sopra steria

MACTAN

La solution de supervision souveraine, adaptative et intelligente pour les environnements complexes

(*) Le monde est tel que nous le façonnons.

The world is how we shape it*

Brique fondamentale de la cybersécurité, la supervision consiste à recueillir et analyser l'ensemble des traces d'utilisation et des journaux de fonctionnement des composants matériels et logiciels du système d'information pour y repérer au plus tôt tout comportement anormal révélateur d'une attaque. Les données collectées sont filtrées, triées, formatées, analysées, puis transmises à un SOC (Security Operations Center) où seront prises les mesures appropriées. Initialement conçu et développé par Sopra Steria pour les besoins d'un organisme de défense nationale, Mactan est une offre de supervision de bout en bout, qui s'adapte aux contraintes des systèmes d'information actuels, complexes et hétérogènes, ainsi qu'à leurs évolutions et à celles des besoins de sécurité. À l'état de l'art, modulaire et standard, Mactan renforce toutes les infrastructures de sécurité, nouvelles ou existantes, face à des menaces toujours plus nombreuses et sophistiquées. Mactan se destine plus particulièrement aux OIV et aux secteurs sensibles tels que la défense, l'énergie, l'industrie, la finance et les administrations régaliennes

Solution de supervision avancée, Mactan permet de :

- **Collecter et centraliser les traces et les événements du système d'information**
- **Filtrer, formater, contrôler, analyser ces données pour repérer des schémas d'attaque**
- **Transférer de façon sécurisée les données, en totalité ou partie, vers un SOC**
- **Archiver les traces brutes pour en préserver l'intégrité et l'auditabilité**

Souveraineté

Un SIEM manipule des données très sensibles.
Mactan conçue et developpée par Sopra Steria, est une solution 100% francaise.
Elle est garante de la sécurité des données mais aussi de la conformité des procédures.

Adaptabilité

Modulaire et standard, Mactan convient à toutes les tailles de SI, à toutes les architectures, et se plie à toutes les contraintes techniques, opérationnelles et organisationnelles.
Souple et personnalisable, il accompagne les évolutions du SI, des enjeux métiers et de la politique de sécurité.

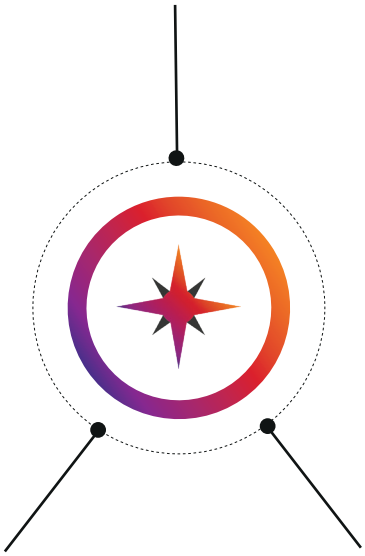
Intelligence

Mactan permet de construire, d'exécuter et d'améliorer sans cesse ses propres règles de détection en tenant compte des contraintes de son SI, de ses spécificités sectorielles et de la Threat Intelligence pour n'ignorer aucun incident de sécurité et minimiser les faux positifs.

Produits, services, extensions : Mactan, une gamme modulaire pour couvrir tous les enjeux

Mactan Rules

Mactan RULES permet de bâtir un jeu de règles de détection sur mesure, conforme au framework MITRE ATT&CK et au format standard Sigma, puis de mettre en place un cycle d'amélioration continue.



Mactan OPS

Version mobile et plug&play, embarquée dans un PC portable durci, Mactan OPS permet la supervision d'un SI temporaire quel que soit sa taille (opération, événement, projet minier/BTP...) par un personnel non spécialisé.

Mactan Platform

Détection sur règles (Sigma) et sur indicateurs de compromission (IoC).
Extensions
- **Mactan NETWORK** : sonde réseau pour la détection d'intrusion (NDR).
- **Mactan TRUST** : audit d'architecture et de configuration pour être conforme à la politique de sécurité du SI en continue.
- Mactan RESPONSE : automatise la réponse aux incidents pour un gain de temps décisif (SOAR).

Dans le Cloud ou On-Premise, les modules Mactan sont indépendants et interopérables avec la plupart des outils du marché.

Mactan est un SIEM de nouvelle génération qui facilite la surveillance des systèmes d'information complexes des organisations sensibles et le déploiement de leurs politiques de sécurité, du siège jusqu'aux opérations sur le terrain.

Pierre Verbaere

Quelques références :

Nous contacter :

Pierre VERBAERE

Product Manager CyberDefense

Tel : 07.72.02.97.66

Mail : contact.mactan@soprasteria.com