WS6 GARR
"Dalla rete all'utente: quando l'utente diventa nodo attivo della rete"
Roma, 16-18 novembre 2005

Rilevazione delle Intrusioni

Sperimentazione ed obiettivi del gruppo GARR "Sec-Sensori"

Guido Buscema

Osservatorio Astronomico di Roma

Gruppo Sec-Sensori

- **Galeotto fu il congresso GARR**
  - **Roma, novembre 2003**
  - **Inizio lavori, aprile 2004 (12 componenti)**
- **Componenti attuali del gruppo**
  - **Alessandro Agostini (CNR IFAC, Firenze)**
  - **Federico Bitelli (Dip.to di Fisica, Roma3)**
  - **Guido Buscema (INAF-OAR, Roma)**
  - **Cecilia Catalano (ISTAT, Roma)**
  - **Roberto Cecchini (INFN, Firenze)**
  - **Giacomo Fazio (INAF-IASF, Palermo)**

Gruppo Sec-Sensori

- **Obiettivo**
  - **Indagare la fattibilità di una struttura distribuita per la rilevazione delle intrusioni**
    - **“Early warning” sulla rete della ricerca**
    - **Sistema di “Intrusion Detection” per le LAN**
  - **Realizzare un servizio GARR**
- **Scenario: Autonomous System 137 GARR (ASGARR)**
  - **Backbone ad alta velocità**
  - **POP distribuiti su tutta l’Italia**
  - **Reti eterogenee**

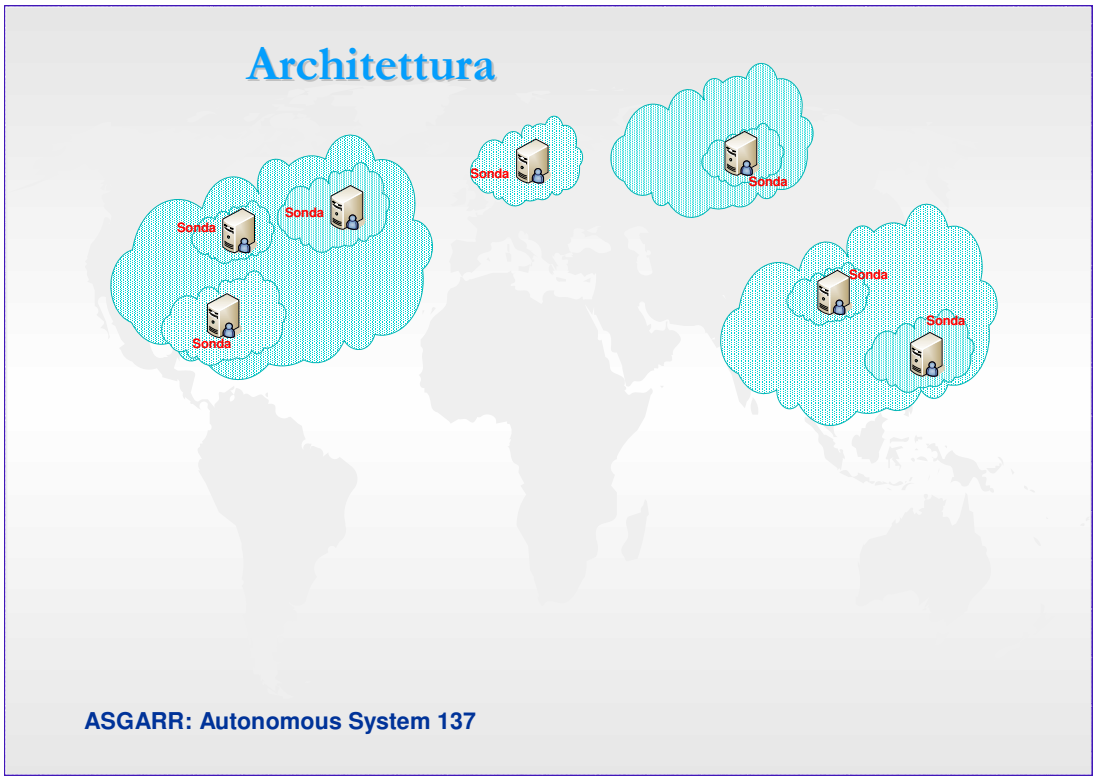
Sec-Sensori - Architettura

Il progetto prevede quattro livelli operativi

- **Sonda**
  - **Registra gli alert di rete rilevati e li invia ai collettori di zona**
- **Collettore**
  - **Colleziona gli alert provenienti dalle sonde in un database**
- **Centro di Distribuzione**
  - **Provvede all'aggiornamento del software e delle regole sulle sonde, oltre alla loro installazione e configurazione**
- **Centro di Controllo**
  - **Consente di monitorare i collettori per un'analisi comparativa globale dei dati**

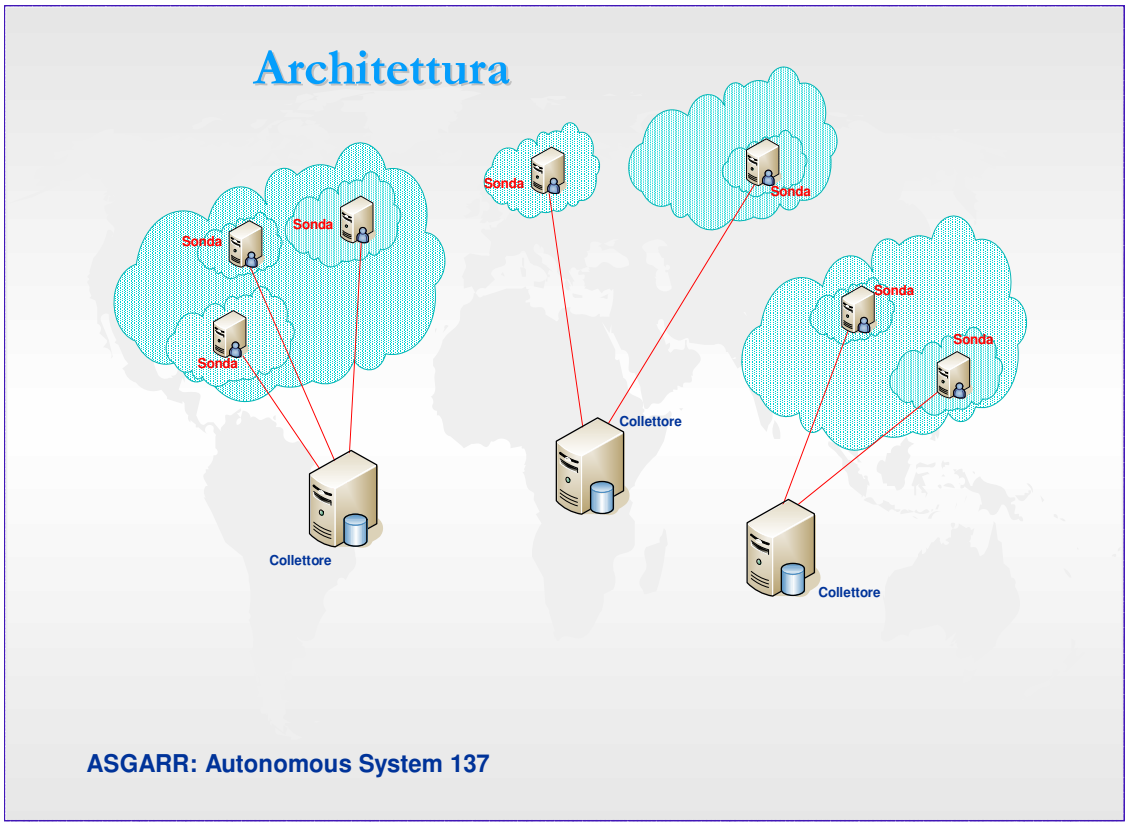
Sonda

- **Si installa e si configura automaticamente**
  - **Centro di Distribuzione (FAI)**
- **Cattura, esamina i pacchetti e registra gli alert**
  - **Snort**
- **Invia i dati ai collettori di riferimento**
  - **SAFT/Sendfile**
- **Invia al responsabile locale gli allarmi rilevati**
- **Scarica automaticamente gli aggiornamenti software**
  - **apt-get con il Centro di Distribuzione**

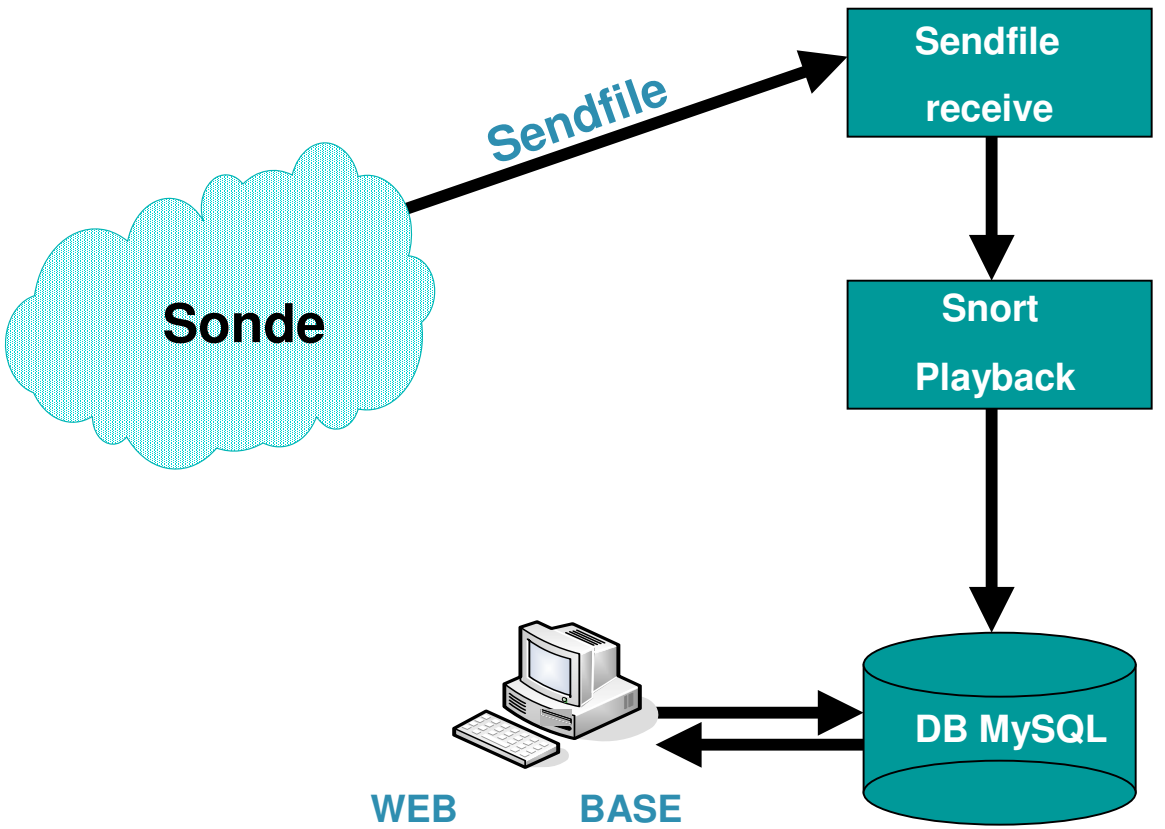


Collettore 1/2

- **Riceve i dati inviati dalle sonde**
  - Sendfile (receive)
- **Li raccoglie in un database MySQL**
  - Snort
- **Analisi dei dati ricevuti**
  - BASE

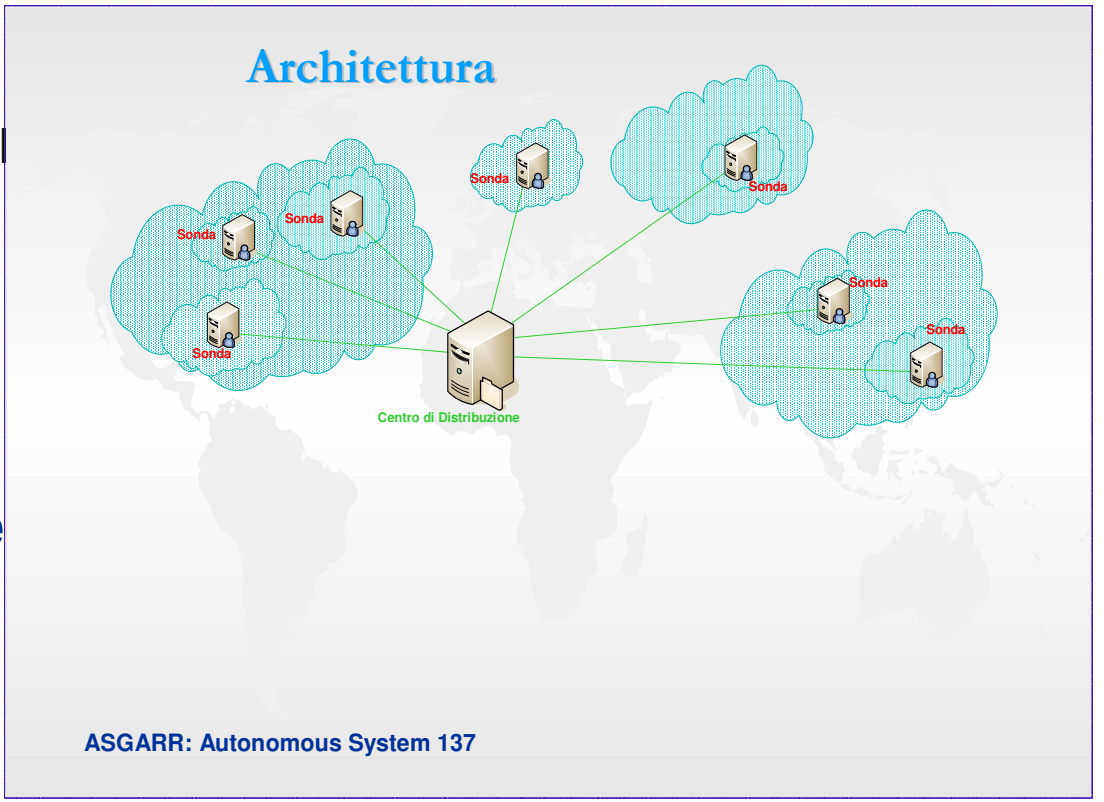


Collettore 2/2



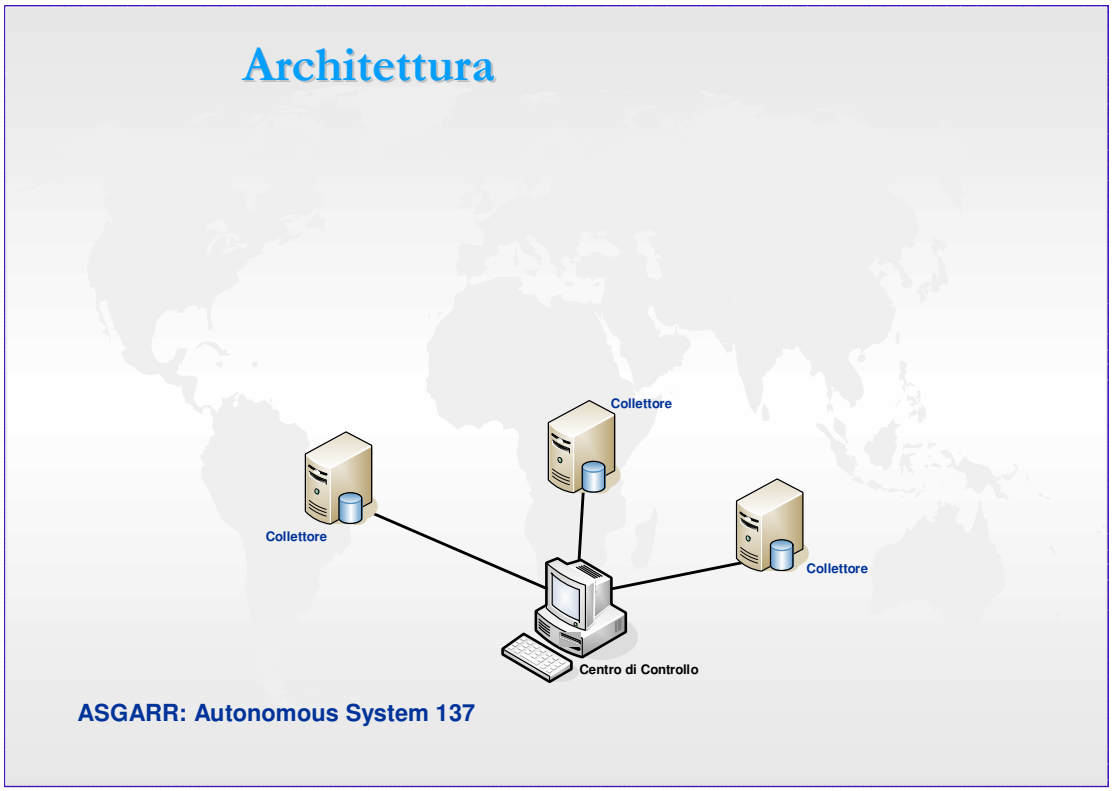
Centro di Distribuzione

- **Acquisisce informazioni di base per le nuove sonde**
  - Interfaccia web sviluppata dal gruppo
- **Configura ed aggiorna il software delle sonde**
  - Mirror Debian (FAI: Fully Automatic Installation)
- **Acquisisce nuove regole di controllo per Snort**
  - Oinkmaster
- **Aggiorna sulle sonde le nuove regole**
  - Pacchetto Debian

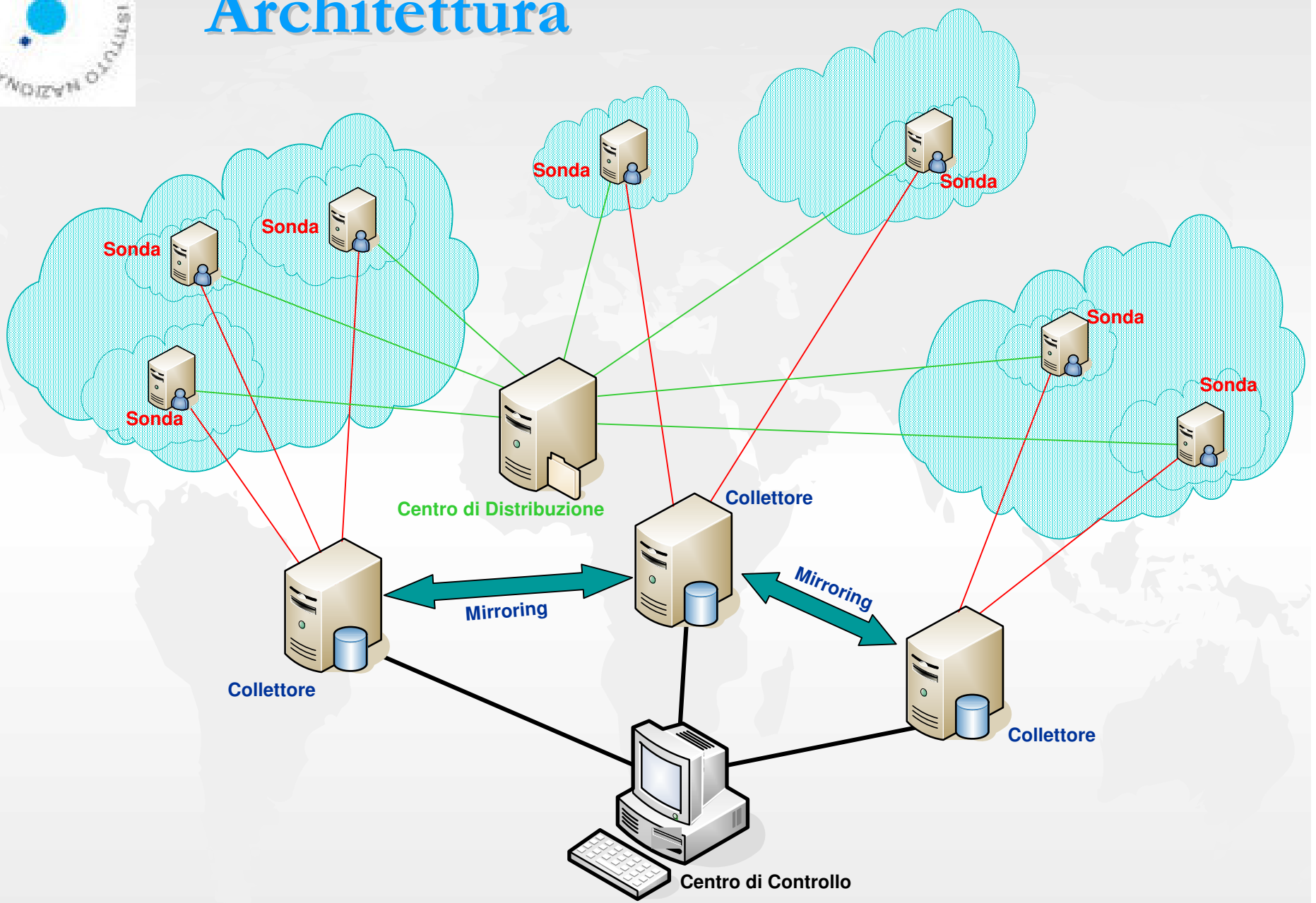


Centro di Controllo

- Gestisce la tabella con i metadati di tutti i collettori
- Correla ed integra dati provenienti da sorgenti multiple (collettori)



Architettura



Confronto con altri DIDS 2/3

- **Valore aggiunto del progetto Sec-Sensori:**
  - **Sonde chiavi in mano utilizzando "qualsiasi" hardware**
  - **Aggiornamenti automatici dei pacchetti software (sistema ed applicativi) delle sonde**
  - **Aggiornamenti automatici delle regole di Snort sulle sonde**
  - **Gestione esterna e centralizzata degli eventi**

e quindi

nessun carico per il system manager locale

Confronto con altri DIDS 3/3

In definitiva la vera caratteristica distintiva

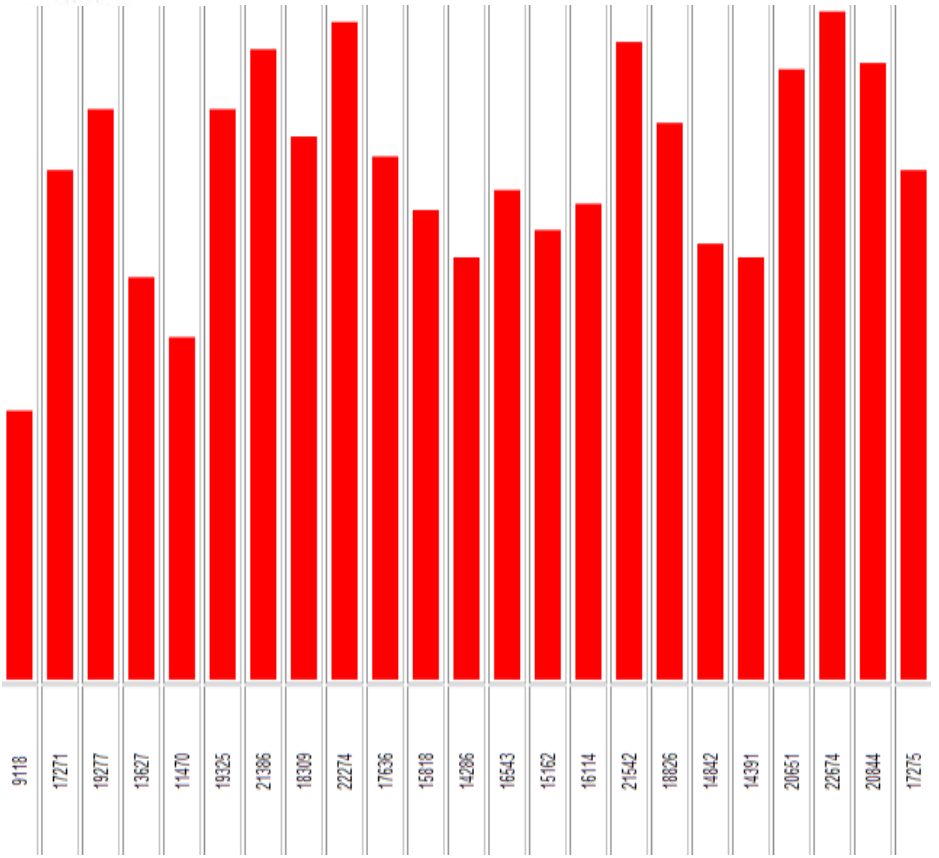
- **Il gruppo Sec-Sensori propone l'attuazione**
  - **Non di un pacchetto software da gestire in proprio**
  - **Ma di un servizio gratuito e completamente automatico**
- **L'utente diventa un nodo attivo**

Stato dei Lavori

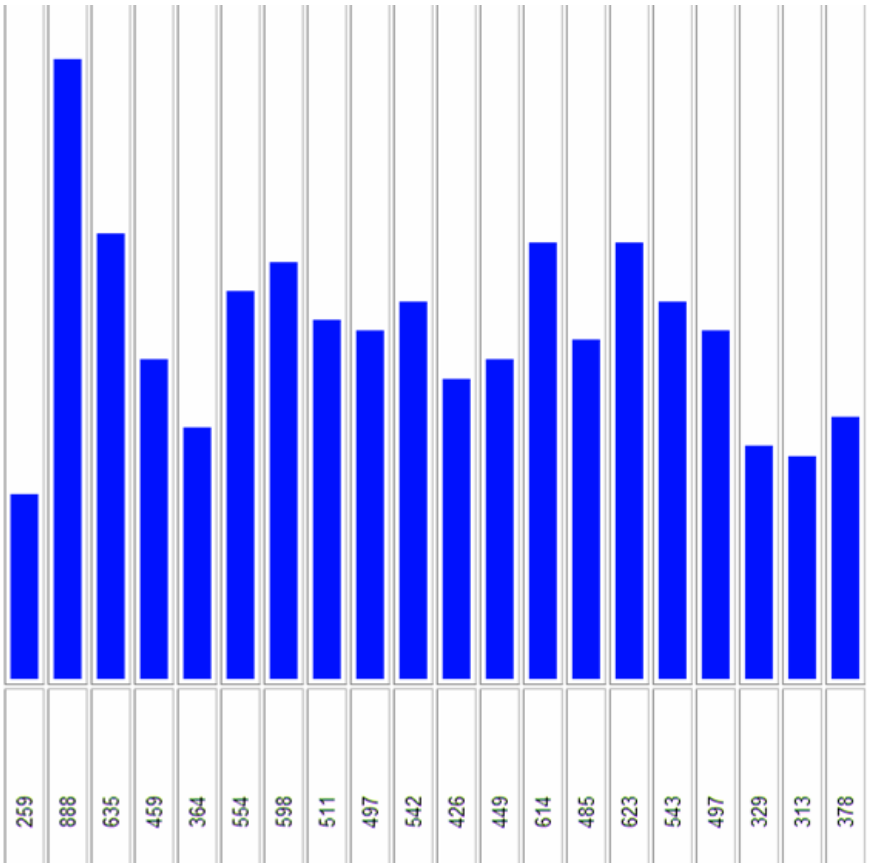
- **È attiva una rete sperimentale**
  - **Sonde(5): Roma, Palermo, Firenze**
  - **Collettori(2): Roma, Palermo**
  - **Centro di Distribuzione(1): Roma**
    - **Ultimato FAI per l'installazione, configurazione ed aggiornamento delle sonde in rete.**
  - **Centro di Controllo(1): Firenze**
    - **Attivo un prototipo di interfaccia grafica per accedere ai dati**

- **Da completare:**
  - **Centro di Distribuzione: versione CD per l'installazione automatica delle sonde**
  - **Centro di Controllo: terminare il front-end grafico (PHP, ADODB, HTML, MySQL)**
  - **Verifica della scalabilità: numero di sonde e collettori ragionevole per una successiva fase di effettiva sperimentazione**

Scelta set di regole



Set completo



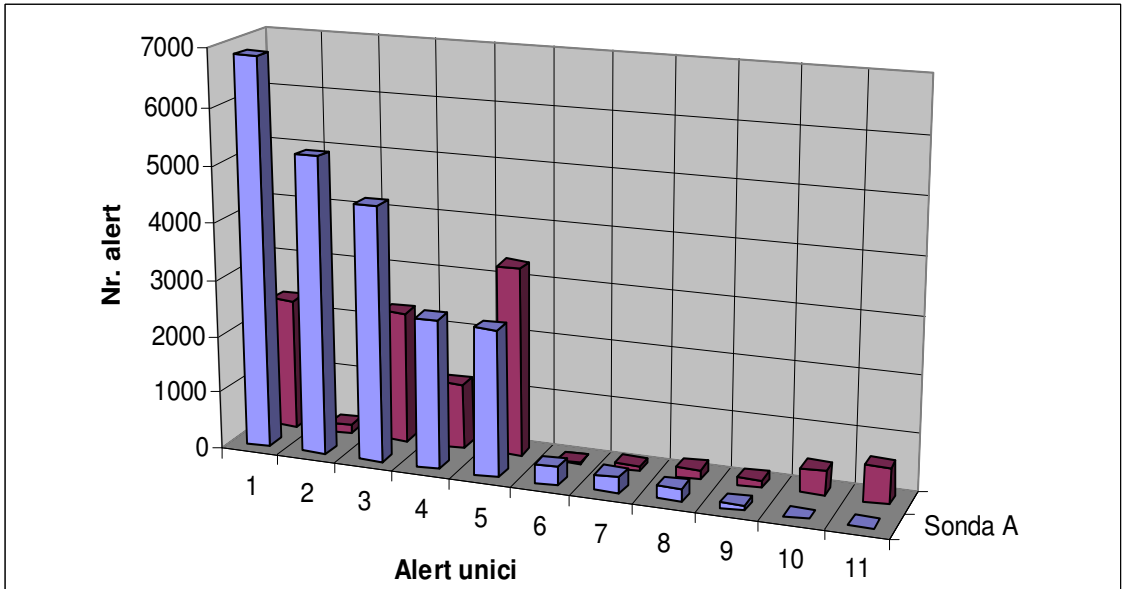
Set ridotto

Confronto dei grafici

- **Dai due grafici precedenti possiamo dedurre che:**
  - **Senza una soglia o riduzione delle regole siamo sommersi dagli alert**
  - **Troppi falsi positivi nascondono i veri attacchi**
  - **Di contro, un numero eccessivamente ridotto di regole potrebbe non far scattare l'allarme**

Attacchi unici

Nr	Nome Attacco	Totale
1	Misc-attack	9161
2	Non classificato	5385
3	Misc-activity	6791
4	Web-application-activity	3681
5	Attempted-recon	5895
6	Web-application-attack	320
7	Bad-unknown	388
8	Non-standard-protocol	399
9	Attempted-admin	215
10	Protocol-command-decode	432
11	Attempted-user	618



	1	2	3	4	5	6	7	8	9	10	11
Sonda A	6850	5233	4480	2623	2562	316	289	231	85	4	1
Sonda B	2311	152	2311	1158	3333	4	99	168	130	428	617

- **Alert unici della Sonda A e della Sonda B**

Porte più gettonate dai tentativi di intrusione

Sonda A

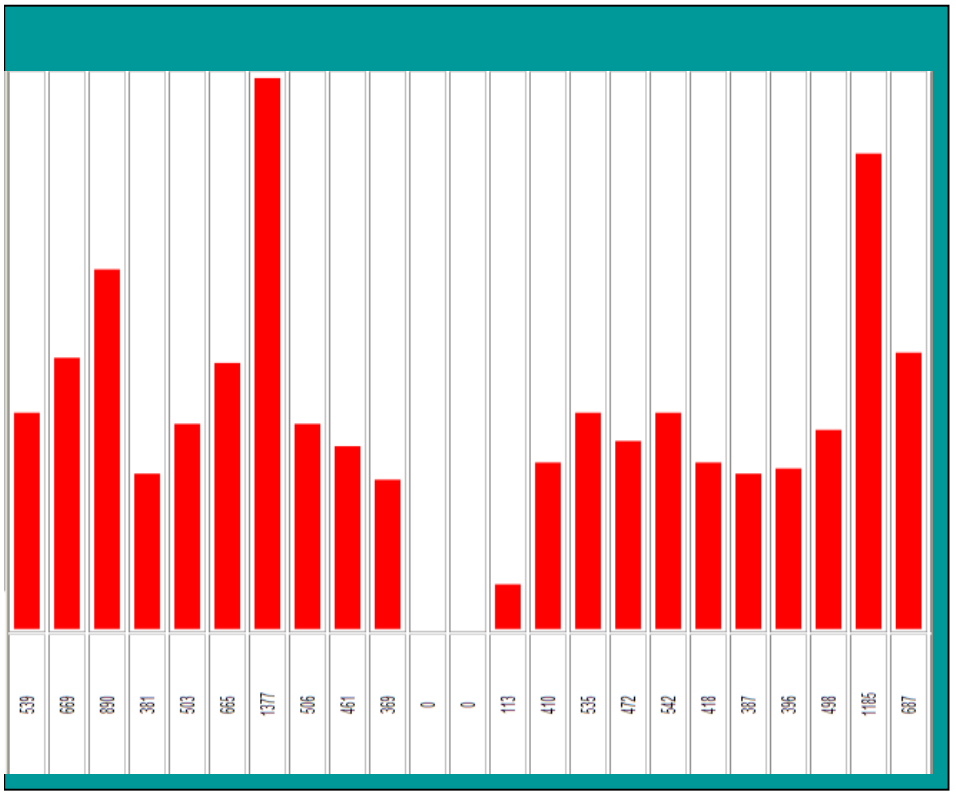
< Port >	< Sensore >	< Occurrences >	< Unici Avvisi >	< Indir. Sorg. >	< Indir. Dest. >
80 [sans] [portsdb] [tantalo] [sstats]	1	11346	7	831	681
8080 / tcp [sans] [portsdb] [tantalo] [sstats]	1	178	2	2	51
/ tcp [sans] [portsdb] [tantalo] [sstats]	1	16	3	5	7
60770 / tcp [sans] [portsdb] [tantalo] [sstats]	1	3	2	1	1
25 / tcp [sans] [portsdb] [tantalo] [sstats]	1	2	2	2	1
3435 / tcp [sans] [portsdb] [tantalo] [sstats]	1	1	1	1	1
52037 / tcp [sans] [portsdb] [tantalo] [sstats]	1	1	1	1	1
42954 / tcp [sans] [portsdb] [tantalo] [sstats]	1	1	1	1	1
33568 / tcp [sans] [portsdb] [tantalo] [sstats]	1	1	1	1	1
62088 / tcp [sans] [portsdb] [tantalo] [sstats]	1	1	1	1	1
50414 / tcp [sans] [portsdb] [tantalo] [sstats]	1	1	1	1	1
38096 / tcp [sans] [portsdb] [tantalo] [sstats]	1	1	1	1	1
3438 / tcp [sans] [portsdb] [tantalo] [sstats]	1	1	1	1	1
52659 / tcp [sans] [portsdb] [tantalo] [sstats]	1	1	1	1	1
44402 / tcp [sans] [portsdb] [tantalo] [sstats]	1	1	1	1	1

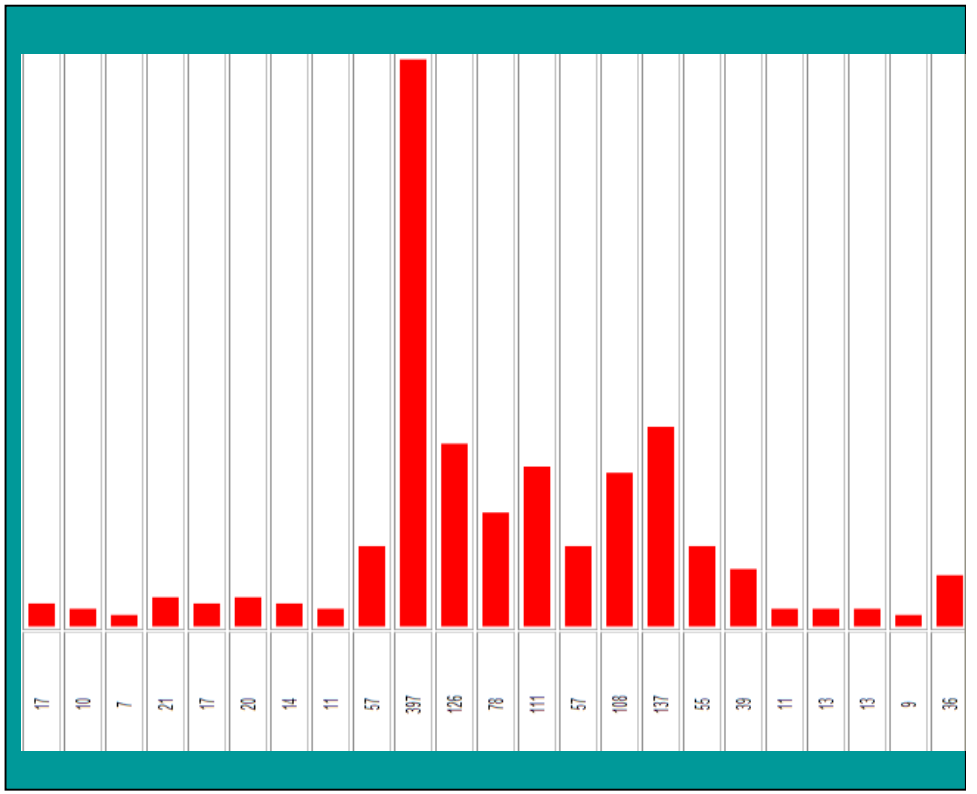
- **25: SMTP**
- **80, 8080:WEB**
- **162: SNMP Trap**
- **443: Http over TLS/SSL**
- **1434: Microsoft SQL Monitor**
- **3306: MySQL**

Sonda B

< Port >	< Sensors >	< Occurrences >	< Unique Alerts >	< Source IP >	< Dest. IP >
1434 / udp	1	4622	2	660	13
162 / udp	1	2985	1	2	1
80 / tcp	1	1708	24	287	9
3306 / tcp	1	427	1	12	2
443 / tcp	1	161	2	22	1
16548 / tcp	1	31	2	1	1
55669 / tcp	1	27	2	1	1
25 / tcp	1	16	3	9	1
16295 / tcp	1	12	1	1	1
50929 / tcp	1	12	1	1	1
41699 / tcp	1	12	1	1	1
15352 / tcp	1	12	1	1	1
18489 / tcp	1	12	1	1	1
14694 / tcp	1	12	1	1	1
19392 / tcp	1	11	2	1	1
37718 / tcp	1	10	1	1	1
46681 / tcp	1	10	2	1	1

Esempio di analisi: SNMP TRAP





- **Sonda B: alert del 25 ottobre; si vede bene il picco dovuto ad alert. È una macchina che scansiona tutte le altre sulla porta 162.**

Conclusioni

Una rete geograficamente distribuita di sensori è realizzabile ed auspicabile

- **Ricadute positive sulle singole realtà locali**
  - **Segnalazione locale di attività anomala**
  - **Non richiede competenze specifiche**
  - **Nessun aggravio del carico di lavoro**
  - **Componenti hardware di basso livello**

- **Su larga scala: segnalazione tempestiva (Early Warning) di anomalie potenzialmente pericolose**

Wanted

Join us

you'll see crackers in action

Mailing List: wg-sec-sensori@garr.it