Penta Sentinel

Solution de surveillance de la sécurité nouvelle génération

Penta Sentinel est une solution complète de gestion des informations et des événements de sécurité (Security Information Event Management, SIEM). Elle a été conçue à l'aide de technologies de pointe par les experts en cybersécurité de la société Penta, est personnalisée pour répondre aux besoins de chacun de nos clients et livrée sous forme de service infogéré. Elle est accompagnée d'un Centre opérationnel de sécurité, joignable 24h/7 ,24j/7, toute l'année, et d'une conformité règlementaire intégrée.

Penta Sentinel fait partie du portefeuille de solutions Penta dédiées à la gestion des risques informatiques et vient s'ajouter aux offres de cloud privé infogéré et aux solutions IaaS de Penta. Elle permet aux entreprises de rester vigilantes et de protéger leurs opérations contre les menaces émergentes.

Hébergée dans les centres de données de Penta à Dubaï et à Genève, Penta Sentinel combine une solution logicielle de pointe à une expertise informatique digne de confiance lorsqu'il s'agit de faire fonctionner et de maintenir les infrastructures informatiques des plus grandes organisations financières dans le monde.

COLLECTE DE DONNÉES

Penta Sentinel collecte systématiquement les journaux de l'ensemble de votre infrastructure informatique, à travers plusieurs méthodes, notamment la surveillance du trafic réseau, le transfert des journaux d'événements système à partir des serveurs, des points de terminaison, des applications, des pare-feu, des systèmes antivirus et antimalware, en plus des agents dédiés configurés pour suivre certains types de flux, de transactions et d'interactions.

CORRÉLATION, ANALYSE ET ALERTES

Penta Sentinel regroupe et normalise toutes les données recueillies, puis analyse ces données pour détecter les anomalies et les activités suspectes susceptibles d'indiquer des menaces réelles. Nos experts du Centre opérationnel de sécurité (Security Operations Centre, SOC) reçoivent les alertes en temps réel, analysent les données à l'aide de méthodes et d'outils sophistiqués, et passent les faux positifs et les négatifs au crible pour identifier les véritables menaces et y répondre en temps réel.

ANALYSE DU COMPORTEMENT UTILISATEUR

Les menaces internes sont une source de préoccupation croissante, car elles peuvent avoir des retombées plus importantes, et plusieurs mois peuvent s'écouler avant de les identifier. C'est la raison pour laquelle Penta Sentinel propose une fonction d'analyse manuelle et automatisée du comportement des utilisateurs, conçue pour détecter les menaces internes potentielles ayant réussi à contourner les pare-feu et les outils antivirus et antimalware.

CENTRE OPÉRATIONNEL DE SÉCURITÉ

Le SOC de Penta Sentinel est le noyau central vers lequel toutes les données et les informations sont transmises. Elles sont ensuite examinées par notre équipe d'experts en cybersécurité, qui surveille et évalue les événements 24h/,24 7j/7, toute l'année, gère la détection des menaces et y répond en temps réel. Penta Sentinel vous permet de bénéficier de votre propre fonction SOC externalisée, ce qui réduit la charge de travail de vos équipes internes et vos budgets informatiques.

THREAT INTELLIGENCE

Outre la détection des menaces à travers l'identification d'anomalies, Penta Sentinel propose une fonction de renseignement sur les menaces qui se base sur leur signature. Cette technologie est optimisée grâce à l'exploitation de plusieurs sources de données provenant de systèmes de détection d'intrusions sur un réseau et sur un hôte, ainsi que plusieurs sources d'informations sur les menaces telles que MITRE ATT&CK®, Snort, Zeek (Bro) et YARA.

CRÉATION DE RAPPORTS

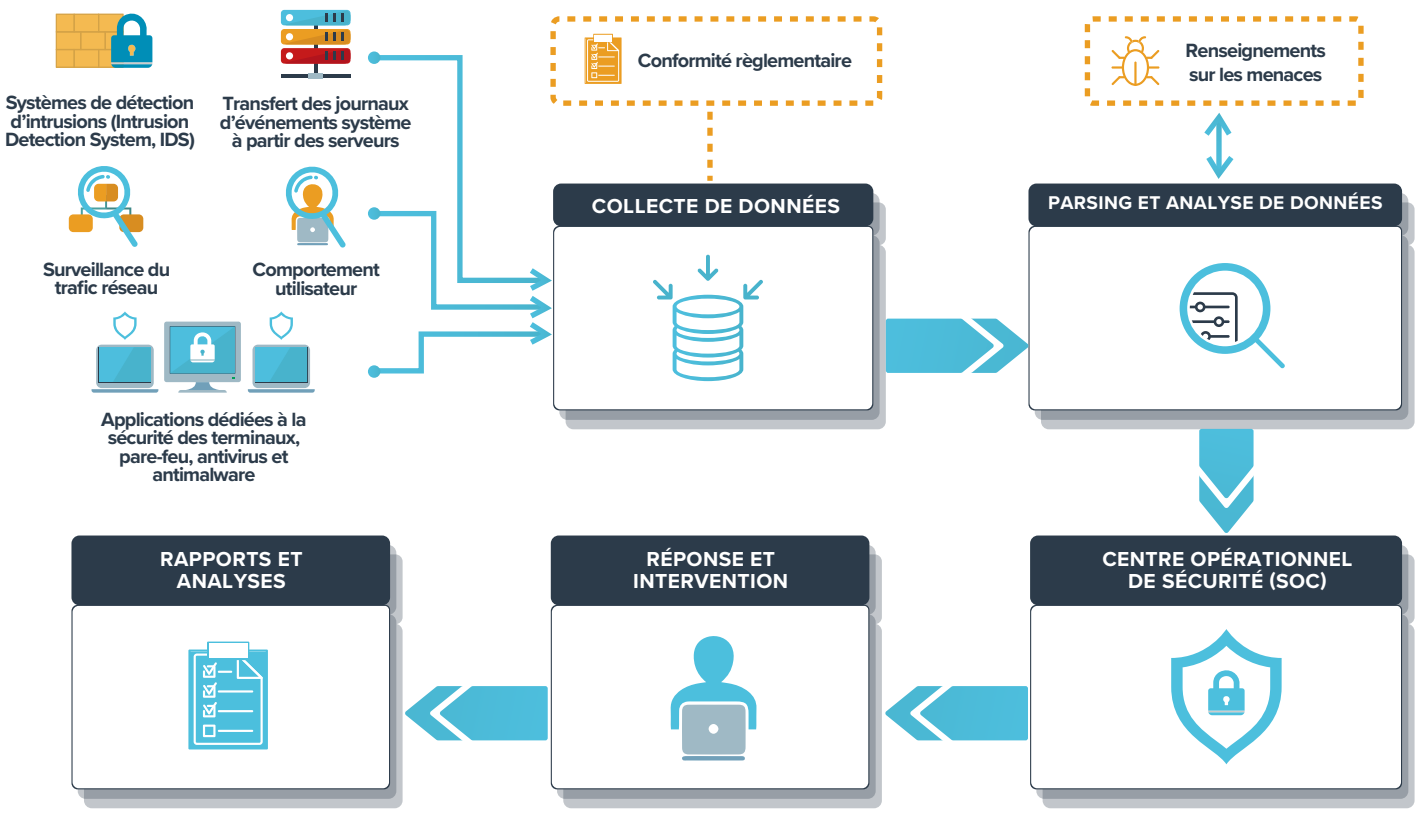
Penta Sentinel propose des rapports automatisés, qui sont examinés et validés par nos experts en cybersécurité, afin de vous o rir une visibilité totale sur la surveillance de votre sécurité et sur l'intégrité de votre infrastructure informatique. Les rapports standards incluent des éléments tels que l'authentification des utilisateurs, les événements de sécurité, le signalement des risques, la sécurité des e-mails et la sécurité du réseau.

CONFORMITÉ RÈGLEMENTAIRE

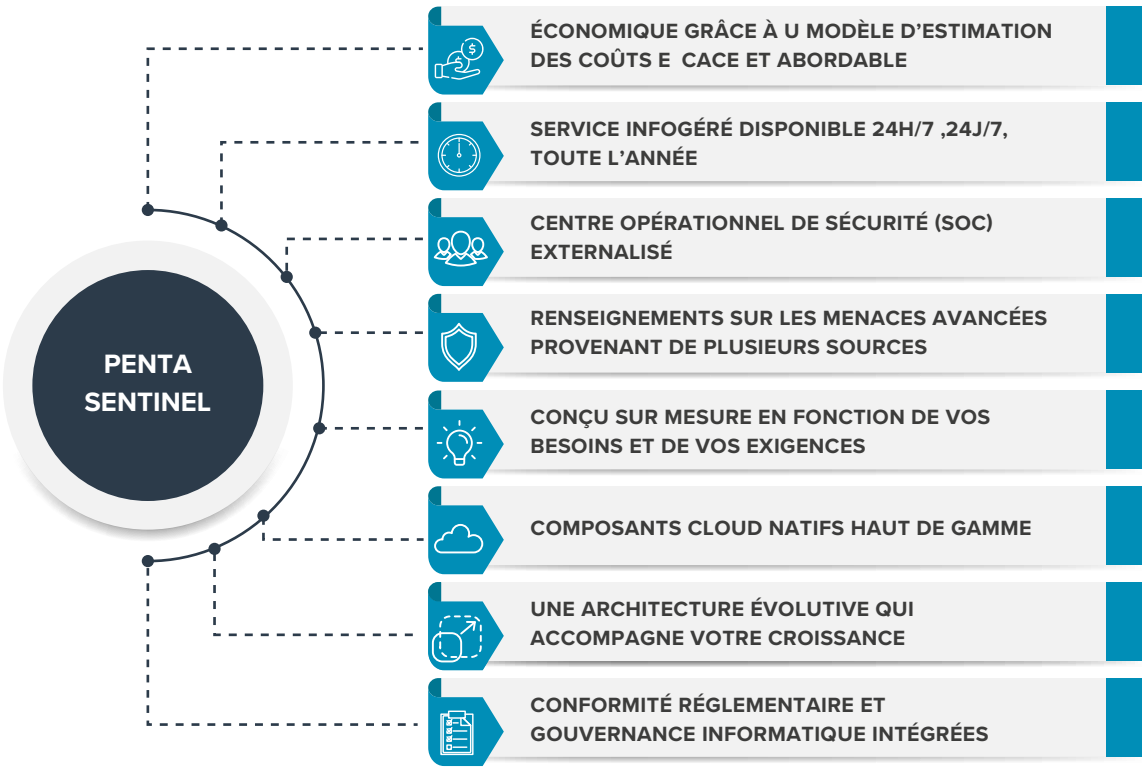
Penta Sentinel est une solution hébergée dans les centres de données de Penta à Dubaï et à Genève. La conformité réglementaire fait donc partie intégrante de cette solution, dès le premier jour, pour toutes les données recueillies et stockées, grâce à l'infrastructure de Penta.

PENTA
penta.ch

VUE D'ENSEMBLE DE LA SOLUTION



POURQUOI CHOISIR PENTA SENTINEL



PENTA
penta.ch

PENTA SENTINEL VS LA COMPÉTITION

	PENTA SENTINEL	SIEM TRADITIONNEL
CONFIGURATION ET CONCEPTION	✓ Déploiement rapide et facile avec encombrement minimal	✗ Processus de mise en oeuvre long, complexe et coûteux
RENSEIGNEMENTS SUR LES MENACES	✓ Accès à plusieurs sources internationales d'informations sur les menaces	✗ Accès à moins de sources d'informations sur les menaces et risque de non détection des menaces plus élevé
SURVEILLANCE ET GESTION	✓ Surveillance automatique basée sur la signature et les comportements, appuyée par l'équipe SOC de Penta dédiée à la gestion des escalades et aux interventions	✗ Nécessite une équipe de professionnels de l'informatique dédiés qui se relayent afin d'être disponibles 24h/7 ,24j/7, toute l'année
CRÉATION DE RAPPORTS	✓ Des rapports complets et simples à comprendre, générés selon un calendrier défini ou lorsqu'ils s'avèrent nécessaires pour l'équipe de gestion et l'équipe technique	✗ Nécessite des compétences techniques en matière de sécurité informatique pour interpréter les rapports et les menaces
CONFORMITÉ RÈGLEMENTAIRE	✓ Conformité et gouvernance informatique intégrées	✗ Solutions de mise en conformité clé en main inexistantes ou disponibles moyennant des frais supplémentaires
HÉBERGEMENT	✓ Sur site ou dans le cloud privé de Penta sur un territoire disposant d'une autorité chargée de la protection des données	✗ Généralement sur des clouds publics exposés à des risques de violation des données ou dans des clouds privés qui ne sont pas soumis à une autorité de protection des données
MODÈLE DE TARIFICATION	✓ Prix mensuel transparent, facturé par adresse IP surveillée.	✗ De nombreux facteurs qui combinent souvent les sources de données et le volume de données, ce qui entraîne une tarification complexe
COÛT GLOBAL	✓ Solution d'entrée de gamme abordable pour une fraction du coût d'exploitation du SIEM existant	✗ Solution d'entrée de gamme onéreuse, coûts de licence et de maintenance imprévisibles

Genève
Rue Bémont 4,
1204 Genève,
Suisse

+41 22 316 1000
sales@penta.ch

Dubaï
Innovation One,
Dubaï International Financial Centre (DIFC)
Dubaï, Émirats arabes unis

+971 4 376 7100
sales@penta.ch

PENTA
penta.ch