STORMSHIELD

SECURITY MANAGEMENT SOLUTION

STORMSHIELD
LOG SUPERVISOR

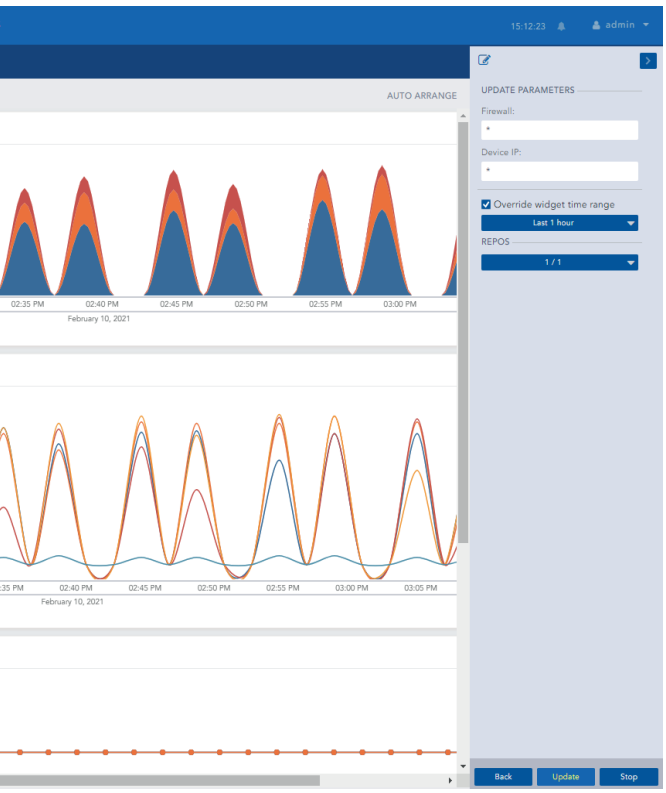
Maximize your infrastructure's cybersecurity

SECURITY
FROM DETECTION TO REMEDIATION

CENTRALIZATION
CORRELATION OF SECURITY EVENTS

VISIBILITY
OF THE WHOLE INFRASTRUCTURE

COMPLIANCE
MANY YEARS OF LEGAL ARCHIVING



Control and enhance your cybersecurity

Faced with increasingly advanced cyber-threats, it is essential for organisations to monitor their data more closely. Stormshield Log Supervisor (SLS) gives you better visibility into network events, while optimising incident response.

Global visibility
- Dashboards, reports and alerts
- Multicriteria search
- Activity reports
- Management of all infrastructure sources

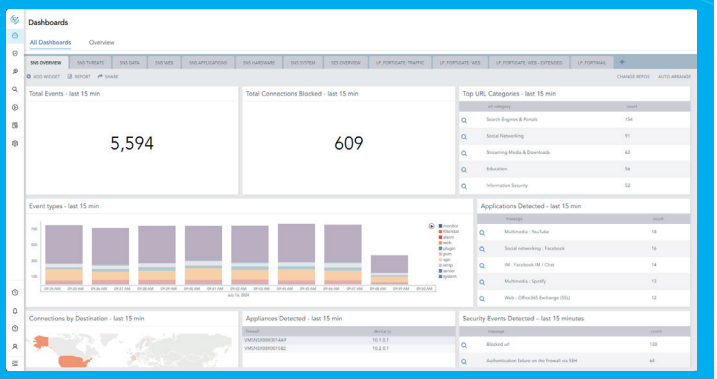
Alerts and detection
- Predefined or customized alert rules
- Implementation of the MITRE ATT&CK matrix
- Incident resolution workflow

Remedial actions
- Automated or manually triggered responses
- Integrated playbooks
- Enriched event contexts

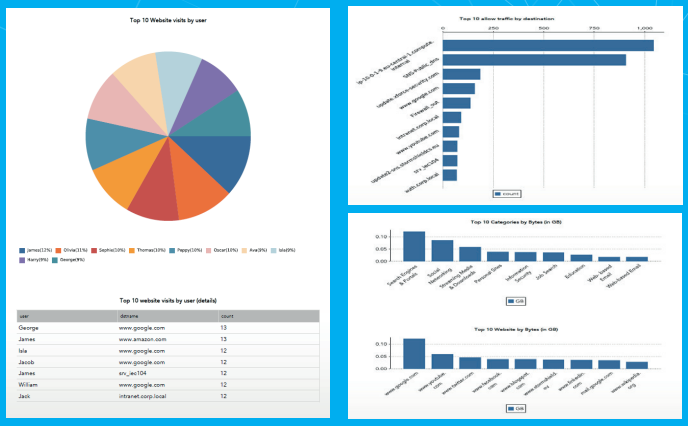
ADMINISTRATION TOOL

SMES AND LARGE COMPANIES

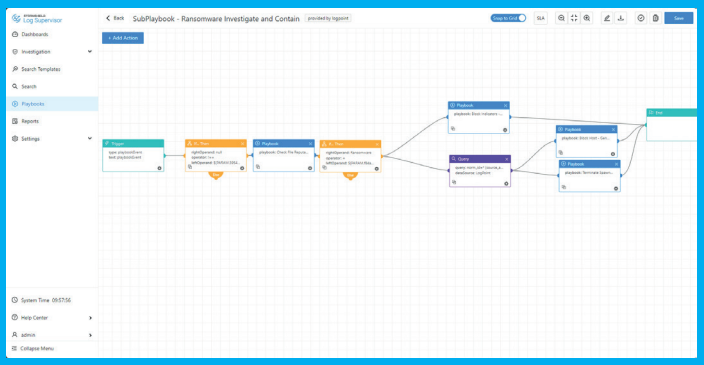
WWW.STORMSHIELD.COM



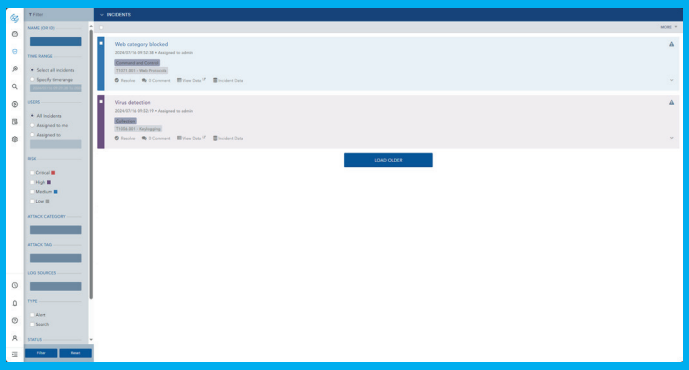
General SLS view



Reports



Remediation and playbooks



Alerts and incident management

FEATURES LIST

LOG MANAGEMENT

- Event collection via syslog (TCP & UDP)
- Secure collection via syslog-TLS
- Syslog Forwarder function
- Events Per Second (EPS): 10,000+
- Normalisation and native indexing of SNS & SES logs
- Log management over multiple years (1+ year)
- More than 300 source types

DASHBOARDS

- General views (threats, data, web applications, hardware and system)
- Customisation of existing widgets
- Creation of new widgets
- More than 20 different types of graphics (histograms, radar, map, etc.)

SEARCH TYPES

- Simple search
- Multicriteria advanced search (log type, time, etc.)
- Predefined searches
- Results displayed as raw logs, normalised logs and graphical logs
- Enrichment with external sources (CSV, IPtoHost, LDAP, GeoIP)
- Navigation through time (minutes, hours, days, specific time range)
- Search history
- Results exported in CSV format

REPORTS

- Manual or automatic generation (hour, day, week or month)
- Customised layout or predefined templates
- Report format: PDF, HTML, XLS, DOCX, CSV
- Reports sent by email

ALERTS AND INCIDENT MANAGEMENT

- Automatic generation based on pre-established rules
- Management of alert criticality (4 levels)
- Incidents assigned to administrators for resolution, with resolution tracking

REMEDIAL ACTIONS

- Predefined playbooks
- Customize and build new playbooks
- Fully automated or manually triggered response

COMPATIBILITY

Hypervisors:

- VMWare ESXi 7.0.3 and later
- Microsoft HyperV: Windows Server 2016, 2019 et 2022

Stormshield Products:

Product	From versions
SNS	3.7.X
SES Evolution	2.4.3