

# 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



- 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

Uses lucene query syntax

Netflow: Dashboard Navigation

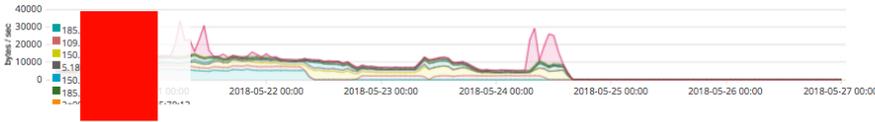
Overview | Conversation Partners | Traffic Analysis | Top-N | Geo Location | Autonomous Systems | Flow Exporters | Raw Flow Records

Netflow: Sources (bytes)



**1,137,451**  
Sources

Netflow: Sources (packets)

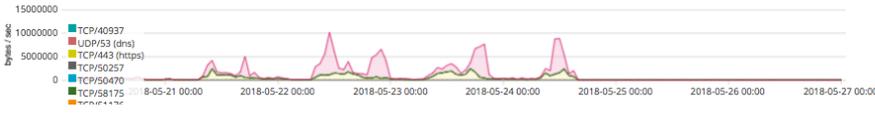


Netflow: Source Ports (bytes)



**128,202**  
Source Ports

Netflow: Source Ports (packets)

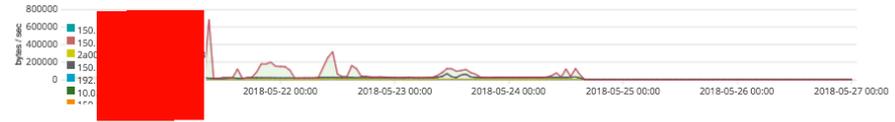


Netflow: Destinations (bytes)

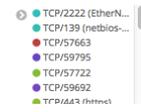


**229,116**  
Destinations

Netflow: Destinations (packets)

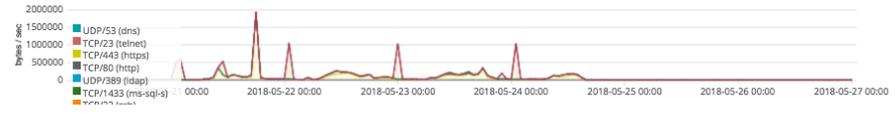


Netflow: Destination Ports (bytes)



**127,810**  
Destination Ports

Netflow: Destination Ports (packets)



# Elastic – Flussi di dati

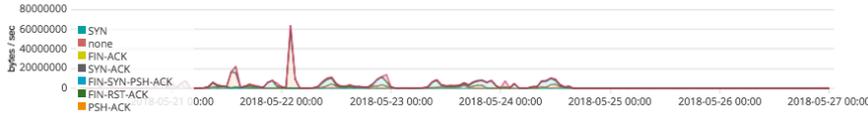
Netflow: TCP Flags (bytes)



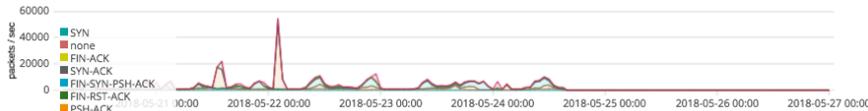
- FIN-SYN-PSH-ACK
- SYN-PSH-ACK
- PSH-ACK
- FIN-ACK
- none
- ACK
- FIN-PSH-ACK

**237**  
TCP Flag States

Netflow: TCP Flags (bytes)



Netflow: TCP Flags (packets)



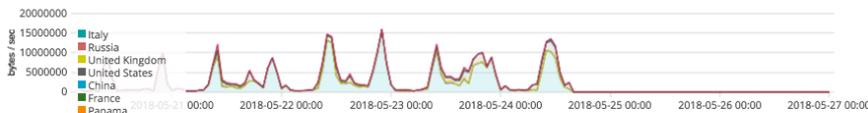
Netflow: Countries (bytes)



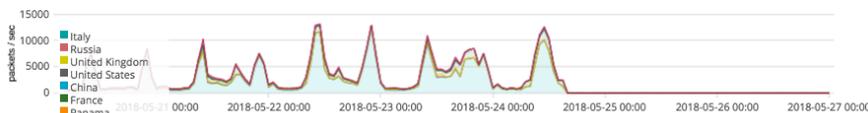
- Italy
- United States
- Netherlands
- Ireland
- Germany
- United Kingdom
- Romania

**221**  
Countries

Netflow: Countries (bytes)



Netflow: Countries (packets)



Netflow: TCP Flags Count

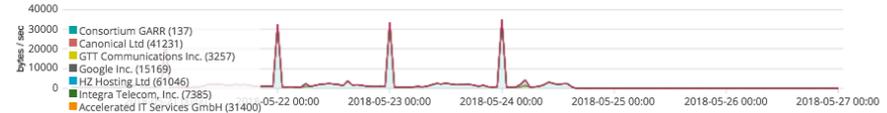
Netflow: Autonomous Systems (bytes)



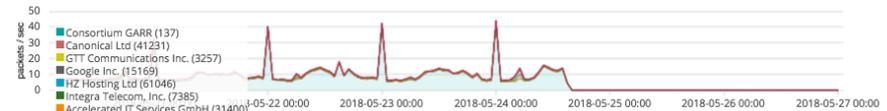
- Consortium GARR ...
- HZ Hosting Ltd (61...
- Incapsula Inc (195...
- Accelerated IT Ser...
- Dell, Inc. (3614)
- Google Inc. (15169)
- Microsoft Corpora...

**74**  
Autonomous Systems

Netflow: Autonomous Systems (bytes)



Netflow: Autonomous Systems (packets)



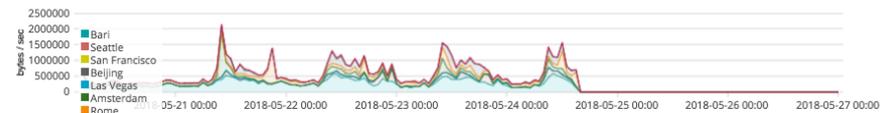
Netflow: Cities (bytes)



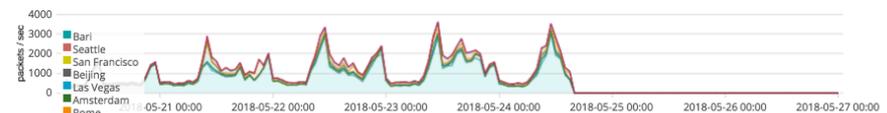
- Bari
- Monterotondo
- Rome
- Mountain View
- Redmond
- Amsterdam
- Seattle

**24,821**  
Cities

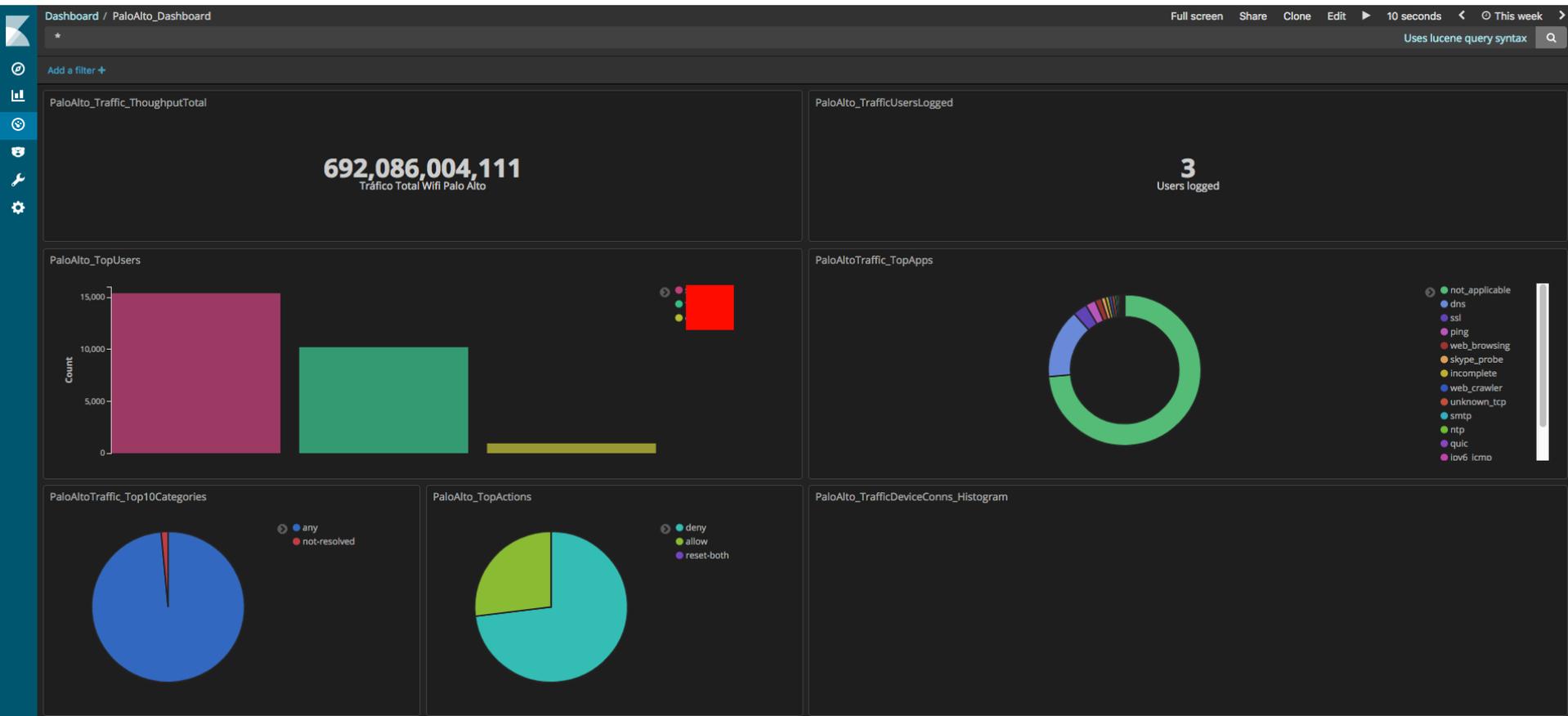
Netflow: Cities (bytes)



Netflow: Cities (packets)



# Elastic – Syslog



# Elastic – Apache

kibana

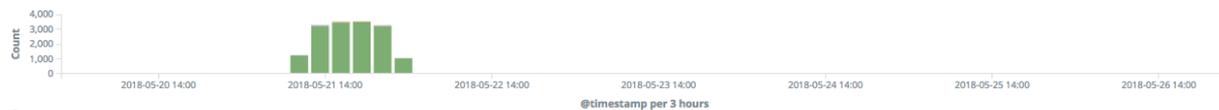
- Discover
- Visualize
- Dashboard
- Timelion
- Dev Tools
- Management

Collapse

Unique IPs map [Filebeat Apache2]



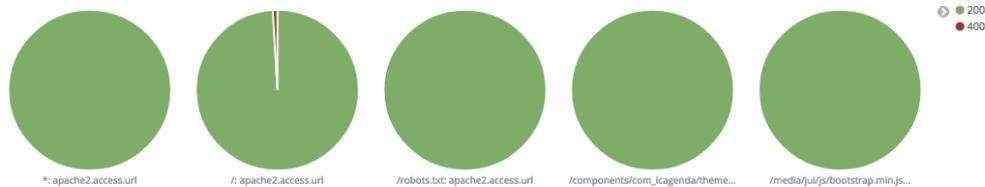
Response codes over time [Filebeat Apache2]



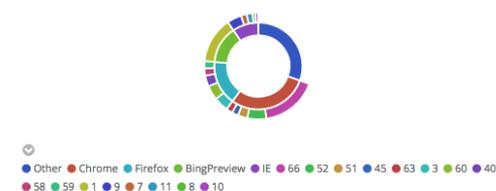
Operating systems breakdown [Filebeat A...]



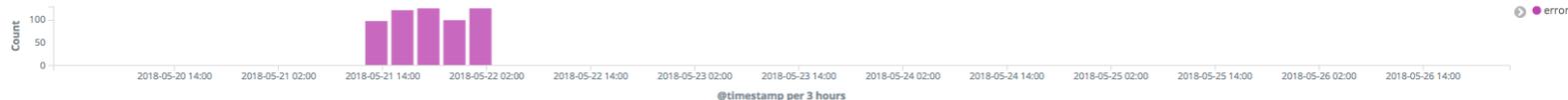
Top URLs by response code [Filebeat Apache2]



Browsers breakdown [Filebeat Apache2]



Error logs over time [Filebeat Apache2]



Apache errors log [Filebeat Apache2]

1-50 of 572

Time	apache2.error.client	apache2.error.level	apache2.error.module	apache2.error.message
May 22nd 2018, 02:56:52.422	-	error	-	[client 163.172.34696] PHP Notice: Only variables should be assigned by reference in /var/www/plugins/content/articlebookeffect/articlebookeffect.php on line 240
May 22nd 2018, 02:56:52.422	-	error	-	[client 163.172.34696] PHP Notice: Only variables should be assigned by reference in /var/www/plugins/content/articlebookeffect/articlebookeffect.php on line 240
May 22nd 2018, 02:56:52.422	-	error	-	[client 163.172.34696] PHP Notice: Only variables should be assigned by reference in /var/www/plugins/content/articlebookeffect/articlebookeffect.php on line 98

- 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



- 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



- <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



- 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>

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

- [wg-sec@garr.it](mailto:wg-sec@garr.it) (generica per tutti)
- [wg-sec-ddos@garr.it](mailto:wg-sec-ddos@garr.it) (sottogruppo DDoS)
- [wg-sec-scan@garr.it](mailto:wg-sec-scan@garr.it) (sottogruppo Intrusion Detection, Network auditing/monitoring)
- [wg-sec-best@garr.it](mailto:wg-sec-best@garr.it) (sottogruppo Best Practice)
- [wg-sec-2081x@garr.it](mailto: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](mailto:ermann.ripepi@imaa.cnr.it)