LÖSUNGEN FÜR DIE PROTOKOLLVERWALTUNG

STORMSHIELD
LOG SUPERVISOR

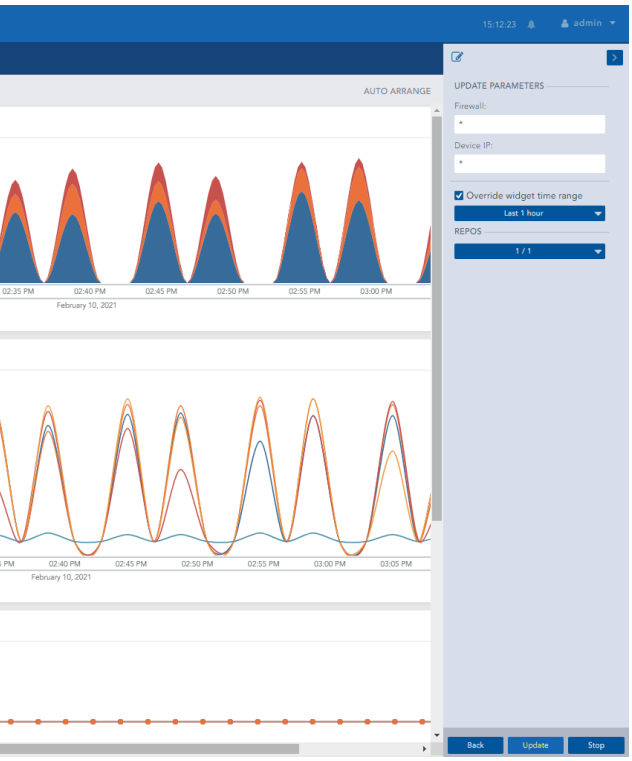
Optimisieren Sie die Qualität Ihrer Daten

FORTGE-SCHRITTENE
ANALYSE DER PROTOKOLLE

KONFORMITÄT
MEHRERE JAHRE RECHTMÄSSIGE ARCHIVE

MANUELLE
UND AUTOMATISCHE BERICHTE

ZENTRALE
VERWALTUNG DER PROTOKOLLE



Beherrschen und steigern Sie Ihre Cybersicherheit

Angesichts der immer fortschrittlicheren Cyber-Bedrohungen müssen die Unternehmen ihre Daten genaustens überwachen. Die Lösung Stormshield Log Supervisor (SLS) ermöglicht es Ihnen, die Übersicht der Protokolle über Ihr Netzwerk zu verbessern und gleichzeitig die Reaktion auf Vorfälle zu optimieren.

Allgemeine Übersicht

- Dashboards, Berichte und Warnungen
- Suche anhand mehrerer Kriterien
- Tätigkeitsberichte
- Einfachere Suche mit einer einfachen und effizienten Sprache

Skalierbarkeit

- Hohes Volumen an verwalteten Firewalls
- Verwaltung zahlreicher Protokolle über mehrere Jahre
- Hochverfügbarkeit

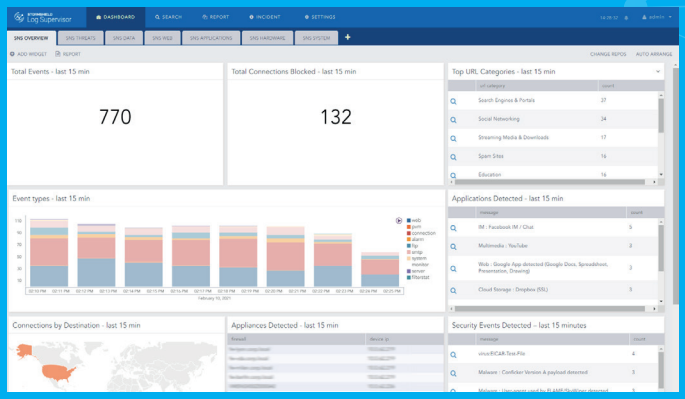
Verwaltung der Vorfälle

- Definition der Warnregeln
- Zuweisung der Warnungen

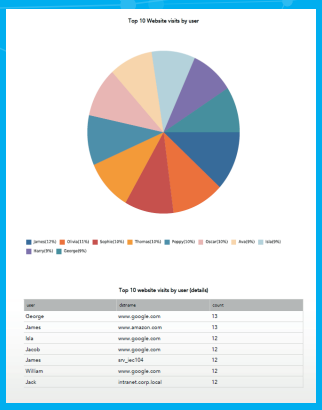
VERWALTUNGSTOOL

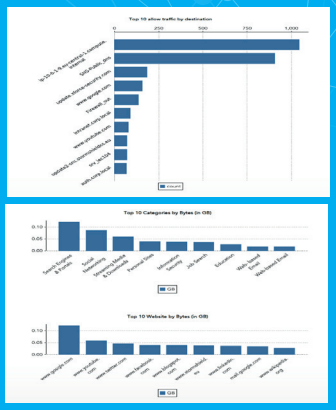
KMU UND GROSSUNTERNEHMEN

WWW.STORMSHIELD.COM

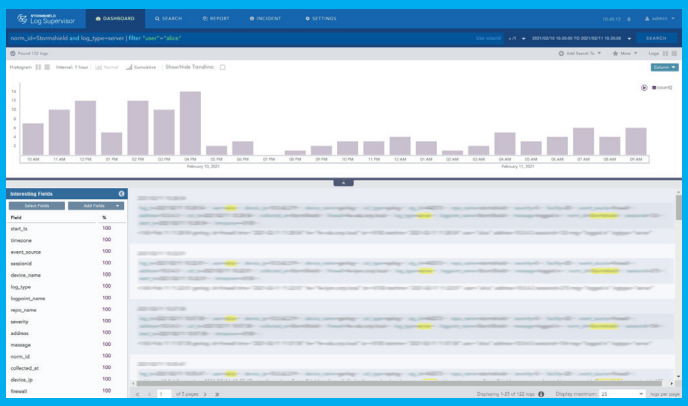


Allgemeine Anzeige von SLS

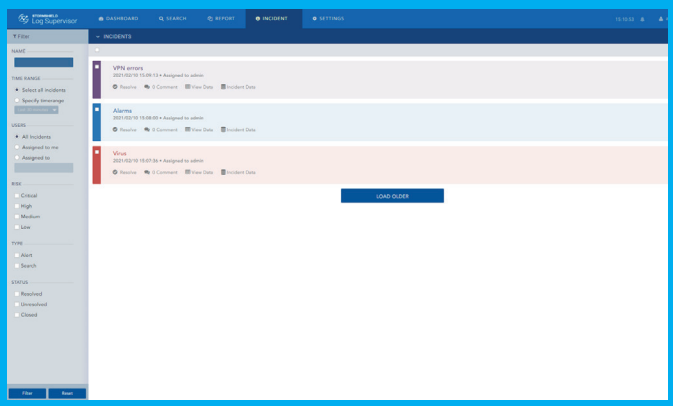




Berichte



Suche der Protokolle



Automatisch weitergeleitete Warnungen

LISTE DER FUNKTIONEN

PROTOKOLLVERWALTUNG

- Erfassung von Ereignissen über Syslog (TCP und UDP)
- Sichere Erfassung über Syslog-TLS
- Funktion Syslog Forwarder
- Events Per Second (EPS): 10.000 und mehr
- Normalisierung und native Indexierung der SNS und SES-Protokolle
- Protokollverwaltung über mehrere Jahre (1 Jahr und mehr)
- Anzahl der Firewalls: 500+

ARTEN DER SUCHE

- Einfaches und vordefiniertes Suchen
- Fortgeschrittene Suche anhand mehrerer Kriterien (Art des Protokolls, Zeit usw.)
- Anzeige der Ergebnisse als Rohdatenprotokolle, normalisierte Protokolle und grafische Protokolle
- Erweiterung mit externen Quellen (CSV, IPtoHost, LDAP, GeoIP)
- Navigation auf Zeitbasis (Minuten, Stunden, Tage, bestimmter Zeitraum)
- Suchverlauf
- Export des Ergebnisses im CSV-Format

DASHBOARDS

- Allgemeine Anzeigen (Bedrohungen, Daten, Web-Anwendungen, Hardware und System)
- Individuelle Gestaltung der bestehenden Widgets
- Erstellung neuer Widgets
- Mehr als 20 verschiedene Arten von Grafiken (Histogramme, Radar, geografische Karte usw.)

WARNUNG UND VERWALTUNG DER VORFÄLLE

- Automatische Erstellung anhand von festgelegten Regeln
- Verwaltung der Kritikalität der Warnungen (4 Stufen)
- Zuweisung der Vorfälle an die Administratoren zur Lösung und Betreuung der Lösung

BERICHTE

- Manuelle oder automatische Erstellung (Uhrzeit, Tag, Woche oder Monat)
- Individuelles Layout oder vordefinierte Vorlagen
- Format der Berichte: PDF, HTML, XLS, DOCX, CSV
- Versand der Berichte per E-Mail

KOMPATIBILITÄT

Hypervisors:

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

Stormshield-Produkte:

Produkt	Ab Version
SNS	3.7.X
SES Evolution	2.4.3