IsNoRisk

L’analyse de risque avec MITRE ATT&CK©

Dominique BUC

Présentation OSSIR du 14 janvier 2025

IsNoRisk

Dominique BUC

Email : dominique.buc@isnorisk.com

30 ans d’expérience en cybersécurité.

Spécialisé dans les logiciels d’analyse de risque.

Editeur de Risicare sur MEHARI diffusé chez plus de 150 grands organismes dans 10 pays.

IsNoRisk

Nous présentons en avant-première IsNoRisk, un logiciel innovant, qui change la donne dans ce que peut apporter un logiciel dans l'analyse des cyber-risques avec pour objectifs :

- Permettre de réaliser une analyse de type ISO 27005 version 2022 (ou EBIOS RM) d'un niveau correct en demandant un effort minimum à l'utilisateur
- Tout en aidant l'expert à produire des études de haut niveau.

IsNoRisk

- Un produit nativement fondé sur l'ISO 27005 : version 2022
- Qui assiste les 5 ateliers d'EBIOS RM
- Qui permet une approche basée sur les événements et sur les biens avec la génération des scénarios stratégiques et opérationnels.
- Une gestion performante de l'écosystème (scénarios stratégiques)
- La capacité de construire automatiquement ces scénarios, ce qui signifie pour les scénarios opérationnels, la construction de « Kill Chains ».
  Or les Chaînes d'attaque « tout le monde en parle mais personne n'en fait »

  IsNoRisk s'est fixé le défi de rendre cela abordable …

IsNoRisk

- Pour modéliser des chaînes d'attaque, il faut déterminer une succession d'actions et il faut pour cela un référentiel d'actions.
  D'où le choix d'intégrer nativement le Framework MITRE ATT&CK

  MITRE ATT&CK est le Framework le plus connu au monde pour décrire le comportement d'un cyberattaquant.
- Il comporte 14 tactiques, 656 techniques et sous-techniques, 159 groupes d'attaque, 710 logiciels malveillants.
- **Tactiques** : Ce sont les objectifs stratégiques que les cyberattaquants cherchent à atteindre lors d'une attaque.
- **Techniques** : Ce sont les méthodes spécifiques utilisées pour atteindre ces objectifs.

IsNoRisk

Je vous propose donc d'aller sur l'outil pour voir :

- Comment réaliser une analyse standard de type ISO 27005 version 2022 avec un minimum d'intervention de l'utilisateur.
- Comment passer ensuite à un niveau d'expertise supérieur avec l'utilisation du générateur d'attaque pour construire des scénarios spécifiques.
- Nous verrons enfin comment l'outil peut vous apporter une compréhension fine de MITRE ATT&CK et de votre posture face à ce Framework.