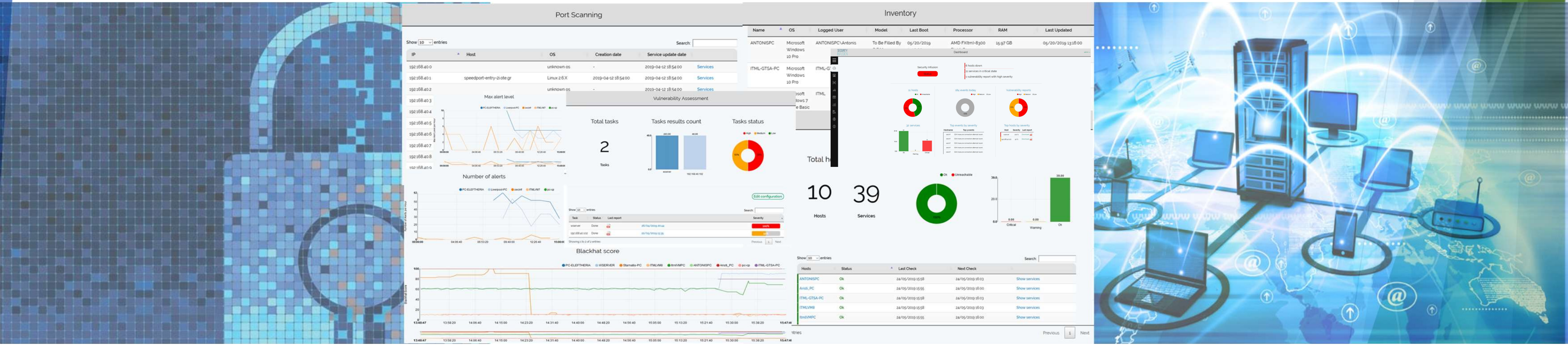
Security Infusion Presentation

March 2020



ITML - The Company

Tailor-made software solutions for cutting edge R&D and smart B2B applications

- Founded in 2011, headquartered in Athens, Greece
- Team: 25 ppl., avg. 70% annual headcount growth for the last two years
- Projected 2019 Turnover: 1.5M€, 100+% year over year sustained growth the last 2 years

Research and innovation intensity

8 Big Data ongoing projects,
ITML budget €1.4M

4 Cybersecurity ongoing projects,
ITML budget €1M

6 Smart Transportation ongoing projects,
ITML budget €1.2M

Big Data Analytics

On demand analytics
Consumer Insights
Data Fusion

Cyber Security

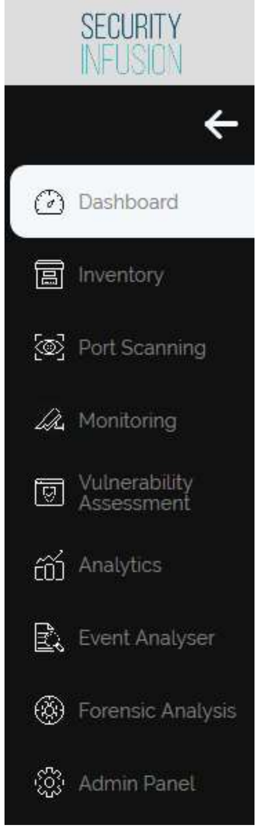
Security Information management
Cyber Security Training

Maritime Solutions

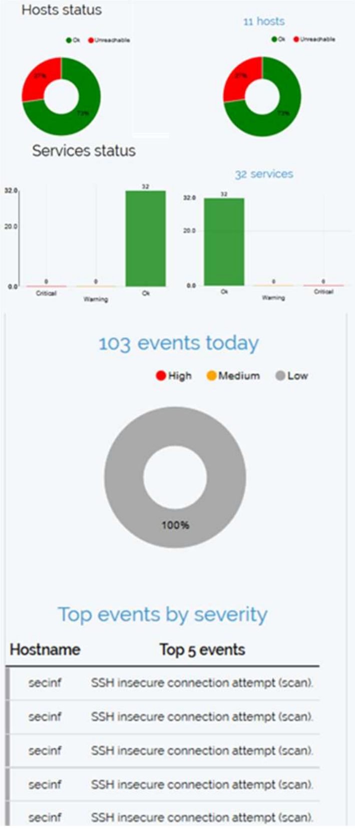
MRV Solution
Vessels Monitoring
ATMOS Cargo Heating

Security Infusion

Features



- Simple, effective and affordable Software As A Service solution for real time IT monitoring and IT security risk mitigation.
- Operational data collected by agents running on target systems (hosts)
- The Infusion Manager, deployed either through the cloud or at the edge of an organization's infrastructure, accumulates and processes collected data
- Built-in capabilities for event management, forensic analysis & vulnerability scans
- Data analytics and machine learning technologies applied for enhanced situational awareness and response



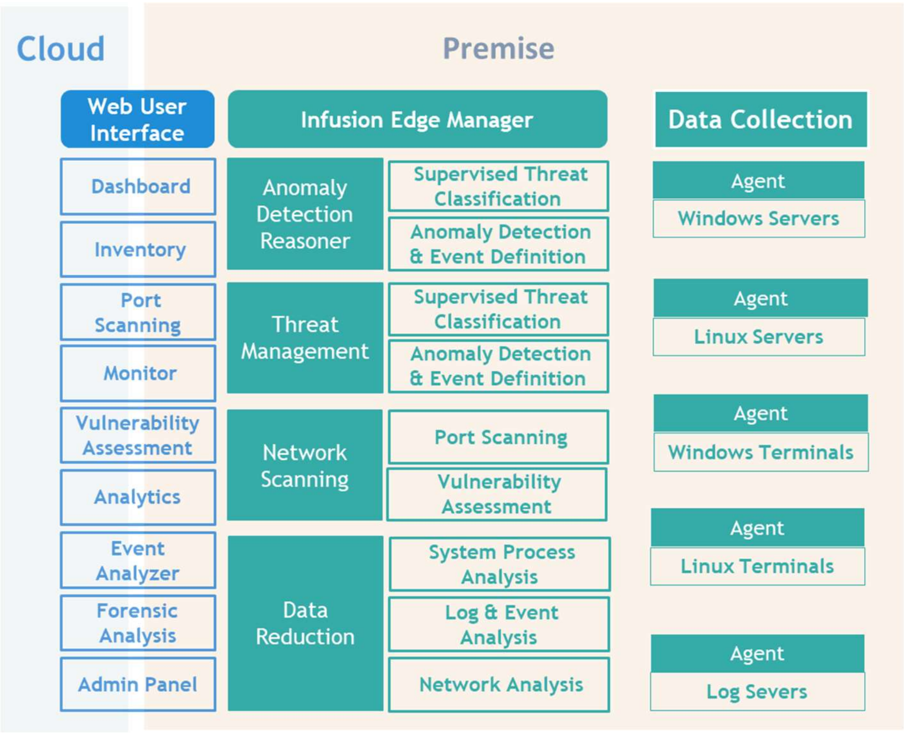
Hostname	Top 5 events
secinf	SSH insecure connection attempt (scan).
secinf	SSH insecure connection attempt (scan).
secinf	SSH insecure connection attempt (scan).
secinf	SSH insecure connection attempt (scan).
secinf	SSH insecure connection attempt (scan).

SECURITY
INFUSION

ITML

Operational Layers & Deployment : Edge & Cloud

Edge Deployment



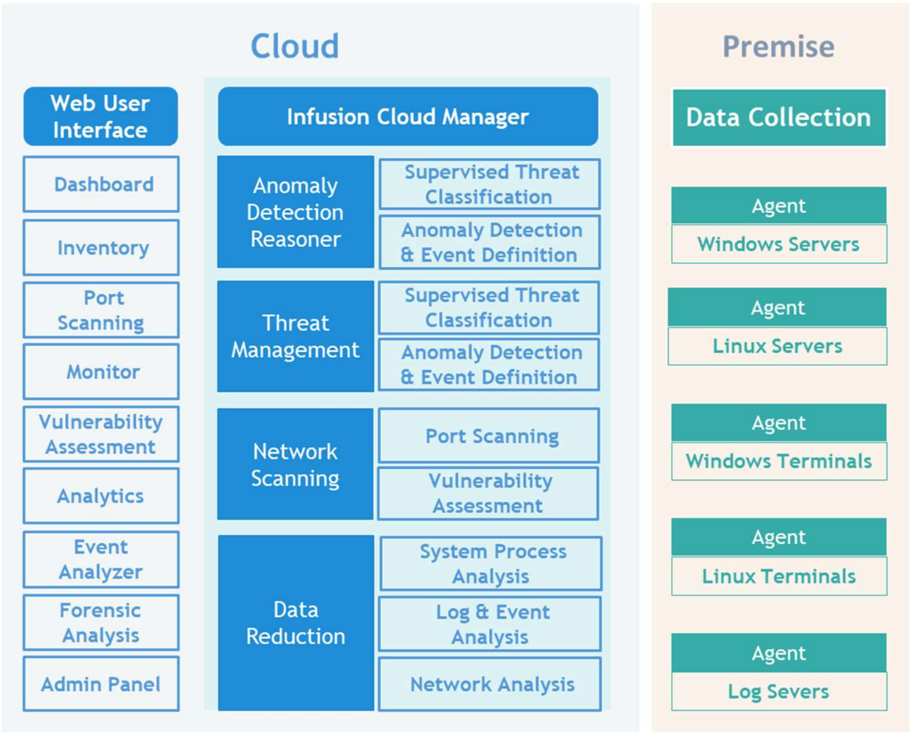
Cloud

- Web User Interface
  - Dashboard
  - Inventory
  - Port Scanning
  - Monitor
  - Vulnerability Assessment
  - Analytics
  - Event Analyzer
  - Forensic Analysis
  - Admin Panel

Premise

- Infusion Edge Manager
  - Anomaly Detection Reasoner
    - Supervised Threat Classification
    - Anomaly Detection & Event Definition
  - Threat Management
    - Supervised Threat Classification
    - Anomaly Detection & Event Definition
  - Network Scanning
    - Port Scanning
    - Vulnerability Assessment
  - Data Reduction
    - System Process Analysis
    - Log & Event Analysis
    - Network Analysis
- Data Collection
  - Agent – Windows Servers
  - Agent – Linux Servers
  - Agent – Windows Terminals
  - Agent – Linux Terminals
  - Agent – Log Severs

Cloud Deployment



Cloud

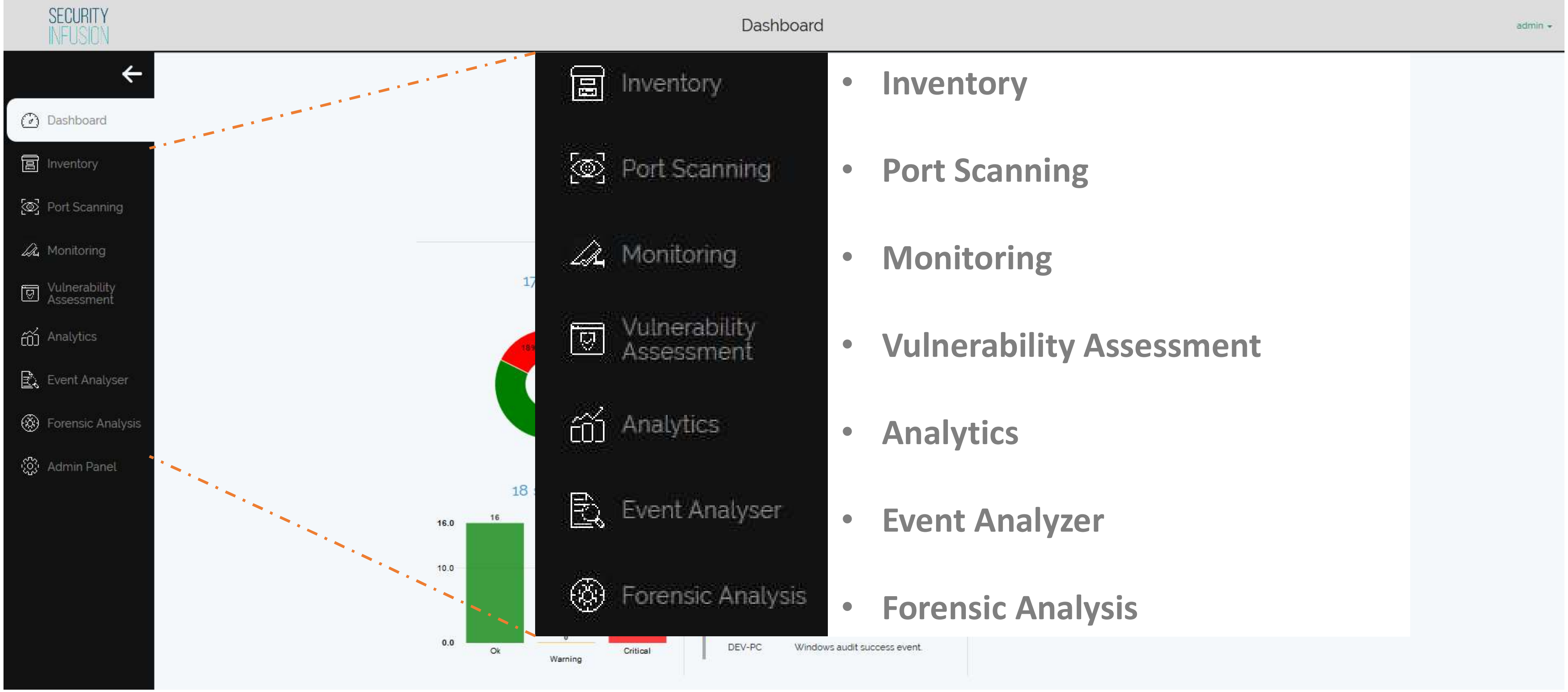
- Web User Interface
  - Dashboard
  - Inventory
  - Port Scanning
  - Monitor
  - Vulnerability Assessment
  - Analytics
  - Event Analyzer
  - Forensic Analysis
  - Admin Panel
- Infusion Cloud Manager
  - Anomaly Detection Reasoner
    - Supervised Threat Classification
    - Anomaly Detection & Event Definition
  - Threat Management
    - Supervised Threat Classification
    - Anomaly Detection & Event Definition
  - Network Scanning
    - Port Scanning
    - Vulnerability Assessment
  - Data Reduction
    - System Process Analysis
    - Log & Event Analysis
    - Network Analysis

Premise

- Data Collection
  - Agent – Windows Servers
  - Agent – Linux Servers
  - Agent – Windows Terminals
  - Agent – Linux Terminals
  - Agent – Log Severs

SECURITY
INFUSION

Functions



- Inventory
- Port Scanning
- Monitoring
- Vulnerability Assessment
- Analytics
- Event Analyzer
- Forensic Analysis

▶ Functions' Detail

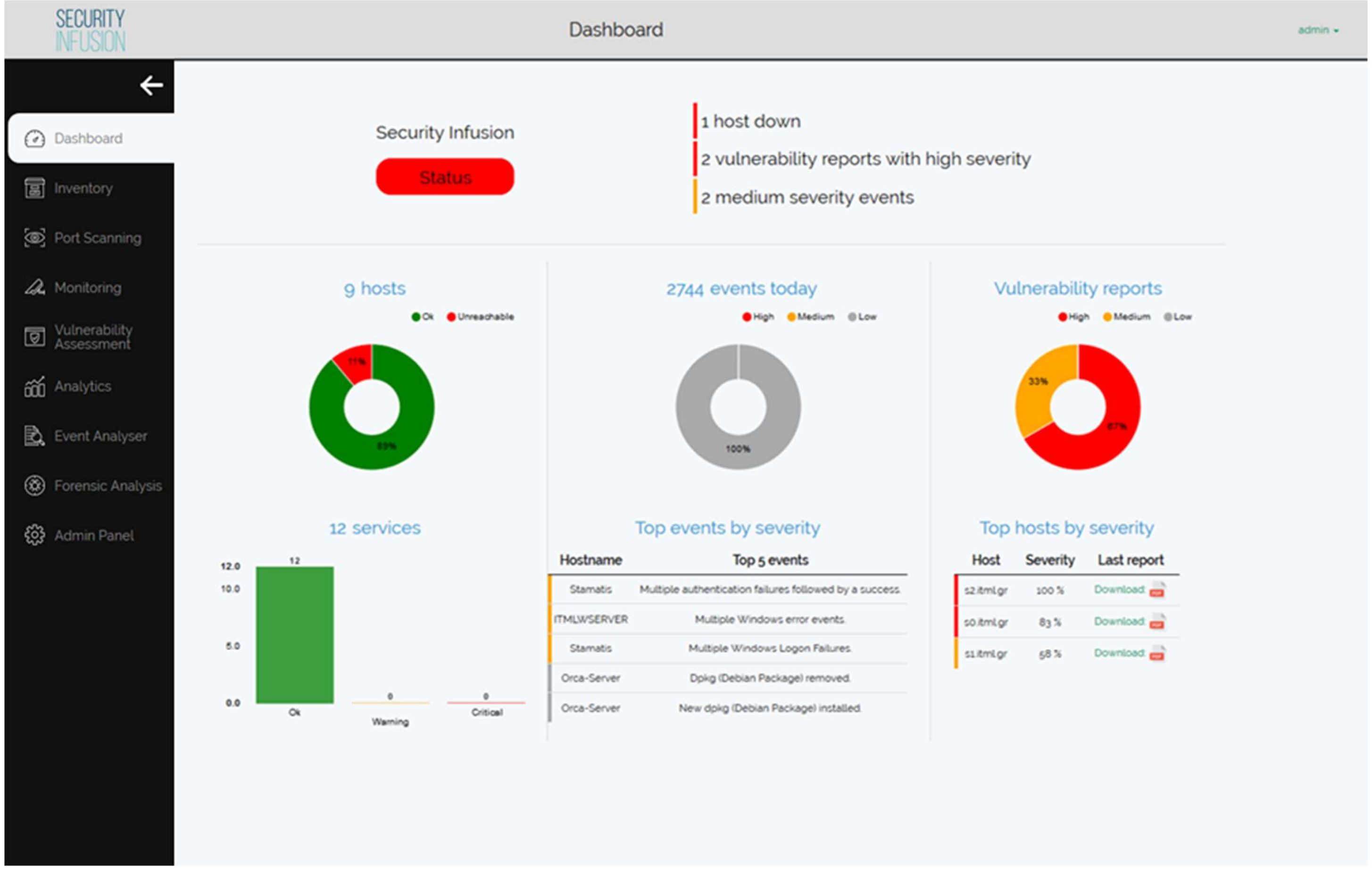
- **Inventory :** Complete listing of each host's fundamentals and resources
- **Port Scanning:** IP–based, hosts' services tracing, initiated by the Infusion Edge Manager as an agent independent, externally driven scan
- **Monitoring:** Real time status and details of system services on monitored hosts
- **Vulnerability Assessment:** Agent independent, Manager initiated, scan for common, publicly defined, vulnerabilities issues. Technical Report generation
- **Analytics:** Real time or historical presentation of host systems' operation
- **Event Analyzer:** Event surveillance, gathering and classification. Configuration of related alerts
- **Forensic Analysis:** Real time or historical, individual and group blackhat scoring. Time related System status, handles, connections and related information analysis

SECURITY INFUSION

▶ Dashboard

Aggregates important information to offer a concentrated overview of the monitored infrastructure’s status and a central navigation pane.

- Hosts Status
- Services
- Events
- Vulnerabilities



Security Infusion

1 host down

2 vulnerability reports with high severity

2 medium severity events

Top events by severity

Hostname	Top 5 events
Stamatis	Multiple authentication failures followed by a success.
ITMLWSERVER	Multiple Windows error events.
Stamatis	Multiple Windows Logon Failures.
Orca-Server	Dpkg (Debian Package) removed.
Orca-Server	New dpkg (Debian Package) installed.

Top hosts by severity

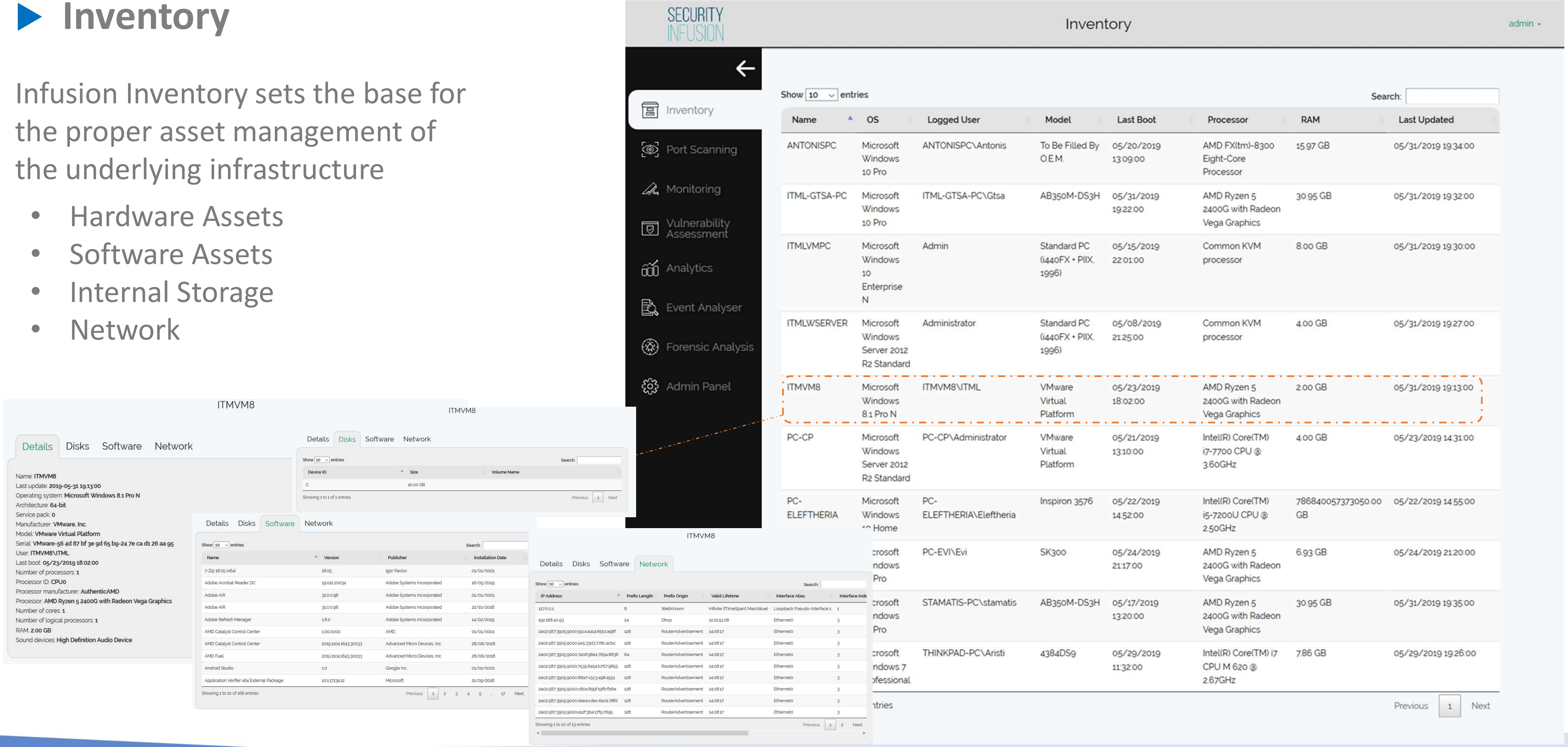
Host	Severity	Last report
s2.itml.gr	100 %	Download
s0.itml.gr	83 %	Download
s1.itml.gr	58 %	Download

SECURITY
INFUSION

Inventory

Infusion Inventory sets the base for the proper asset management of the underlying infrastructure

- Hardware Assets
- Software Assets
- Internal Storage
- Network



SECURITY INFUSION

Inventory

admin

Show 10 entries

Search:

Name	OS	Logged User	Model	Last Boot	Processor	RAM	Last Updated
ANTONISPC	Microsoft Windows 10 Pro	ANTONISPC\Antonis	To Be Filled By O.E.M.	05/20/2019 13:09:00	AMD FX(tm)-8300 Eight-Core Processor	15.97 GB	05/31/2019 19:34:00
ITML-GTSA-PC	Microsoft Windows 10 Pro	ITML-GTSA-PC\Gtsa	AB350M-DS3H	05/31/2019 19:22:00	AMD Ryzen 5 2400G with Radeon Vega Graphics	30.95 GB	05/31/2019 19:32:00
ITMLVMPC	Microsoft Windows 10 Enterprise N	Admin	Standard PC (i440FX + PIIX, 1996)	05/15/2019 22:01:00	Common KVM processor	8.00 GB	05/31/2019 19:30:00
ITMLWSERVER	Microsoft Windows Server 2012 R2 Standard	Administrator	Standard PC (i440FX + PIIX, 1996)	05/08/2019 21:25:00	Common KVM processor	4.00 GB	05/31/2019 19:27:00
ITMVM8	Microsoft Windows 8.1 Pro N	ITMVM8\ITML	VMware Virtual Platform	05/23/2019 18:02:00	AMD Ryzen 5 2400G with Radeon Vega Graphics	2.00 GB	05/31/2019 19:13:00
PC-CP	Microsoft Windows Server 2012 R2 Standard	PC-CP\Administrator	VMware Virtual Platform	05/21/2019 13:10:00	Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz	4.00 GB	05/23/2019 14:31:00
PC-ELEFTHERIA	Microsoft Windows 10 Home	PC-ELEFTHERIA\Eleftheria	Inspiron 3576	05/22/2019 14:52:00	Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz	786840057373050.00 GB	05/22/2019 14:55:00
	crosoft ndows Pro	PC-EVI\Evi	SK300	05/24/2019 21:17:00	AMD Ryzen 5 2400G with Radeon Vega Graphics	6.93 GB	05/24/2019 21:20:00
	crosoft ndows Pro	STAMATIS-PC\stamatis	AB350M-DS3H	05/17/2019 13:20:00	AMD Ryzen 5 2400G with Radeon Vega Graphics	30.95 GB	05/31/2019 19:35:00
	crosoft ndows 7 ofessional	THINKPAD-PC\Aristi	4384DS9	05/29/2019 11:32:00	Intel(R) Core(TM) i7 CPU M 620 @ 2.67GHz	7.86 GB	05/29/2019 19:26:00

ntries

Previous 1 Next

ITMVM8

Name: **ITMVM8**
Last update: **2019-05-31 19:13:00**
Operating system: **Microsoft Windows 8.1 Pro N**
Architecture: **64-bit**
Service pack: **0**
Manufacturer: **VMware, Inc.**
Model: **VMware Virtual Platform**
Serial: **VMware-56 4d 87 bf 3e 9d 65 b9-24 7e ca d1 26 aa 95**
User: **ITMVM8\ITML**
Last boot: **05/23/2019 18:02:00**
Number of processors: **1**
Processor ID: **CPU0**
Processor manufacturer: **AuthenticAMD**
Processor: **AMD Ryzen 5 2400G with Radeon Vega Graphics**
Number of cores: **1**
Number of logical processors: **1**
RAM: **2.00 GB**
Sound devices: **High Definition Audio Device**

ITMVM8

Show 10 entries

Search:

Device ID	Size	Volume Name
C:	40.00 GB	

Showing 1 to 1 of 1 entries

Previous 1 Next

Show 10 entries

Search:

Name	Version	Publisher	Installation Date
7-Zip 18.05 (x64)	18.05	Igor Pavlov	01/01/0001
Adobe Acrobat Reader DC	19.012.20034	Adobe Systems Incorporated	16/05/2019
Adobe AIR	31.0.0.96	Adobe Systems Incorporated	01/01/0001
Adobe AIR	31.0.0.96	Adobe Systems Incorporated	22/10/2018
Adobe Refresh Manager	1.8.0	Adobe Systems Incorporated	14/02/2019
AMD Catalyst Control Center	1.00.0000	AMD	01/01/0001
AMD Catalyst Control Center	2015.1104.1643.30033	Advanced Micro Devices, Inc.	28/06/2018
AMD Fuel	2015.1104.1643.30033	Advanced Micro Devices, Inc.	28/06/2018
Android Studio	1.0	Google Inc.	01/01/0001
Application Verifier x64 External Package	10.1.17134.12	Microsoft	21/09/2018

Showing 1 to 10 of 166 entries

Previous 1 2 3 4 5 … 17 Next

ITMVM8

Show 10 entries

Search:

IP Address	Prefix Length	Prefix Origin	Valid Lifetime	Interface Alias	Interface Inde
127.0.0.1	8	WellKnown	Infinite ([TimeSpan]::MaxValue)	Loopback Pseudo-Interface 1	1
192.168.40.93	24	Dhcp	12:22:51:08	Ethernet0	3
2a02:587:3905:9000:51c4:a414:65b1:a98f	128	RouterAdvertisement	14:08:17	Ethernet0	3
2a02:587:3905:9000:5e5:33d3:778c:acbc	128	RouterAdvertisement	14:08:17	Ethernet0	3
2a02:587:3905:9000:7408:98e1:769a:8838	64	RouterAdvertisement	14:08:17	Ethernet0	3
2a02:587:3905:9000:7535:6454:b767:9855	128	RouterAdvertisement	14:08:17	Ethernet0	3
2a02:587:3905:9000:88a7:c5c3:498:4551	128	RouterAdvertisement	14:08:17	Ethernet0	3
2a02:587:3905:9000:c804:899f:19fb:fb6e	128	RouterAdvertisement	14:08:17	Ethernet0	3
2a02:587:3905:9000:d4e4:cdec:6a74:78fd	128	RouterAdvertisement	14:08:17	Ethernet0	3
2a02:587:3905:9000:e12f:3ba:17f9:7695	128	RouterAdvertisement	14:08:17	Ethernet0	3

Showing 1 to 10 of 13 entries

Previous 1 2 Next

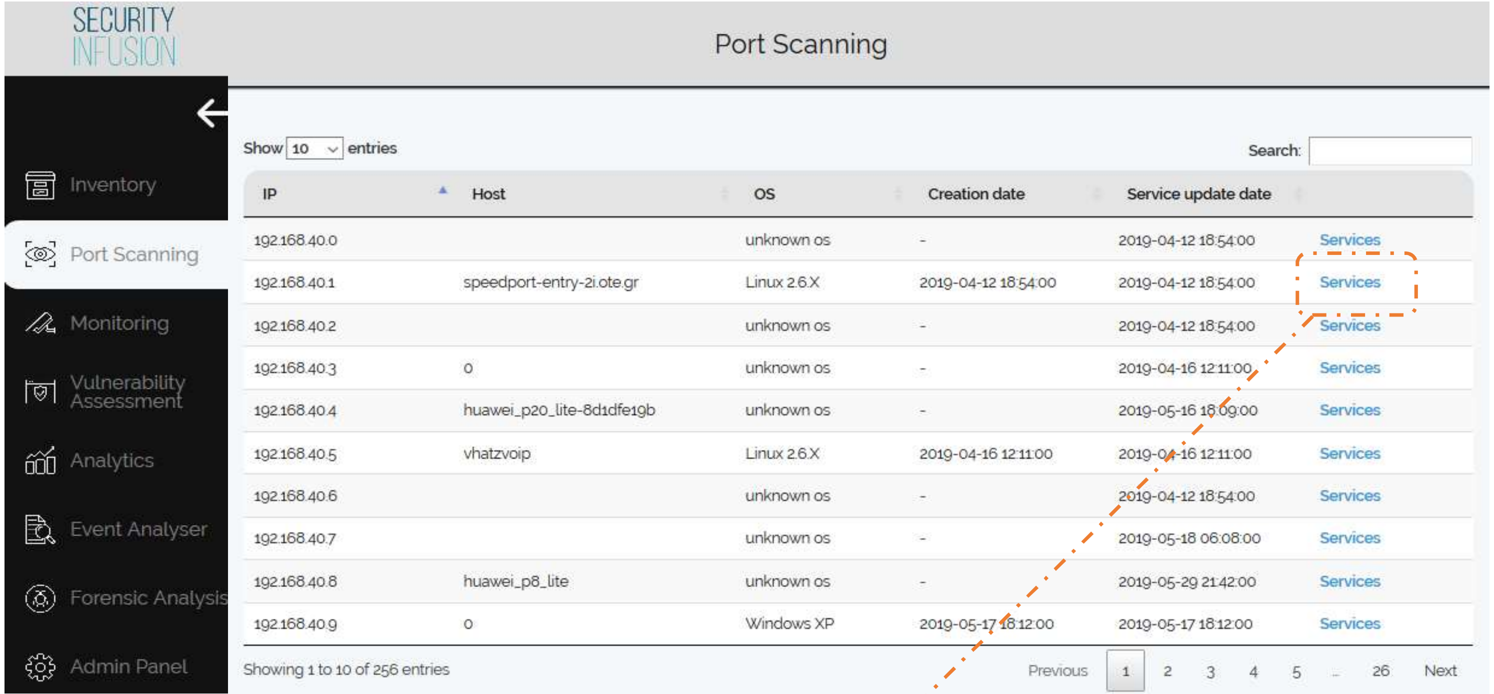
SECURITY INFUSION

ITML

Port Scanning

Ip-based, inbound scan of the LAN’s devices’ services for increased situational awareness

- Inspection of open ports
- Detection & Assessment of network services



Port Scanning

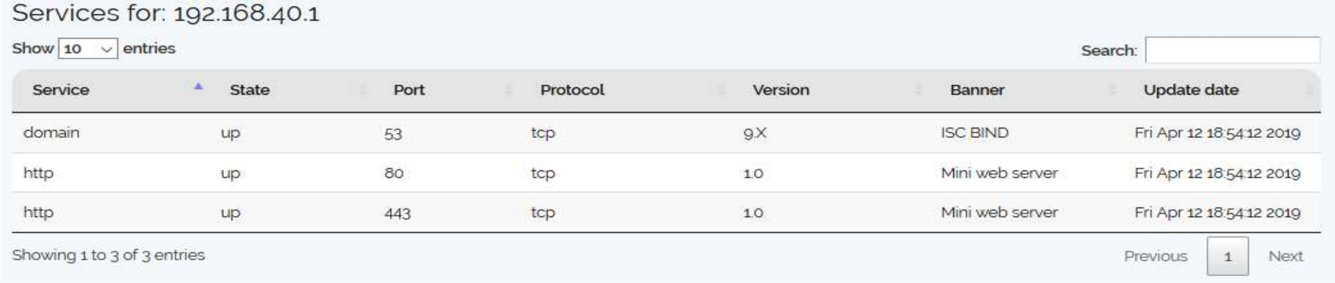
Show 10 entries

Search:

IP	Host	OS	Creation date	Service update date	
192.168.40.0		unknown os	-	2019-04-12 18:54:00	Services
192.168.40.1	speedport-entry-2i.ote.gr	Linux 2.6.X	2019-04-12 18:54:00	2019-04-12 18:54:00	Services
192.168.40.2		unknown os	-	2019-04-12 18:54:00	Services
192.168.40.3	0	unknown os	-	2019-04-16 12:11:00	Services
192.168.40.4	huawei_p20_lite-8d1dfe19b	unknown os	-	2019-05-16 18:09:00	Services
192.168.40.5	vhatzvoip	Linux 2.6.X	2019-04-16 12:11:00	2019-04-16 12:11:00	Services
192.168.40.6		unknown os	-	2019-04-12 18:54:00	Services
192.168.40.7		unknown os	-	2019-05-18 06:08:00	Services
192.168.40.8	huawei_p8_lite	unknown os	-	2019-05-29 21:42:00	Services
192.168.40.9	0	Windows XP	2019-05-17 18:12:00	2019-05-17 18:12:00	Services

Showing 1 to 10 of 256 entries

Previous 1 2 3 4 5 ... 26 Next



Services for: 192.168.40.1

Show 10 entries

Search:

Service	State	Port	Protocol	Version	Banner	Update date
domain	up	53	tcp	9.X	ISC BIND	Fri Apr 12 18:54:12 2019
http	up	80	tcp	1.0	Mini web server	Fri Apr 12 18:54:12 2019
http	up	443	tcp	1.0	Mini web server	Fri Apr 12 18:54:12 2019

Showing 1 to 3 of 3 entries

Previous 1 Next

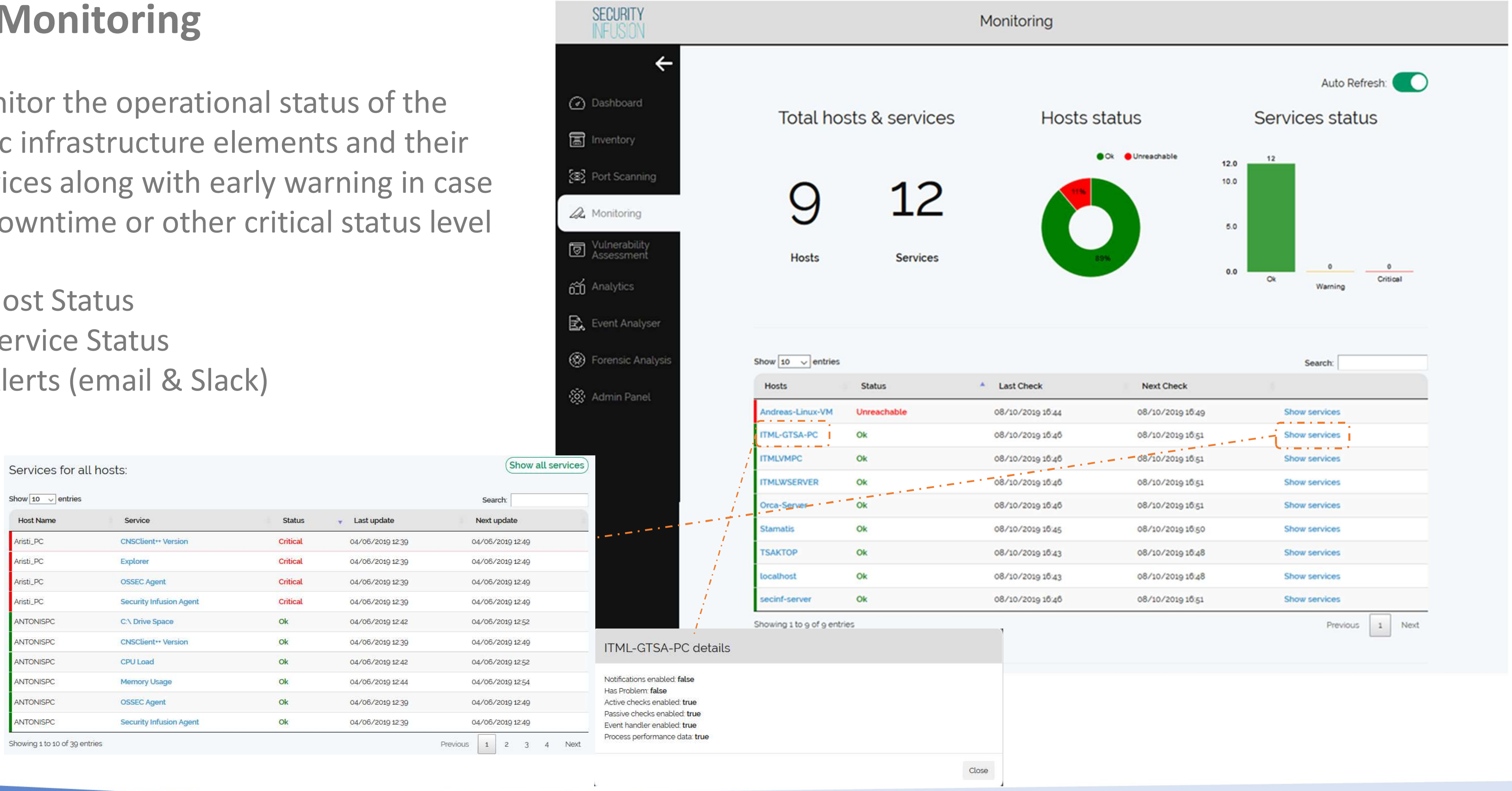
SECURITY
INFUSION

ITML

▶ Monitoring

Monitor the operational status of the basic infrastructure elements and their services along with early warning in case of downtime or other critical status level

- Host Status
- Service Status
- Alerts (email & Slack)



Show 10 entries Search:

Hosts	Status	Last Check	Next Check	
Andreas-Linux-VM	Unreachable	08/10/2019 16:44	08/10/2019 16:49	Show services
ITML-GTSA-PC	Ok	08/10/2019 16:46	08/10/2019 16:51	Show services
ITMLVMPC	Ok	08/10/2019 16:46	08/10/2019 16:51	Show services
ITMLWSERVER	Ok	08/10/2019 16:46	08/10/2019 16:51	Show services
Orca-Server	Ok	08/10/2019 16:46	08/10/2019 16:51	Show services
Stamatis	Ok	08/10/2019 16:45	08/10/2019 16:50	Show services
TSAKTOP	Ok	08/10/2019 16:43	08/10/2019 16:48	Show services
localhost	Ok	08/10/2019 16:43	08/10/2019 16:48	Show services
secinf-server	Ok	08/10/2019 16:46	08/10/2019 16:51	Show services

Showing 1 to 9 of 9 entries Previous 1 Next

Services for all hosts: Show all services

Show 10 entries Search:

Host Name	Service	Status	Last update	Next update
Aristi_PC	CNSClient++ Version	Critical	04/06/2019 12:39	04/06/2019 12:49
Aristi_PC	Explorer	Critical	04/06/2019 12:39	04/06/2019 12:49
Aristi_PC	OSSEC Agent	Critical	04/06/2019 12:39	04/06/2019 12:49
Aristi_PC	Security Infusion Agent	Critical	04/06/2019 12:39	04/06/2019 12:49
ANTONISPC	C:\ Drive Space	Ok	04/06/2019 12:42	04/06/2019 12:52
ANTONISPC	CNSClient++ Version	Ok	04/06/2019 12:39	04/06/2019 12:49
ANTONISPC	CPU Load	Ok	04/06/2019 12:42	04/06/2019 12:52
ANTONISPC	Memory Usage	Ok	04/06/2019 12:44	04/06/2019 12:54
ANTONISPC	OSSEC Agent	Ok	04/06/2019 12:39	04/06/2019 12:49
ANTONISPC	Security Infusion Agent	Ok	04/06/2019 12:39	04/06/2019 12:49

Showing 1 to 10 of 39 entries Previous 1 2 3 4 Next

ITML-GTSA-PC details

Notifications enabled: **false**
Has Problem: **false**
Active checks enabled: **true**
Passive checks enabled: **true**
Event handler enabled: **true**
Process performance data: **true**

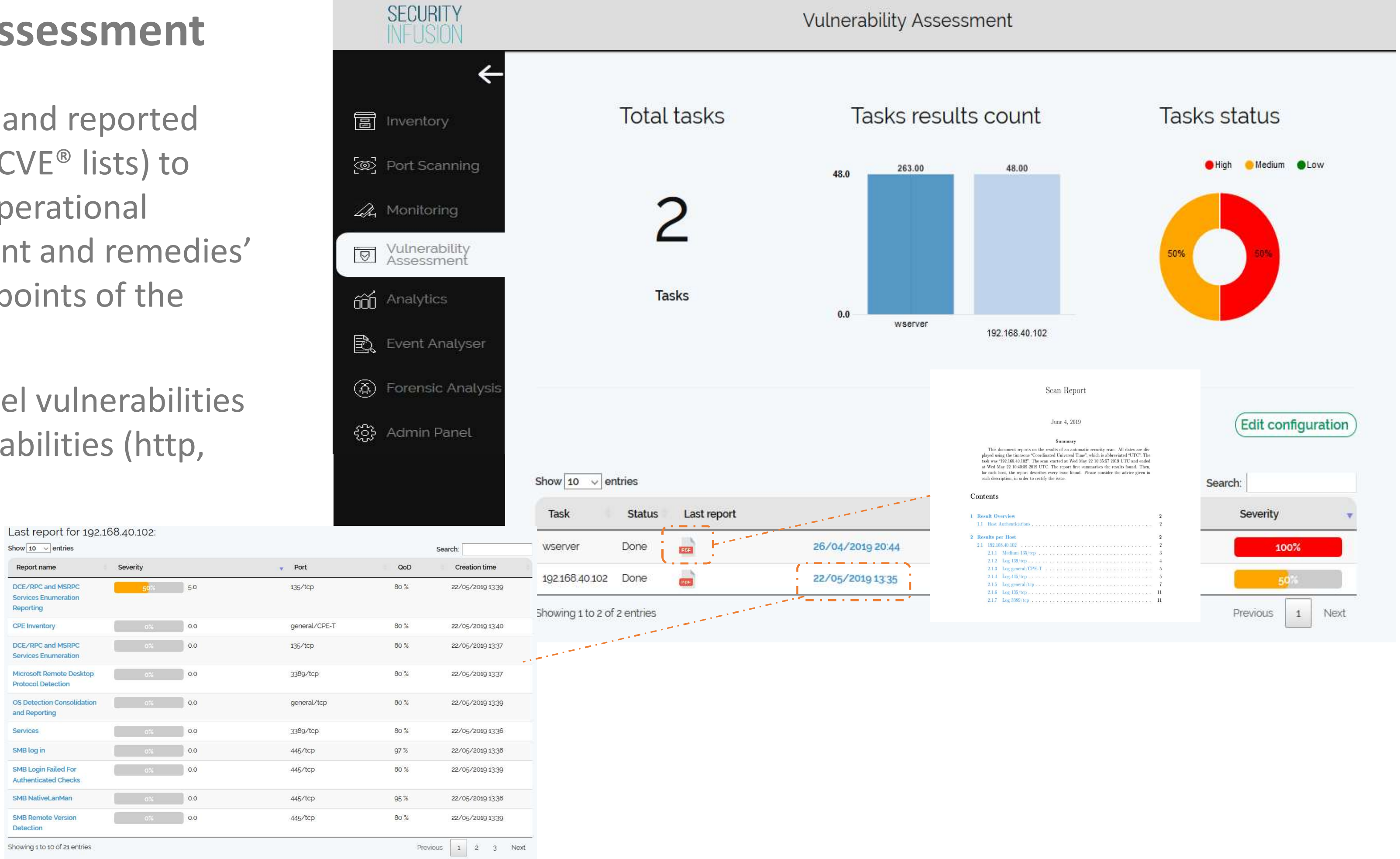
Close

SECURITY INFUSION

Vulnerability Assessment

Scan for publicly known and reported vulnerability issues (i.e. CVE® lists) to detect soft points and operational issues. Impact assessment and remedies' suggestions on the soft points of the infrastructure

- Operating System level vulnerabilities
- Services Level Vulnerabilities (http, smtp, etc.)
- Report Generation



Show 10 entries

Search:

Task	Status	Last report		Severity
wserver	Done	PDF	26/04/2019 20:44	100%
192.168.40.102	Done	PDF	22/05/2019 13:35	50%

Showing 1 to 2 of 2 entries

Previous 1 Next

Scan Report

June 4, 2019

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "192.168.40.102". The scan started at Wed May 22 10:35:57 2019 UTC and ended at Wed May 22 10:40:59 2019 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

Last report for 192.168.40.102:

Show 10 entries

Search:

Report name	Severity		Port	QoD	Creation time
DCE/RPC and MSRPC Services Enumeration Reporting	50%	5.0	135/tcp	80 %	22/05/2019 13:39
CPE Inventory	0%	0.0	general/CPE-T	80 %	22/05/2019 13:40
DCE/RPC and MSRPC Services Enumeration	0%	0.0	135/tcp	80 %	22/05/2019 13:37
Microsoft Remote Desktop Protocol Detection	0%	0.0	3389/tcp	80 %	22/05/2019 13:37
OS Detection Consolidation and Reporting	0%	0.0	general/tcp	80 %	22/05/2019 13:39
Services	0%	0.0	3389/tcp	80 %	22/05/2019 13:36
SMB log in	0%	0.0	445/tcp	97 %	22/05/2019 13:38
SMB Login Failed For Authenticated Checks	0%	0.0	445/tcp	80 %	22/05/2019 13:39
SMB NativeLanMan	0%	0.0	445/tcp	95 %	22/05/2019 13:38
SMB Remote Version Detection	0%	0.0	445/tcp	80 %	22/05/2019 13:39

Showing 1 to 10 of 21 entries

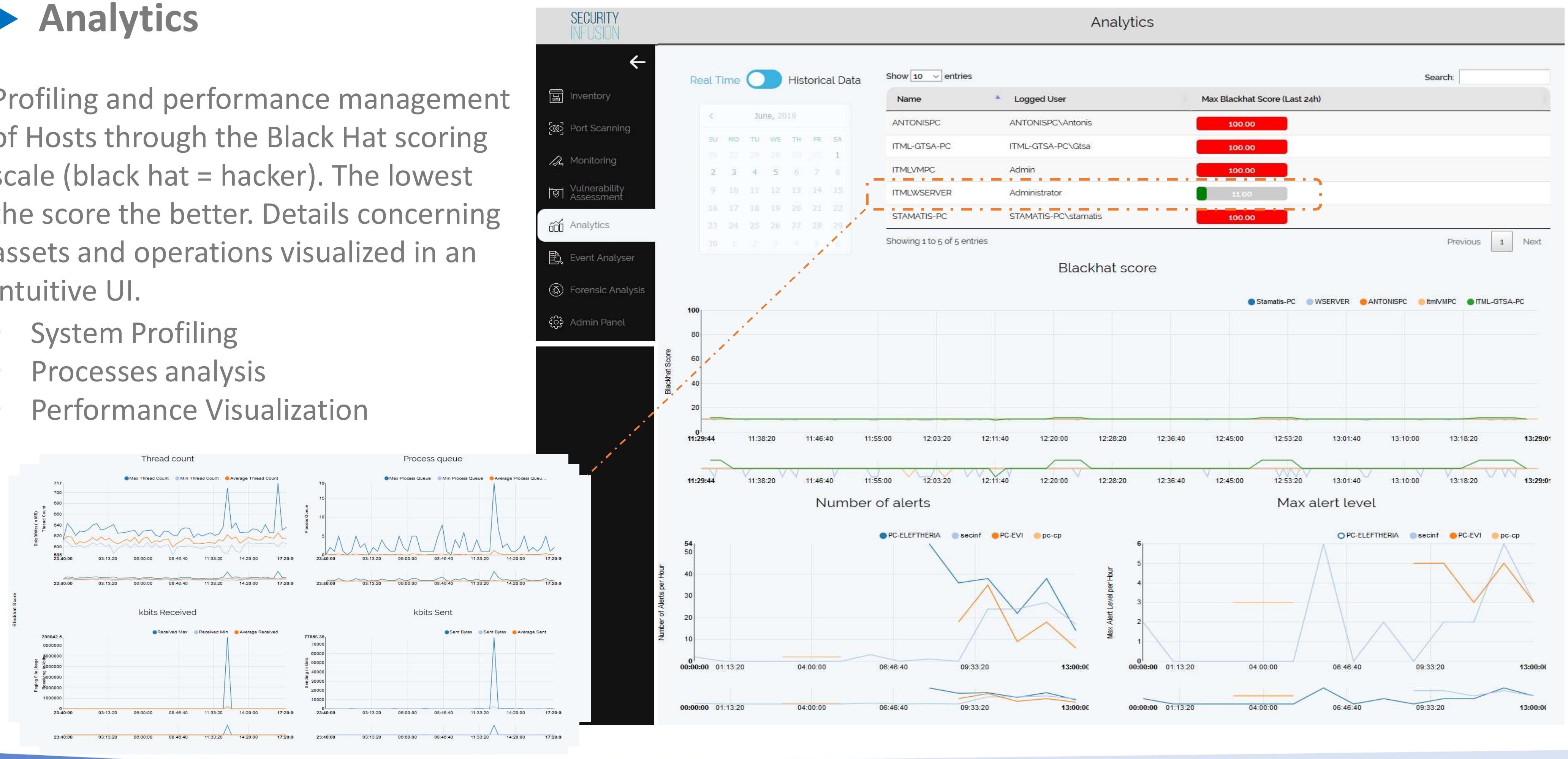
Previous 1 2 3 Next

SECURITY INFUSION

Analytics

Profiling and performance management of Hosts through the Black Hat scoring scale (black hat = hacker). The lowest the score the better. Details concerning assets and operations visualized in an intuitive UI.

- System Profiling
- Processes analysis
- Performance Visualization



Show 10 entries

Search:

Name	Logged User	Max Blackhat Score (Last 24h)
ANTONISPC	ANTONISPC\Antonis	100.00
ITML-GTSA-PC	ITML-GTSA-PC\Gtsa	100.00
ITMLVMPC	Admin	100.00
ITMLWSERVER	Administrator	11.00
STAMATIS-PC	STAMATIS-PC\stamatis	100.00

Showing 1 to 5 of 5 entries

Previous 1 Next

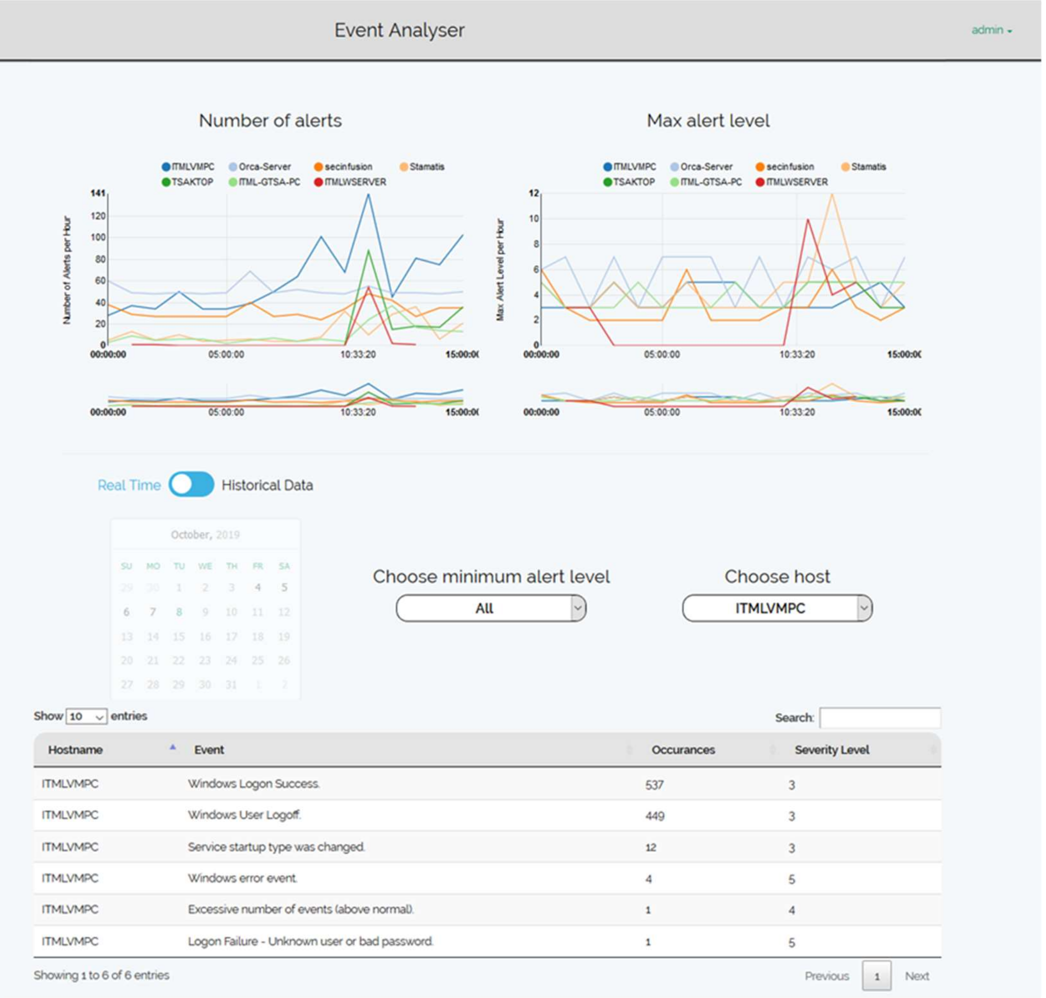
SECURITY INFUSION

ITML

Event Analyzer

Accumulation and classification of Hosts events, including file integrity, logs, rootcheck and processes. built on open components (i.e. OSSEC toolkit). Rule based alerts for active response where needed.

- log analysis
- file integrity
- Windows registry monitoring
- rootkit detection
- Support and protection on multiple operating systems



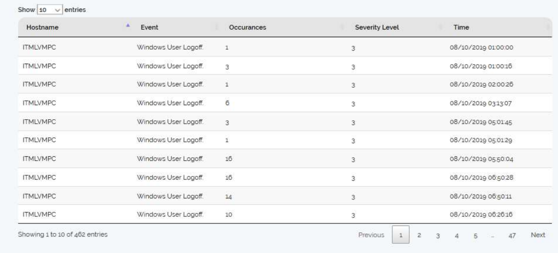
Show 10 entries

Search:

Hostname	Event	Occurances	Severity Level
ITMLVMPC	Windows Logon Success.	537	3
ITMLVMPC	Windows User Logoff.	449	3
ITMLVMPC	Service startup type was changed.	12	3
ITMLVMPC	Windows error event.	4	5
ITMLVMPC	Excessive number of events (above normal).	1	4
ITMLVMPC	Logon Failure - Unknown user or bad password.	1	5

Showing 1 to 6 of 6 entries

Previous 1 Next

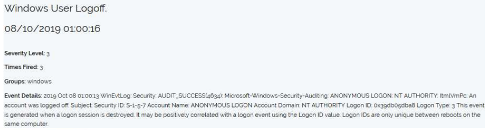


Show 10 entries

Hostname	Event	Occurances	Severity Level	Time
ITMLVMPC	Windows User Logoff.	1	3	08/10/2019 01:00:00
ITMLVMPC	Windows User Logoff.	3	3	08/10/2019 01:00:16
ITMLVMPC	Windows User Logoff.	1	3	08/10/2019 02:00:26
ITMLVMPC	Windows User Logoff.	6	3	08/10/2019 03:13:07
ITMLVMPC	Windows User Logoff.	3	3	08/10/2019 05:01:45
ITMLVMPC	Windows User Logoff.	1	3	08/10/2019 05:01:29
ITMLVMPC	Windows User Logoff.	16	3	08/10/2019 05:50:04
ITMLVMPC	Windows User Logoff.	16	3	08/10/2019 06:50:28
ITMLVMPC	Windows User Logoff.	14	3	08/10/2019 06:50:11
ITMLVMPC	Windows User Logoff.	10	3	08/10/2019 06:26:16

Showing 1 to 10 of 462 entries

Previous 1 2 3 4 5 … 47 Next



Windows User Logoff.

08/10/2019 01:00:16

Severity Level: 3

Times Fired: 3

Groups: windows

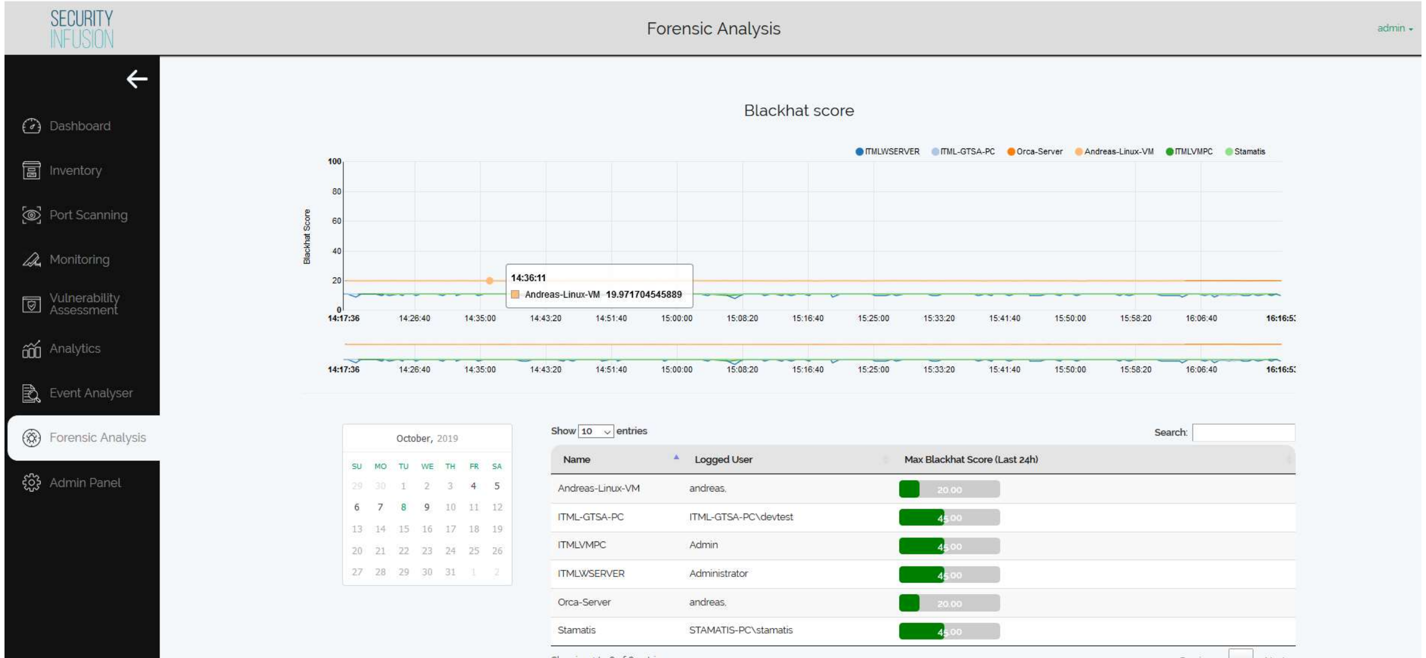
Event Details: 2019 Oct 08 01:00:13 WinEvtLog: Security: AUDIT_SUCCESS(4634): Microsoft-Windows-Security-Auditing: ANONYMOUS LOGON: NT AUTHORITY: ItmlVmPc: An account was logged off. Subject: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x39db05dba8 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.

Security Infusion

Forensic Analysis

Real time or historical snapshots of the hosts with detailed analysis on processes and features.
Allows thorough & precise retrospective on operational events & impact

- System Score
- Status
- Handles
- Connections
- General system info



October, 2019

SU	MO	TU	WE	TH	FR	SA
29	30	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2

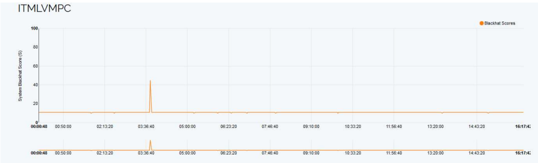
Show 10 entries

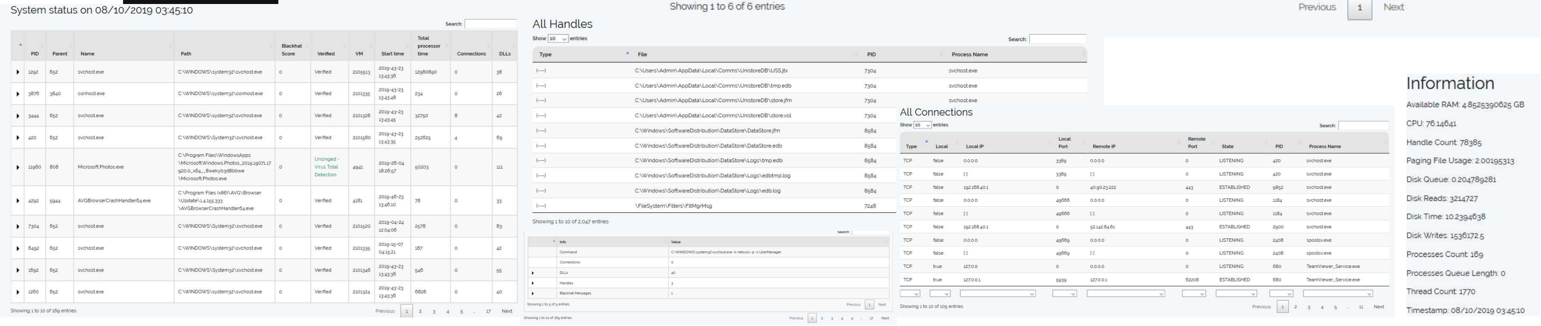
Search:

Name	Logged User	Max Blackhat Score (Last 24h)
Andreas-Linux-VM	andreas,	20.00
ITML-GTSA-PC	ITML-GTSA-PC\devtest	45.00
ITMLVMPC	Admin	45.00
ITMLWSERVER	Administrator	45.00
Orca-Server	andreas,	20.00
Stamatis	STAMATIS-PC\stamatis	45.00

Showing 1 to 6 of 6 entries

Previous 1 Next





System status on 08/10/2019 03:45:10

Search:

PID	Parent	Name	Path	Blackhat Score	Verified	VM	Start time	Total processor time	Connections	DLLs
1292	652	svchost.exe	C:\WINDOWS\system32\svchost.exe	0	Verified	2105513	2019-43-23 13:43:36	12980890	0	38
3876	3840	conhost.exe	C:\WINDOWS\system32\conhost.exe	0	Verified	2101335	2019-43-23 13:43:48	234	0	26
3444	652	svchost.exe	C:\WINDOWS\system32\svchost.exe	0	Verified	2101328	2019-43-23 13:43:45	32750	8	42
420	652	svchost.exe	C:\WINDOWS\System32\svchost.exe	0	Verified	2101580	2019-43-23 13:43:35	252625	4	69
11960	808	Microsoft.Photos.exe	C:\Program Files\WindowsApps \Microsoft.Windows.Photos_2019.19071.17920.0_x64__8wekyb3d8bbwe \Microsoft.Photos.exe	0	Unsinged - Virus Total Detection	4941	2019-26-04 18:26:57	50203	0	111
4292	5944	AVGBrowserCrashHandler64.exe	C:\Program Files (x86)\AVG\Browser \Update\1.4.155.333 \AVGBrowserCrashHandler64.exe	0	Verified	4181	2019-46-23 13:46:10	78	0	33
7304	652	svchost.exe	C:\WINDOWS\System32\svchost.exe	0	Verified	2101520	2019-04-24 12:04:06	2578	0	83
6492	652	svchost.exe	C:\WINDOWS\system32\svchost.exe	0	Verified	2101335	2019-15-07 04:15:21	187	0	42
1692	652	svchost.exe	C:\WINDOWS\System32\svchost.exe	0	Verified	2101346	2019-43-23 13:43:36	546	0	55
1260	652	svchost.exe	C:\WINDOWS\system32\svchost.exe	0	Verified	2101324	2019-43-23 13:43:36	6828	0	40

Showing 1 to 10 of 169 entries

Previous 1 2 3 4 5 … 17 Next

All Handles

Show 10 entries

Search:

Type	File	PID	Process Name
(---)	C:\Users\Admin\AppData\Local\Comms\UnistoreDB\USS.jtx	7304	svchost.exe
(---)	C:\Users\Admin\AppData\Local\Comms\UnistoreDB\tmp.edb	7304	svchost.exe
(---)	C:\Users\Admin\AppData\Local\Comms\UnistoreDB\store.jfm	7304	svchost.exe
(---)	C:\Users\Admin\AppData\Local\Comms\UnistoreDB\store.vol	7304	
(---)	C:\Windows\SoftwareDistribution\DataStore\DataStore.jfm	8584	
(---)	C:\Windows\SoftwareDistribution\DataStore\DataStore.edb	8584	
(---)	C:\Windows\SoftwareDistribution\DataStore\Logs\tmp.edb	8584	
(---)	C:\Windows\SoftwareDistribution\DataStore\Logs\edbtmp.log	8584	
(---)	C:\Windows\SoftwareDistribution\DataStore\Logs\edb.log	8584	
(---)	\FileSystem\Filters\FltMgrMsg	7248	

Showing 1 to 10 of 2,047 entries

Search:

	Info	Value
	Command	C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s UserManager
	Connections	0
▸	DLLs	40
▸	Handles	3
▸	Blackhat Messages	1

Showing 1 to 5 of 5 entries

Previous 1 Next

Showing 1 to 10 of 169 entries

Previous 1 2 3 4 5 … 17 Next

All Connections

Show 10 entries

Search:

Type	Local	Local IP	Local Port	Remote IP	Remote Port	State	PID	Process Name
TCP	false	0.0.0.0	3389	0.0.0.0	0	LISTENING	420	svchost.exe
TCP	false	[::]	3389	[::]	0	LISTENING	420	svchost.exe
TCP	false	192.168.40.1	0	40.90.23.222	443	ESTABLISHED	9852	svchost.exe
TCP	false	0.0.0.0	49666	0.0.0.0	0	LISTENING	1184	svchost.exe
TCP	false	[::]	49666	[::]	0	LISTENING	1184	svchost.exe
TCP	false	192.168.40.1	0	52.142.84.61	443	ESTABLISHED	2900	svchost.exe
TCP	false	0.0.0.0	49669	0.0.0.0	0	LISTENING	2408	spoolsv.exe
TCP	false	[::]	49669	[::]	0	LISTENING	2408	spoolsv.exe
TCP	true	127.0.0	0	0.0.0.0	0	LISTENING	680	TeamViewer_Service.exe
TCP	true	127.0.0.1	5939	127.0.0.1	62208	ESTABLISHED	680	TeamViewer_Service.exe

Showing 1 to 10 of 105 entries

Previous 1 2 3 4 5 … 11 Next

Information

Available RAM: 4.8525390625 GB

CPU: 76.14641

Handle Count: 78385

Paging File Usage: 2.00195313

Disk Queue: 0.204789281

Disk Reads: 3214727

Disk Time: 10.2394638

Disk Writes: 1536172.5

Processes Count: 169

Processes Queue Length: 0

Thread Count: 1770

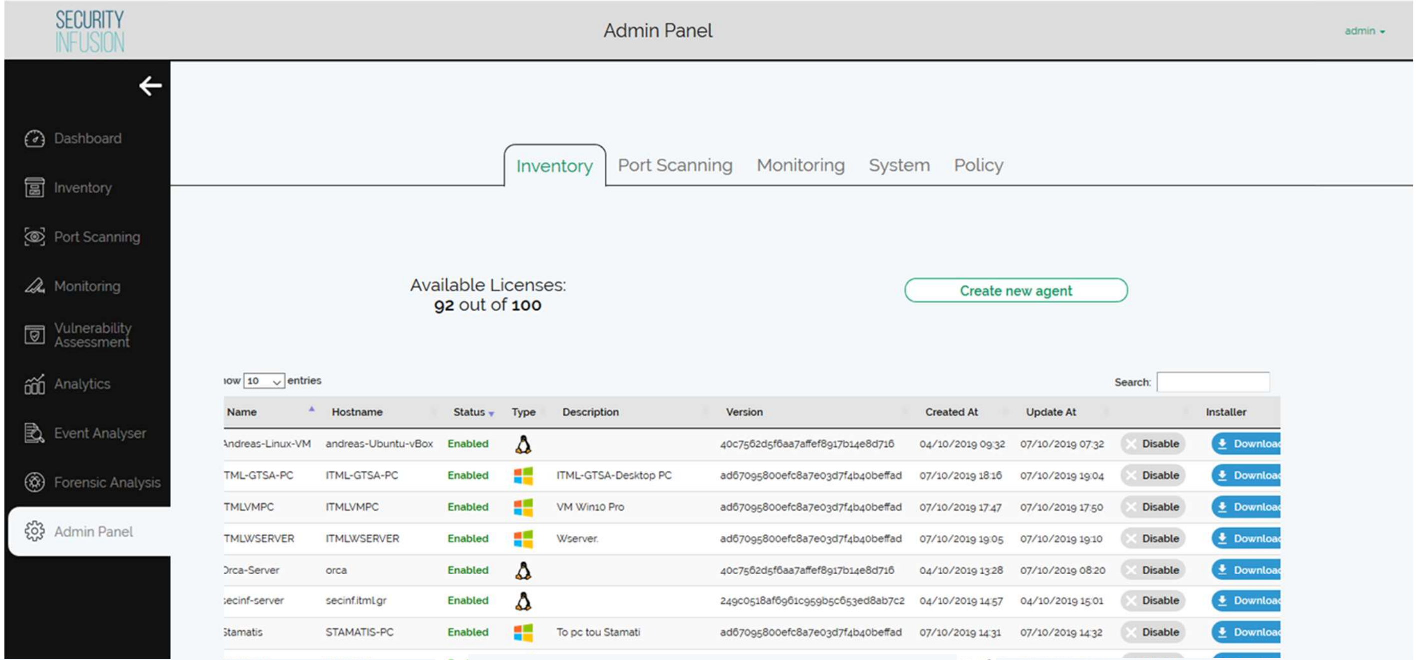
Timestamp: 08/10/2019 03:45:10

Security Infusion

▶ Administration

Manage Hosts, agents, port scanning scans, notifications, alerts and policies concerning the running of the application

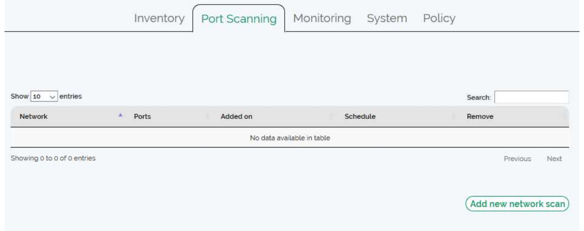
- Agents & Inventory management
- Port Scanning settings
- Monitored Services & Notifications
- Infusion System status
- Policies



Available Licenses:
92 out of 100

ıow 10 entries

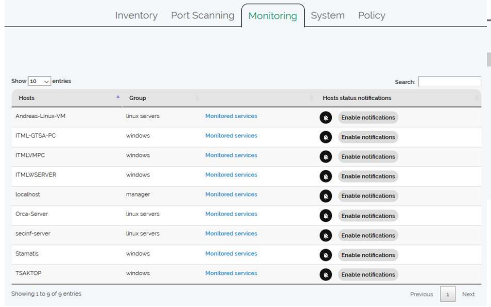
Name	Hostname	Status	Type	Description	Version	Created At	Update At		Installer
Andreas-Linux-VM	andreas-Ubuntu-vBox	Enabled	🐧		40c7562d5f6aa7affef8917b14e8d716	04/10/2019 09:32	07/10/2019 07:32	✕ Disable	Downloa
TML-GTSA-PC	ITML-GTSA-PC	Enabled	⊞	ITML-GTSA-Desktop PC	ad67095800efc8a7e03d7f4b40beffad	07/10/2019 18:16	07/10/2019 19:04	✕ Disable	Downloa
TMLVMPC	ITMLVMPC	Enabled	⊞	VM Win10 Pro	ad67095800efc8a7e03d7f4b40beffad	07/10/2019 17:47	07/10/2019 17:50	✕ Disable	Downloa
TMLWSERVER	ITMLWSERVER	Enabled	⊞	Wserver.	ad67095800efc8a7e03d7f4b40beffad	07/10/2019 19:05	07/10/2019 19:10	✕ Disable	Downloa
Orca-Server	orca	Enabled	🐧		40c7562d5f6aa7affef8917b14e8d716	04/10/2019 13:28	07/10/2019 08:20	✕ Disable	Downloa
secinf-server	secinf.itml.gr	Enabled	🐧		249c0518af6961c959b5c653ed8ab7c2	04/10/2019 14:57	04/10/2019 15:01	✕ Disable	Downloa
Stamatis	STAMATIS-PC	Enabled	⊞	To pc tou Stamati	ad67095800efc8a7e03d7f4b40beffad	07/10/2019 14:31	07/10/2019 14:32	✕ Disable	Downloa
		Enal					2019 08:		



Show 10 entries

Network	Ports	Added on	Schedule	Remove
No data available in table				

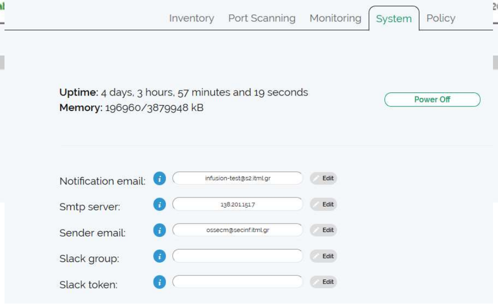
Showing 0 to 0 of 0 entries



Show 10 entries

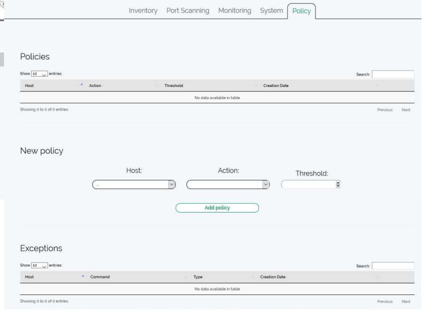
Hosts	Group		Hosts status notifications
Andreas-Linux-VM	linux servers	Monitored services	Enable notifications
ITML-GTSA-PC	windows	Monitored services	Enable notifications
ITMLVMPC	windows	Monitored services	Enable notifications
ITMLWSERVER	windows	Monitored services	Enable notifications
localhost	manager	Monitored services	Enable notifications
Orca-Server	linux servers	Monitored services	Enable notifications
secinf-server	linux servers	Monitored services	Enable notifications
Stamatis	windows	Monitored services	Enable notifications
TSAKTOP	windows	Monitored services	Enable notifications

Showing 1 to 9 of 9 entries



Uptime: 4 days, 3 hours, 57 minutes and 19 seconds
Memory: 196960/3879948 kB

Notification email: infusion-test@s2.itml.gr
Smtp server: 138.201.151.7
Sender email: ossecm@secinf.itml.gr
Slack group:
Slack token:



Policies

Show 10 entries

Host	Action	Threshold	Creation Date
No data available in table			

Showing 0 to 0 of 0 entries

New policy

Host: Action: Threshold:

Exceptions

Show 10 entries

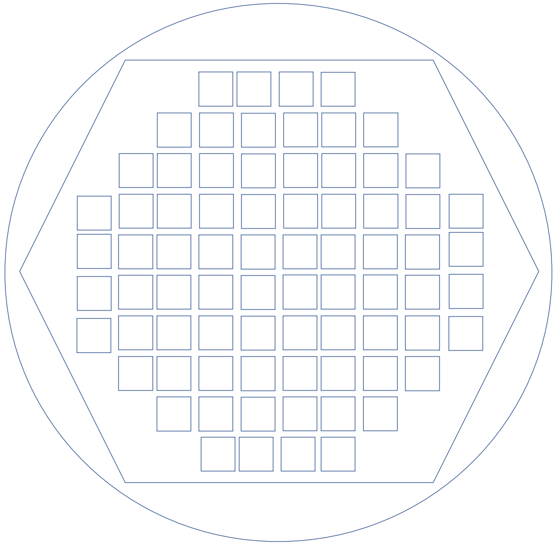
Host	Command	Type	Creation Date
No data available in table			

Showing 0 to 0 of 0 entries

SECURITY
INFUSION

ITML

SECURITY
INFUSION



ITML