Product Brief

Stamus Security Platform

Visibilité réseau actionale et détection de menaces

- Meilleur traçabilité et visibilité
- Une détection plus complète
- Des déclarations de compromission pour les menaces avérées
- Une intelligence des menaces évolutive
- Des intégrations simples
- Des résultats immédiats

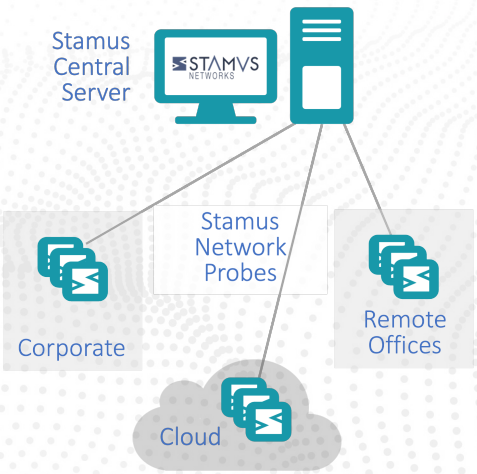
La plateforme de sécurité Stamus (SSP) est une solution de détection et réponse réseau ouverte qui fournit une visibilité réseau actionable et une détection de menaces.

Stamus Network Probes

Les sondes réseau Stamus inspectent et analysent tout le trafic réseau pour effectuer une détection de menaces en temps réel, enrichir les événements résultants avec des métadonnées étendues et capturer des transactions de protocole réseau. La sonde transmet toutes ces données au serveur central Stamus pour une analyse et détection complémentaire.

Stamus Central Server

Le serveur central Stamus fournit la gestion centralisée des sondes, gère la “threat intelligence” externe, gère l’ensemble de règles, le stockage consolidé des événements et reste un point d’intégration centrale. Il comprend une couche supplémentaire de détection de menaces basée sur l'apprentissage automatique et algorithmique, et permet un triage automatisé des événements grâce au tagging et la classification. Enfin, le serveur central Stamus fournit une interface utilisateur puissante pour la recherche de menaces et l'investigation d'incidents.



SSP supports all combinations of physical, virtual, and cloud installations.

Les équipes de sécurité utilisent la plateforme de sécurité Stamus pour la détection automatisée, la recherche de menaces proactive, l'investigation d'incidents et l'application des politiques informatiques. En fin de compte, le système aide les équipes d'exploitation de sécurité (SecOps) et réseau (NetOps) à:

Réduire les risques de votre organisation - découvrir les menaces connues et inconnues pesant sur les actifs critiques de vos réseaux cloud et sur site.

Éliminer les angles morts du réseau - surveiller le trafic nord-sud ainsi que le trafic est-ouest avec les sondes réseau Stamus à tous les points critiques de vos réseaux cloud et sur site.

Éradiquer la fatigue des alertes - le système notifie les systèmes et le personnel de réponse aux incidents uniquement lorsqu'il identifie des menaces urgentes et imminentes.

Réduire la charge de travail de vos analystes SOC - libère du temps à votre personnel, en leur permettant de se concentrer sur des mesures de sécurité proactives, plutôt que de passer en revue des milliers d'alertes.

Accélérer considérablement la réponse aux incidents - enquêter rapidement sur les problèmes potentiels avec des résultats transparents et explicables, appuyés par une traçabilité importante.

Voir les résultats immédiatement - la plateforme de sécurité Stamus est facile à installer, configurer et intégrer avec d'autres éléments de votre pile technologique de sécurité.

Étendre vos capacités - tirer parti de l'intelligence des menaces et des ensembles de règles tierces - transformer facilement une recherche de menaces en logique de détection personnalisée

Découvrir les menaces cachées - même le système le plus avancé ne peut pas tout détecter automatiquement, la plateforme Stamus Security est livrée avec une console de threat hunting guidée qui rend la recherche rapide et efficace.

SSP est disponible en deux niveaux de licence fonctionnels - Stamus Network Detection (Stamus ND) et Stamus Network Detection and Response (Stamus NDR). Ci-dessous une comparaison.

	Stamus ND	Stamus NDR
Détection de menaces basée sur des listes de signatures et de réputation	✓	✓
Enrichissement de données et capture d'événements basés sur le flux et le protocole	✓	✓
Étiquetage et classification pour le tri automatique des événements	✓	✓
Chasse aux menaces guidée	✓	✓
Moteurs de détection d'apprentissage automatique et algorithmiques		✓
Stamus threat intelligence et détection personnalisable		✓
Informations orientées actifs		✓
Declarations of Compromise™ | de menaces à haute fidélité		✓

A PROPOS DE STAMUS NETWORKS

Stamus Networks croit en un monde où les défenseurs sont des héros et où ceux qu'ils protègent restent en sécurité. Alors que les organisations font face à des menaces provenant d'adversaires bien financés, nous poursuivons sans relâche des solutions qui rendent le travail des défenseurs plus facile et plus impactant.

Leader mondial des solutions de sécurité réseau basées sur Suricata, Stamus Networks aide les équipes de sécurité d'entreprise à en savoir plus, à réagir plus rapidement et à réduire leur risque grâce aux informations recueillies à partir de l'activité réseau en cloud et sur site.

Notre plateforme de sécurité Stamus combine le meilleur des systèmes de détection d'intrusions (IDS), de surveillance de sécurité réseau (NSM) et de détection et réponse réseau (NDR) en une seule solution qui expose les menaces sérieuses et imminentes aux actifs critiques et permet une réponse rapide.

STAMUS NETWORKS

For more information, contact

NETMETRIX

info@netmetrix.fr
https://www.netmetrix.fr

