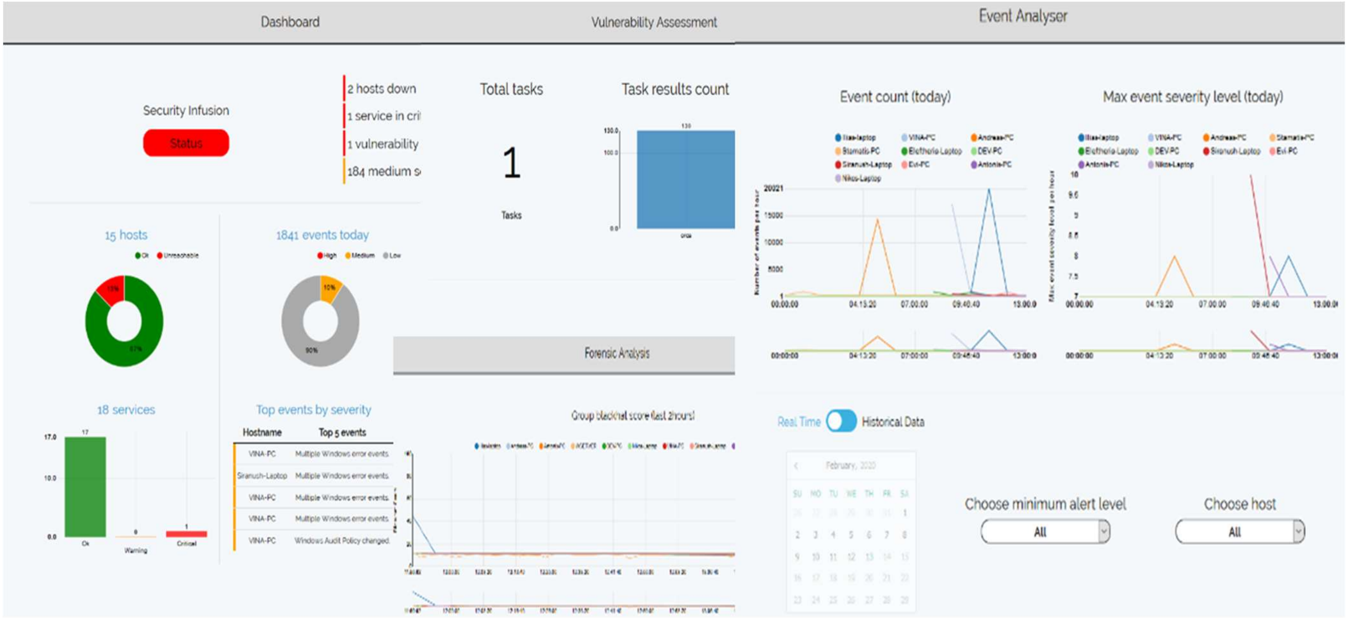
SECURITY
INFUSION

ITML Security Infusion

IT Operations and Cyber Security Information Management

The Challenge

Digital transformation is turning IT Operations into the most significant element of daily business activities. Abstraction and Convergence of ICT infrastructure are transforming corporate assets while cloud and mobility are multiplying operational challenges proportionally to the opportunities they create. In this landscape, digital security has transpired over the technological domain and is now the subject of regulation, compliance and financial governance.
As digital transactions and data 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.



Security Infusion: Real Time ICT Monitoring, Assessment and Alerting

ITML developed Security Infusion to be an application for IT operations monitoring with elements of cyber security management, designed to run and operate in a simple and intuitive manner.
ICT resources, services running on them, network and computing events, are monitored, reviewed and analyzed in real time, while relative data are collected and stored for further classification and forensic purposes, using data analytics and machine learning algorithms.
Security Infusion can be deployed either through the cloud or at the edge of an organization's infrastructure, without overloading the network with unnecessary traffic and chatter. The application's architecture ensures that vital information is collected, processed, measured and presented in a timely and compact fashion, when needed, as needed.
Eventually, built-in machine learning makes time and data growth an ally for better situational awareness and response; the more data it collects the more effective it becomes.

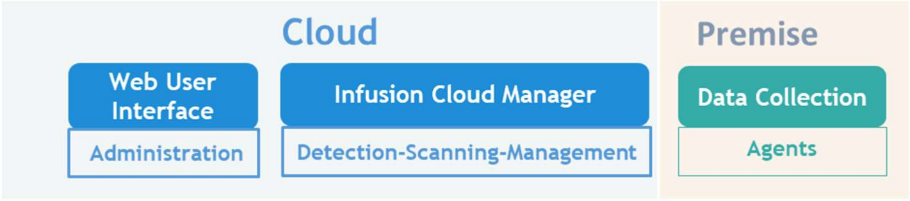
The Stack

Security Infusion is an agent-based software solution that collects, analyzes, visualizes and presents real time data concerning the operations and security status of an organization's IT resources. Furthermore, to enable retrospective forensic analysis, the program stores data related with past logs and events, so that they can be retrieved when necessary. Furthermore, the application has the ability to perform regular or on-demand, agent-independent scans on the managed infrastructure, namely port scanning and vulnerability assessment, providing reports and remedy proposals for issues it might detect. The application realizes its functions through the following components:

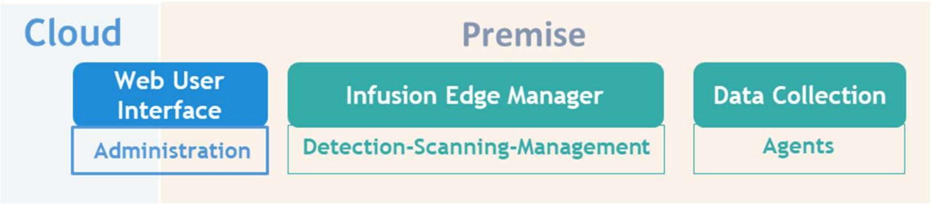
- Infusion Agents: Windows & Linux Systems
- Infusion Manager
- Infusion Web Interface

While the agents reside in the systems (hosts) they monitor, the manager can be deployed either at the edge of the infrastructure or through the cloud.

Infusion Cloud Manager Deployment



Infusion Edge Manager Deployment

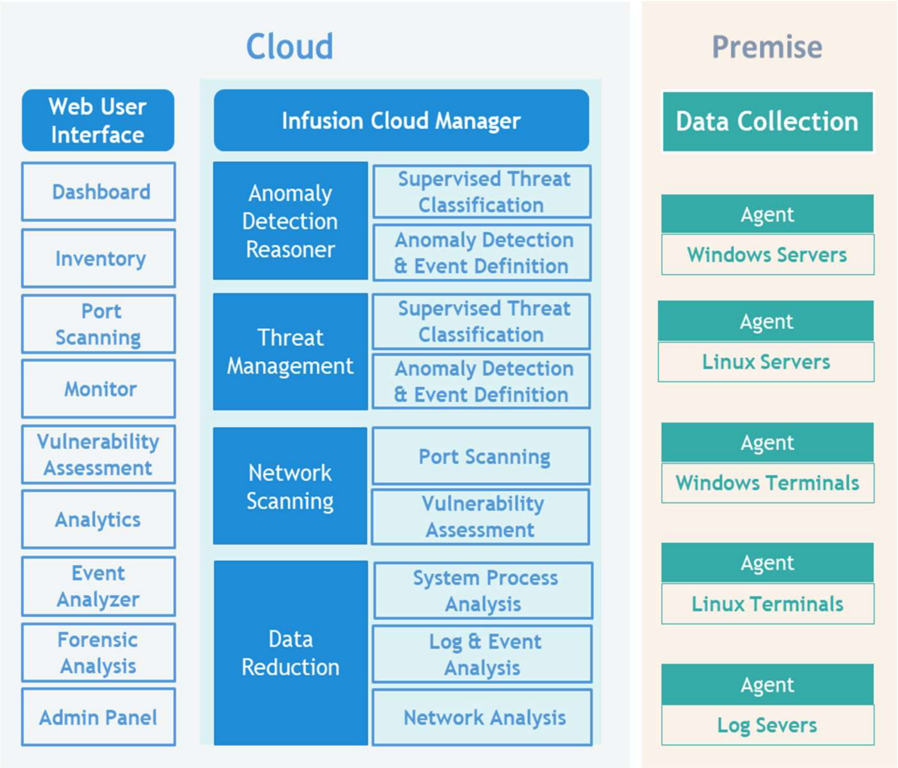


The **Agents** run seamlessly on the hosts, collecting data on every operational aspect of the system. Two types of host agents are available: **Windows Agent** and **Linux Agent** for systems running the corresponding OS. Infusion agents can also be installed on systems that take the role of a Log Server, in order to monitor and collect network-related operational information.

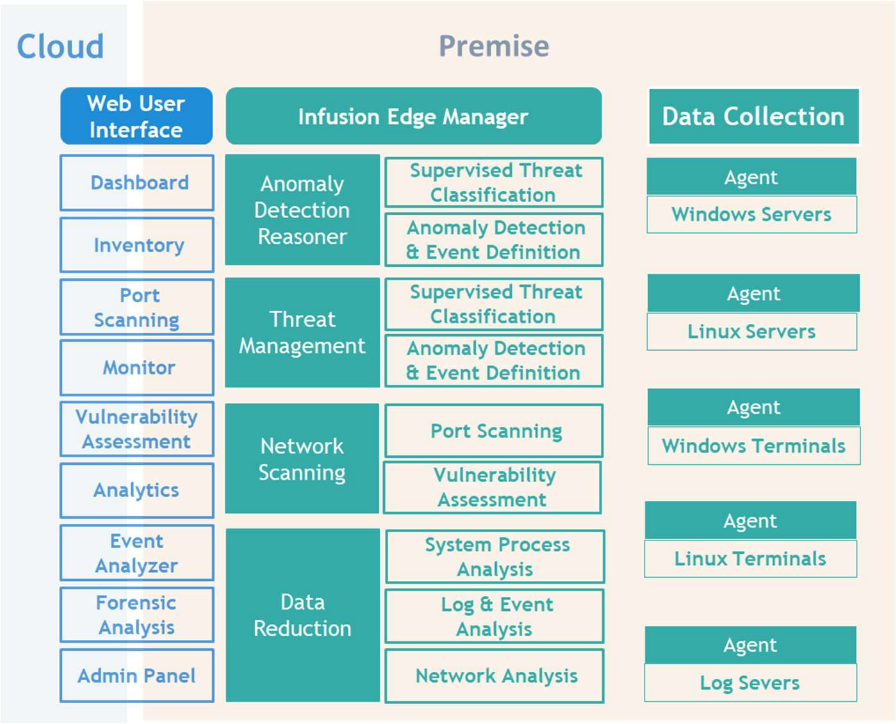
The collected data are accumulated on the **Infusion Manager** where they are processed and transformed into exploitable information. Machine learning algorithms are applied to the datasets created, so with time, the precision of the analysis increases. Besides the objective of accurately detecting anomalies and risks, a threat response framework is also realized-through reports and remedy proposals. The Infusion Manager environment can be installed on a virtual or a physical machine, residing either at the logical edge of the monitored infrastructure (Edge Manager) or in the cloud (Cloud Manager).

The **Web User Interface** is a simple, intuitive administration environment that visualizes the operational information as processed, analyzed and aggregated by the Edge Manager. The information and action proposals are presented and administered through seven functions plus a central Dashboard that aggregates important information elements. Eight application tabs correspond to these functions: Dashboard, Inventory, Port Scanning, Monitoring, Vulnerability Assessment, Analytics, Event Analyzer, Forensic Analysis and the admin panel with the relative settings options.

The Cloud Stack



The Edge Stack



The Features

Dashboard	Aggregates important information to provide an overview of the monitored infrastructure's status and a central navigation pane. • Hosts Status • Services • Events • Vulnerabilities
Inventory	Complete listing of each host's fundamentals and resources • Hardware & Software Assets. • Internal Storage. • Network.
Port Scanning	IP–based, hosts' services tracing, initiated by the Infusion Edge Manager as an agent independent, externally driven scan • Inspection of open ports. • Detection & Assessment the relative operating network services.
Monitoring	Real time status and details of system services on monitored hosts • Total Hosts & Services details • Host Status • Service Status.
Vulnerability Assessment	Agent independent, Manager initiated, scan for common, publicly defined, vulnerabilities issues (i.e. CVE® lists). Technical Reporting. • Operating System level vulnerabilities. • Services Level Vulnerabilities (http, smtp, etc.). • Report Generation.
Analytics	Real time or historical presentation of host systems' operation • Operational Performance Visualization.
Event Analyzer	Event surveillance, gathering and classification. Configuration of related alerts. Host events gathering and classification, including file integrity, log monitoring, rootcheck, and processes. Based on open standards (i.e. OSSEC toolkit). • Log analysis. • File integrity. • Windows registry monitoring. • Rootkit detection. • Support and protection on multiple operating systems. • General system info
Forensic Analysis	Real time or historical snapshots of the monitored infrastructure, with detailed information about activity and events concerning processes, services, files, logs and generally all aspects of operation. • System Score. • Status details. • Handles details. • Connections details.

Minimum System Requirements

Infusion Edge Manager

	< 20 Agents	< 100 Agents
Platform	AMD64	AMD64
CPU	2 CPUS	2 CPUS
Memory	4G	6G
–	Fully configurable per agent. 75KB per snapshot of the system. Example: Keeping 1 month of data, for five servers with one snapshot per minute: 30 days x 5 agents x 24 hours x 60 min x 75Kb = 16GB	

Windows Agent Requirements

	Minimum	Recommended
OS	Window s 7	Windows 10 or higher
Requirements	32bit/64bit	32bit/64bit
CPU	Intel i3	Intel i5
Memory	2G	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	2G	4G

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