont approfondies et méticuleuses, et qu'elles ne négligent aucune piste.

Questions à se poser durant la phase éradication :

1. Tous les logiciels malveillants et toutes les zones affectées ont-ils été supprimés ?
2. Avez-vous revérifié toutes les zones susceptibles d'avoir été affectées ?
3. Avez-vous nettoyé tout autre désordre résultant de l'attaque ? (Contenu publié sur votre site web ou vos canaux médiatiques, par exemple)

5. Récupération

La phase de récupération consiste à **restaurer** les systèmes affectés et à les **remettre en service**.

Cette phase doit être menée avec précaution pour éviter qu'un autre incident ne se produise.

Ce processus peut prendre des jours, des semaines ou des mois, en fonction de la gravité de la violation.

Le NIST recommande de **commencer par renforcer immédiatement votre sécurité globale**, puis de vous concentrer sur des changements continus et à long terme afin de maintenir vos systèmes aussi sûrs que possible.

Les éléments importants à prendre en compte au cours de cette phase sont le moment où les opérations seront entièrement rétablies, la manière dont vous vérifierez que tout fonctionne normalement et la durée pendant laquelle vous continuerez à surveiller la situation jusqu'à ce que vous soyez vraiment sûr que tout est rentré dans l'ordre.

Questions à se poser durant la phase récupération.

1. Quand les systèmes fonctionneront-ils à nouveau normalement ?
2. Quels outils et procédures utiliserez-vous en permanence pour vérifier que les systèmes restaurés fonctionnent normalement ?
3. Le système peut-il être restauré à partir d'une sauvegarde fiable ?
4. Pendant combien de temps allez-vous surveiller la situation jusqu'à ce que vous puissiez être sûr que tout va bien ?

6. Activités post incident / Leçons apprises

Débriefing post-incident avec toutes les parties concernées.

Devrait idéalement avoir lieu quelques jours après que l'incident a été résolu avec succès, et pas plus de deux semaines après, afin que tout soit encore frais dans les esprits.

Les éléments clés de cette phase sont les suivants

- Un examen complet de l'incident, de la découverte à la récupération. L'examen doit se concentrer sur des questions telles que les suivantes Tout le monde a-t-il suivi les procédures du CSIRP ? A-t-il été efficace ? Y a-t-il eu des points faibles ou des choses qui pourraient être améliorées ? Que pourrait-on faire différemment la prochaine fois ? Comment des incidents similaires pourraient-ils être évités à l'avenir ?

- Une évaluation et une mise à jour de votre plan d'intervention en fonction des conclusions tirées de l'examen.

- La création d'un rapport de suivi qui servira de référence lors de la gestion d'incidents similaires. Le fait de disposer d'une chronologie formelle des événements (avec des informations horodatées telles que les journaux de données) est également utile pour les procédures légales telles que les audits.
- …

- Une évaluation du préjudice total causé par la violation, y compris une estimation monétaire. Cette évaluation est également utile pour des raisons juridiques telles que les poursuites judiciaires.

- Régler toutes les questions en suspens pour lesquelles vous n'avez pas eu le temps de le faire pendant l'incident, par exemple compléter la documentation correspondante et veiller à ce que toutes les parties concernées soient informées.

Questions à se poser durant la phase Activités post incident :

1. Quels sont les changements à apporter à la sécurité ?
2. Quelles faiblesses la violation a-t-elle exploitées et **comment peut-on prévenir** à l'avenir ?
3. Avez-vous procédé à un examen approfondi de l'incident et rédigé un rapport de suivi ?
4. Avez-vous informé toutes les personnes concernées ?
5. Avez-vous tout préparé pour faire face au processus d'audit post-incident ?

Sylvain Porchet

https://www.linkedin.com/in/sporchet/

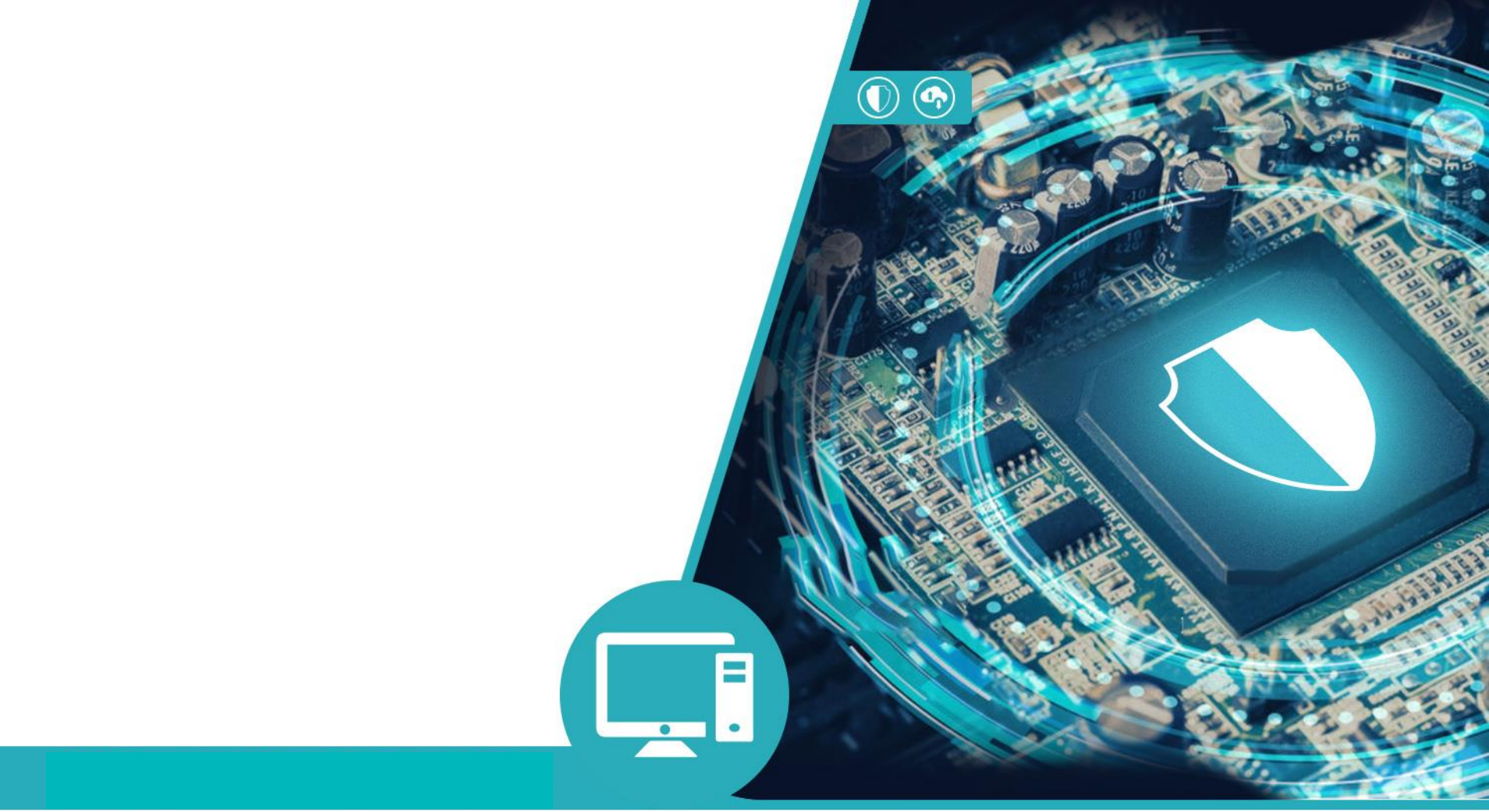
Sharekey

ID : 8NBKLQY5

https://app.sharekey.com/member/8NBKLQY5

www.evolink.ch

EVOLINK Security



EVOLINK
Security