GarrLab e primi risultati

url-shortener e Wazuh

Giuseppe De Marco
Università della Calabria

WORKSHOP GARR 2020

NET MAKERS

Consortium GARR

- **S**ecurity **I**nformation 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/

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

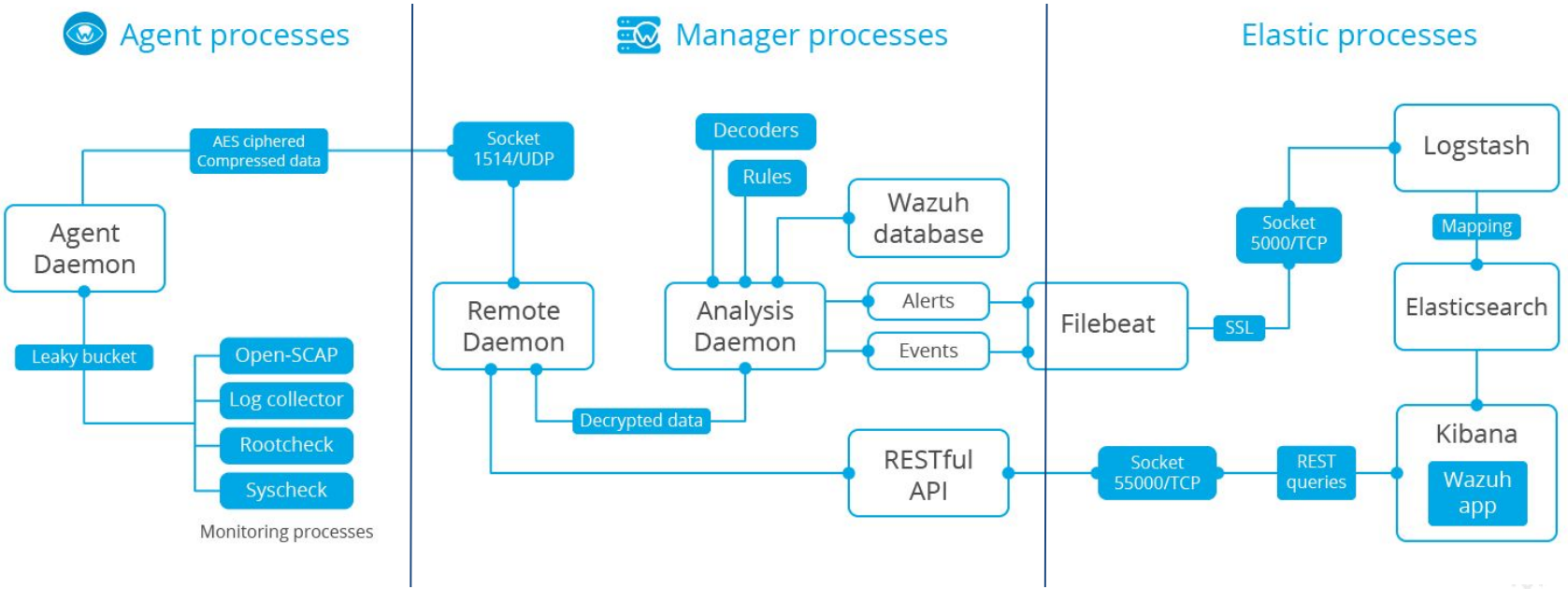
TrendMicro 2003 - 2013 CodeBase
OSSEC Fork
ansi C and Python
GNU GPL 2 LICENSE

elasticsearch

Search Engine
Lucene Full Text RestFul API
Java
Apache 2 LICENSE

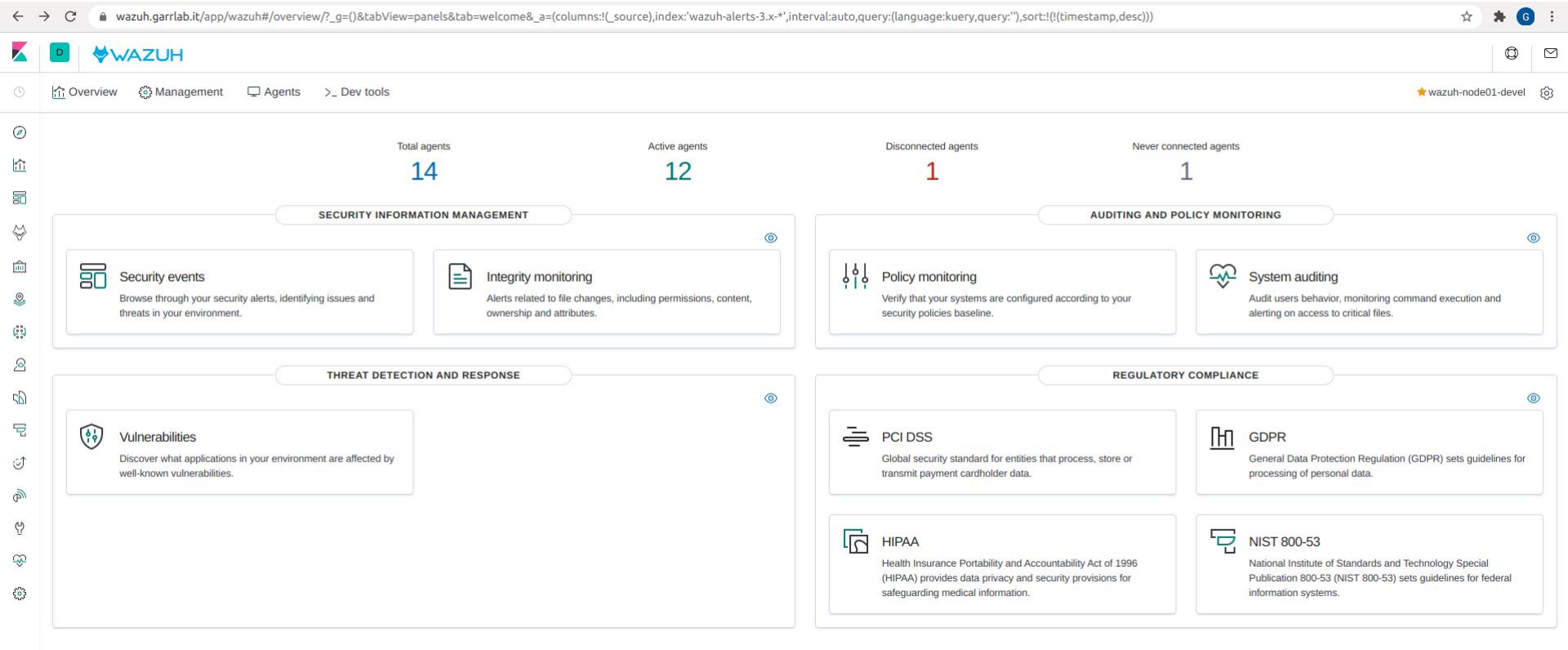
Data visualization dashboard (UX)
Javascript
Elastic License/Apache License

The Big Picture

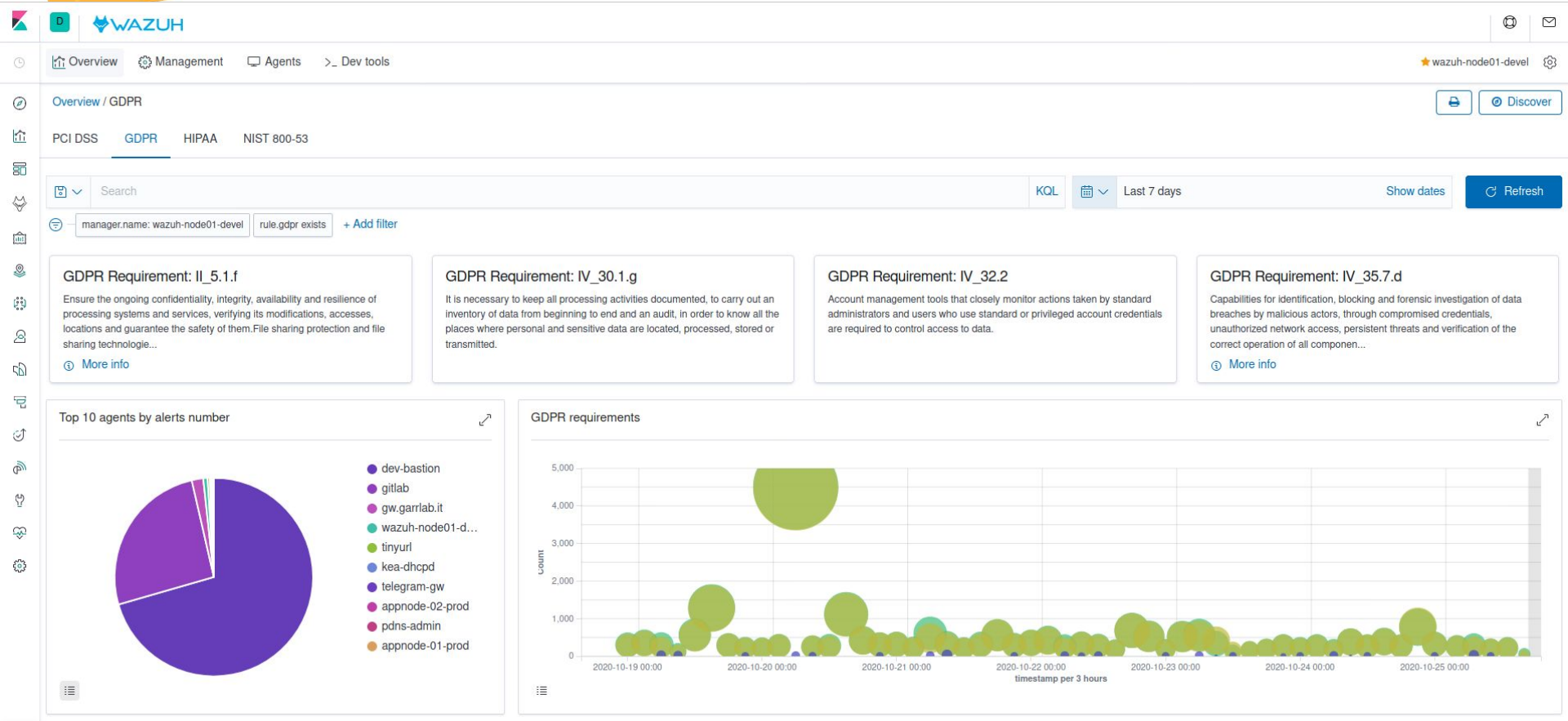


Welcome to the SIEM (the Machine)

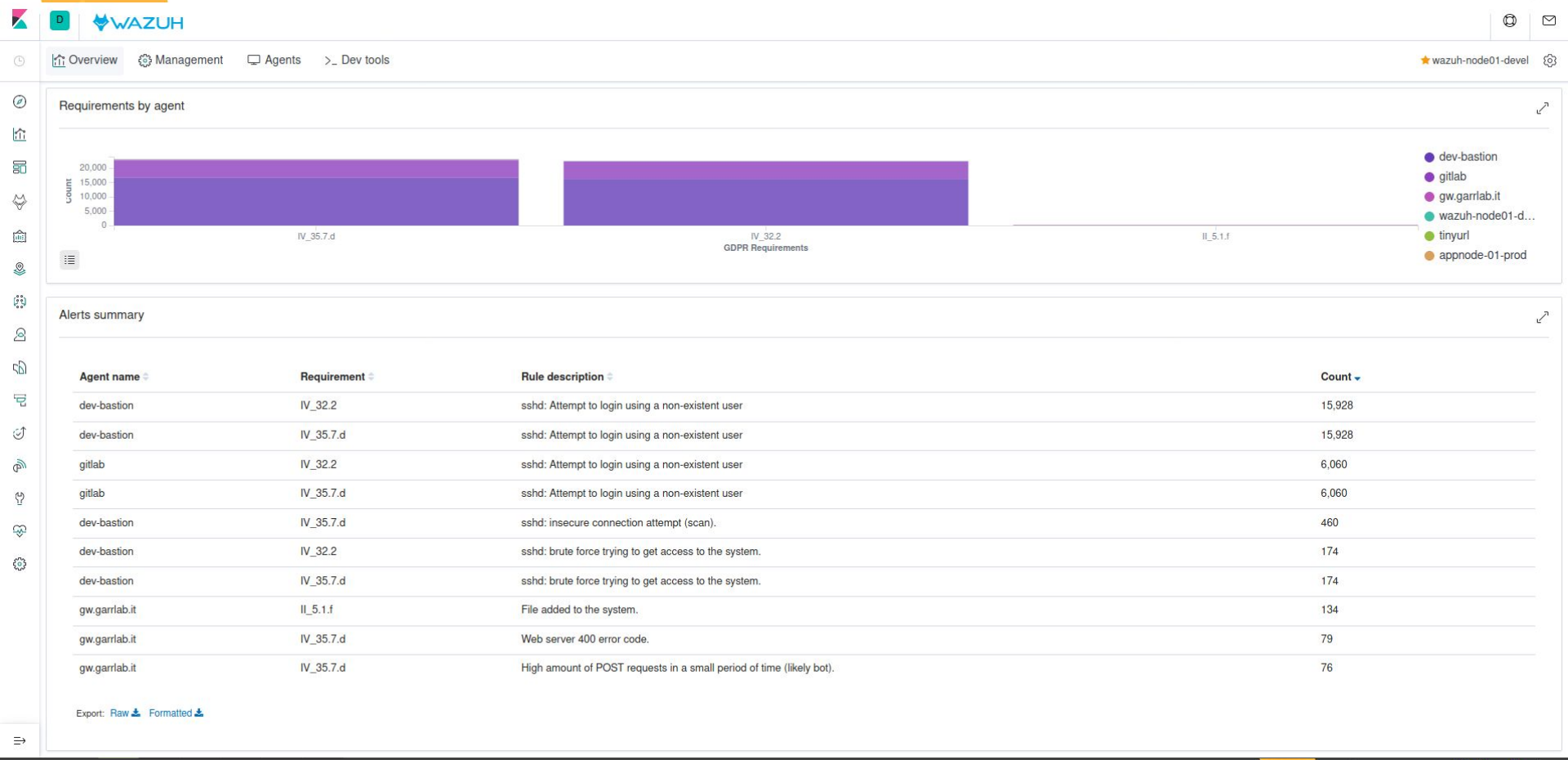
Overview



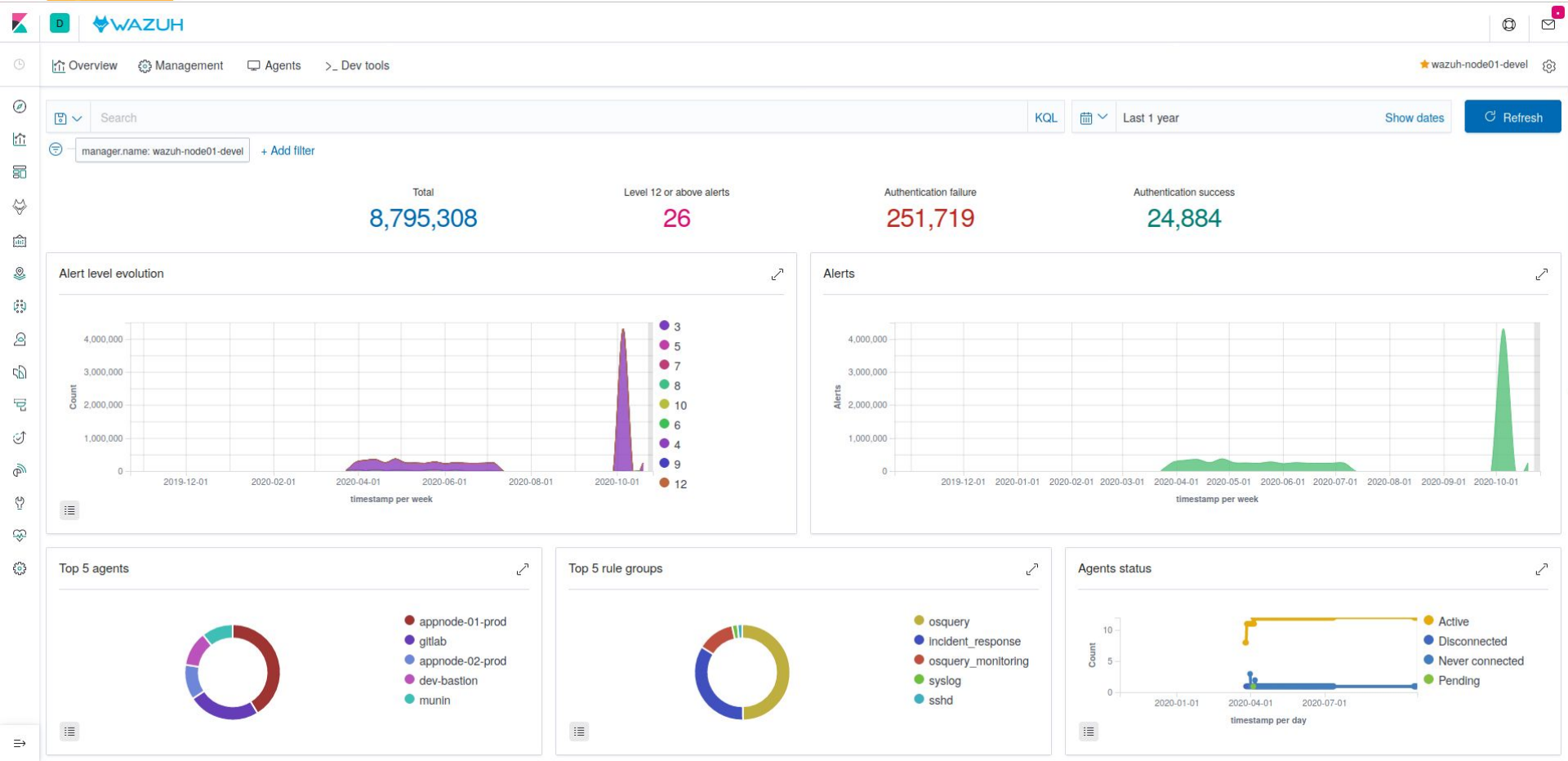
GDPR requirements and remediations (Part I)



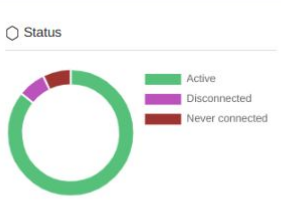
GDPR requirements and remediations (Part II)



Security Events (Part I)



Agents Installed



Details

Active	Disconnected	Never connected	Agents coverage
12	1	1	85.71%

Last registered agent: tinyurl

Most active agent: dev-bastion

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)

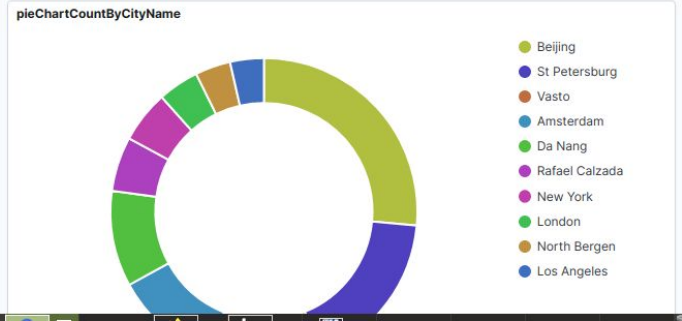
Custom Dashboard: Top 100 Threats

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

Things not done

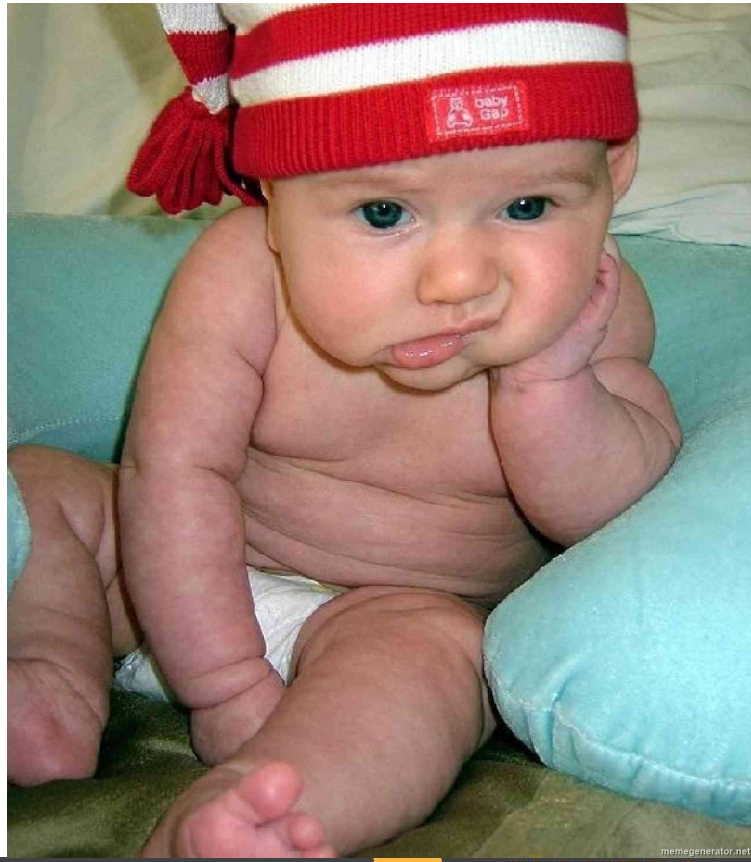
That would have been useful

A fully integrated **N**etwork **I**ntrusion **D**etection **S**ystem profile based on :

SURICATA

zeek

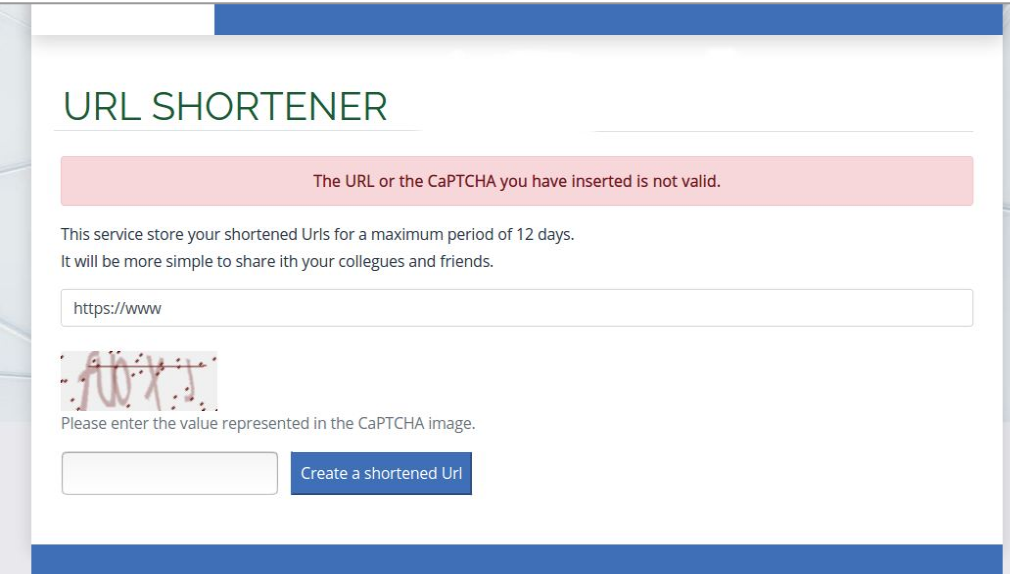
We know how we would do it, Security Onion!
https://github.com/Security-Onion-Solutions/securityonion

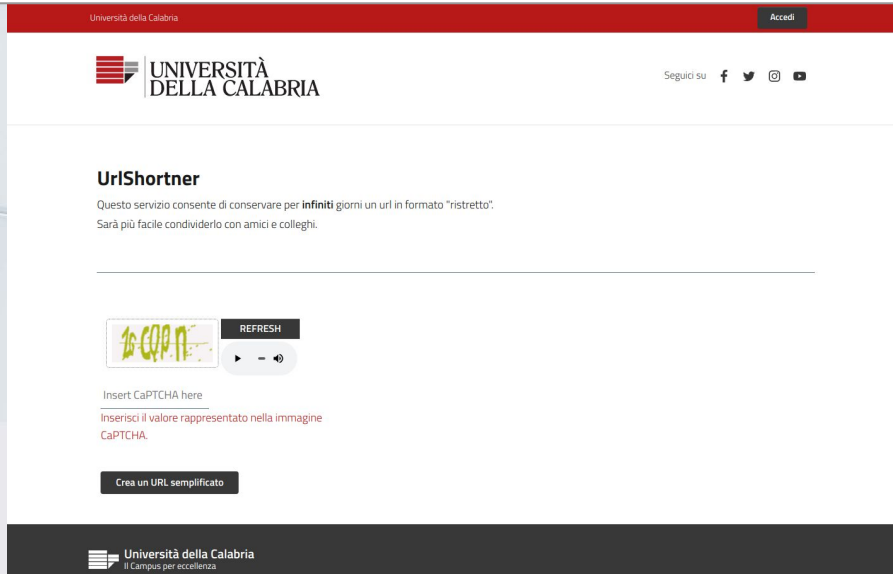


url-shortener

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





Is there any questions?

giuseppe.demarco@unical.it