



## Qui sommes-nous ?



Entreprise suisse, active depuis 2001 dans les services IT pour des missions critiques à données sensibles, nous proposons des solutions sécurisées et totalement adaptées à tous types d'activités.

Nous sommes un moteur d'innovation pour les entreprises qui souhaitent dynamiser leurs activités et se concentrer sur la création de valeur pour leurs clients.


Nous leur proposons des solutions IT totalement adaptées à leurs besoins et à l'accomplissement de leurs ambitions et les soutenons dans leur vision.

- Cloud Privé
- Modern Workplace
- Sécurité de l'information
- Robotic Process Automation
- Services managés



*Pour en savoir plus*  
*Contactez-nous dès à présent!*

**Globaz - Votre partenaire IT pour la vie !**

 Sous-la-Velle 6 | 2340 Le Noirmont  
Av. de la Rasude 2 | 1006 Lausanne  
Av. Edouard-Dubois 20 | 2000 Neuchâtel

 [www.globaz.ch](http://www.globaz.ch)

 [info@globaz.ch](mailto:info@globaz.ch)

 +41 32 957 60 00



**vCISO** by  **globaz**



## Ransomware

**L'information est essentielle pour se préparer aux cyberattaques !**

Avec une augmentation de 13 % des attaques par ransomware en une seule année\*, soit une hausse plus importante que les cinq dernières années combinées, ces dernières deviennent un sujet brûlant de la cybersécurité.

Longtemps mal connues ou comprises des dirigeants, les attaques successives et très médiatisées ont stimulé l'intérêt pour les aspects opérationnels de la cybersécurité, aspects spécifiques aux ransomwares.

Les dirigeants demandant désormais aux professionnels de la cybersécurité plus d'informations sur les risques, les stratégies de défense et les besoins budgétaires.

*Vous avez besoin de réunir les informations pour sensibiliser les dirigeants de votre entreprise aux ransomwares et plaider en faveur de l'investissement dans des mesures préventives et des plans de réponses stratégiques?*

***vCISO est fait pour vous !***





La priorité absolue pour les dirigeants est d'obtenir des informations sur les stratégies visant à empêcher les ransomwares d'avoir un impact sur les plans de sauvegarde et de restauration des données. Ils veulent également savoir :

- ce qu'il faudra pour rétablir des opérations minimales après une compromission
- dans quelle mesure l'entreprise est prête à faire appel aux forces de l'ordre en cas d'attaque
- dans quelle mesure elle est prête à faire appel à des enquêteurs spécialisés dans la cybersécurité

## vCISO est là pour vous aider !

### Améliorer la communication et les rapports à la direction

Les dirigeants souhaitent plus de communication de la part des praticiens de la cybersécurité qui s'occupent des ransomwares au sein de leur entreprise. Les rapports doivent également contenir plus de détails, de profondeur et d'explications pour s'assurer que les dirigeants comprennent parfaitement le paysage, afin de prendre des décisions plus éclairées et de soutenir les appels à l'investissement dans la cybersécurité.



**vCISO** vous aide à mettre en œuvre de nouveaux processus de reporting et créer un consensus avec les dirigeants sur les informations qui leur importent le plus afin de fournir des rapports puissants qui soutiennent le processus de prise de décision.

### Tempérer l'excès de confiance si nécessaire

Si les professionnels de la cybersécurité ont l'impression que leur direction est trop confiante face aux ransomwares, il est important d'apporter une dose de réalité. Soyez clair et réaliste sur les menaces auxquelles l'entreprise est confrontée et sur sa capacité à répondre à une attaque par ransomware. Rendez la menace compréhensible.



**vCISO** vous aidera à expliquer clairement les conséquences très réelles que les ransomwares peuvent avoir sur vos activités et sur la santé à long terme de votre entreprise.



### Adapter votre message

Selon le type d'entreprise dans laquelle vous travaillez et le type de données qu'elle gère, les équipes dirigeantes peuvent avoir un niveau variable de tolérance au risque. Comprenez et concentrez-vous sur les principaux domaines de préoccupations de vos dirigeants.



Présentez les risques à vos dirigeants d'une manière qui corresponde spécifiquement à leurs préoccupation, et construisez vos rapports en fonction de ce qui est le plus important. **vCISO est conçu pour ça !**

### Justifier vos investissements

Veillez à tirer parti d'une Direction plus réceptive non seulement pour justifier les investissements technologiques, mais aussi pour insister davantage sur la mise en place d'une cybersécurité plus résiliente.



### Expliquer clairement que la défense contre les ransomwares est la responsabilité de tous

Il est important que les entreprises comprennent que la défense contre les ransomwares est l'affaire de tous et qu'elles évitent de compartimenter les responsabilités et la visibilité des connaissances, des politiques et des processus en matière de ransomwares.

**Conçue par un CISO, la plateforme vCISO est un outil de pointe pour vous aider à protéger votre entreprise.**

