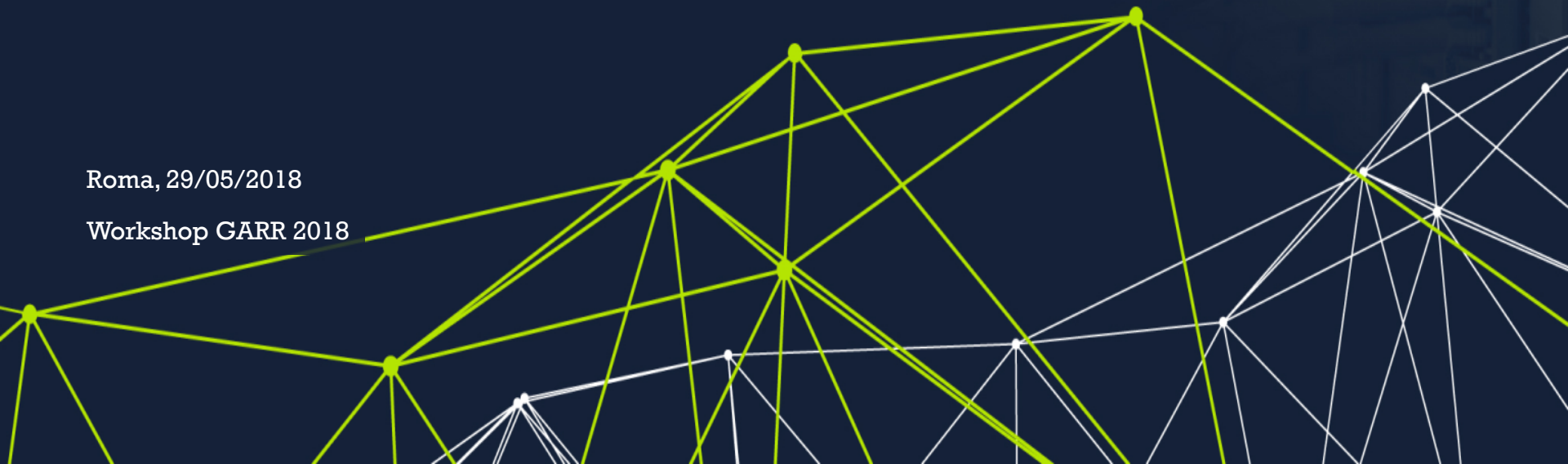
Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

Gruppo di lavoro sulla Cybersecurity

ERMANN RIPEPI



Roma, 29/05/2018

Workshop GARR 2018

Gruppo di lavoro

- Inizio attività Settembre 2016
- Analisi dei dati ed individuazione delle vulnerabilità
- Riunioni periodiche organizzate in videoconferenza
- Prima presentazione del gruppo al Workshop GARR 2017

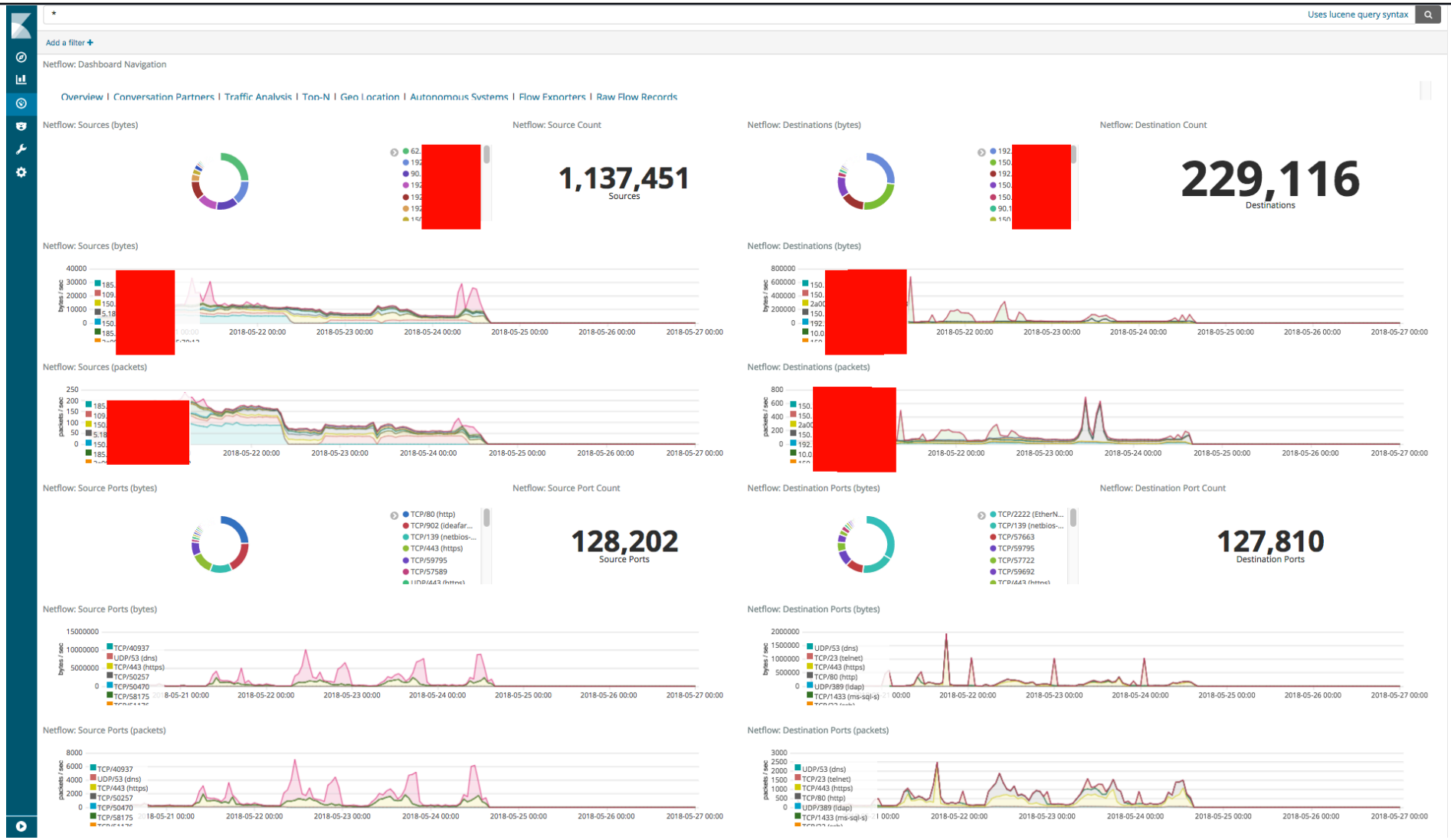
Gruppo di lavoro – tematiche

- Analisi dei dati
- Threat Information sharing all'interno della comunità GARR
- Consigli tecnici per la gestione di una rete

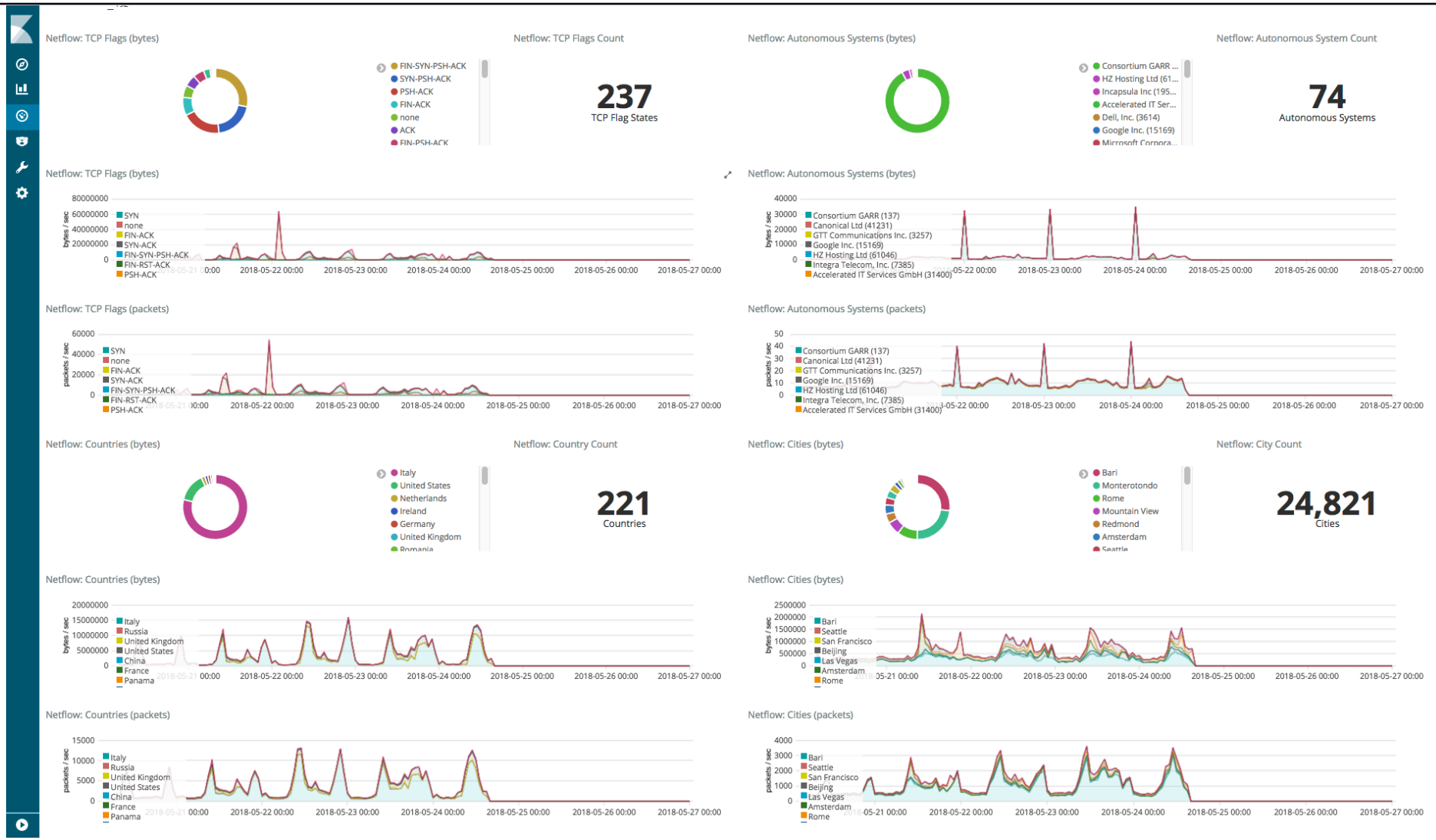
Elastic – lavoro in corso

- Implementazione di Elastic come strumento di analisi dei dati
  - Adatto ad analizzare in near real time grandi quantità di dati
  - Può gestire informazioni tra di loro eterogenee (differenti tipologie di sorgenti e dati, es. router/firewall, web-server apache, syslog, flow data, snmp trap)
  - Si possono effettuare correlazioni tra i dati
  - E' possibile configurare degli alert in base a delle soglie (es. mail, sms, telegram)
  - La soluzione è molto scalabile

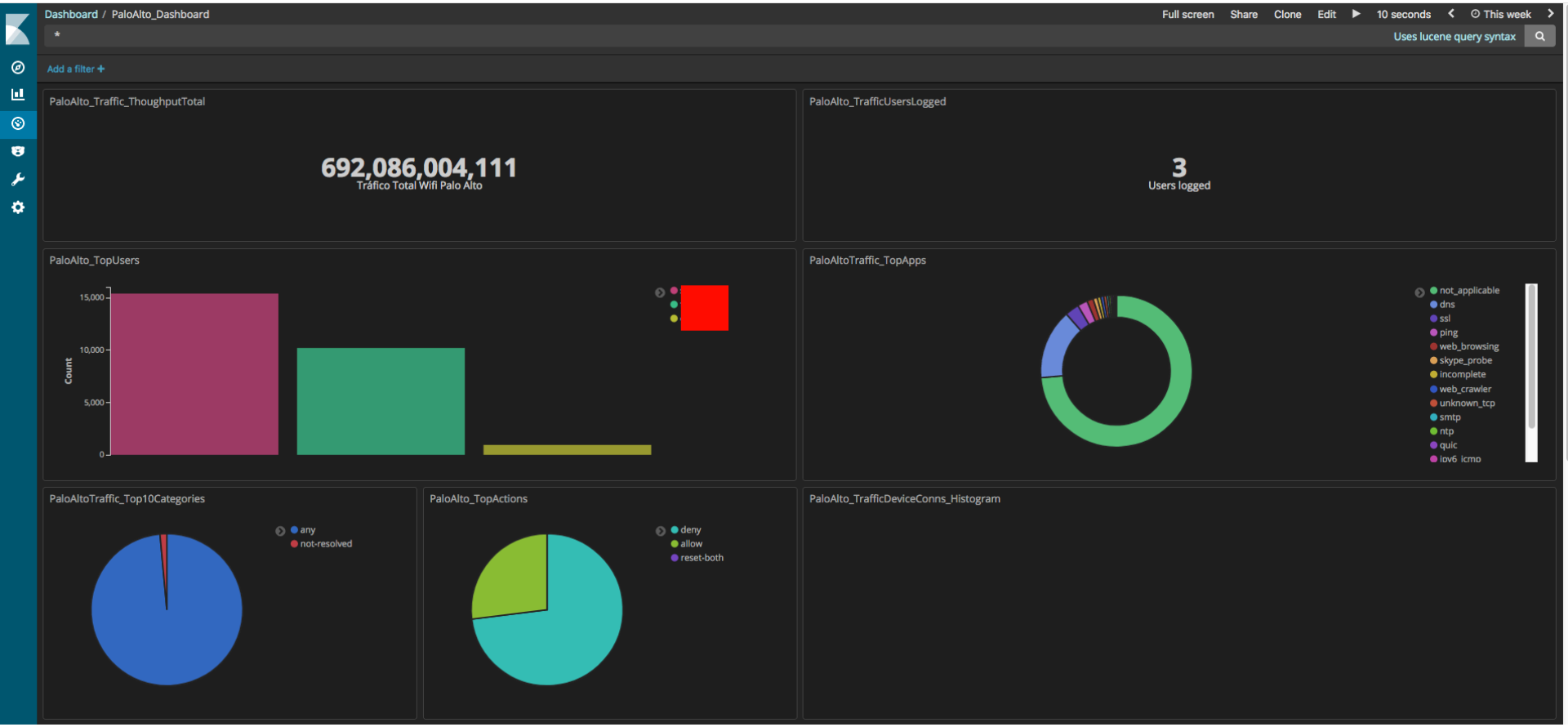
Elastic – Flussi di dati



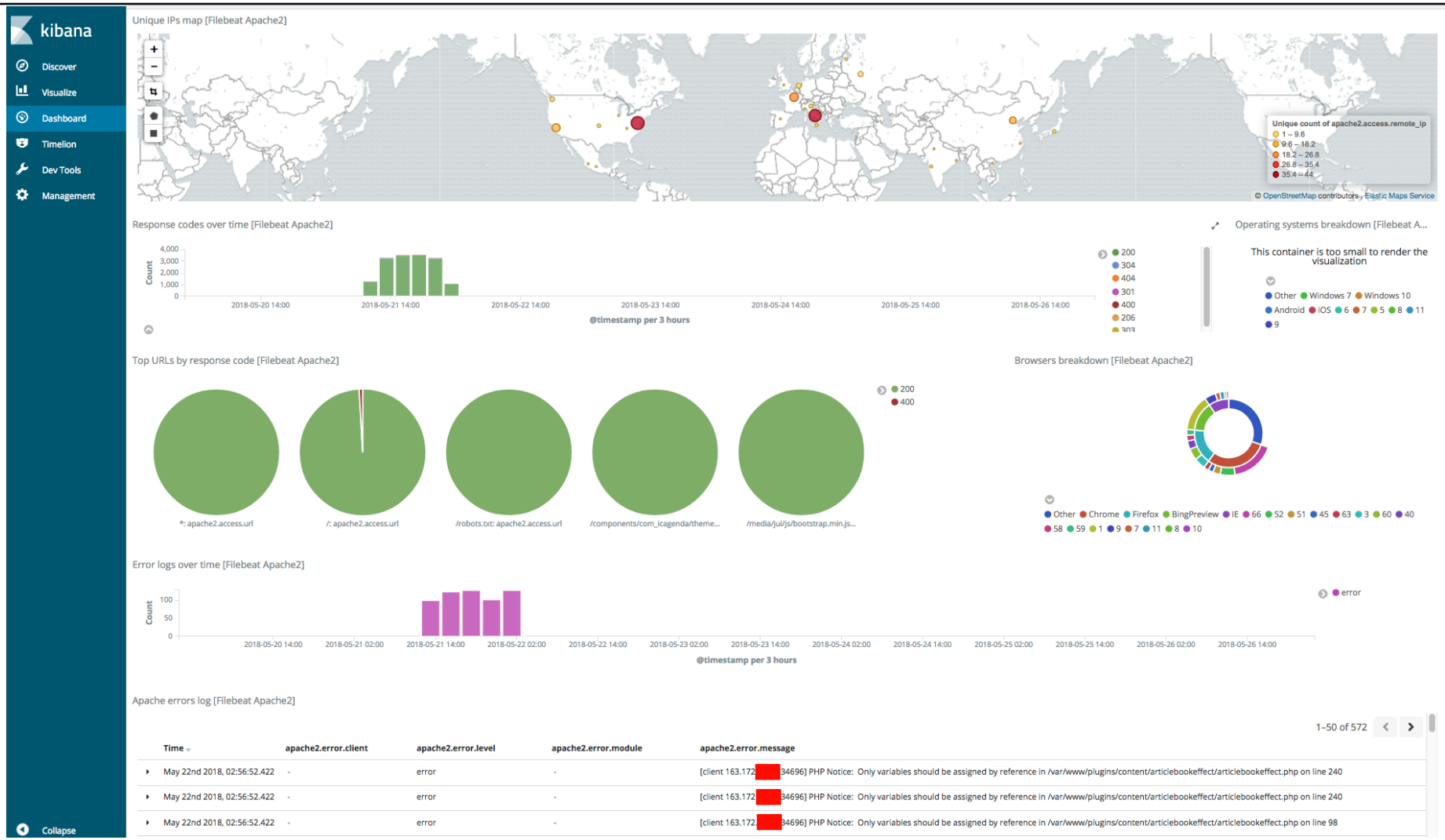
Elastic – Flussi di dati



Elastic – Syslog



Elastic – Apache



Elastic – oltre le dashboard

- Le dashboard sono utili per avere un dettaglio di colpo d'occhio e per un analisi real time

- Per un'analisi approfondita è necessario effettuare delle query specifiche o creare dashboard specifiche per esempio per effettuare correlazione tra dati differenti (syslog, netflow, snmp trap)

- Le dashboard possono essere utili per dimensionare un web-server in base agli accessi e alla tipologia di sorgenti o per verificare se ci sono cambiamenti rispetto a delle baseline che potrebbero significare che c'è un attacco in corso

- Il sistema può generare una Rest API al verificarsi di un determinato evento che faccia partire degli automatismi

Elastic – sottogruppo di lavoro

Francesco Izzi – CNR IMAA

Fulvio Galeazzi - Consortium GARR

Simone Bonetti – CERT Università di Bologna

Francesco Sansone – CNR IFC

Nino Ciurleo - Consortium GARR

Programmi futuri – Security Onion

- Security Onion
  - Distribuzione/repository linux open source di Network Security Monitor (NSM)
  - La GUI è principalmente basata sullo stack Elastic
  - Con Securityonion è possibile gestire i più diffusi strumenti di sicurezza: suricata, snort, bro, argus, netsniff, capme, ecc...
  - Essendo basata su Elastic si possono gestire anche log provenienti da sorgenti esterne come apparati di rete, desktop pc, e altro, usando come sistema di trasporto syslog, beat (filebeat, winbeat), ecc…
  - La documentazione in rete è notevole e la comunità di sviluppatori/utilizzatori è molto attiva

Programmi futuri – Buone regole per la gestione della rete

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

- Regole di base come:
  - Configurare filtri anti-spoofing sui router
  - Filtrare l'accesso verso i servizi esposti non essenziali
  - Utilizzare il più possibile risorse interne (server ntp, dns, mail)
  - Bloccare determinate porte TCP/UDP ritenute vulnerabili (es. 445, 19, 25…)
  - Tenere aggiornati apparati di rete, desktop e server, eliminare dispositivi in eos, eol, ecc...
  - Applicare le misure minime per le PA

Programmi futuri – Threat Information sharing

- Threat Information sharing all'interno della comunità GARR
  - MISP installati presso le sedi e che si scambiano informazioni, oscurando i dati sensibili (es. sorgenti tipiche di attacchi verso la comunità GARR, malware, vulnerabilità note)
  - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing - progetto co-finanziato dalla Unione Europea: http://www.misp-project.org

Partecipare ai gruppi di lavoro

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

- wg-sec@garr.it (generica per tutti)
- wg-sec-ddos@garr.it (sottogruppo DDoS)
- wg-sec-scan@garr.it (sottogruppo Intrusion Detection, Network auditing/monitoring)
- wg-sec-best@garr.it (sottogruppo Best Practice)
- wg-sec-2081x@garr.it (sottogruppo 802.1X wired)

Grazie per l'attenzione

Ermann Ripepi
Consiglio Nazionale delle Ricerche
Istituto di Metodologie per l'Analisi Ambientale

ermann.ripepi@imaa.cnr.it