SOLUTION DE GESTION DE LOGS

STORMSHIELD
LOG SUPERVISOR

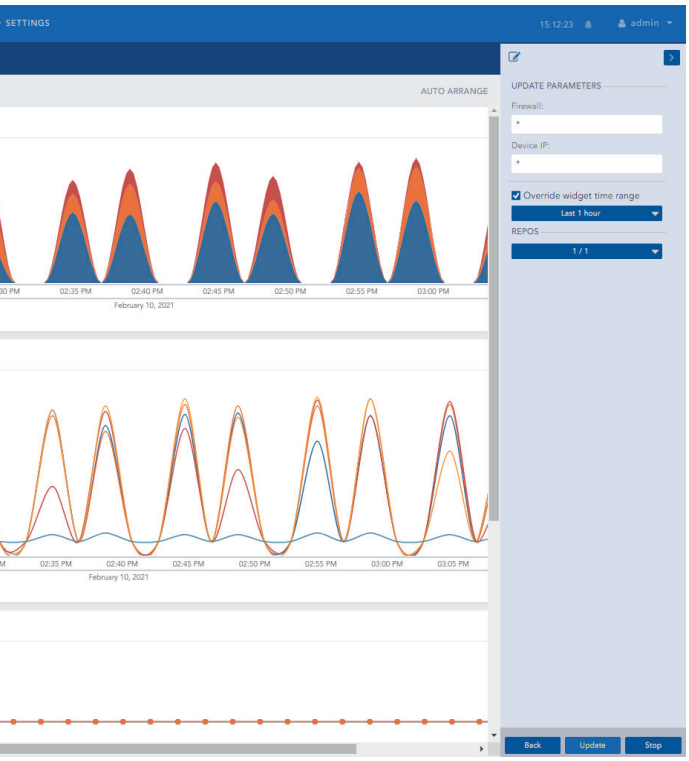
Maximisez le potentiel de vos données

ANALYSE
AVANCÉE DES JOURNAUX

CONFORMITÉ
PLUSIEURS ANNÉES D'ARCHIVES LÉGALES

RAPPORTS
MANUELS ET AUTOMATIQUES

GESTION
CENTRALISÉE DE LOGS



Contrôlez et augmentez votre cybersécurité

Face aux cyber-menaces de plus en plus avancées, il est primordial que les organisations surveillent leurs données au plus près. La solution Stormshield Log Supervisor (SLS) vous permet d'améliorer la visibilité des logs sur votre réseau tout en optimisant la réponse aux incidents.

Visibilité globale
- Tableaux de bord, rapports et alertes
- Recherche multicritères
- Rapports d'activité
- Recherche facilitée avec un langage simple et efficace

Scabilité
- Gestion de centaines de pare-feux
- Gestion de nombreux logs sur plusieurs années
- Haute disponibilité

Gestion des incidents
- Définition des règles d'alerte
- Attribution des alertes

OUTIL D'ADMINISTRATION

PME ET GRANDES ENTREPRISES

WWW.STORMSHIELD.COM

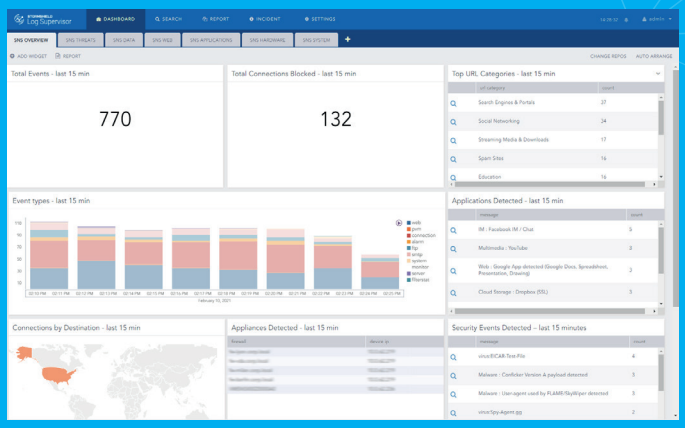
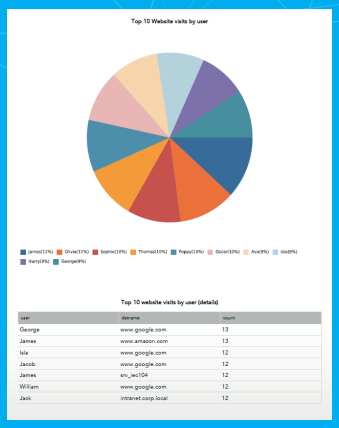
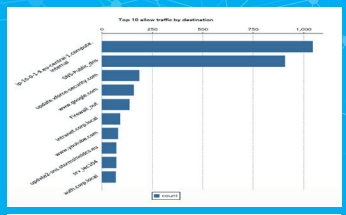
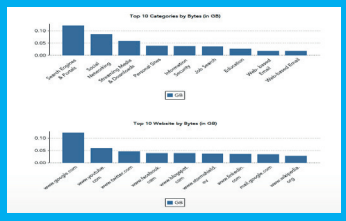


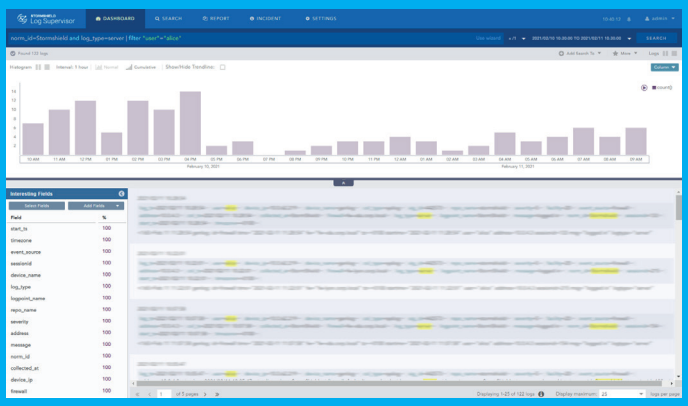
Tableau de bord



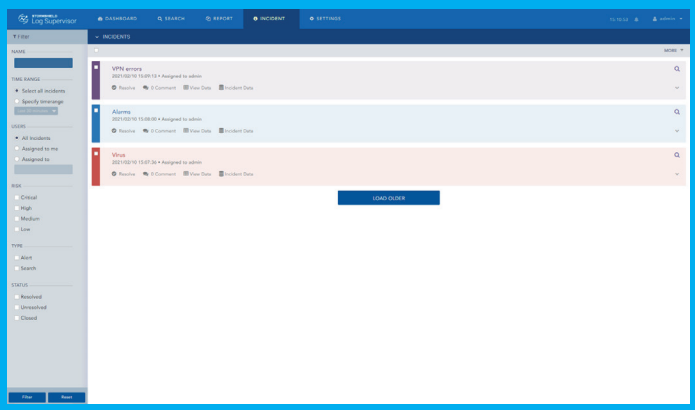




Rapports



Recherche des logs



Alertes et gestion d'incidents

LISTE DES FONCTIONNALITÉS

GESTION DE LOGS

- Collecte d'événements via syslog (TCP et UDP)
- Collecte sécurisée via syslog-TLS
- Fonction Syslog Forwarder
- Events Per Second (EPS) : 10 000 et plus
- Normalisation et indexation native des logs SNS et SES
- Gestion des logs sur plusieurs années (1 an et plus)
- Nombre de pare-feux: 500 et plus

TABLEAUX DE BORD

- Vues globales (menaces, données, applications web, hardware et système)
- Personnalisation des widgets existants
- Création de nouveaux widgets
- Plus de 20 types de graphiques différents (histogrammes, radar, carte géographique...)

TYPES DE RECHERCHE

- Recherche simple
- Recherche avancée multicritères (type de log, temps...)
- Recherches prédéfinies
- Affichage du résultat en log brut, log normalisé et graphique
- Enrichissement avec des sources externes (CSV, IPtoHost, LDAP, GeoIP)
- Navigation dans le temps (minutes, heures, jours, plage spécifique)
- Historique des recherches
- Export du résultat en CSV

RAPPORTS

- Génération manuelle ou automatique (heure, jour, semaine ou mois)
- Personnalisation de la mise en page ou modèles prédefinis
- Format des rapports : PDF, HTML, XLS, DOCX, CSV
- Envoi des rapports par email

ALERTE ET GESTION D'INCIDENTS

- Génération automatique à partir de règles établies
- Gestion de la criticité des alertes (4 niveaux)
- Assignation des incidents aux administrateurs pour résolution et suivi de la résolution

COMPATIBILITÉ

Hyperviseurs :

- VMWare ESXi 6.5 et 7
- Microsoft HyperV: Windows Server 2016

Produits Stormshield :

Produit	À partir des versions
SNS	3.7.X
SES Evolution	2.4.3