



Cyberpack™

Baie intégrée de recopie et d'analyse de trafic multi-technologies

Système opérationnel pour combiner compréhension des flux et analyse de cyber sécurité sur tout environnement réseau IT et OT

Objectif

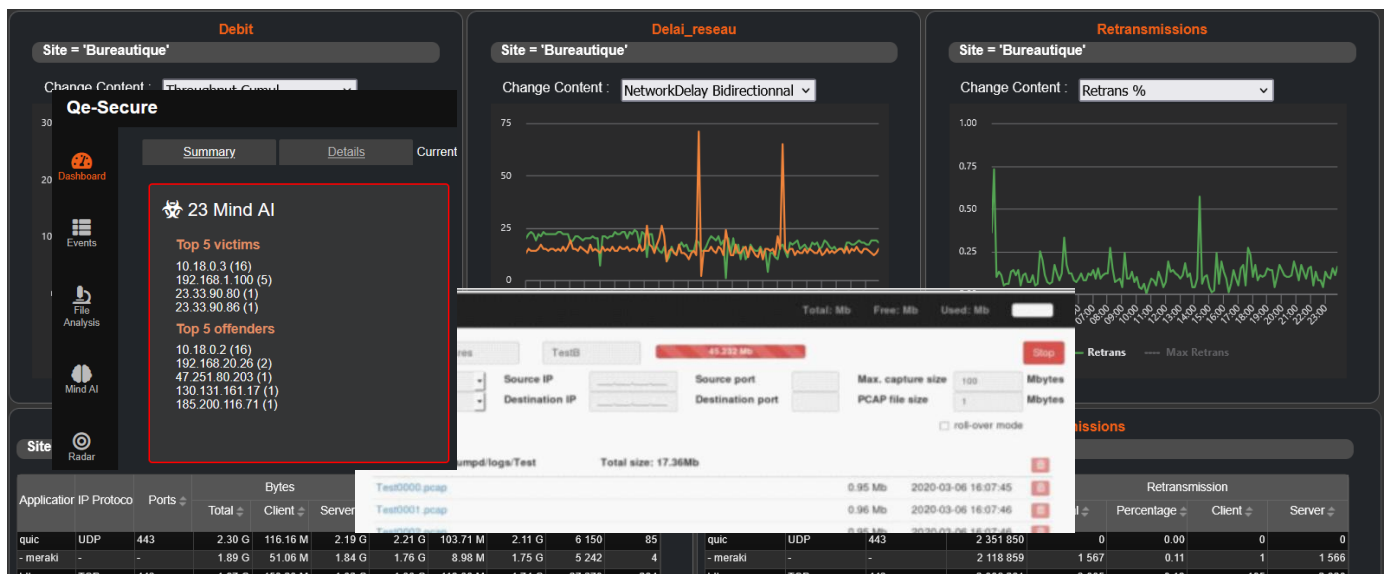
Cyberpack™ est une solution d'allentis intégrant, dans un même système configuré à la demande, une architecture globale permettant la recopie du trafic réseau sur tout type de liens cuivre ou optique et des sondes d'analyses dédiées à la compréhension du trafic et à la répartition des flux sur les réseaux, ainsi qu'à la surveillance des menaces de cybersécurité qui pèsent sur ces réseaux.



Cyberpack OT-L20

Châssis modulaire

Dans un châssis modulaire, Cyberpack™ embarque les TAP, agrégateurs, sondes d'analyse et sondes de capture massive permettant de positionner la solution sur tout environnement pour une analyse profonde de la nature des trafics échangés et des menaces de cybersécurité.



Identification des menaces – Qualification des échanges – Analyse approfondie de la payload

Votre réseau, plus performant et plus sûr au quotidien

Multi-technologies d'interception sur liens optiques et cuivre

Disponibles en configuration pour 10 à 30 lignes en analyse, les Cyberpack sont configurés à la livraison suivant les différentes technologies de raccordement attendues en cuivre et ou en optique en fibres multimodes ou monomodes.

L'agrégation de tous les liens recopiés est préconfigurée en sortie vers les sondes d'analyse sélectionnées (au moins deux types de sondes).

Découverte des échanges et analyse de cybersécurité

Au moins deux types de technologies d'analyse sont embarqués dans les baies Cyberpack pour d'une part la découverte des flux par Qe-Streams IT ou Qe-Streams OT ou encore avec Qe-Packets, et d'autre part pour la surveillance des événements de cybersécurité sur les environnements en surveillance.

Intégration aux SIEM

Comme pour l'ensemble des solutions allentis, les données d'analyse peuvent aisément être intégrées aux SIEM mis en place au sein des organisations au niveau des différents SOC afin d'intégrer et de corréliser les indicateurs ainsi collectés avec les autres éléments nécessaires à une lecture éclairée du fonctionnement des environnements IT et OT.

Autonomie

Sur des demandes d'analyse des flux nécessitant l'insertion sur des réseaux de tout type, Cyberpack est donc la solution pour garantir aux équipes d'exploitation une mise à disposition rapide de toute l'architecture technique pour installation rapide sur toute technologie de transport des données.

Dans le cas d'un fonctionnement totalement déconnecté en mode « boîte noire », les capacités d'analyse avec historisation des indicateurs voire avec le stockage massif de l'ensemble des communications garantissent aux exploitants de longues périodes significatives du fonctionnement des réseaux en surveillance.

Mobilité

Cyberpack est aussi disponible sous forme d'un châssis industriel robuste « projetable » sur différents sites. Ces baies sont déplaçables facilement au sein des différentes salles informatiques, en datacenter, ou envoyées sur sites distants par des moyens de transport standard.

Support

L'expérience unique d'allentis dans le déploiement et le support de larges configurations de copie de trafic et d'analyse permet de bénéficier d'un accompagnement complet des projets. Cet accompagnement est disponible depuis la phase de configuration de la baie Cyberpack en collaboration avec les clients, son déploiement et l'optimisation de sa configuration jusqu'à la maintenance et au support H24 7/7.

Pré-requis de configuration d'une baie Cyberpack™

A déterminer à la commande :

Technologies en recopie	Préciser le nombre de TAP en cuivre et/ou optique (fibres monomodes ou multimodes)
Agrégation	Préconfiguration en recopie de tous les flux copiés vers les ports d'entrée des sondes (possibilité de définir des configurations de recopie particulières – spécifications à la commande)
Analyse	Au moins deux technologies de sondes Qe – Qe-Secure, Qe-Streams IT, Qe-Streams OT ou Qe-Packets