FICHE TECHNIQUE

Présentation de la solution MISP

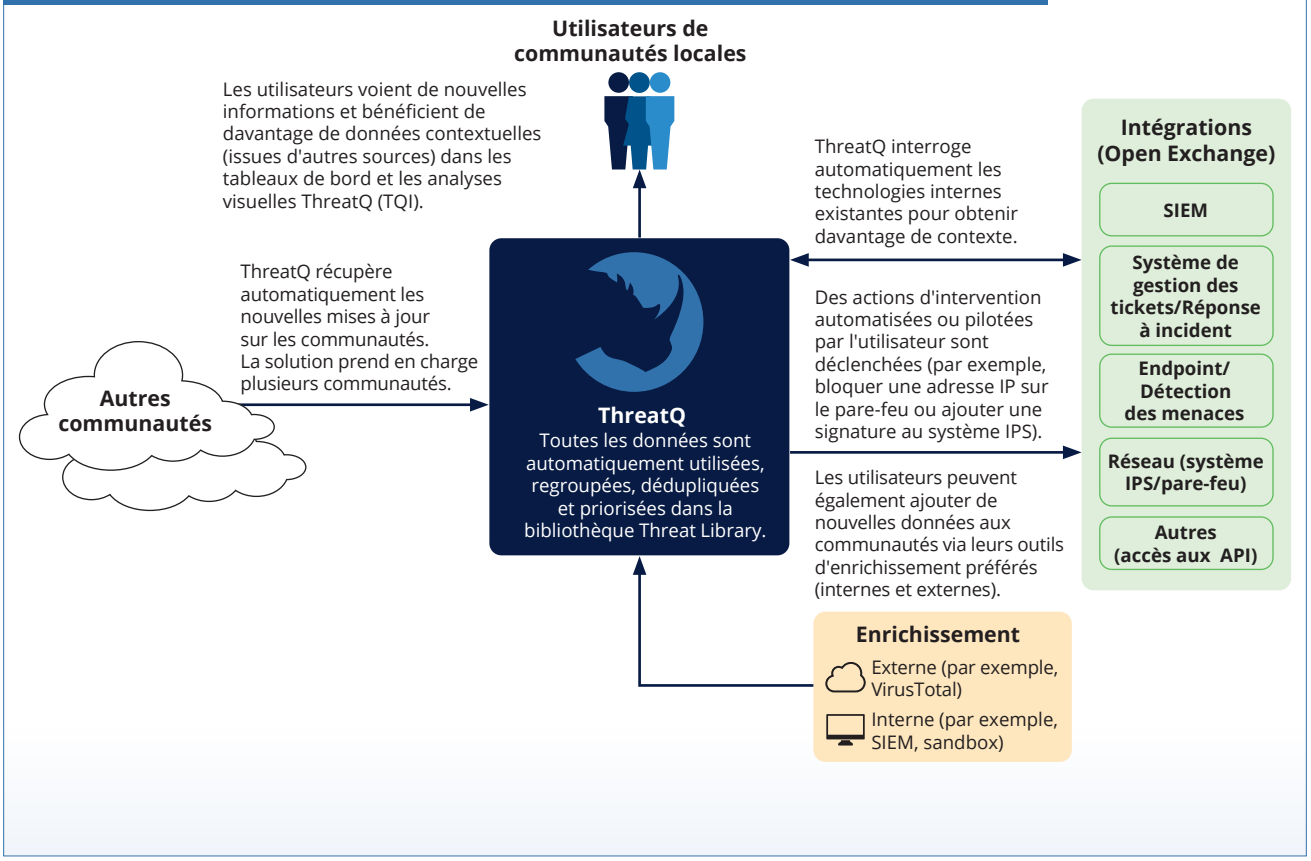
L'utilisation conjointe de ThreatQ et de MISP permet de collecter des données inestimables sur les menaces émergentes, tout en mettant en corrélation ces informations avec d'autres sources. Grâce à nos différentes intégrations MISP, les entreprises sont en mesure de récupérer des données de Threat Intelligence, de les analyser et de créer des investigations, puis de republier ces données sur MISP. Ainsi, elles peuvent non seulement créer leur propre instance MISP, mais aussi tirer parti de communautés basées sur cette plate-forme.

POINTS CLÉS

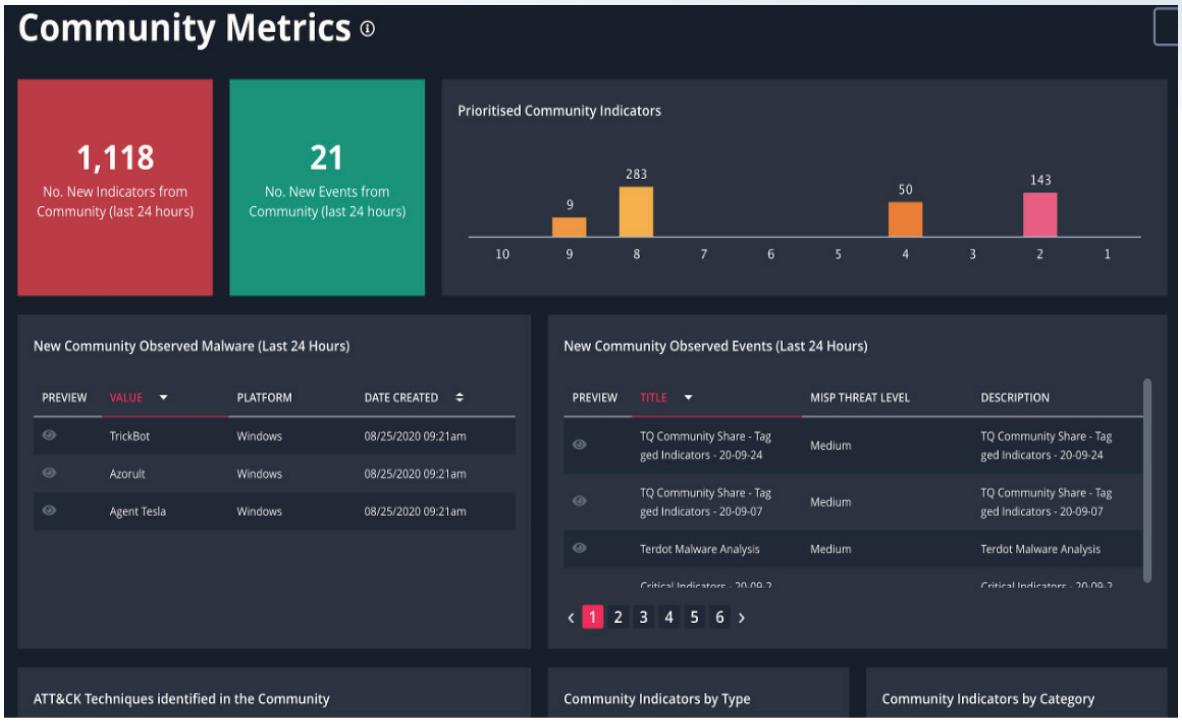
Importation de données de Threat Intelligence depuis MISP

Grâce à notre connecteur d'importation MISP Import Connector, les entreprises peuvent intégrer des événements MISP dans la plate-forme ThreatQ, et ces événements sont associés à des indicateurs liés aux données stockées dans la bibliothèque Threat Library. Ce connecteur permet également d'incorporer les données MITRE ATT&CK marquées par rapport à l'événement MISP source (par exemple, les données sur les adversaires, les techniques ATT&CK et les logiciels malveillants).

IMPORTATION DE DONNÉES DE THREAT INTELLIGENCE DEPUIS UNE COMMUNAUTÉ MISP



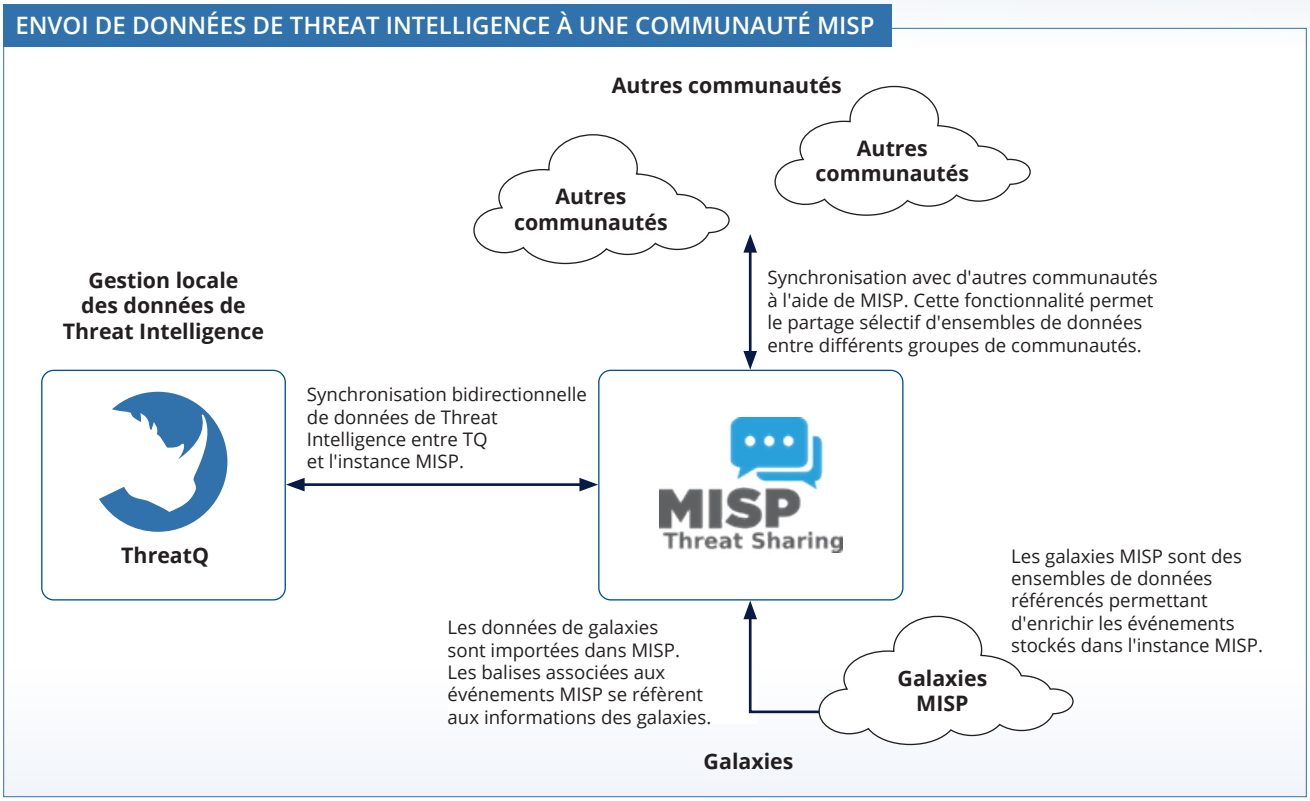
Avec les tableaux de bord ThreatQ, les utilisateurs ont la possibilité de visualiser dans une vue unique les données importées de MISP, et donc d'effectuer des tâches de suivi et d'investigation, le cas échéant. Cette fonctionnalité est particulièrement utile si vous avez besoin de mesures détaillées ou si vous souhaitez voir des tendances spécifiques.



Vous pouvez également lancer ThreatQ Investigations depuis un événement MISP ingéré. Comme cette solution d'investigation prend en charge les analyses collaboratives et les interventions en temps réel, elle constitue une aide non négligeable pour les équipes (threat hunting, réponse à incident, analyse en Threat Intelligence) qui ont besoin d'exploiter rapidement les nouvelles données de communautés et d'identifier leur impact possible.

Exportation de données de ThreatQ vers MISP

ThreatQ ingère et priorise les informations de Threat Intelligence à partir de sources à la fois externes et internes. Cette solution peut ainsi contribuer à l'identification des menaces et à leur mise en évidence à l'aide des données contextuelles riches de la bibliothèque Threat Library, de l'attribution de scores et de la solution ThreatQ Investigations. Le connecteur MISP Export peut capturer automatiquement ces informations importantes, puis les partager avec la communauté MISP sous forme d'événements MISP dédiés. Les données connexes (adversaires, techniques MITRE ATT&CK et logiciels malveillants) sont automatiquement associées à l'événement MISP dans un format compatible avec les galaxies MISP, si vous les utilisez.



Flux de Threat Intelligence

ThreatQ autorise l'ingestion directe de clusters de galaxie MISP comme source d'enrichissement de la bibliothèque Threat Library de ThreatQ. Exemples de clusters de galaxie MISP pris en charge :

- Attaquants
- Menaces connues
- Ransomwares
- Logiciels malveillants Android
- Outils d'accès à distance
- Logiciels malveillants bancaires
- Pays
- Outils (utilisés par les adversaires)

En plus des données de Threat Intelligence issues des galaxies mentionnées ci-dessus, les clients peuvent exploiter des données spécifiques sur la COVID-19 pour contrer les campagnes de désinformation, la diffusion de fausses informations médicales et les cybermenaces qui profitent de la pandémie ou y sont associées.

Pour plus d'informations, visitez le marketplace ThreatQ

Importation MISP | Exportation MISP | Galaxies MISP | Instance MISP COVID-19

ThreatQuotient s'est donné pour mission d'améliorer l'efficacité des opérations de sécurité à l'aide d'une plate-forme entièrement axée sur les menaces. En intégrant les technologies et les processus existants d'une entreprise dans une architecture de sécurité unique, ThreatQuotient accélère et simplifie les investigations et la collaboration, non seulement au sein des équipes mais également entre les outils. Grâce à l'automatisation, la priorisation et la visualisation, les solutions ThreatQuotient réduisent le bruit et mettent en évidence les menaces prioritaires afin de permettre aux ressources souvent limitées de se concentrer sur les événements à haut risque et de prendre des décisions avisées. ThreatQuotient est basé dans le nord de la Virginie, et possède des filiales chargées des opérations internationales en Europe, en Asie-Pacifique et dans la région Moyen-Orient/Afrique du Nord. Pour plus d'informations, visitez **www.threatquotient.com**.

THREATQUOTIENT
Sales@ThreatQ.com • +1 703.574.9885

© ThreatQuotient, Inc.