Forum: Propositions de logiciels

Topic: Countercept Chainsaw #

Subject: Countercept Chainsaw #

Publié par: Tof81

Contribution le : 11/01/2022 16:26:09

Logiciel en mode commande pour identifier rapidement les menaces dans les journaux d'événements Windows :

https://github.com/countercept/chainsaw

téléchargement : https://github.com/countercept/chainsaw/releases/tag/v1.1.5

L'application elle-même n'a pas vraiment d'interface. En fait, elle utilise CMD pour communiquer avec l'utilisateur. Assurez-vous d'ajouter le chemin vers une session CMD dans laquelle vous assumez le rôle de l'administrateur. L'application elle-même permet à tout utilisateur averti de rechercher et d'extraire les journaux d'événements en utilisant divers algorithmes de recherche et en se basant sur l'ID de l'événement, la correspondance des chaînes de caractères

On peut chasser les menaces en utilisant des règles de détection spécifiques appelées Sigma. Il s'agit d'une fonctionnalité intégrée à cette application, qui se trouve au cœur de sa fonction

Pour utilisateurs avertis ...

Rien à voir avec Chainsaw, logiciel pour découper de gros fichiers, qui semble ne plus être supporté (http://www.chainsaw-filesplitter.de = site inaccessible).