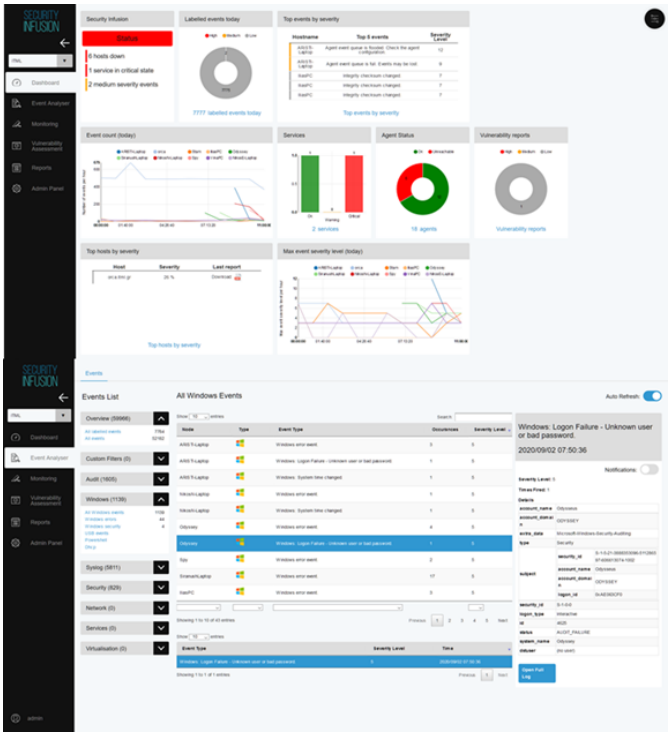
SECURITY INFUSION

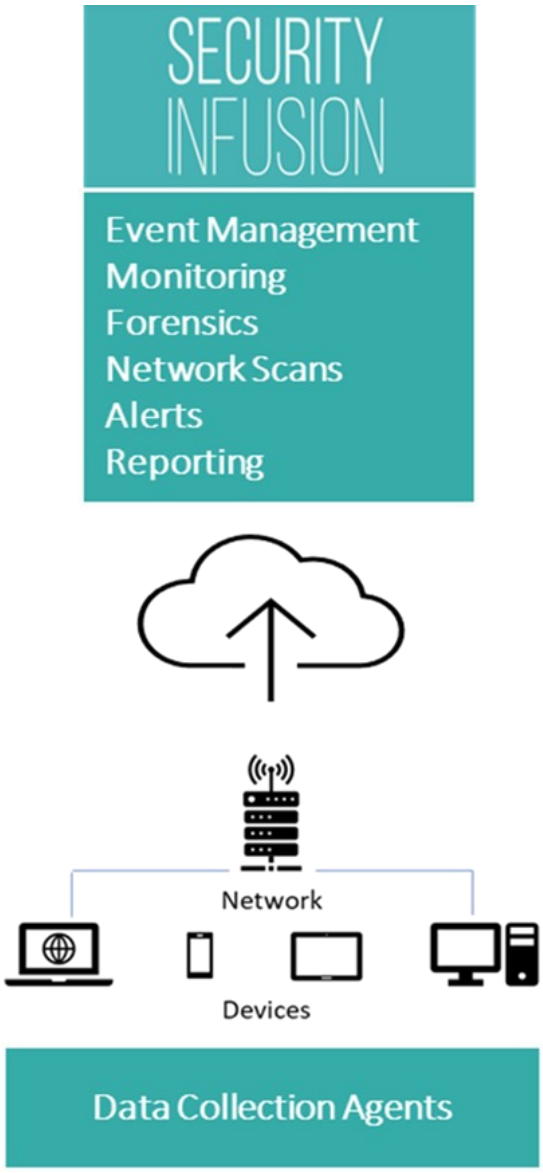
ITML Security Infusion

IT Operations and Cyber Security Information Management

A Management & Control Baseline for IT operations

ITML developed Security Infusion as a software that provides, in one single solution, basic features of SIEM, Monitoring and IDS systems, constituting a Control Baseline of ICT operations, with integrated risk mitigation and regulatory compliance capabilities.
The application is delivered as SaaS and it can be deployed fast and without complexity.
The agent-based software solution collects, analyzes, visualizes, and presents near real time and historical data about the operation and security status of an organization's IT resources.
To enable retrospective forensic analysis, the program stores data related with past logs and events, so that they can be retrieved when necessary.





Additionally, the application has the ability to perform regular or on-demand scans on the managed infrastructure, namely port scanning, and vulnerability assessment, thus providing reports and remedy proposals for issues it might detect.
Security Infusion runs on Docker containers that are orchestrated by Kubernetes. This architecture is optimal for cloud operation, enabling high availability and better management of the application, while it also facilitates the fulfillment of different user needs at different time periods, especially when scale-up or scale-down actions are needed.

SECURITY INFUSION

ITML

Features Table

Dashboard	Aggregates important information to provide an overview of the monitored infrastructure's status and a central navigation pane. • Hosts Status • Services • Events • Vulnerabilities
Event Analyzer	Surveillance and data gathering of events on monitored systems (hosts) and network, including file integrity monitoring, log monitoring, rootcheck, and process monitoring. • Configurable filtering of events • Log analysis • File integrity • Windows registry monitoring. • Rootkit detection • Syslog events • Windows and Linux support Infusion event analyzer is built on open components (i.e. OSSEC toolkit) gathering relative operational data and triggers rule-based alerts enabling active response where needed.
Monitoring	Monitoring Agent-based Nodes monitoring • Host Status, including performance, processes, and full inventory • Service Status • Email Notifications. Infusion monitoring provides operational awareness and early warning
Vulnerability Assessment & Port Scanning	Detection of common cybersecurity vulnerabilities. Agent-based assessment built around specific operational requirements and policies along with publicly known and reported vulnerability issues (i.e. CVE® lists). • Operating System level vulnerabilities • Services Level Vulnerabilities (http, smtp, etc.). • Report Generation • IP–based, hosts' services tracing • Inspection of open ports • Detection & Assessment the relative operating network services Infusion Vulnerability Assessment provides the administrator with essential information on the Nodes (agent hosts) status enabling them to get insight, impact assessment and proposed solutions about soft points in their infrastructure
Reports	Event reporting based on applied filters. Online view and downloadable pdf report generator. Download options: • Full log • Formatted data • Alert data
Admin Panel	• Agents & Master Agents creation & download • Port Scanning configuration • Monitoring configuration • Custom Filters configuration • Reporting configuration • Account management

SECURITY INFUSION

Minimum System Requirements

Windows Agent Requirements

	Minimum	Recommended
OS	Windows 7	Windows 10 or higher
Platform	32bit/64bit	32bit/64bit
CPU	Intel i3	Intel i5
Memory	3G	4G

Linux Agent Requirements

	Minimum	Recommended
OS	Centos 7 or Ubuntu 18.04	Centos 7 or Ubuntu 18.04
Platform	32bit/64bit	32bit/64bit
Software requirements	JRE 1.8	JRE 1.8
CPU	Intel i3	Intel i5
Memory	3G	4G

Master Agent Requirements

Master agent collects all the network-related data (i.e. syslog) and performs local network scans (i.e. ports scanning & vulnerability assessment).

	Minimum	Recommended
OS	Centos 7	Centos 7
Platform	32bit/64bit	32bit/64bit
CPU	Intel i5	Intel i5
Memory	4G	4G

Visit the Security Infusion product site: **https://security-infusion.com/** to see proposed subscription plans, watch tutorial videos and register for a 14-day free trial.

Get more: Contact ITML to obtain more information about Security Infusion and how you can benefit from Data Analytics and Machine Learning to manage, control, and secure your ICT Assets.

www.itml.gr/security-infusion **info@itml.gr**