

WG-SEC-SCAN

Gruppo di lavoro sulla cybersecurity
“Network Auditing”

Ermann Ripepi - ermann.ripepi@imaa.cnr.it

Consiglio Nazionale delle Ricerche - Istituto di Metodologie per l'Analisi Ambientali

Workshop GARR 2017 | Roma, 4-7 Aprile 2017



Gruppo di lavoro

- Inizio attività Settembre 2016
- 22 partecipanti al gruppo, di cui ~8 presenti alle videoconferenze
 - Riunioni generali con cadenza mensile
 - Riunioni specifiche dei sottogruppi in base alle necessità
- Web Application
 - SCARR (NESSUS) <https://www.cert.garr.it/servizi/scarr>
 - Kali Linux, Parrot Security OS
 - Open Web Application Security Project (OWASP)
- Best Practices di carattere tecnico
 - Hardening = processo di analisi e messa in sicurezza di un host riducendo i punti di attacco
- Analisi dei log e flussi di dati
 - ELK STACK

Analisi dei log e flussi di dati

- ELK Stack (Elastic), perché?
 - Fu proposto durante la creazione dei GdL del WS2016
 - C'erano già competenze all'interno del gruppo
 - È una piattaforma scalabile e flessibile

- Sottogruppo di lavoro "ELK"
 - Francesco Izzi: CNR-IMAA
 - Francesco Sansone: CNR-IFC
 - Fulvio Galeazzi: Consortium GARR
 - Nino Ciurleo: Consortium GARR
 - Ermann Ripepi: CNR-IMAA

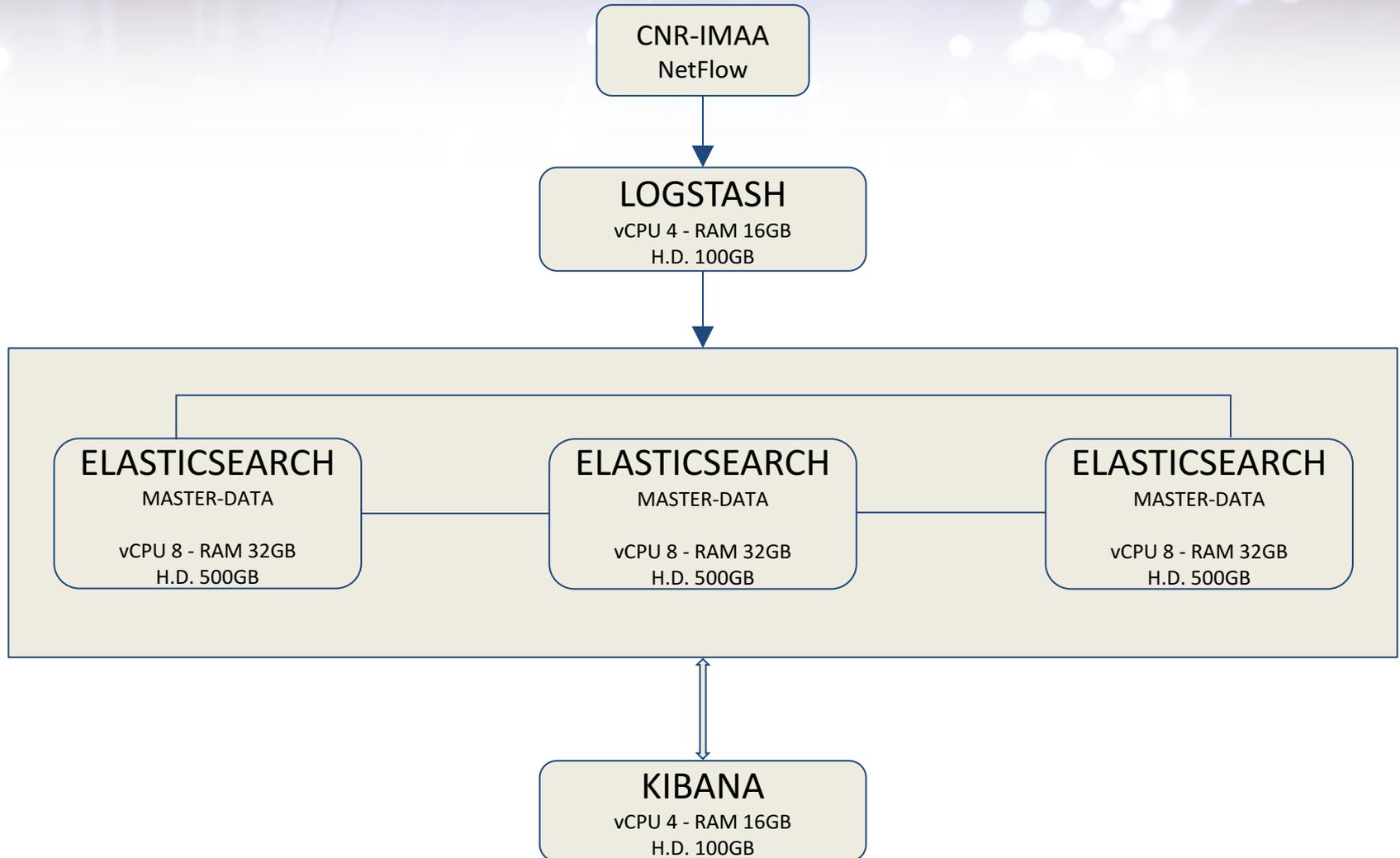
Analisi dei log e flussi di dati

- Componenti di ELK
 - Logstash – collettore di dati
 - Elasticsearch – cerca, analizza e archivia i dati
 - Kibana – front end per visualizzare i dati

RISORSE UTILIZZATE

- Utilizzo della piattaforma Cloud OpenStack di GARR-X Progress
- 5 virtual machines
 - vCPU 32
 - RAM 128GB
 - Storage 1,7TB (~200GB per servizi e ~1,5TB per archiviazione)
- Sistema Operativo
 - Ubuntu Server 16.04 LTS 64 bit

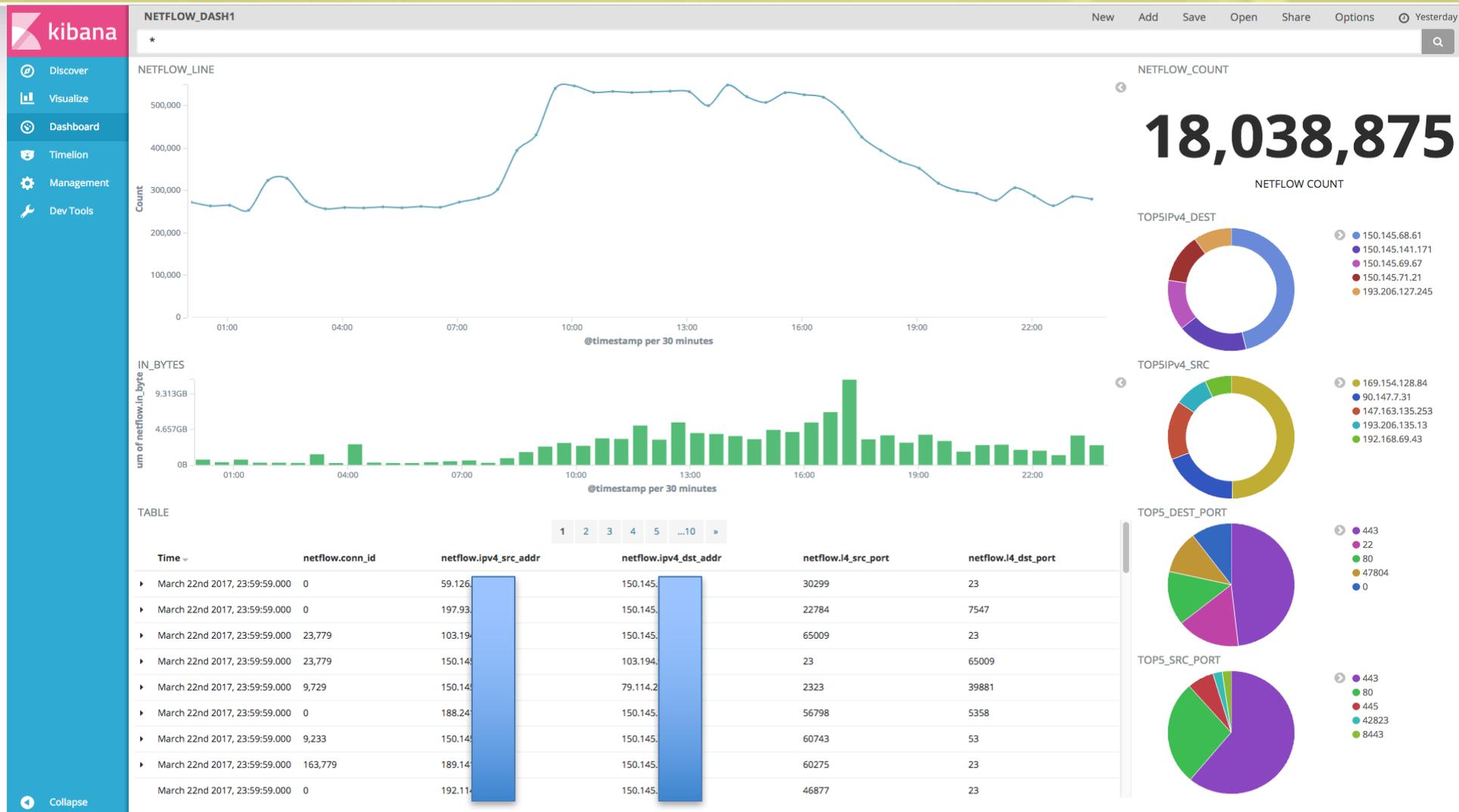
CLUSTER ELK



Traffico NetFlow

- Stream di dati campionati 1:1
 - Traffico sede utente ~ 25 Mbps
 - Traffico NetFlow ~ 211 Kbps, ~ 2,28 GB al giorno

Dashboard NetFlow IPv4



Dashboard NetFlow IPv4

 kibana

- Discover
- Visualize
- Dashboard
- Timelion
- Management
- Dev Tools

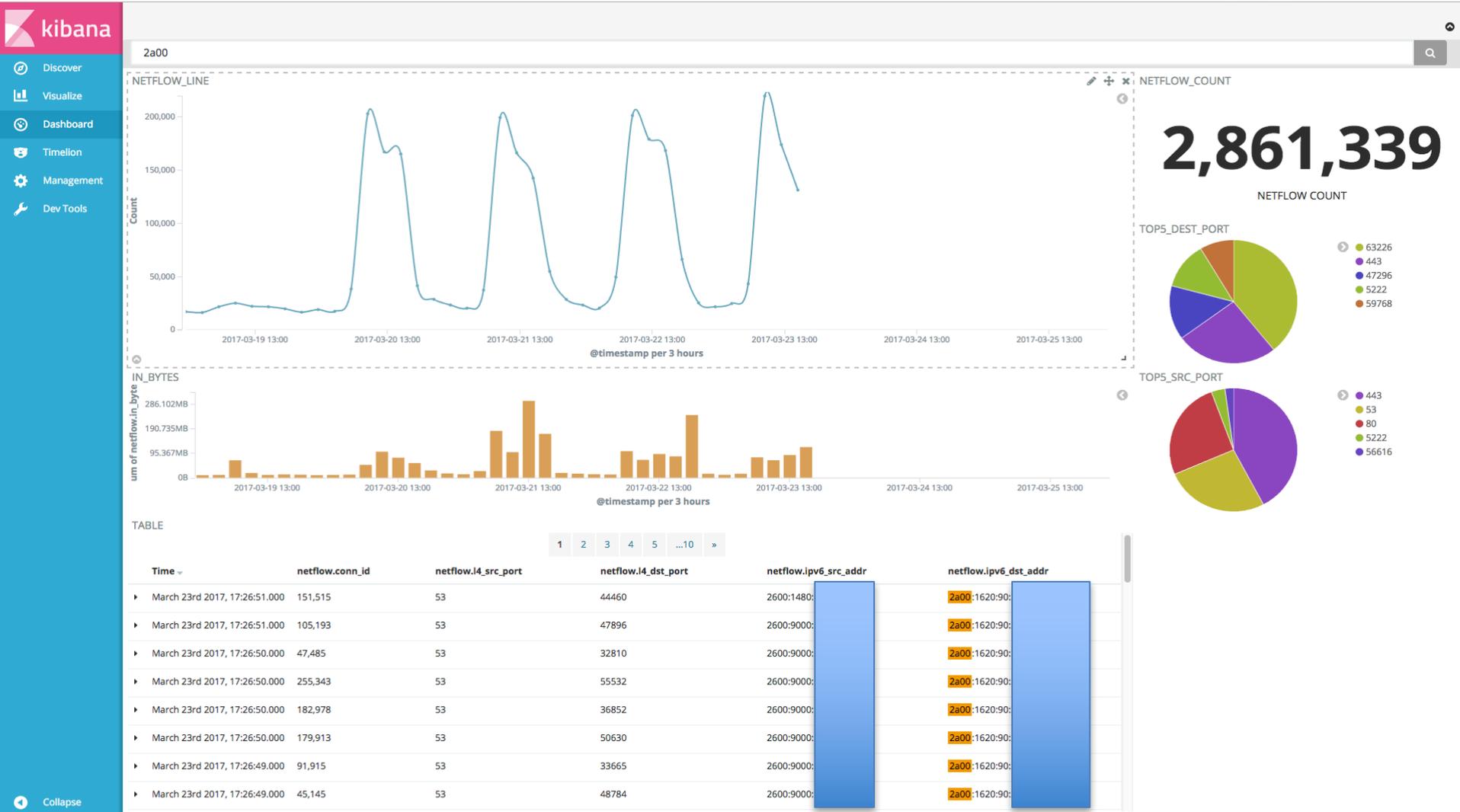
 Collapse

Doc: logstash-2017.03.26/netflow/AVsMohBgsP3U7JXJjwE6

Table JSON

⊙ @timestamp	March 26th 2017, 23:59:59.000
t @version	1
t _id	AVsMohBgsP3U7JXJjwE6
t _index	logstash-2017.03.26
# _score	1
t _type	netflow
t host	150.145.1.1
# netflow.conn_id	0
# netflow.direction	0
⊙ netflow.first_switched	March 26th 2017, 23:59:59.000
# netflow.flow_seq_num	7,167,133
# netflow.flowset_id	256
# netflow.fw_event	3
# netflow.icmp_type	0
# netflow.in_bytes	60B
# netflow.in_pkts	1
# netflow.input_snmp	14
t netflow.ipv4_dst_addr	150.145.1.1
t netflow.ipv4_src_addr	190.15.1.1
# netflow.14_dst_port	5358
# netflow.14_src_port	56906
⊙ netflow.last_switched	March 26th 2017, 23:59:59.000
# netflow.output_snmp	0
# netflow.protocol	6
# netflow.src_tos	0
# netflow.tcp_flags	2
# netflow.version	9
? tags	⚠
t type	netflow

Dashboard NetFlow IPv6



Dashboard NetFlow IPv6

 kibana

- Discover
- Visualize
- Dashboard
- Timelion
- Management
- Dev Tools

 Collapse

Doc: logstash-2017.03.29/netflow/AVsb1hC6sP3U7JXJTmQL

Table | JSON

⊙ @timestamp	March 29th 2017, 22:51:05.000
t @version	1
t _id	AVsb1hC6sP3U7JXJTmQL
t _index	logstash-2017.03.29
# _score	1
t _type	netflow
t host	150.145. [redacted]
# netflow.conn_id	114,438
# netflow.direction	0
⊙ netflow.first_switched	March 29th 2017, 22:51:06.000
# netflow.flow_seq_num	1,145,380
# netflow.flowset_id	258
# netflow.fw_event	1
# netflow.icmp_type	0
# netflow.in_bytes	179B
# netflow.in_pkts	1
# netflow.input_snmp	14
t netflow.ipv6_dst_addr	2a00:1620: [redacted]
t netflow.ipv6_src_addr	2607:f208: [redacted]
# netflow.14_dst_port	59518
# netflow.14_src_port	53
⊙ netflow.last_switched	March 29th 2017, 22:51:06.000
# netflow.output_snmp	500,030,000
# netflow.protocol	17
# netflow.src_tos	0
# netflow.tcp_flags	0
# netflow.version	9
? tags	⚠
t type	netflow

Strategie per il futuro

- ELK STACK
 - Integrare l'analisi dei log (syslog)
 - Configurare sistemi di alert
 - Configurare automatismi che intervengano a seguito di un certo evento
- NTOP
- Continuare il lavoro relativo alle Web Application e Best Practices
- “Popolare” il wiki <https://wiki-wg-sec.garr.it>

GRAZIE !

wg-sec-scan@garr.it

<http://lx1.dir.garr.it/cgi-bin/mailman/listinfo/wg-sec-scan>

<https://wiki-wg-sec.garr.it>