

IT Operations Monitoring and Security Information Management with ITML Security Infusion

Align IT operations with cyber security



Cloud or Edge based monitoring software, running local agents for collection of operational data

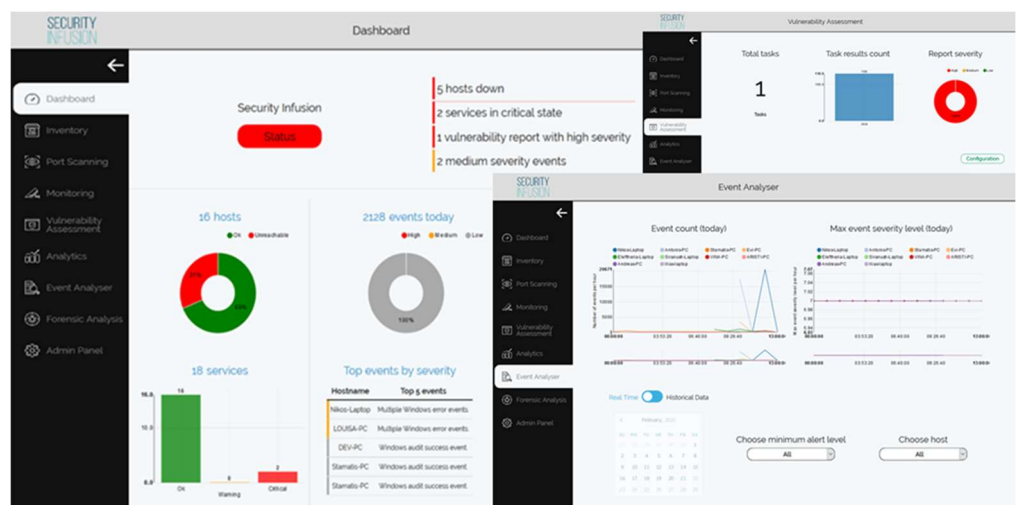
Real time evaluation of operations and alerting for issues on hosts, network, processes and services.

Vulnerability assessment based on process profiling, rule-based intrusion detection using Machine Learning techniques.

Data processing and analytics – real time data streams and operational history (events, logs)

Detailed forensic analysis for hosts, network and related services

Licensing per monitored node/installed agent.



A Challenging ICT Landscape

Abstraction and Convergence of ICT infrastructure have transformed corporate assets while cloud and mobility are multiplying operational challenges. Cyber security is omnipresent as data and information are growing in value; cyber threats are the norm, not the extraordinary. IT security is now an integral part of business operations and not a fringe area of technological particularities.

Monitor ICT Operations

Security Infusion aligns IT operations management with cyber security challenges in a simple and intuitive manner. The application is a comprehensive web-based monitoring platform for cyber security awareness and protection. Resources and services are surveyed in real time and information is collected and stored for further study through data analytics.

A Versatile Solution

Processing can be performed either at the edge of the managed infrastructure or through the cloud. Flexible architecture and deployment options ensure that vital information is collected, processed, measured and presented in a timely and compact fashion, when needed, as needed.

Eventually, machine learning makes time and data growth an ally for better situational awareness and response; the more data the manager collects the more effective it becomes.

The Stack

Security Infusion is an agent-based software solution collecting, analyzing and visualizing operational data and security status of an organization’s IT resources. The application realizes its functions through the following components:

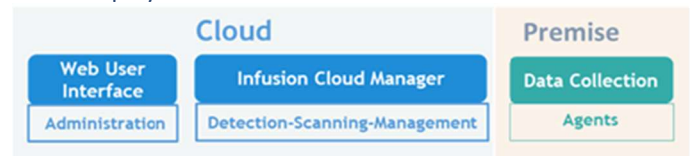
- Infusion Agents
- Infusion Manager (Edge or Cloud based)
- Infusion Web Interface

Additionally, the manager can run agent-independent scans of the managed infrastructure, namely port scanning and vulnerability assessment, providing reports with risk mitigation proposals.

Edge Deployment



Cloud Deployment

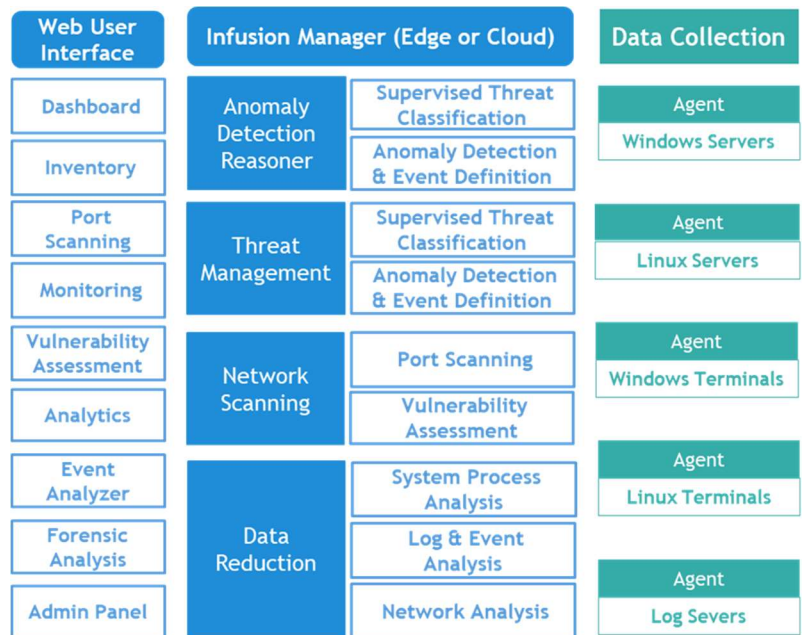


Monitoring and relevant functionalities are realized through the main dashboard and seven additional operational tabs corresponding to the featured functions: Inventory, Port Scanning, Monitoring, Vulnerability Assessment, Analytics, Event Analyzer, Forensic Analysis. An eighth tab contains the admin panel of the app with the relative settings options.

Features

Functions designed to optimize the administrative overview while remain simple and straightforward

- Inventory: ICT Assets
- Port Scanning: Services running on devices.
- Monitoring: Host Status, Service Status, Alerts (email & Slack).
- Vulnerability Assessment: According to public vulnerability issues (i.e. CVE® lists). Report Generation.
- Analytics: System Profiling, Processes analysis, Performance Visualization.
- Event Analyzer
- Forensic Analysis



Web User Interface

The application provides a comprehensive and straightforward user experience. Its features are accessed through a web interface with a sidebar that accumulates the eight function tabs that let the user navigate through the dashboard and the seven corresponding functions

Get more: Contact ITML to obtain more information about Security Infusion and find out 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