

# GarrLab e primi risultati

url-shortener e Wazuh

Giuseppe De Marco  
Università della Calabria

WORK  
SHOP  
GARR  
2020

NET  
MAKERS

 Consortium  
GARR



- Security Information and **E**vent **M**anagement
- Cloud, On-Premises and Container security
- Agents: **E**ndpoint **D**etection and **R**esponse
- Agents-less: Log Data Analysis and SSH polling
- File Integrity Monitoring
- Configuration inventory, Common Vulnerabilities and Exposure scanner
- Compliant to **PCI DSS**, **HIPAA**, **GDPR**, **NIST 800-53**

<https://wazuh.com/>



## **django** url-shortener

- bit-shuffling approach to avoid predictable URLs
- Deterministic, no collisions will occur
- Rest API (token auth)
- Image and Audio Captcha
- Bootstrap Italia Compliant (AGID Guidelines)

<https://gitlab.garrlab.it/peppelinux/tinyurl>

<https://github.com/UniversitaDellaCalabria/urlShortener>



## SIEM Crew (shuffled)

- Ermann Ripepi ..... CNR IMAA
- Damiano Verzulli..... Università di Chieti
- Michele Pinassi ..... Università di Siena
- Giuseppe De Marco . Università della Calabria
- Enrico Ardizzoni ..... Università di Ferrara
- Francesco Izzi ..... CNR IMAA
- Simona Venuti ..... GARR
- Simone Bonetti ..... CERT-UniBo
- Luca Vanni ..... ICRANET
- Michele Albrigo ..... Università di Verona
- Marco Cappellacci ... Università di Urbino
- Marco Nesler ..... Università di Trento
- Salvatore Todaro ..... Università di Messina
- Marco Pirovano ..... Università Bocconi
- Giorgio Giorgetti ..... Università di Trieste
- Luca Deri ..... nTOP lead
- Fulvio Galeazzi ..... GARR

GARR Lab bot

# A SIEM with an Open Source Stack



TrendMicro 2003 - 2013 CodeBase  
OSSEC Fork  
ansi C and Python  
GNU GPL 2 LICENSE

Search Engine  
Lucene Full Text RestFul API  
Java  
Apache 2 LICENSE

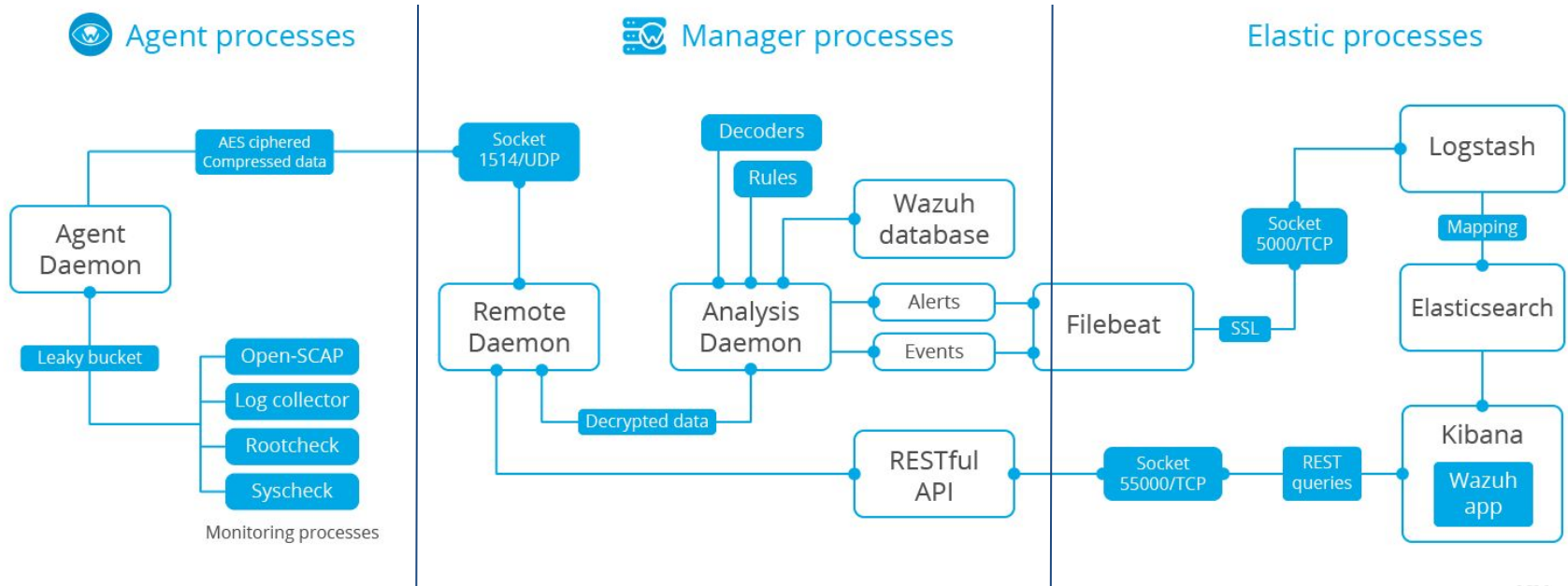


elasticsearch



Data visualization dashboard (UX)  
Javascript  
Elastic License/Apache License

# The Big Picture



# Welcome to the SIEM (the Machine)

## Overview

Wazuh Overview

Agents: 14 Total agents, 12 Active agents, 1 Disconnected agents, 1 Never connected agents

### SECURITY INFORMATION MANAGEMENT

- Security events**  
Browse through your security alerts, identifying issues and threats in your environment.
- Integrity monitoring**  
Alerts related to file changes, including permissions, content, ownership and attributes.

### AUDITING AND POLICY MONITORING

- Policy monitoring**  
Verify that your systems are configured according to your security policies baseline.
- System auditing**  
Audit users behavior, monitoring command execution and alerting on access to critical files.

### THREAT DETECTION AND RESPONSE

- Vulnerabilities**  
Discover what applications in your environment are affected by well-known vulnerabilities.

### REGULATORY COMPLIANCE

- PCI DSS**  
Global security standard for entities that process, store or transmit payment cardholder data.
- GDPR**  
General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.
- HIPAA**  
Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides data privacy and security provisions for safeguarding medical information.
- NIST 800-53**  
National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.

# GDPR requirements and remediations (Part I)

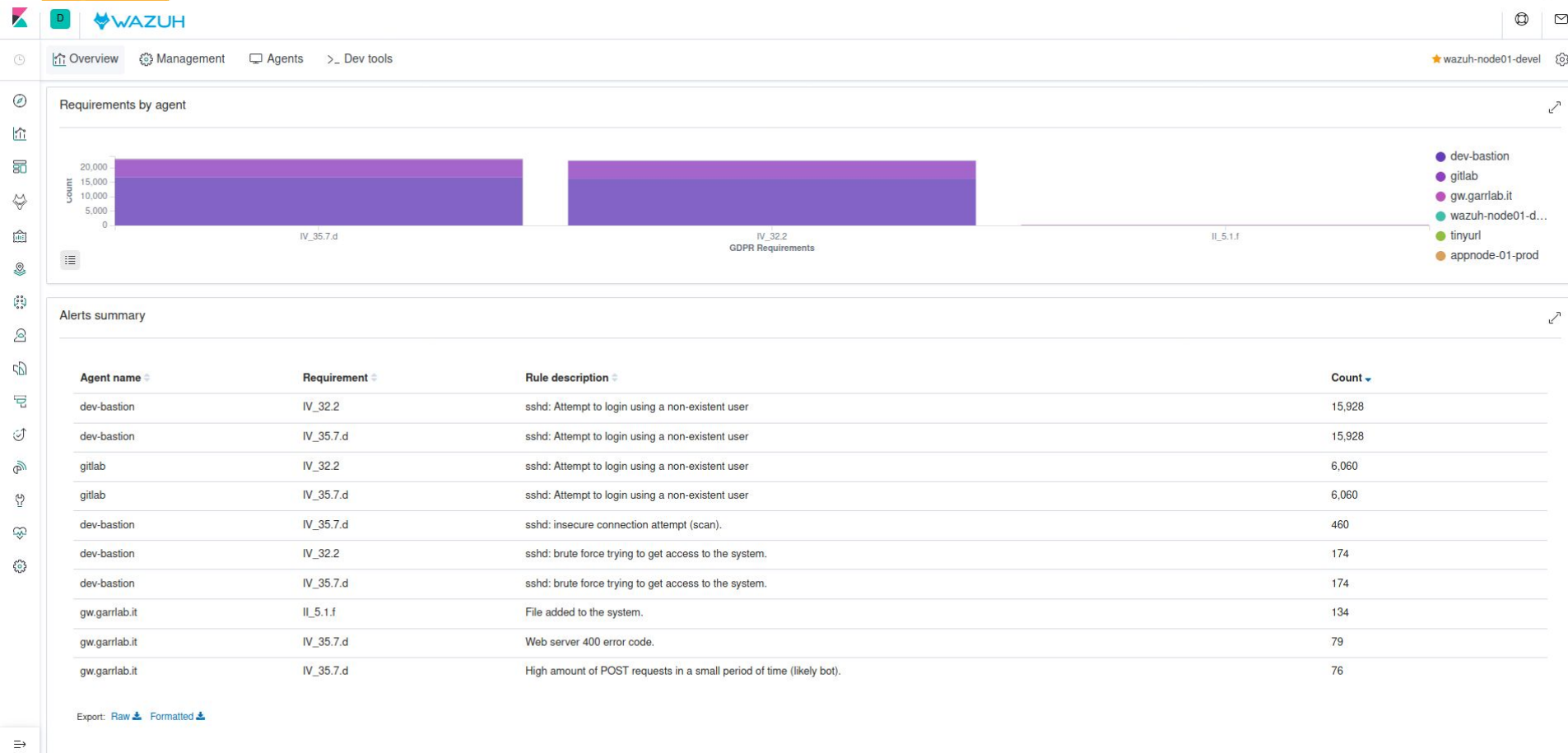
The screenshot displays the Wazuh dashboard interface. At the top, the navigation bar includes 'Overview', 'Management', 'Agents', and 'Dev tools'. The current view is 'Overview / GDPR'. Below this, there are tabs for 'PCI DSS', 'GDPR', 'HIPAA', and 'NIST 800-53'. A search bar is present with filters for 'manager.name: wazuh-node01-devel' and 'rule\_gdpr exists'. The main content area is divided into four panels, each representing a specific GDPR requirement:

- GDPR Requirement: II\_5.1.f**: Ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. Verifying its modifications, accesses, locations and guarantee the safety of them. File sharing protection and file sharing technology...
- GDPR Requirement: IV\_30.1.g**: It is necessary to keep all processing activities documented, to carry out an inventory of data from beginning to end and an audit, in order to know all the places where personal and sensitive data are located, processed, stored or transmitted.
- GDPR Requirement: IV\_32.2**: Account management tools that closely monitor actions taken by standard administrators and users who use standard or privileged account credentials are required to control access to data.
- GDPR Requirement: IV\_35.7.d**: Capabilities for identification, blocking and forensic investigation of data breaches by malicious actors, through compromised credentials, unauthorized network access, persistent threats and verification of the correct operation of all componen...

Below these panels, there are two charts:

- Top 10 agents by alerts number**: A pie chart showing the distribution of alerts across various agents. The legend includes: dev-bastion, gitlab, gw.garrlab.it, wazuh-node01-d..., tinyurl, kea-dhcpd, telegram-gw, appnode-02-prod, pdns-admin, and appnode-01-prod.
- GDPR requirements**: A bubble chart showing the count of alerts for each requirement over time (timestamp per 3 hours). The y-axis represents the count (0 to 5,000), and the x-axis shows timestamps from 2020-10-19 00:00 to 2020-10-25 00:00. A significant peak is visible around 2020-10-20 00:00.

# GDPR requirements and remediations (Part II)





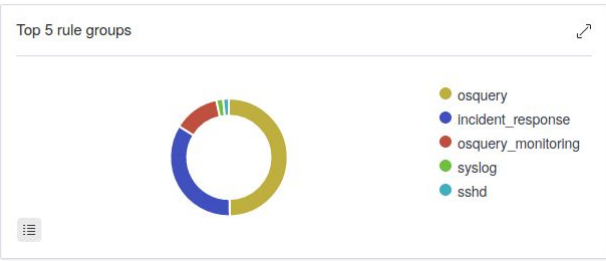
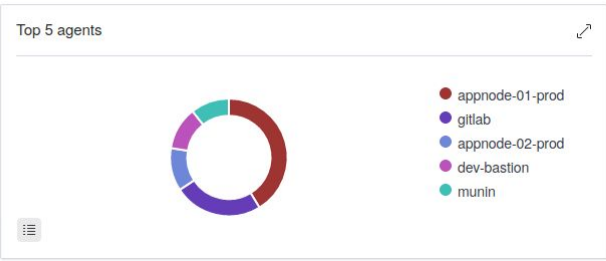
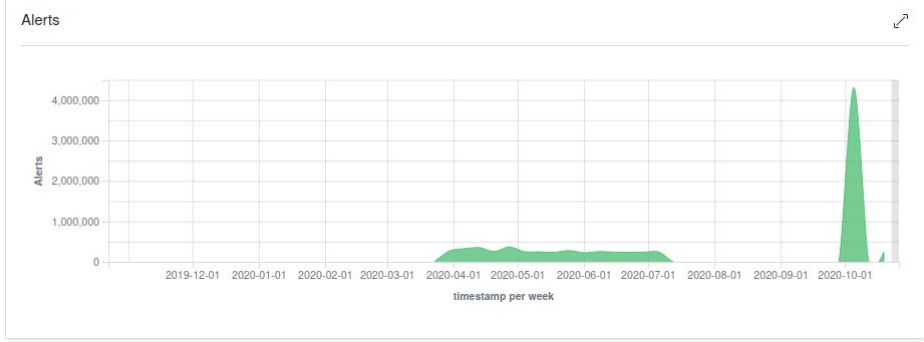
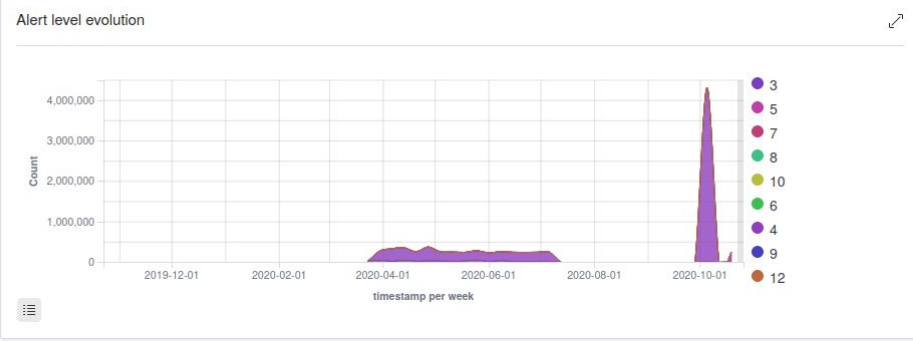
# Security Events (Part I)

Search KQL Last year Show dates Refresh

manager.name: wazuh-node01-devel + Add filter

Total **8,795,308**      Level 12 or above alerts **26**

Authentication failure **251,719**      Authentication success **24,884**



# Agents Installed

Status



Active  
Disconnected  
Never connected

Details

Active 12 Disconnected 1 Never connected 1 Agents coverage 85.71%

Last registered agent tinyurl  
Most active agent dev-bastion

Q Add filter or search

Refresh

+ Add new agent

ID	Name	IP	Status	Group	OS name	OS version	Version	Registration date	Last keep alive	Actions
001	dev-bastion	172.16.16.254	Active	default,ubuntu	Ubuntu	18.04.4 LTS	Wazuh v3.13.0	2020/03/31 16:34:38	2020/10/19 19:09:50	
002	pdns-admin	172.16.16.105	Active	default,ubuntu	Ubuntu	18.04.4 LTS	Wazuh v3.12.0	2020/03/31 16:34:38	2020/10/19 19:09:49	
003	gitlab	172.16.16.101	Active	default,ubuntu	Ubuntu	18.04.4 LTS	Wazuh v3.12.0	2020/03/31 16:34:38	2020/10/19 19:09:45	
004	garr-bar-devel	any	Never connected	ubuntu	-	-	-	2020/03/31 16:34:38	-	
005	telegram-gw	172.16.16.102	Active	default,ubuntu	Ubuntu	18.04.4 LTS	Wazuh v3.12.0	2020/03/31 16:34:38	2020/10/19 19:09:52	
006	pgdb-01	172.16.16.104	Active	default,ubuntu	Ubuntu	18.04.4 LTS	Wazuh v3.12.0	2020/03/31 16:34:38	2020/10/19 19:09:51	
007	gw.garrlab.it	192.168.0.153	Active	default,ubuntu,nginx	Ubuntu	18.04.4 LTS	Wazuh v3.12.3	2020/03/31 16:34:38	2020/10/19 19:09:53	
008	powerdns-as	172.16.16.103	Active	default,ubuntu	Ubuntu	18.04.4 LTS	Wazuh v3.12.0	2020/03/31 16:34:38	2020/10/19 19:09:53	
009	appnode-02-prod	172.16.16.3	Active	default,ubuntu	Ubuntu	18.04.4 LTS	Wazuh v3.12.0	2020/03/31 16:34:38	2020/10/19 19:09:51	
010	kea-dhcpd	172.16.16.110	Active	default,ubuntu	Ubuntu	18.04.4 LTS	Wazuh v3.12.3	2020/03/31 16:34:38	2020/10/19 19:09:49	
011	munin	172.16.16.108	Active	default,ubuntu	Ubuntu	18.04.4 LTS	Wazuh v3.12.0	2020/03/31 16:34:38	2020/10/19 19:09:51	
012	appnode-01-prod	172.16.16.2	Active	default,ubuntu	Ubuntu	18.04.4 LTS	Wazuh v3.12.0	2020/03/31 16:34:38	2020/10/19 19:09:50	
013	jessie	10.0.3.10	Disconnected	default,debian	Debian GNU/Linux	8	Wazuh v3.12.0	2020/04/04 01:10:07	2020/04/04 14:38:31	
014	tinyurl	172.16.16.112	Active	default,debian,nginx,django	Ubuntu	18.04.4 LTS	Wazuh v3.12.0	2020/04/06 12:15:02	2020/10/19 19:09:53	

14 items (1.17 seconds)

# Artifacts and Customizations

## Things done, for real

1. Documentation, Knowledge management (<https://gitlab.garrlab.it/siem/wazuh>)
2. Wodles enabled:
  - OSQuery, OpenSCAP (Simone Bonetti)
3. Disaster Recovery
4. 2 Custom Dashboards:
  - Top 100 Threats (Giuseppe De Marco, Francesco Izzi)
  - SSH Anomalies (Damiano Verzulli)
5. Lucene API and Wazuh-API usage notes (Giuseppe De Marco, Francesco Izzi)
6. Telegram BOT (Giuseppe De Marco, Francesco Izzi)
7. Custom Decoders and Rules:
  - FortiGate Custom Rules (Michele Pinassi)
  - HTTPd Log Auditing (Apache2 and NginX) Injections (XSS, SQL) and Error Codes
  - Shibboleth IdP Login events and Brute Force Detection
  - django-audit-wazuh (<https://github.com/peppelinux/django-audit-wazuh>)

# Custom Dashboard: Top 100 Threats



Dashboard / Wazuh Alerts

Full screen Share Clone Edit

Search

KQL

Last 1 year

Show dates

Refresh

+ Add filter

## Alert summary

Rule ID	Description	Level	Count
5108	System running out of memory. Availability of the system is in risk.	12	6
31151	Multiple web server 400 error codes from same source ip.	10	14
31533	High amount of POST requests in a small period of time (likely bot).	10	75
5712	sshd: brute force trying to get access to the system.	10	968
5302	User missed the password to change UID to root.	9	7
19005	SCA summary: CIS benchmark for Debian/Linux 9 L2: Score less than 30% (17)	9	2
19005	SCA summary: CIS benchmark for Debian/Linux 9 L2: Score less than 30% (10)	9	15
5904	Information from the user was changed.	8	8
5902	New user added to the system.	8	12
5901	New group added to the system.	8	16
5104	Interface entered in promiscuous(sniffing) mode.	8	39
5758	Maximum authentication attempts exceeded.	8	94
5701	sshd: Possible attack on the ssh server (or version gathering).	8	248
19004	SCA summary: CIS benchmark for Debian/Linux 9 L1: Score less than 50% (37)	7	1
19004	SCA summary: CIS benchmark for Debian/Linux 9 L1: Score less than 50% (38)	7	10
2903	Dpkg (Debian Package) removed.	7	41
553	File deleted.	7	73
510	Host-based anomaly detection event (rootcheck).	7	82
19007	CIS benchmark for Debian/Linux 9 L1: Ensure core dumps are restricted	7	2
19007	CIS benchmark for Debian/Linux 9 L1: Ensure HTTP Server is not enabled	7	2
19007	CIS benchmark for Debian/Linux 9 L2: Ensure auditing for processes that start prior to auditd is enabled	7	3
19007	CIS benchmark for Debian/Linux 9 L1: Ensure bootloader password is set	7	3
19007	CIS benchmark for Debian/Linux 9 L1: Ensure IPv6 default deny firewall policy	7	5
19007	CIS benchmark for Debian/Linux 9 L1: Ensure IP forwarding is disabled	7	5

## AccessMap

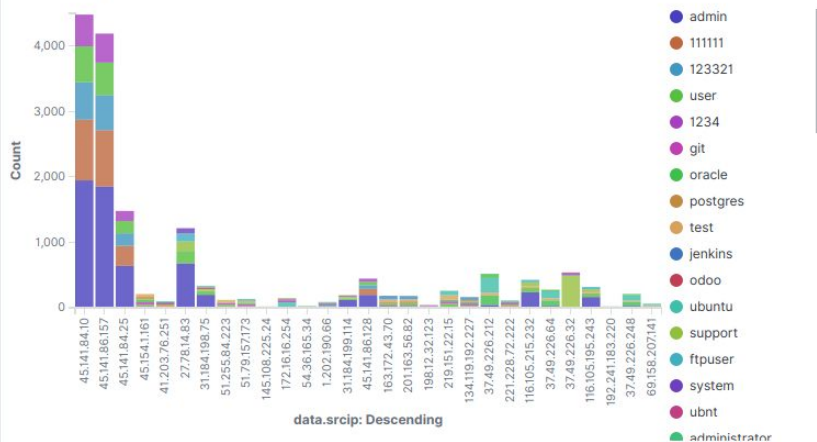


## pieChartCountByCityName



# Custom Dashboard: SSH Fails

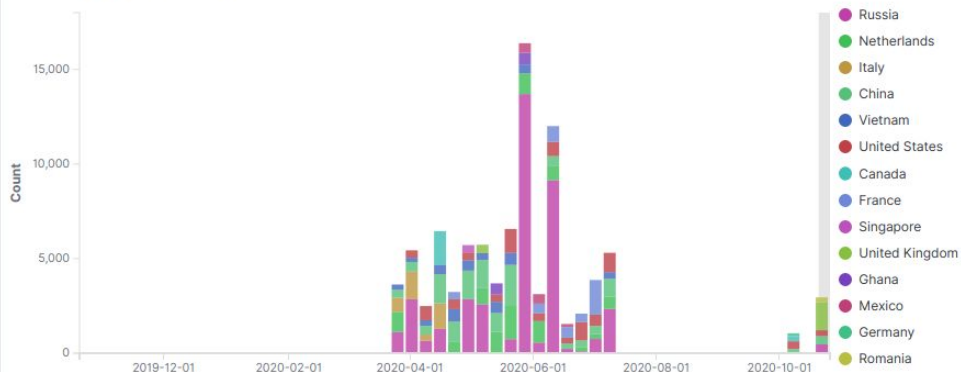
### SSH-FailedLogin\_TOP30\_by\_IP



### SSH-FailedLogin\_TOP30\_by\_Country



### SSH-Failed\_login\_trend\_by\_country



### SSH-Failed-login tag cloud



# Things not done

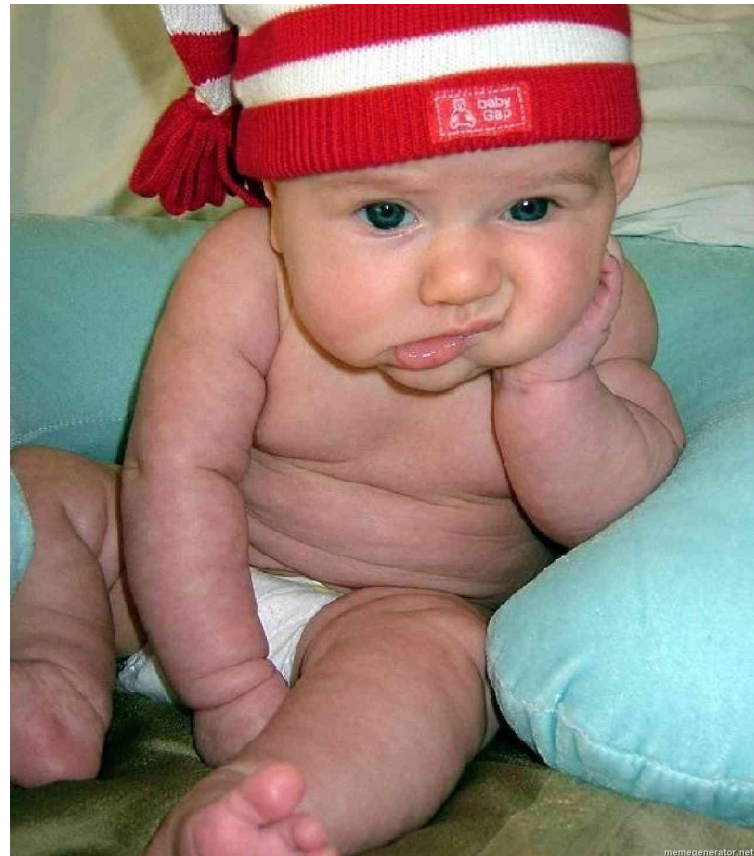
That would have been useful

A fully integrated **Network Intrusion Detection System** profile based on :



We know how we would do it, Security Onion!

<https://github.com/Security-Onion-Solutions/securityonion>



# url-shortener

<https://url.garrlab.it>

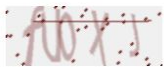


- Mobile ready
- Based on python [short url](#)
- Full **int18n** support (Gettext):
  - available languages italian, english (Elis Bertazzon GARR)
- Audio (localized!) and Image **CaPTCHA** validation
- **Rest API** with Basic and Token Authentication
- django-audit-wazuh for Wazuh **SIEM integration**
- <https://url.garrlab.it>

## URL SHORTENER

The URL or the CaPTCHA you have inserted is not valid.

This service store your shortened Urls for a maximum period of 12 days.  
It will be more simple to share ith your collegues and friends.



Please enter the value represented in the CaPTCHA image.

Create a shortened Url

Università della Calabria

Accedi



Seguici su [f](#) [t](#) [i](#) [v](#)

### UrlShortner

Questo servizio consente di conservare per **infiniti** giorni un url in formato "ristretto".  
Sarà più facile condividerlo con amici e colleghi.



REFRESH



Insert CaPTCHA here

Inserisci il valore rappresentato nella immagine  
CaPTCHA.

Crea un URL semplificato

*That's all Folks!*

**Is there any questions?**

[giuseppe.demarco@unical.it](mailto:giuseppe.demarco@unical.it)