Inceptrack™

Baie intégrée d'interception de trafic multi-technologies

Les besoins d'interception des flux échangés sur les grands SI ou sur les réseaux desservis par les opérateurs sont de plus en plus nombreux. Les flux doivent être analysés sans à priori sur les événements observés. Malgré tous les dispositifs d'analyse et de corrélation disponibles actuellement sur le marché, seules des données brutes peuvent permettre d'expertiser précisément et de manière fiable l'origine de multiples incidents non répertoriés dans les bases de connaissance des systèmes de surveillance disponibles sur le marché. Pourtant, ces incidents sont de plus en plus fréquemment rencontrés (dysfonctionnements réseau ou applicatifs, attaques multiples, etc ...).
Dans un châssis compact mobile, InceptRack embarque les TAP, agrégateurs et sondes de capture massive permettant de positionner la solution sur tout environnement nécessitant la capture massive de fichiers bruts des données échangés à des fins d'expertise avancée.

- Multi-technologies d'interception sur liens optiques et cuivre
- Intégration complète de tous les éléments pour interception agrégation et capture
- Modularité totale en fonction des besoins
- Capture de l'intégralité des données jusque 40 To de données en version standard
- Enregistrement des données au format pcap pour importation sur tout système d'analyse avancée

Illustration 1 : baie InceptRack configurée pour expertise sur liens fibre et cuivre

Notre baie d'interception fournit :

- les TAP pour copie de trafic : tous les TAP de la gamme Tapics sur les différentes technologies disponibles du cuivre jusqu'à l'optique à 100 Gbps, sur tout type de support et tout type de connectique actuellement disponible sur les réseaux peuvent être intégrés.
- les agrégateurs : les modèles 7020 ou 7280 d'Arista sont intégrés aux baies avec les technologies adaptées aux liens en surveillance sur lesquels les TAP sont connectés .
- la capture massive par Qe-Packets : ces sondes de stockage massif des flux échangés sont issues de la gamme QE. Elles permettent un stockage circulaire de 80 To de données. Toutes les données sont stockées sous forme de multiples fichiers au format pcap reconnu de manière standard par tous les tous les systèmes d'analyse du marché des outils d'analyse forensic. En standard, des fonctions de filtrage en pré-capture ou post-capture sont disponibles au travers d'une interface de paramétrage épurée à l'extrême pour faciliter la prise en main par toute équipe technique qui n'aurait pas été formée préalablement à son exploitation.

- mobilité : InceptRack permet une grande mobilité des baies par le choix de châssis robustes montés sur roulettes pour faciliter leur manutention et leur projection sur les sites nécessitant les expertises attendues.

Une autonomie complète pour toute mission en expertise de flux

Sur des demandes d'analyse des flux nécessitant l'insertion sur des réseaux de tout type, InceptRack est donc la solution pour garantir aux équipes d'intervention une mise à disposition rapide de toute l'architecture technique pour installation rapide sur toute technologie de transport des données. Pré-câblé avant intervention avec les technologies et connectiques cibles, l'agrégateur embarqué redirige les flux interceptés vers la sonde de capture massive Qe-Packets. Connectée sur un réseau d'administration, la prise de main à distance autorise la lecture et la récupération des données tout au long de la mission. Une première analyse et les premiers filtrages peuvent ainsi être effectuées depuis un site distant pour un rapatriement en ligne des données. De plus, en mode connecté, les conditions d'agrégation peuvent à tout moment être modifiées elles aussi à distance lorsqu'il est décidé de stopper l'analyse d'un lien ou d'en définir de nouveaux à paramétrer en analyse.

Dans le cas d'un fonctionnement totalement déconnecté en mode « boîte noire », les capacités de stockage de la sonde embarquée garantissent aux exploitants de longues périodes significatives avant récupération de la baie pour analyse des données. Fonction des débits effectifs cumulés des liens analysés, les équipes techniques choisiront le mode de capture (circulaire ou linéaire) suivant les attentes formulées en termes d'expertise attendue.

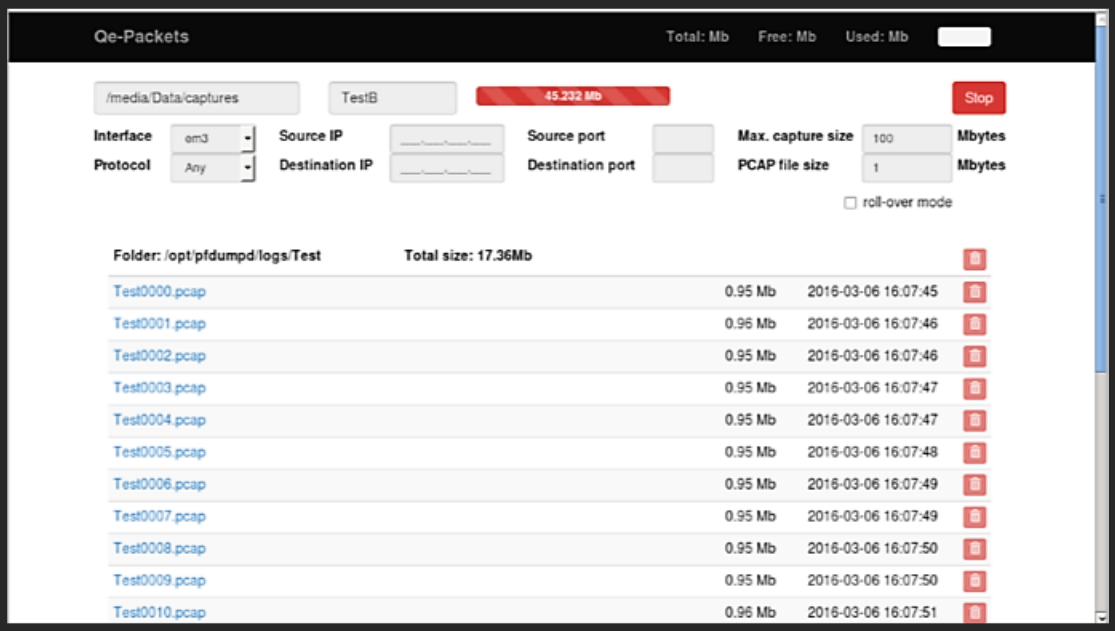

Illustration 2 : sélection de fichiers de capture pcap après filtrage

Architecture mobile robuste adaptée aux besoins dédiés

Comme décrit plus haut, InceptRack est livré sous forme d'un châssis industriel robuste pré-équipé pour les équipes techniques dédiées à intervenir sur les différentes problématiques nécessitant l'interception des flux. Ces baies sont déplaçables facilement au sein des différentes salles informatiques, en datacenter, ou projetées sur sites distants par des moyens de transport standard.

A propos d'allentis

allentis est une PME française spécialisée dans les systèmes de contrôle de la performance et de la sécurité des échanges en réseau de flux de données. Elle a conçu et fabrique les systèmes QE d'analyse de flux (Qe-Secure pour la détection de menaces, Qe-Streams et Qe-Flows pour l'analyse de performances et la cartographie des flux WAN, SD-WAN et LAN, Qe-Packets pour la capture massive de données, Qualevent pour l'hypervision métier), et la gamme TAPICS de composants réseau pour la réplication et l'isolation de trafic

© 2023 allentis sas. All rights reserved. allentis, the allentis logo, TAPICS, the TAPICS logo, vTAPICS, dTAPICS, QE, Qe-Secure, Qe-Streams, Qe-Flows, Qe-Packets, Qe-MIND are registered trademarks of allentis. Other trademarks mentioned in this document belong to their respective owners.

allentis
info@allentis.eu
www.allentis.eu