SECRICOM

Seamless Communication for Crisis Management

Presentation for Final Conference Communication infrastructure security monitoring and control centre

26th April 2012

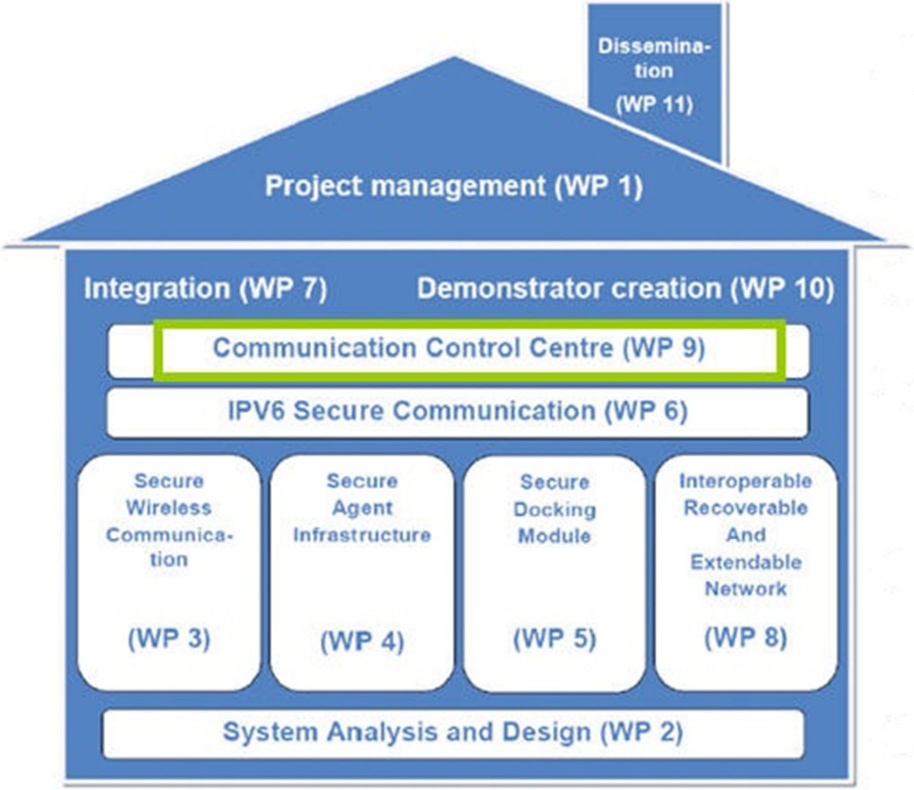
Nextel S.A.

Ingeniería y Consultoría

SEVENTH FRAMEWORK PROGRAMME

Contents

- ★ Work organization
- ★ Objectives and challenges
- ★ Tasks overview
- ★ Achievements
- ★ Conclusions


Dissemination (WP 11)
Project management (WP 1)
Integration (WP 7)
Demonstrator creation (WP 10)
Communication Control Centre (WP 9)
IPV6 Secure Communication (WP 6)
Secure Wireless Communication (WP 3)
Secure Agent Infrastructure (WP 4)
Secure Docking Module (WP 5)
Interoperable Recoverable And Extendable Network (WP 8)
System Analysis and Design (WP 2)

Work organization

- Duration: 12 months, M21 to M34
- WP Leader — Nextel S.A. Ingeniería y Consultoría
- Task leaders
  - T9.1 — iTTi e-technologies & business
  - T9.2 — ARDACO
  - T9.3 — Nextel S.A. Ingeniería y Consultoría
- Task supporters — BRITISH APCO, bumar, GEOTHERMAL ANYWHERE

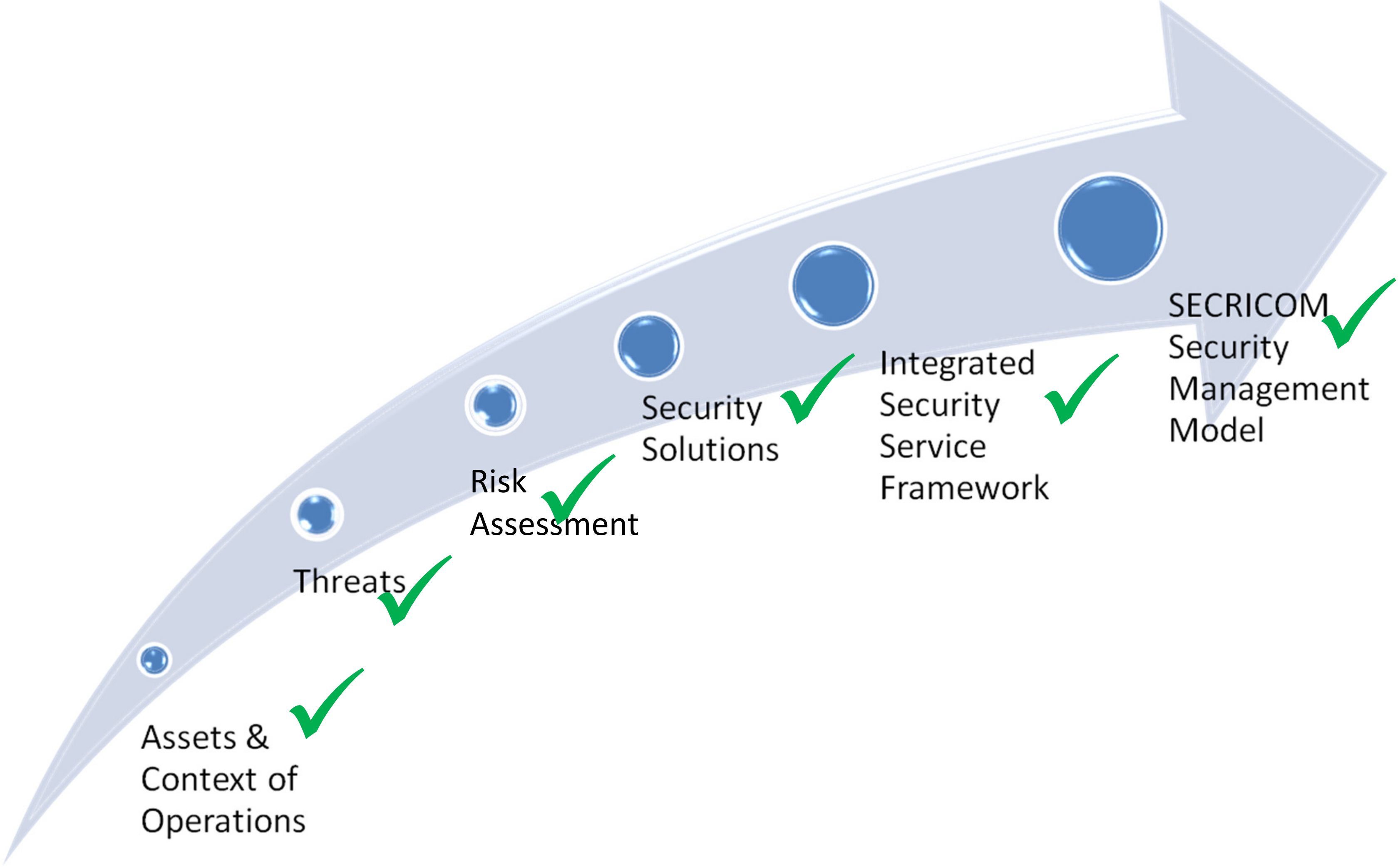
Objectives and challenges

- Technological
  - Design a **Security Model** suitable for secure and interoperable communications under crisis.
  - Research challenges for SECRICOM information security management solutions:
    - Heterogeneous communication infrastructure from independent civil forces
    - Border cross distributed interoperable infrastructures in cooperation
    - Dynamically reconfigurable security settings for diverse communication-data exchange contexts
    - Seamless operation for the end-users
- Pragmatic
  - Challenges of engaging with end users in such a way that **meaningful requirements** were obtained

Security model approach

- Intelligent security framework and middleware services for adaptive information security management.
  - Increased scope for asset protection: information protection mechanisms, access control and usage policies, scalable network architecture, auditing tools, and security assurance monitoring.
  - Improved detection and network forensic solutions: new traffic patterns and enhanced event correlation mechanism.
  - Enhanced reaction for hostile environments: control mechanisms for traffic blocking, alternative routing and isolation.
  - Fast recovery for crisis critical communications: quick and efficient recovering plans and mechanisms.

Security Roadmap



Assets & Context of Operations ✓

Threats ✓

Risk Assessment ✓

Security Solutions ✓

Integrated Security Service Framework ✓

SECRICOM Security Management Model ✓

Tasks breakdown

- T9.1 Threat analysis and challenges for dynamic heterogeneous communication infrastructure domains
- T9.2 Security Mechanisms and Protocols
- T9.3 Security Model and Service Definition

T9.1 Threat analysis and challenges

- Overview
  - Analyze SECRICOM security framework and potential security threats and perform a risk assessment
- Deliverables
  - D9.1 SECRICOM Security requirements (M34)

T9.1 Achievements	
SECRICOM system operation analysis.	✓
SECRICOM critical networking, information and operational assets analysis.	✓
Threats identified, Vulnerabilities analysis, risk assessment, risk treatment requirements & security management requirements available.	✓
SECRICOM communications continuity plan established	✓

- Highlights: Users oriented security workshop’s resulting report

T9.2 Security Mechanisms and Protocols

- Overview
  - Define enhanced security policy mechanisms for multi-domain environments
- Deliverables
  - D9.2 SECRICOM Security Mechanisms and protocols (M34)

T9.2 Achievements	FR
Security requirements analysis	✓
Security mechanisms and protocol specification delivered	✓

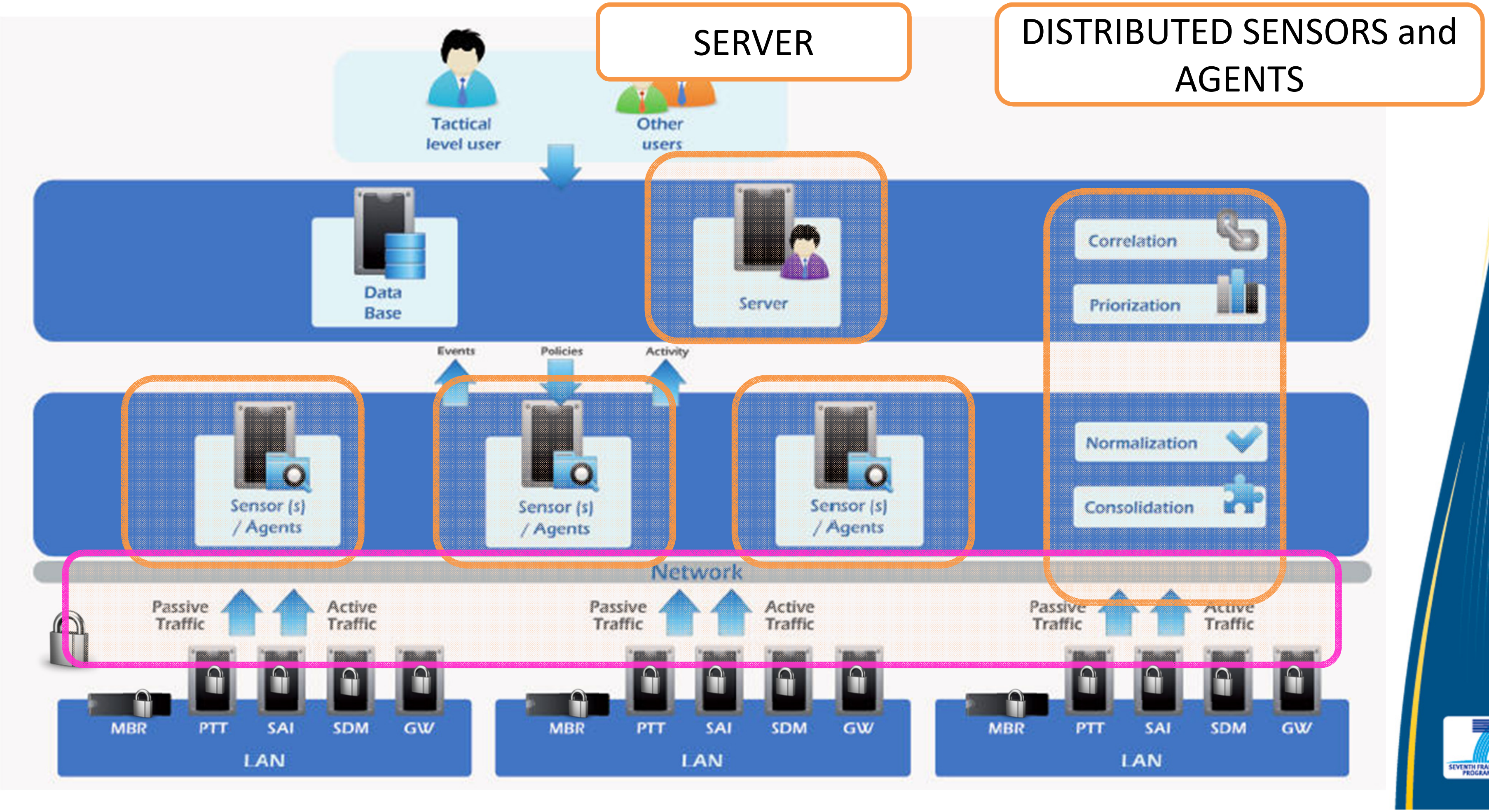
T9.3 Security Model and Service

- Overview
  - Enhance security management automation
  - Information consolidation middleware for enhanced recovery and fast reaction of critical communications
- Deliverables
  - D9.3 SECRICOM Security Model Definition (M34)

T9.3 Achievements	
Security model specification	✓
Security model supporting tool	✓

Achievements

★Basic and coherent approach to information security management model

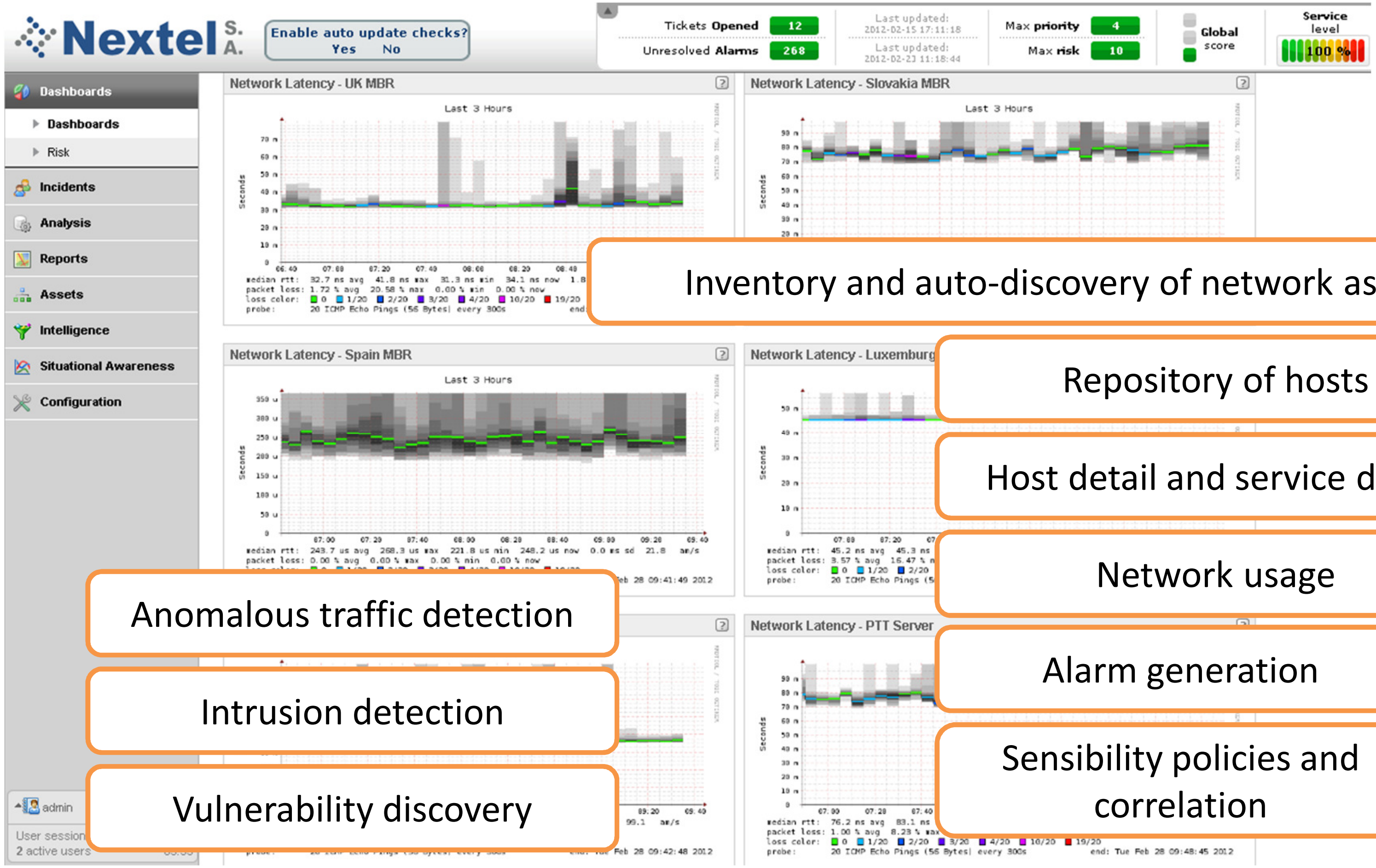


SERVER

DISTRIBUTED SENSORS and AGENTS

Achievements

- ★ Security Monitoring and Control Centre SW



Inventory and auto-discovery of network assets

Repository of hosts

Host detail and service detail

Network usage

Alarm generation

Sensibility policies and correlation

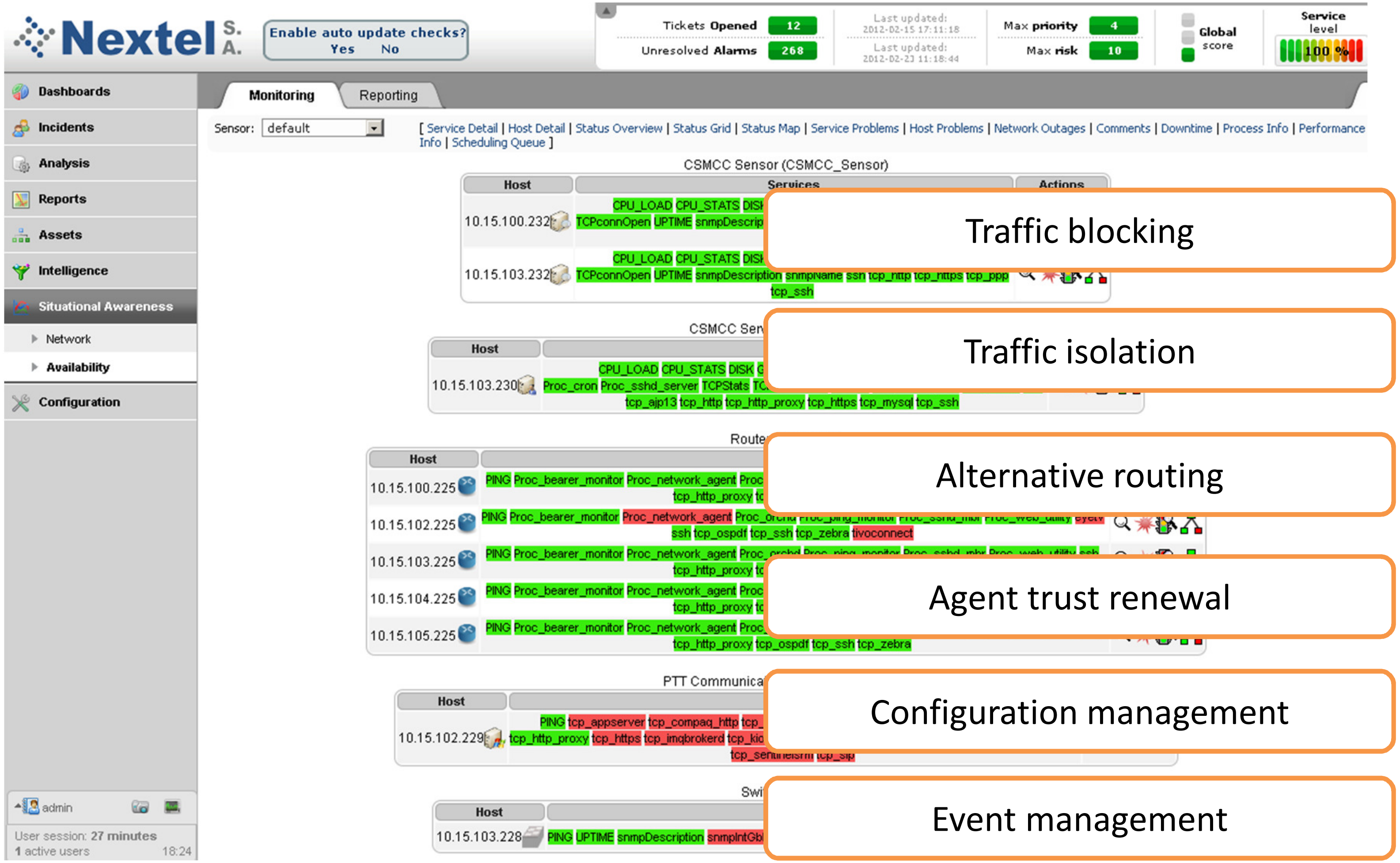
Anomalous traffic detection

Intrusion detection

Vulnerability discovery

Achievements

★Security awareness and control services



CSMCC Sensor (CSMCC_Sensor)

Host	Services	Actions
10.15.100.232	CPU_LOAD CPU_STATS DISK TCPconnOpen UPTIME snmpDescrip	
10.15.103.232	CPU_LOAD CPU_STATS DISK TCPconnOpen UPTIME snmpDescription snmpName ssh tcp_http tcp_https tcp_ppp tcp_ssh	

CSMCC Ser

Host	
10.15.103.230	CPU_LOAD CPU_STATS DISK G Proc_cron Proc_sshd_server TCPStats TC tcp_ajp13 tcp_http tcp_http_proxy tcp_https tcp_mysql tcp_ssh

Route

Host	
10.15.100.225	PING Proc_bearer_monitor Proc_network_agent Proc tcp_http_proxy tc
10.15.102.225	PING Proc_bearer_monitor Proc_network_agent Proc_orchd Proc_ping_monitor Proc_sshd_mbr Proc_web_utility eyetv ssh tcp_ospdf tcp_ssh tcp_zebra tivoconnect
10.15.103.225	PING Proc_bearer_monitor Proc_network_agent Proc_orchd Proc_ping_monitor Proc_sshd_mbr Proc_web_utility ssh tcp_http_proxy tc
10.15.104.225	PING Proc_bearer_monitor Proc_network_agent Proc tcp_http_proxy tc
10.15.105.225	PING Proc_bearer_monitor Proc_network_agent Proc tcp_http_proxy tcp_ospdf tcp_ssh tcp_zebra

PTT Communica

Host	
10.15.102.229	PING tcp_appserver tcp_compaq_http tcp_ tcp_http_proxy tcp_https tcp_imqbrokerd tcp_kid tcp_sentinelsrm tcp_sip

Swi

Host	
10.15.103.228	PING UPTIME snmpDescription snmpIntGbl

Traffic blocking

Traffic isolation

Alternative routing

Agent trust renewal

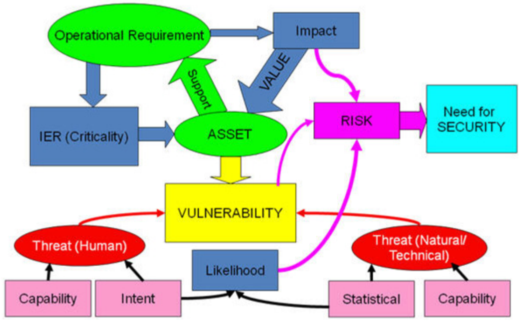
Configuration management

Event management

Achievements

- Cross-check risk analysis and requirements with end-users

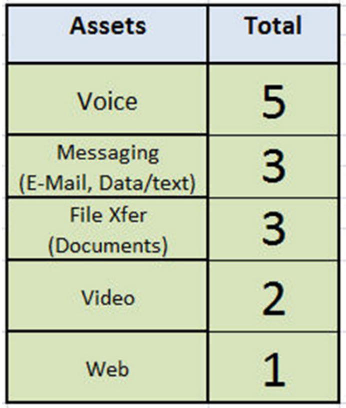
- Methodology
  - Risk assessment process to security requirements
  - From Information Exchange Requirements to Assets identification
  - Discussion towards expected results



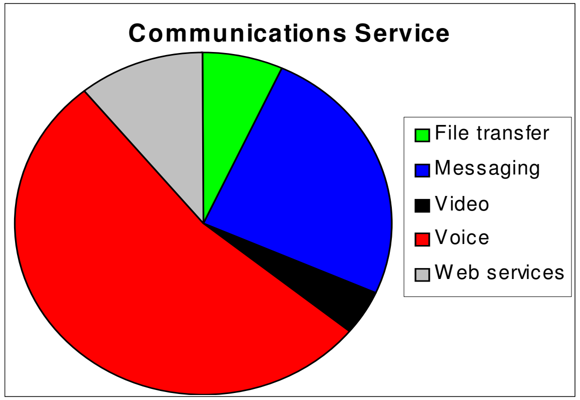
Assets	Strategic			Tactical			Operational		
	Confidentiality	Integrity	Availability	Confidentiality	Integrity	Availability	Confidentiality	Integrity	Availability
File Xfer (Documents)									
Messaging (E-Mail, Data/text)									
Video									
Voice									
Web									

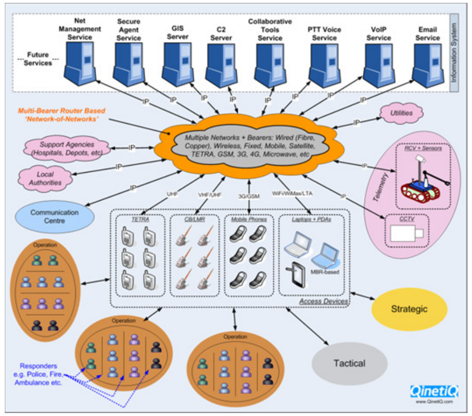
Achievements

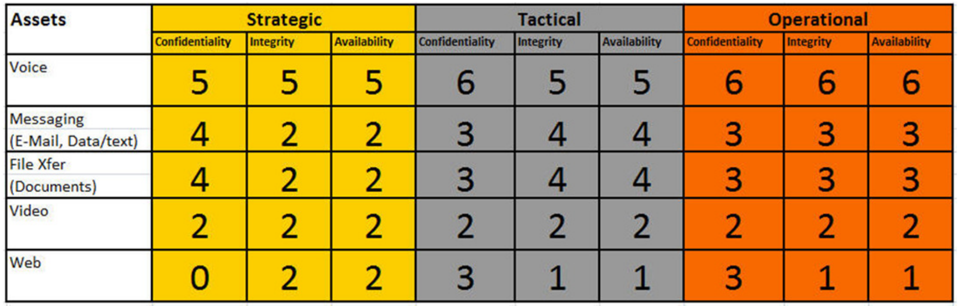
- ★Cross-check risk analysis and requirements with end-users



Assets	Total
Voice	5
Messaging (E-Mail, Data/text)	3
File Xfer (Documents)	3
Video	2
Web	1





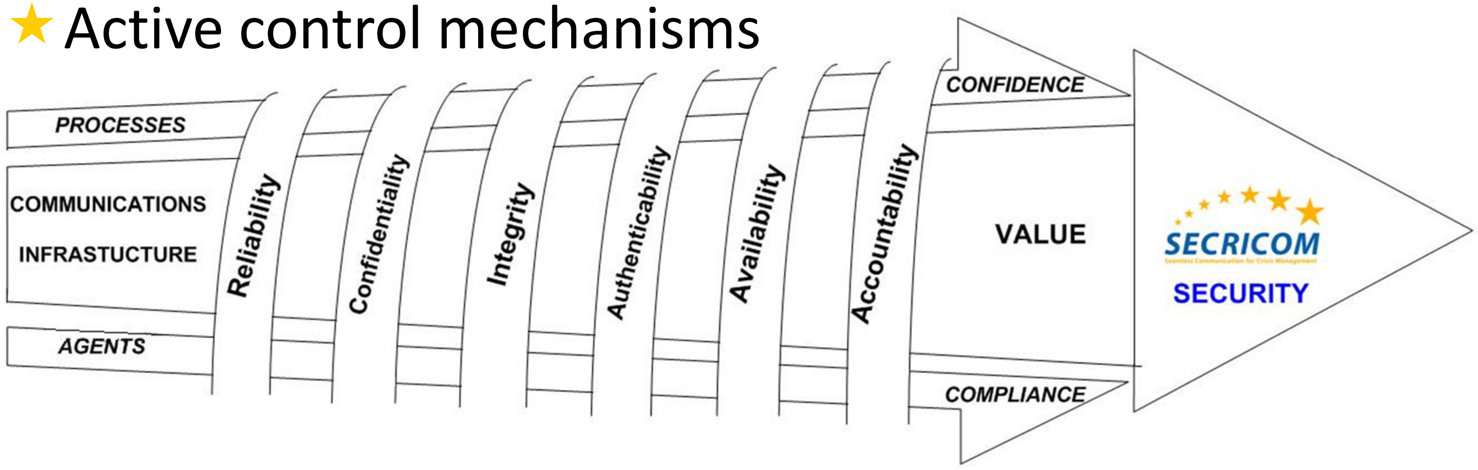


Assets	Strategic			Tactical			Operational		
	Confidentiality	Integrity	Availability	Confidentiality	Integrity	Availability	Confidentiality	Integrity	Availability
Voice	5	5	5	6	5	5	6	6	6
Messaging (E-Mail, Data/text)	4	2	2	3	4	4	3	3	3
File Xfer (Documents)	4	2	2	3	4	4	3	3	3
Video	2	2	2	2	2	2	2	2	2
Web	0	2	2	3	1	1	3	1	1

Conclusions

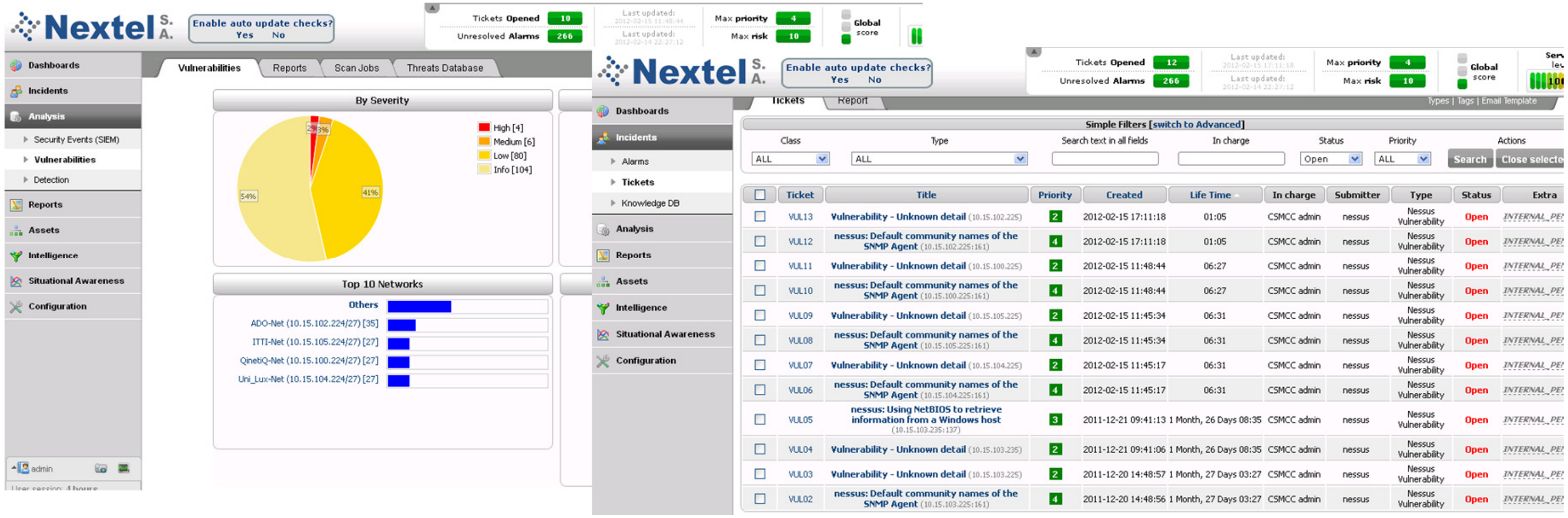
- SECRICOM system operation analysis ✓
  - Threats identification and security management requirements
- Security requirement analysis ✓
- SECRICOM security model definition ✓
- Security model supporting tool deployment and components integration ✓
  - Security information collection and security status monitoring
  - Active control mechanisms

Awareness and Control



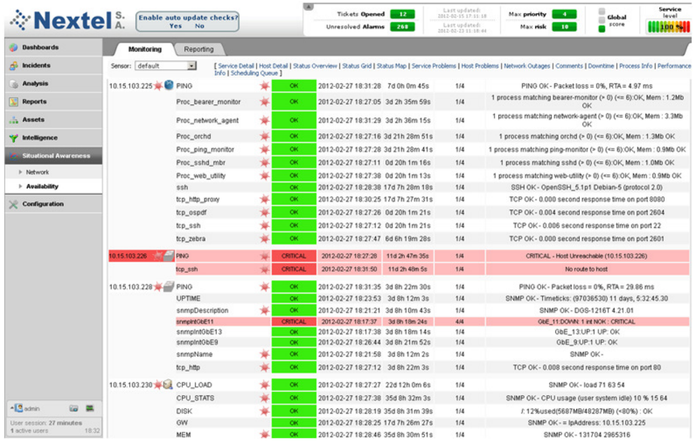
Conclusions

- ★ Hardening of individual component
- ★ Network protection



□	Ticket	Title	Priority	Created	Life Time	In charge	Submitter	Type	Status	Extra
□	VUL13	Vulnerability - Unknown detail (10.15.102.225)	2	2012-02-15 17:11:18	01:05	CSMCC admin	nessus	Nessus Vulnerability	Open	INTERNAL_PE
□	VUL12	nessus: Default community names of the SNMP Agent (10.15.102.225:161)	4	2012-02-15 17:11:18	01:05	CSMCC admin	nessus	Nessus Vulnerability	Open	INTERNAL_PE
□	VUL11	Vulnerability - Unknown detail (10.15.100.225)	2	2012-02-15 11:48:44	06:27	CSMCC admin	nessus	Nessus Vulnerability	Open	INTERNAL_PE
□	VUL10	nessus: Default community names of the SNMP Agent (10.15.100.225:161)	4	2012-02-15 11:48:44	06:27	CSMCC admin	nessus	Nessus Vulnerability	Open	INTERNAL_PE
□	VUL09	Vulnerability - Unknown detail (10.15.105.225)	2	2012-02-15 11:45:34	06:31	CSMCC admin	nessus	Nessus Vulnerability	Open	INTERNAL_PE
□	VUL08	nessus: Default community names of the SNMP Agent (10.15.105.225:161)	4	2012-02-15 11:45:34	06:31	CSMCC admin	nessus	Nessus Vulnerability	Open	INTERNAL_PE
□	VUL07	Vulnerability - Unknown detail (10.15.104.225)	2	2012-02-15 11:45:17	06:31	CSMCC admin	nessus	Nessus Vulnerability	Open	INTERNAL_PE
□	VUL06	nessus: Default community names of the SNMP Agent (10.15.104.225:161)	4	2012-02-15 11:45:17	06:31	CSMCC admin	nessus	Nessus Vulnerability	Open	INTERNAL_PE
□	VUL05	nessus: Using NetBIOS to retrieve information from a Windows host (10.15.103.235:137)	3	2011-12-21 09:41:13	1 Month, 26 Days 08:35	CSMCC admin	nessus	Nessus Vulnerability	Open	INTERNAL_PE
□	VUL04	Vulnerability - Unknown detail (10.15.103.235)	2	2011-12-21 09:41:06	1 Month, 26 Days 08:35	CSMCC admin	nessus	Nessus Vulnerability	Open	INTERNAL_PE
□	VUL03	Vulnerability - Unknown detail (10.15.103.225)	2	2011-12-20 14:48:57	1 Month, 27 Days 03:27	CSMCC admin	nessus	Nessus Vulnerability	Open	INTERNAL_PE
□	VUL02	nessus: Default community names of the SNMP Agent (10.15.103.225:161)	4	2011-12-20 14:48:56	1 Month, 27 Days 03:27	CSMCC admin	nessus	Nessus Vulnerability	Open	INTERNAL_PE

- ★ Instant network visibility and control features


Nextel S.A.
Enable auto update checks? Yes No
Tickets Opened 12
Unresolved Alarms 268
Last updated: 2012-02-15 17:11:18
Last updated: 2012-02-23 11:18:44
Max priority 4
Max risk 10
Global score
Service level
100 %
Dashboards
Incidents
Analysis
Reports
Assets
Intelligence
Situational Awareness
Network
Availability
Configuration
admin
Monitoring
Reporting
Sensor: default
[Service Detail | Host Detail | Status Overview | Status Grid | Status Map | Service Problems | Host Problems | Network Outages | Comments | Downtime | Process Info | Performance Info | Scheduling Queue]

10.15.103.225	PING	OK	2012-02-27 18:31:28	7d 0h 0m 45s	1/4	PING OK - Packet loss = 0%, RTA = 4.97 ms
	Proc_bearer_monitor	OK	2012-02-27 18:27:05	3d 2h 35m 59s	1/4	1 process matching bearer-monitor (> 0) (<= 6):OK, Mem : 1.2Mb OK
	Proc_network_agent	OK	2012-02-27 18:31:29	3d 2h 36m 15s	1/4	1 process matching network-agent (> 0) (<= 6):OK, Mem : 3.3Mb OK
	Proc_orchd	OK	2012-02-27 18:27:16	3d 21h 28m 51s	1/4	1 process matching orchd (> 0) (<= 6):OK, Mem : 1.3Mb OK
	Proc_ping_monitor	OK	2012-02-27 18:27:28	3d 21h 28m 41s	1/4	1 process matching ping-monitor (> 0) (<= 6):OK, Mem : 0.9Mb OK
	Proc_sshd_mbr	OK	2012-02-27 18:27:11	0d 20h 1m 16s	1/4	1 process matching sshd (> 0) (<= 6):OK, Mem : 1.0Mb OK
	Proc_web_utility	OK	2012-02-27 18:27:38	0d 20h 1m 13s	1/4	1 process matching web-utility (> 0) (<= 6):OK, Mem : 0.9Mb OK
	ssh	OK	2012-02-27 18:28:38	17d 7h 28m 18s	1/4	SSH OK - OpenSSH_5.1p1 Debian-5 (protocol 2.0)
	tcp_http_proxy	OK	2012-02-27 18:30:25	17d 7h 27m 31s	1/4	TCP OK - 0.000 second response time on port 8080
	tcp_ospdf	OK	2012-02-27 18:27:26	0d 20h 1m 21s	1/4	TCP OK - 0.004 second response time on port 2604
	tcp_ssh	OK	2012-02-27 18:27:12	0d 20h 1m 21s	1/4	TCP OK - 0.006 second response time on port 22
	tcp_zebra	OK	2012-02-27 18:27:47	6d 6h 19m 28s	1/4	TCP OK - 0.000 second response time on port 2601
10.15.103.226	PING	CRITICAL	2012-02-27 18:27:28	11d 2h 47m 35s	1/4	CRITICAL - Host Unreachable (10.15.103.226)
	tcp_ssh	CRITICAL	2012-02-27 18:31:50	11d 2h 48m 5s	1/4	No route to host
10.15.103.228	PING	OK	2012-02-27 18:31:35	3d 8h 22m 30s	1/4	PING OK - Packet loss = 0%, RTA = 29.86 ms
	UPTIME	OK	2012-02-27 18:23:53	3d 8h 12m 3s	1/4	SNMP OK - Timeticks: (97036530) 11 days, 5:32:45.30
	snmpDescription	OK	2012-02-27 18:21:21	3d 8h 10m 43s	1/4	SNMP OK - DGS-1216T 4.21.01
	snmpIntGbE11	CRITICAL	2012-02-27 18:17:37	3d 8h 18m 24s	4/4	GbE_11:DOWN: 1 int NOK : CRITICAL
	snmpIntGbE13	OK	2012-02-27 18:17:38	3d 8h 18m 14s	1/4	GbE_13:UP:1 UP: OK
	snmpIntGbE9	OK	2012-02-27 18:26:44	3d 8h 21m 52s	1/4	GbE_9:UP:1 UP: OK
	snmpName	OK	2012-02-27 18:21:58	3d 8h 12m 2s	1/4	SNMP OK -
	tcp_http	OK	2012-02-27 18:27:12	3d 8h 22m 3s	1/4	TCP OK - 0.008 second response time on port 80
10.15.103.230	CPU_LOAD	OK	2012-02-27 18:27:27	22d 12h 0m 6s	1/4	SNMP OK - load 71 63 54
	CPU_STATS	OK	2012-02-27 18:27:38	35d 8h 32m 3s	1/4	SNMP OK - CPU usage (user system idle) 10 % 15 64
	DISK	OK	2012-02-27 18:28:19	35d 8h 31m 39s	1/4	/: 12%used(5687MB/48287MB) (<80%) : OK
	GW	OK	2012-02-27 18:28:25	17d 7h 26m 27s	1/4	SNMP OK - = IpAddress: 10.15.103.225
	MEM	OK	2012-02-27 18:28:46	35d 8h 30m 51s	1/4	SNMP OK - 131704 2965316

User session: 27 minutes
1 active users 18:32

Contact

Mikel Uriarte Itzazelaia, R&D Manager Nextel S.A.
muriarte@nextel.es

http://www.nextel.es

Support services in ENS implementation:
National Security Plan

ENSTool

National Security Plan

Description Law 11/2007 on the Citizens' Electronic Access to Public Services (LAECSP in Spanish), which governs the basic aspects of e-Administration, recognizes the right of citizens to interact with Public...

Nextel S.A. en Securmática

SERVICIOS

IT Consulting

Telematic Applications

Outsourcing

Telematic Projects

IT Security

I+D+i

Soporte técnico
902 540 430

¿Quieres **trabajar** con nosotros?

Copyright Nextel S.A. All Rights Reserved. Aviso Legal Mapa Web Intranet