PLEDGER

Paving the way for next-generation edge computing

pledger-project.eu

The Pledger Security Approach

1st Future ICT Workshop
Athens, Greece, 25/5/2022

Dr. Olga Segou
Netcompany-Intrasoft

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under the Grant Agreement No 871536

This project has received funding from the European Union’s Horizon 2020 Research and Innovation Programme under the Grant Agreement No 871536

Pledger Overview and Security Architecture

Introduction to Pledger

Pledger is an innovative project that will deliver a set of tools and processes to enable:

a) **edge computing providers** to enhance the stability and performance effectiveness of their edge infrastructures, through modelling the overheads and optimal groupings of concurrently running services, runtime analysis and adaptation,

b) **edge computing adopters** to understand the computational nature of their applications, investigate abstracted and understandable QoS metrics, facilitate trust and smart contracting over their infrastructures and identify how they can balance their cost and performance.

By providing this toolset, the project will also allow third parties to act as independent validators of QoS features in IoT applications.

Security concerns

However, the complex and decentralised nature of Edge-Cloud infrastructures, along with their dynamic nature introduces cyber risks:

- When applications and services can be instantiated and turn down in seconds, have critical QoS demands and perform data-intensive operations, it is crucial to ensure that the infrastructure is **appropriately hardened,** and **proper cybersecurity assets are in place to address evolving cyber threats and ensure privacy and service continuity.**

- **INTRA leads the security and integration tasks in the project and provides digital assets such as CI/CD, the Streamhandler platform and the virtualised Intrusion Detection system.**

Threat analysis

In the case of Edge-Cloud deployments, it is necessary not only to apply threat modelling, but also extend it in key areas.

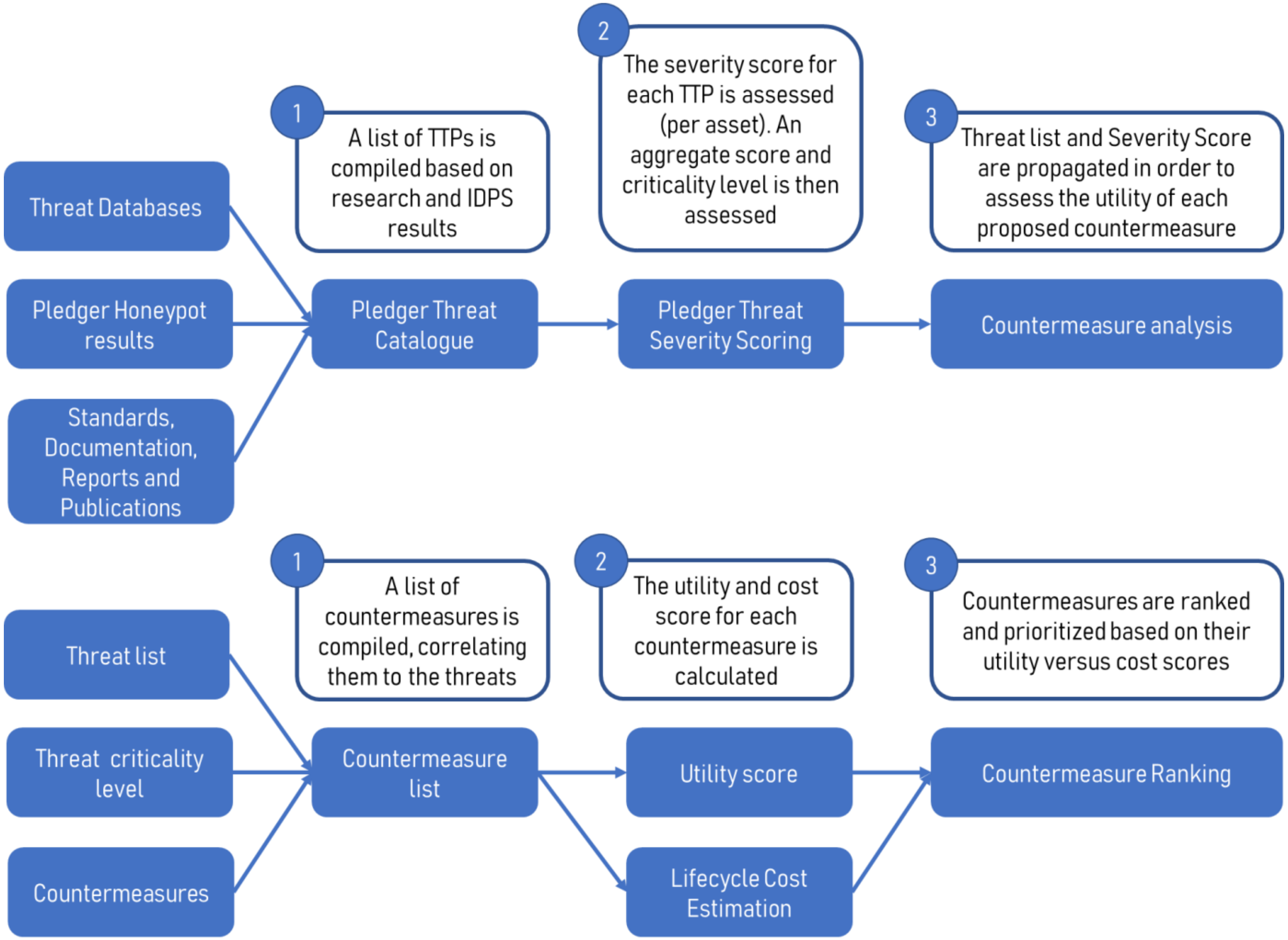
- When it comes to the deployment of services on the mobile edge, multiple stakeholders may be involved, **forming complicated value chains.**

- Taking into account the complexity of the integration of multiple software, hardware, network and storage technologies, there needs to be a complete methodology that also provides a way to **prioritise threats and remediations.**

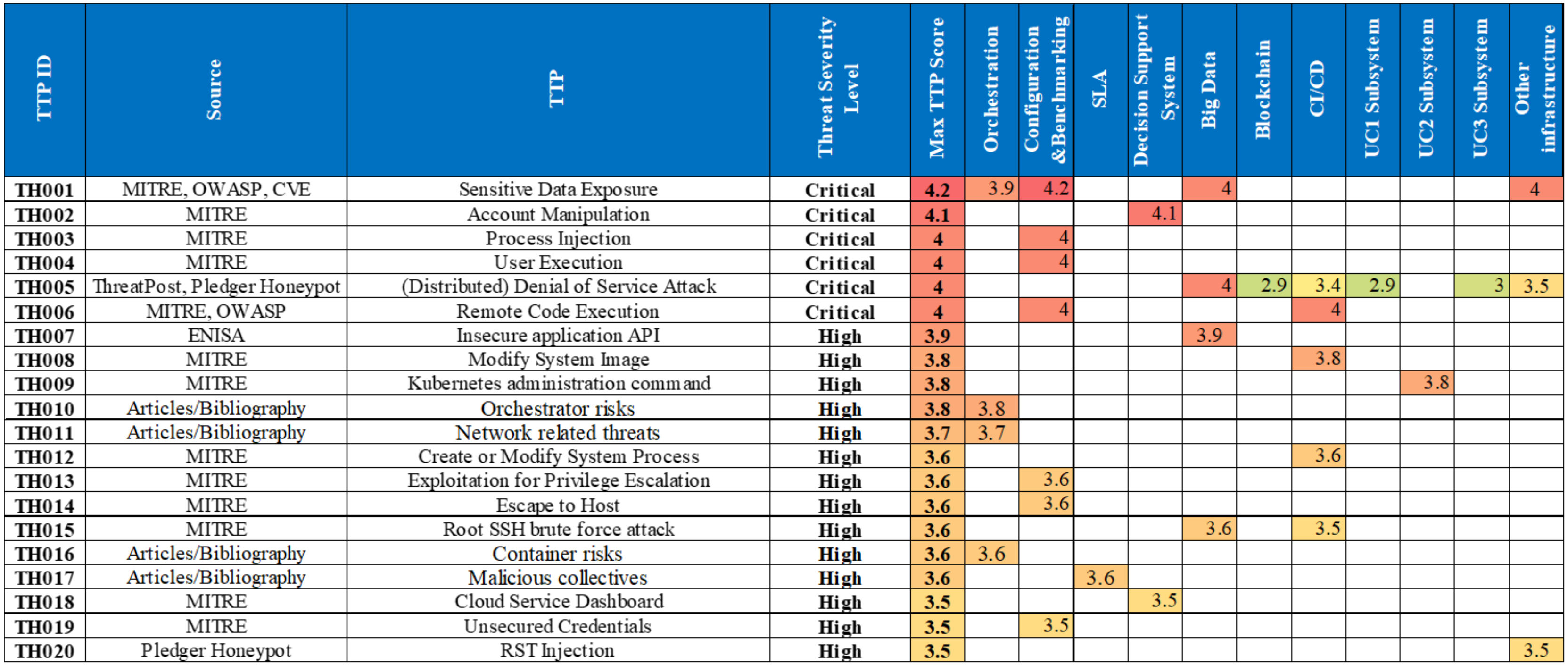
- Furthermore, new factors other than the traditional Confidentiality, Integrity and Availability triplet should be accounted for, especially for use cases with strict QoS/QoE requirements. **Degradation of service quality can easily become a major problem in mission-critical services.**

The Pledger threat analysis methodology

Figure 1: Threat analysis methodology, loosely based on MITRE TARA method.


1
A list of TTPs is compiled based on research and IDPS results
2
The severity score for each TTP is assessed (per asset). An aggregate score and criticality level is then assessed
3
Threat list and Severity Score are propagated in order to assess the utility of each proposed countermeasure
Threat Databases
Pledger Honeypot results
Standards, Documentation, Reports and Publications
Pledger Threat Catalogue
Pledger Threat Severity Scoring
Countermeasure analysis
1
A list of countermeasures is compiled, correlating them to the threats
2
The utility and cost score for each countermeasure is calculated
3
Countermeasures are ranked and prioritized based on their utility versus cost scores
Threat list
Threat criticality level
Countermeasures
Countermeasure list
Utility score
Lifecycle Cost Estimation
Countermeasure Ranking

Top-20 threats to Pledger Cloud-Edge Infrastructure

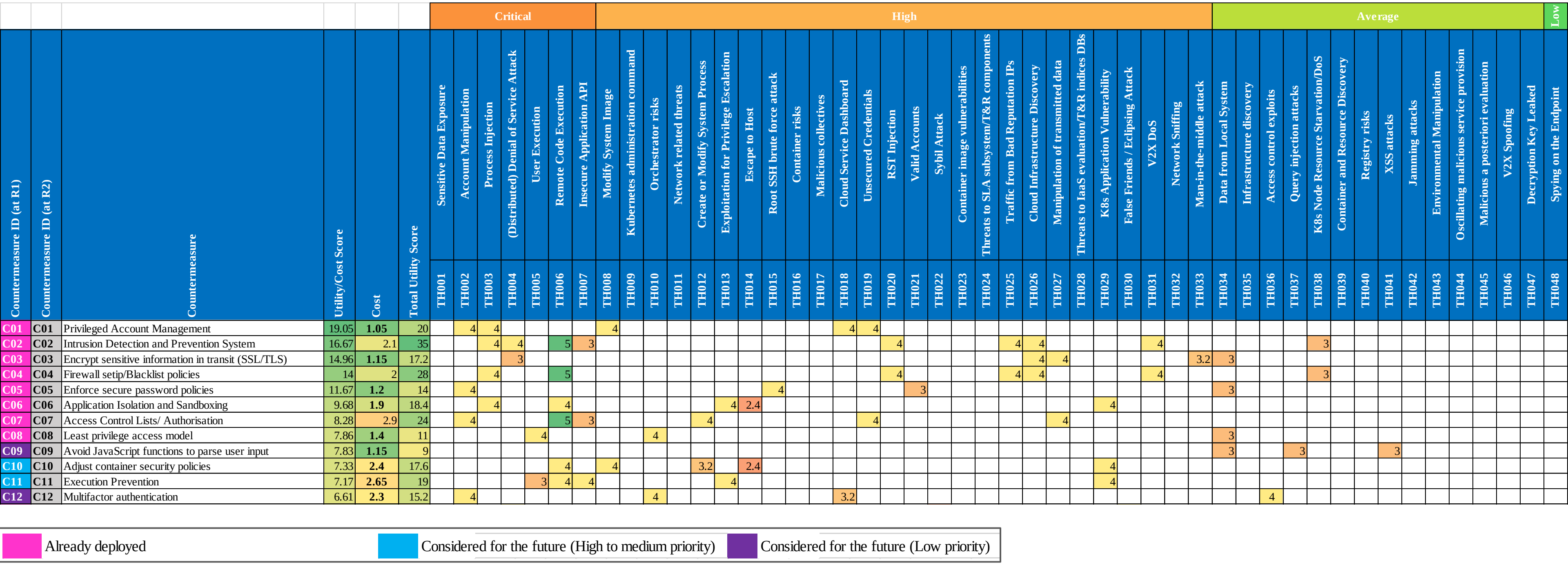


TTP ID	Source	TTP	Threat Severity Level	Max TTP Score	Orchestration	Configuration &Benchmarking	SLA	Decision Support System	Big Data	Blockchain	CI/CD	UC1 Subsystem	UC2 Subsystem	UC3 Subsystem	Other infrastructure
TH001	MITRE, OWASP, CVE	Sensitive Data Exposure	Critical	4.2	3.9	4.2			4						4
TH002	MITRE	Account Manipulation	Critical	4.1				4.1							
TH003	MITRE	Process Injection	Critical	4		4									
TH004	MITRE	User Execution	Critical	4		4									
TH005	ThreatPost, Pledger Honeypot	(Distributed) Denial of Service Attack	Critical	4					4	2.9	3.4	2.9		3	3.5
TH006	MITRE, OWASP	Remote Code Execution	Critical	4		4					4				
TH007	ENISA	Insecure application API	High	3.9					3.9						
TH008	MITRE	Modify System Image	High	3.8							3.8				
TH009	MITRE	Kubernetes administration command	High	3.8									3.8		
TH010	Articles/Bibliography	Orchestrator risks	High	3.8	3.8										
TH011	Articles/Bibliography	Network related threats	High	3.7	3.7										
TH012	MITRE	Create or Modify System Process	High	3.6							3.6				
TH013	MITRE	Exploitation for Privilege Escalation	High	3.6		3.6									
TH014	MITRE	Escape to Host	High	3.6		3.6									
TH015	MITRE	Root SSH brute force attack	High	3.6					3.6		3.5				
TH016	Articles/Bibliography	Container risks	High	3.6	3.6										
TH017	Articles/Bibliography	Malicious collectives	High	3.6			3.6								
TH018	MITRE	Cloud Service Dashboard	High	3.5				3.5							
TH019	MITRE	Unsecured Credentials	High	3.5		3.5									
TH020	Pledger Honeypot	RST Injection	High	3.5											3.5

Table 1. Top-20 Threats

- Assessed 10 types of sources {reports, standards, documentation, MITRE, CVE, ThreatPost, Press, Scientific articles, ENISA, live results from the Pledger Honeypot}
- Identified 48 threats to the Pledger Edge-Cloud Architecture and Use Cases
- Columns indicate Pledger Subsystems
- Next Step: Assign “weight” to subsystems (i.e. single points of failure, components with high number of integration points etc.

Top-10 Countermeasures



						Critical							High																
Countermeasure ID (at R1)	Countermeasure ID (at R2)	Countermeasure	Utility/Cost Score	Cost	Total Utility Score	Sensitive Data Exposure	Account Manipulation	Process Injection	(Distributed) Denial of Service Attack	User Execution	Remote Code Execution	Insecure Application API	Modify System Image	Kubernetes administration command	Orchestrator risks	Network related threats	Create or Modify System Process	Exploitation for Privilege Escalation	Escape to Host	Root SSH brute force attack	Container risks	Malicious collectives	Cloud Service Dashboard	Unsecured Credentials	RST Injection	Valid Accounts	Sybil Attack	Container image vulnerabilities	Threats to SLA subsystem/T&R components
						TH001	TH002	TH003	TH004	TH005	TH006	TH007	TH008	TH009	TH010	TH011	TH012	TH013	TH014	TH015	TH016	TH017	TH018	TH019	TH020	TH021	TH022	TH023	TH024
C01	C01	Privileged Account Management	19.05	1.05	20		4	4					4										4	4					
C02	C02	Intrusion Detection and Prevention System	16.67	2.1	35			4	4		5	3													4				
C03	C03	Encrypt sensitive information in transit (SSL/TLS)	14.96	1.15	17.2				3																				
C04	C04	Firewall setip/Blacklist policies	14	2	28			4			5														4				
C05	C05	Enforce secure password policies	11.67	1.2	14		4													4						3			
C06	C06	Application Isolation and Sandboxing	9.68	1.9	18.4			4			4							4	2.4										
C07	C07	Access Control Lists/ Authorisation	8.28	2.9	24		4				5	3					4							4					
C08	C08	Least privilege access model	7.86	1.4	11					4					4														
C09	C09	Avoid JavaScript functions to parse user input	7.83	1.15	9																								
C10	C10	Adjust container security policies	7.33	2.4	17.6						4		4				3.2		2.4										
C11	C11	Execution Prevention	7.17	2.65	19					3	4	4						4											
C12	C12	Multifactor authentication	6.61	2.3	15.2		4								4								3.2						

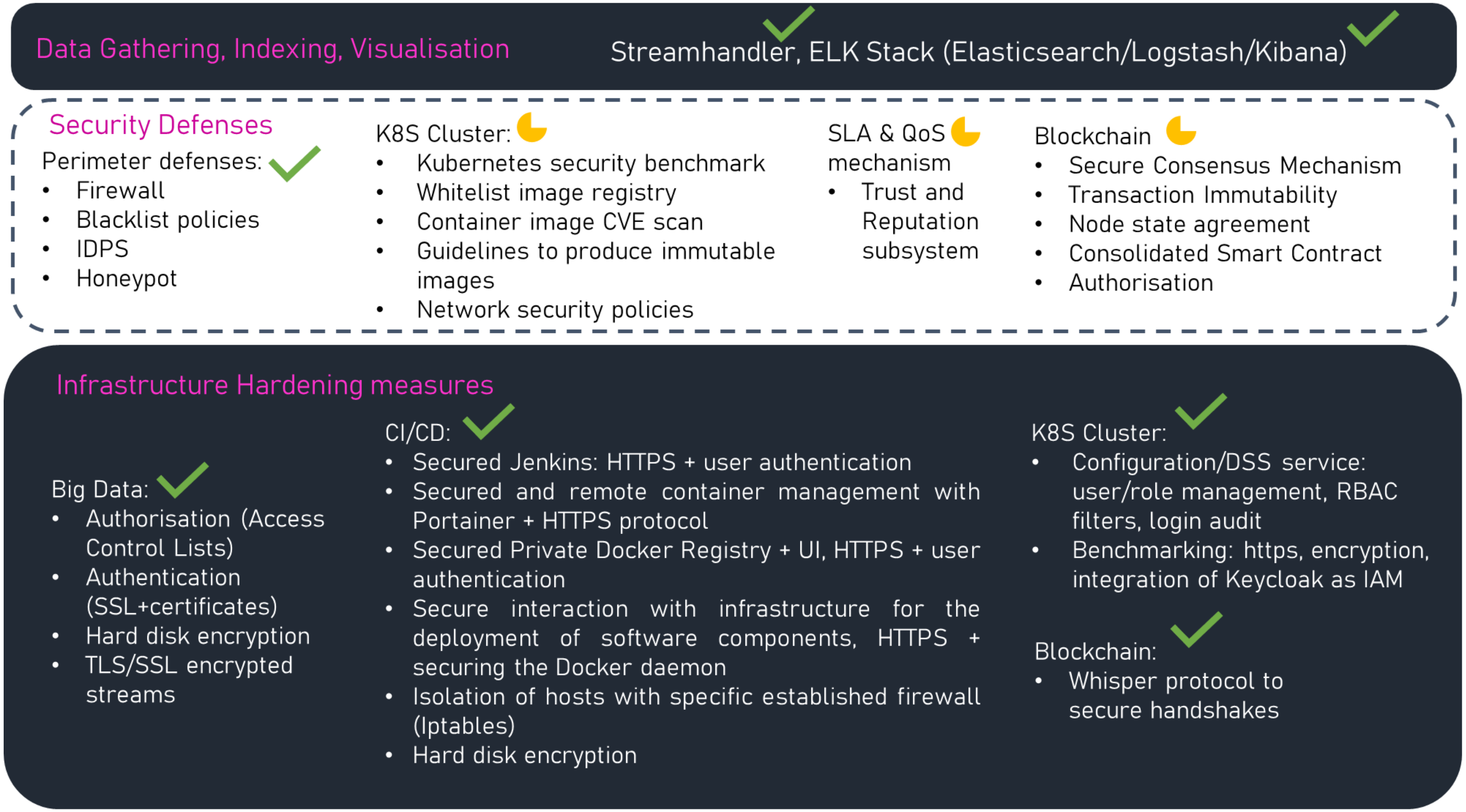
		High									Average														Low
Countermeasure ID (at R1)	Countermeasure ID (at R2)	Traffic from Bad Reputation IPs	Cloud Infrastructure Discovery	Manipulation of transmitted data	Threats to IaaS evaluation/T&R indices DBs	K8s Application Vulnerability	False Friends / Eclipsing Attack	V2X DoS	Network Sniffing	Man-in-the-middle attack	Data from Local System	Infrastructure discovery	Access control exploits	Query injection attacks	K8s Node Resource Starvation/DoS	Container and Resource Discovery	Registry risks	XSS attacks	Jamming attacks	Environmental Manipulation	Oscillating malicious service provision	Malicious a posteriori evaluation	V2X Spoofing	Decryption Key Leaked	Spying on the Endpoint
		TH025	TH026	TH027	TH028	TH029	TH030	TH031	TH032	TH033	TH034	TH035	TH036	TH037	TH038	TH039	TH040	TH041	TH042	TH043	TH044	TH045	TH046	TH047	TH048
C01	C01																								
C02	C02	4	4					4							3										
C03	C03		4	4						3.2	3														
C04	C04	4	4					4							3										
C05	C05										3														
C06	C06					4																			
C07	C07			4																					
C08	C08										3														
C09	C09										3			3				3							
C10	C10					4																			
C11	C11					4																			
C12	C12												4												

■ Already deployed ■ Considered for the future (High to medium priority) ■ Considered for the future (Low priority)

Table 2. Top-10 Countermeasures.

A total of 45 unique countermeasures, including utility, aggregated utility, cost and utility/cost ratio estimations.

High-level concept for Security tasks



Data Gathering, Indexing, Visualisation

Streamhandler ✓, ELK Stack (Elasticsearch/Logstash/Kibana) ✓

Security Defenses

Perimeter defenses: ✓
- Firewall
- Blacklist policies
- IDPS
- Honeypot

K8S Cluster: ◕
- Kubernetes security benchmark
- Whitelist image registry
- Container image CVE scan
- Guidelines to produce immutable images
- Network security policies

SLA & QoS ◕ mechanism
- Trust and Reputation subsystem

Blockchain ◕
- Secure Consensus Mechanism
- Transaction Immutability
- Node state agreement
- Consolidated Smart Contract
- Authorisation

Infrastructure Hardening measures

Big Data: ✓
- Authorisation (Access Control Lists)
- Authentication (SSL+certificates)
- Hard disk encryption
- TLS/SSL encrypted streams

CI/CD: ✓
- Secured Jenkins: HTTPS + user authentication
- Secured and remote container management with Portainer + HTTPS protocol
- Secured Private Docker Registry + UI, HTTPS + user authentication
- Secure interaction with infrastructure for the deployment of software components, HTTPS + securing the Docker daemon
- Isolation of hosts with specific established firewall (Iptables)
- Hard disk encryption

K8S Cluster: ✓
- Configuration/DSS service: user/role management, RBAC filters, login audit
- Benchmarking: https, encryption, integration of Keycloak as IAM

Blockchain: ✓
- Whisper protocol to secure handshakes

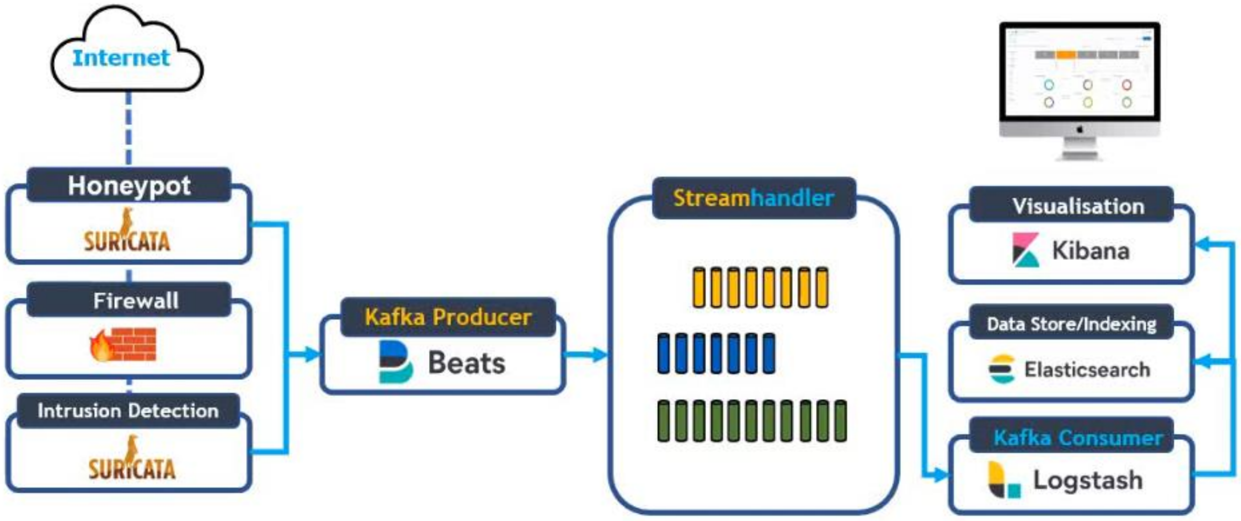
Figure 2: High-level architecture.

This project has received funding from the European Union’s Horizon 2020 Research and Innovation Programme under the Grant Agreement No 871536

A glimpse of our security demo

Streamhandler Setup

Figure 3: Architecture overview.



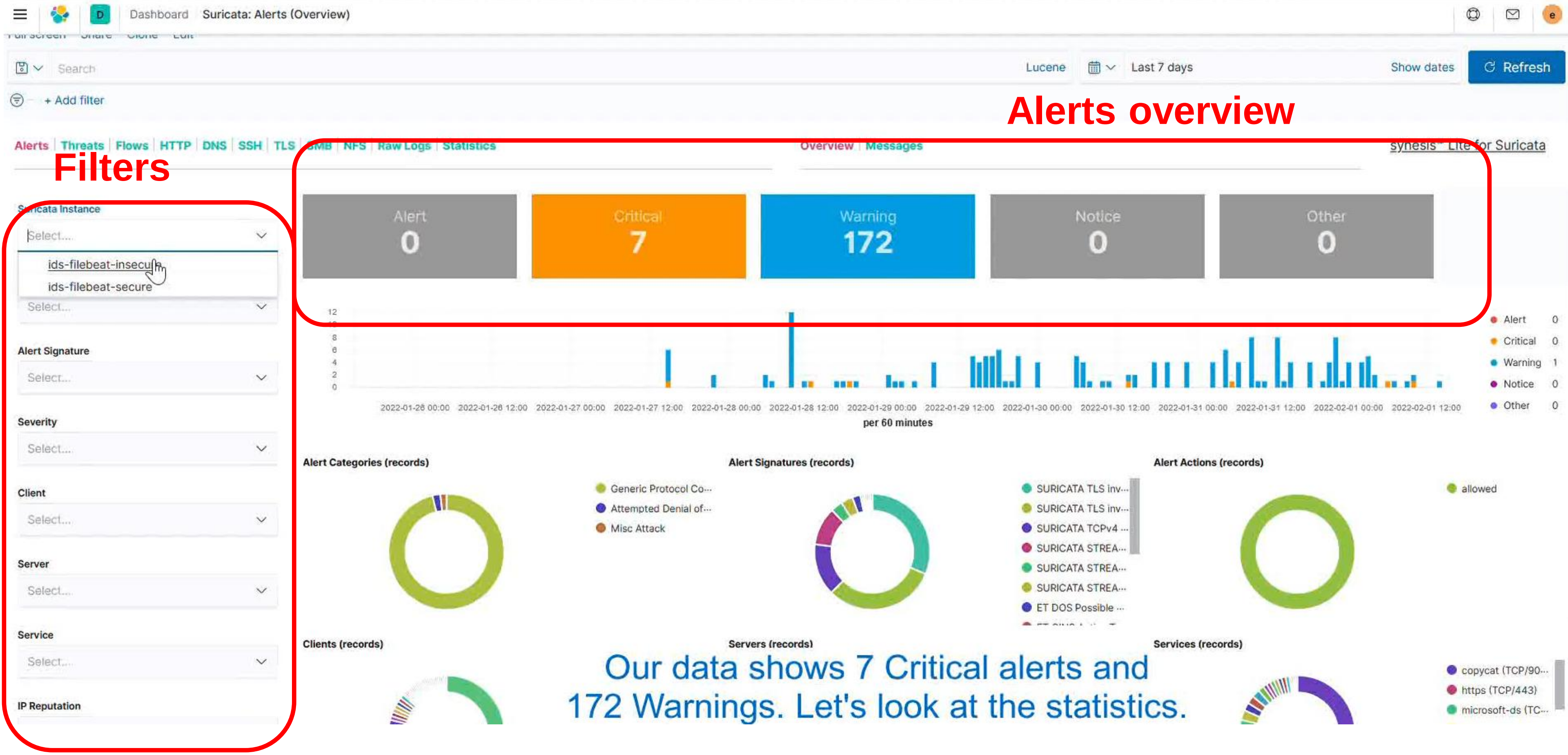
This setup allows us to scale up to multiple IDS instances.

This allows an Infrastructure/Service provider to monitor the cyberhealth of their tenants.

Individual clients can still access their own IDS instances and review the information directly, or even deploy an all-in-one VM that features the security service and the ELK stack.

Aggregated data from 2 IDS instances (27/01/2022-1/02/2022)

Figure 4. Real threat data reported by the IDS instances.



Alerts overview

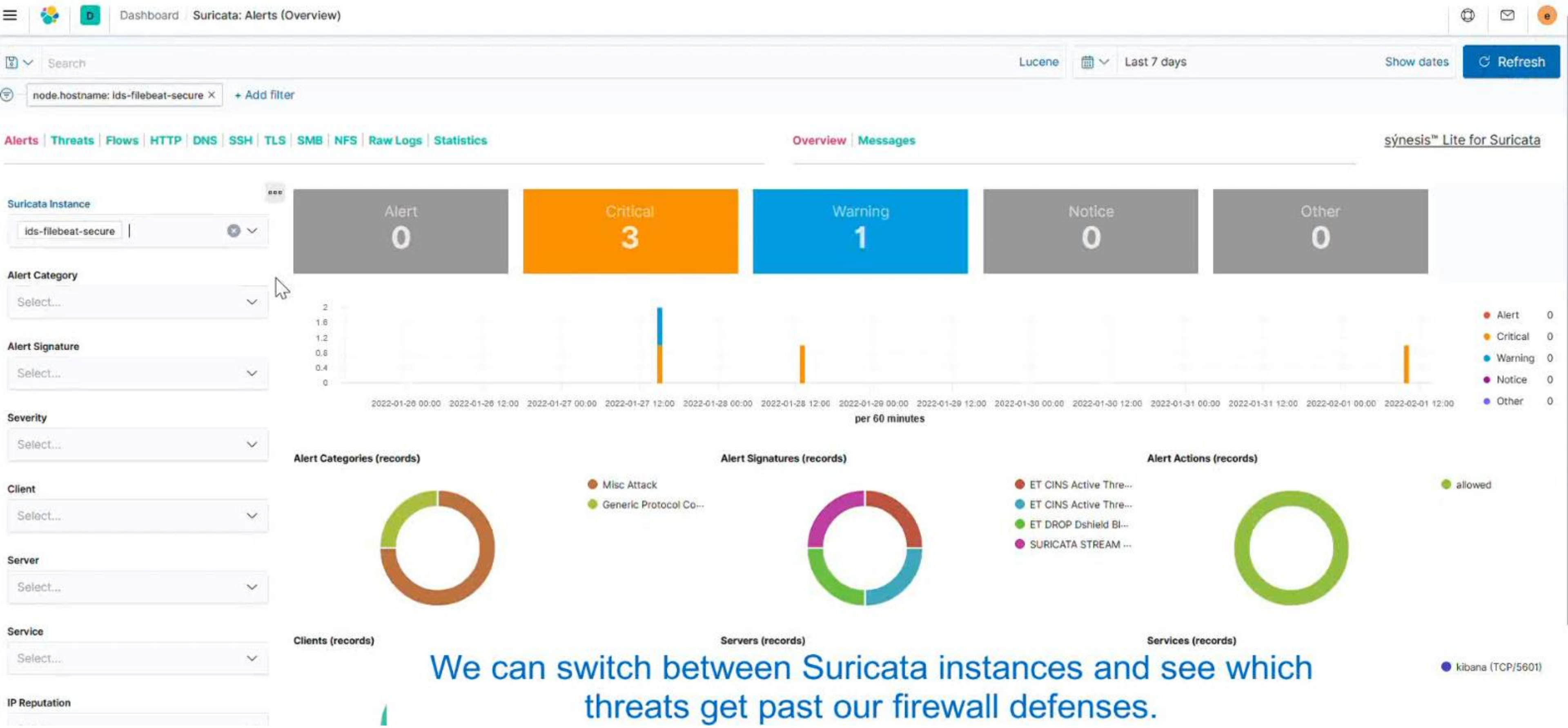
Filters

Our data shows 7 Critical alerts and 172 Warnings. Let's look at the statistics.

PLEDGER

Switching to the view from one instance

Figure 5: Data from one instance.



Dashboard Suricata: Alerts (Overview)

Search Lucene Last 7 days Show dates Refresh

node.hostname: ids-filebeat-secure × + Add filter

Alerts | Threats | Flows | HTTP | DNS | SSH | TLS | SMB | NFS | Raw Logs | Statistics

Overview | Messages

sýnesis™ Lite for Suricata

Suricata Instance: ids-filebeat-secure

Alert Category: Select...

Alert Signature: Select...

Severity: Select...

Client: Select...

Server: Select...

Service: Select...

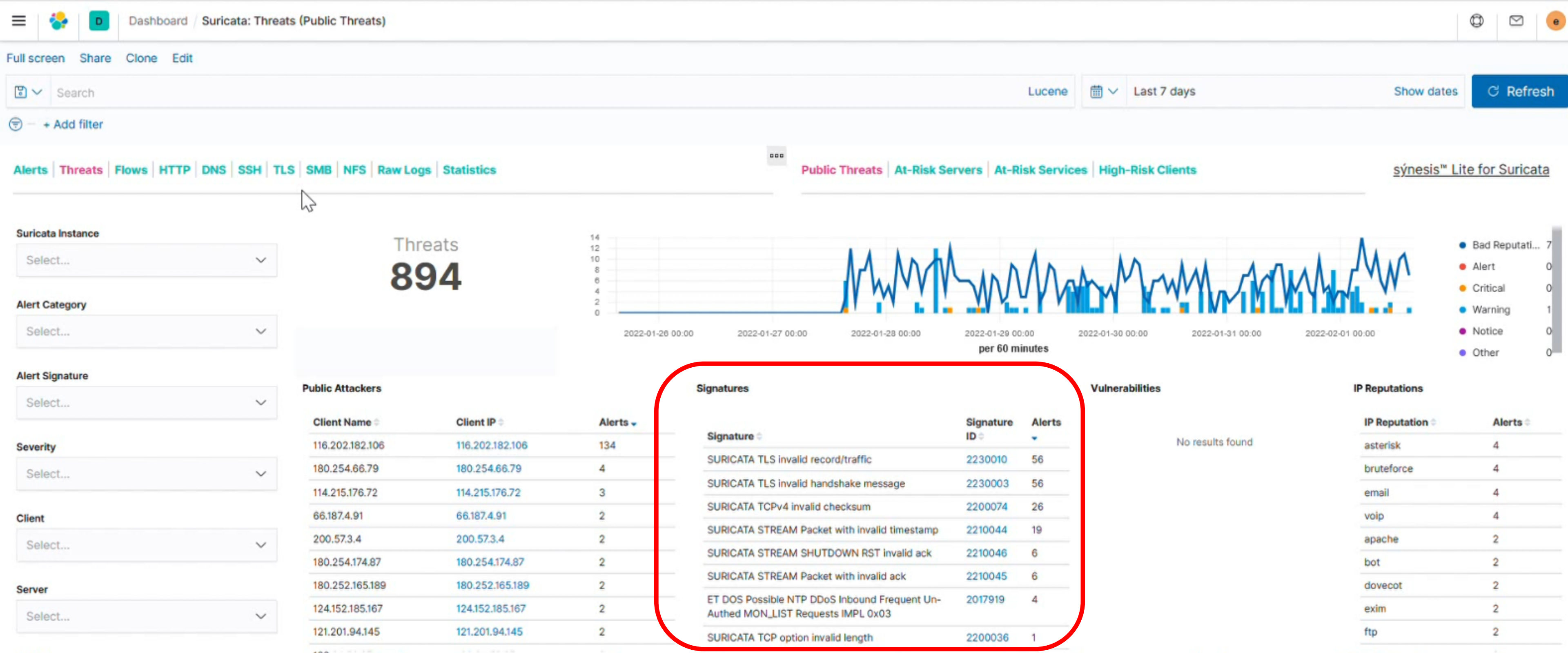
IP Reputation

Alert	Critical	Warning	Notice	Other
0	3	1	0	0

We can switch between Suricata instances and see which threats get past our firewall defenses.

Threats view

Figure 6. Threat signatures.



Dashboard / Suricata: Threats (Public Threats)

Full screen Share Clone Edit

Search Lucene | Last 7 days Show dates | Refresh

+ Add filter

Alerts | Threats | Flows | HTTP | DNS | SSH | TLS | SMB | NFS | Raw Logs | Statistics

Public Threats | At-Risk Servers | At-Risk Services | High-Risk Clients

sýnesis™ Lite for Suricata

Suricata Instance: Select...

Alert Category: Select...

Alert Signature: Select...

Severity: Select...

Client: Select...

Server: Select...

Service: Select...

Threats
894

●	Bad Reputati...	7
●	Alert	0
●	Critical	0
●	Warning	1
●	Notice	0
●	Other	0

Public Attackers

Client Name	Client IP	Alerts
116.202.182.106	116.202.182.106	134
180.254.66.79	180.254.66.79	4
114.215.176.72	114.215.176.72	3
66.187.4.91	66.187.4.91	2
200.57.3.4	200.57.3.4	2
180.254.174.87	180.254.174.87	2
180.252.165.189	180.252.165.189	2
124.152.185.167	124.152.185.167	2
121.201.94.145	121.201.94.145	2
120		

Exp

Signatures

Signature	Signature ID	Alerts
SURICATA TLS invalid record/traffic	2230010	56
SURICATA TLS invalid handshake message	2230003	56
SURICATA TCPv4 invalid checksum	2200074	26
SURICATA STREAM Packet with invalid timestamp	2210044	19
SURICATA STREAM SHUTDOWN RST invalid ack	2210046	6
SURICATA STREAM Packet with invalid ack	2210045	6
ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03	2017919	4
SURICATA TCP option invalid length	2200036	1

Vulnerabilities

No results found

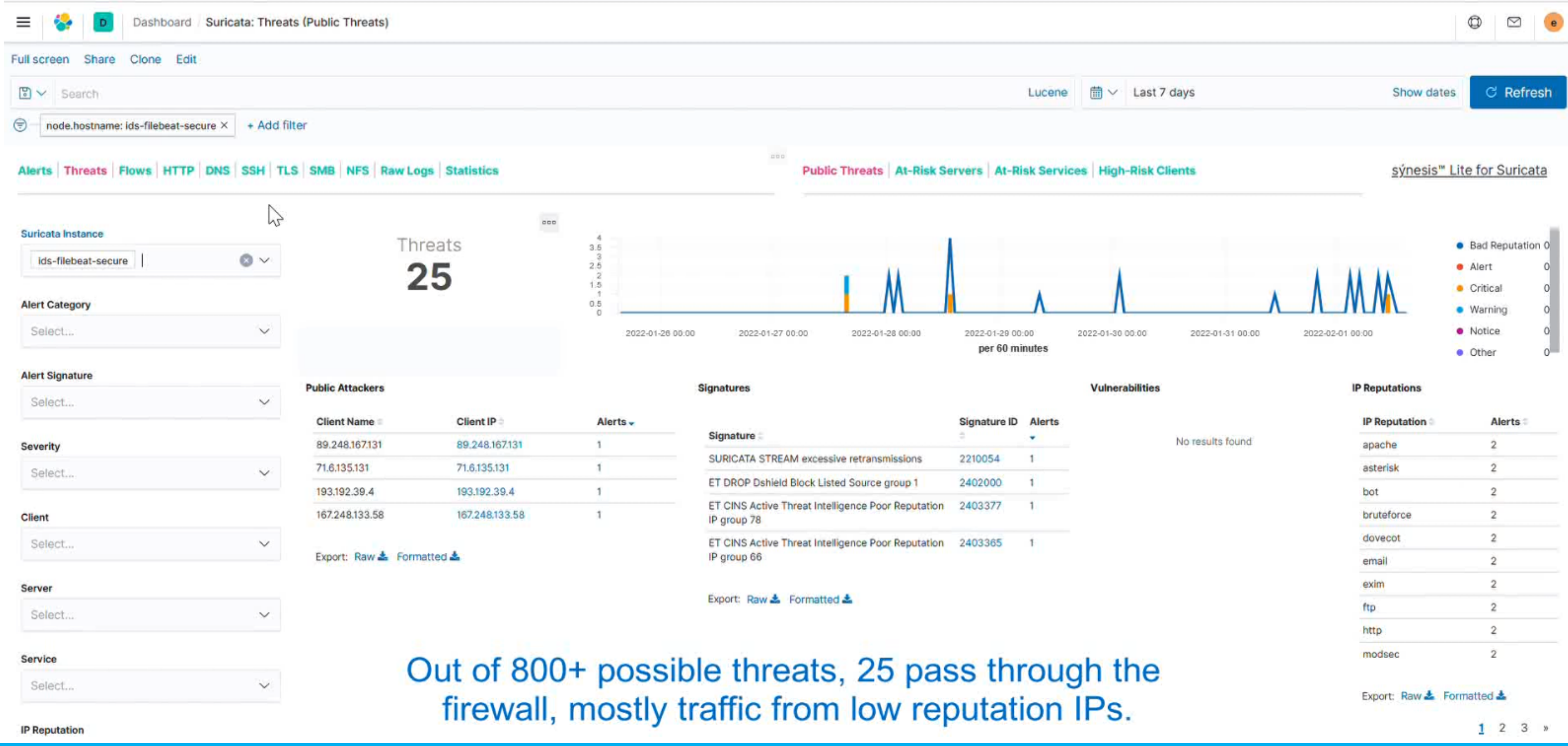
IP Reputations

IP Reputation	Alerts
asterisk	4
bruteforce	4
email	4
voip	4
apache	2
bot	2
dovecot	2
exim	2
ftp	2

The Threats tab provides an overview of the detected threats. NTP-based amplification DDoS is a frequent phenomenon, but is blocked from our firewall.

Low Reputation IP traffic

Figure 7. Remaining threats after remediation.



node.hostname: ids-filebeat-secure

Suricata Instance: ids-filebeat-secure

Alert Category: Select...

Alert Signature: Select...

Severity: Select...

Client: Select...

Server: Select...

Service: Select...

IP Reputation

Threats
25

● Bad Reputation	0
● Alert	0
● Critical	0
● Warning	0
● Notice	0
● Other	0

Public Attackers

Client Name	Client IP	Alerts
89.248.167.131	89.248.167.131	1
71.6.135.131	71.6.135.131	1
193.192.39.4	193.192.39.4	1
167.248.133.58	167.248.133.58	1

Export: Raw Formatted

Signatures

Signature	Signature ID	Alerts
SURICATA STREAM excessive retransmissions	2210054	1
ET DROP Dshield Block Listed Source group 1	2402000	1
ET CINS Active Threat Intelligence Poor Reputation IP group 78	2403377	1
ET CINS Active Threat Intelligence Poor Reputation IP group 66	2403365	1

Export: Raw Formatted

Vulnerabilities

No results found

IP Reputations

IP Reputation	Alerts
apache	2
asterisk	2
bot	2
bruteforce	2
dovecot	2
email	2
exim	2
ftp	2
http	2
modsec	2

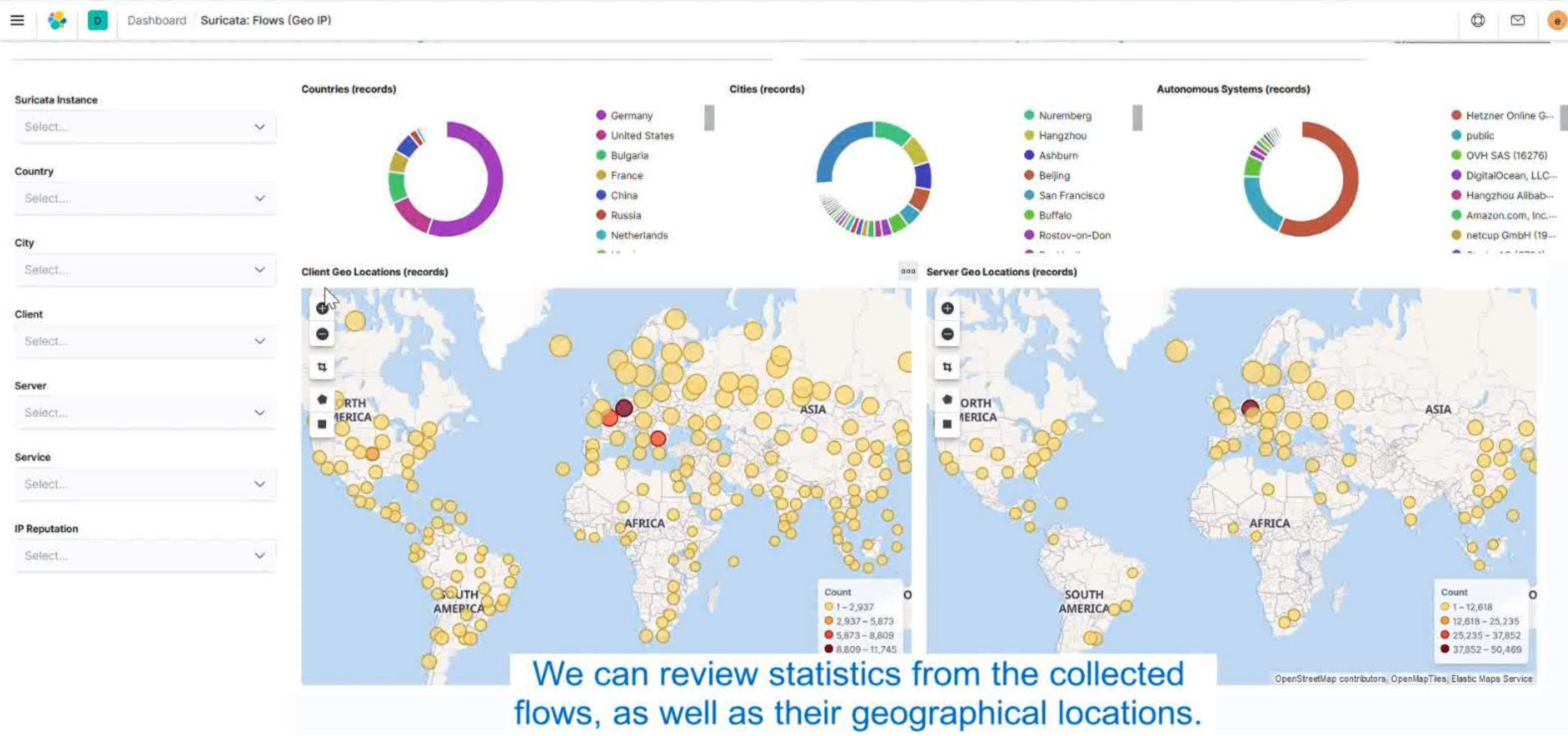
Export: Raw Formatted

1 2 3 »

Out of 800+ possible threats, 25 pass through the firewall, mostly traffic from low reputation IPs.

Geographical locations of offending flows

Figure 8. Geographical statistics (aggregated data view)



Dashboard Suricata: Flows (Geo IP)

Suricata Instance: Select...

Country: Select...

City: Select...

Client: Select...

Server: Select...

Service: Select...

IP Reputation: Select...

We can review statistics from the collected flows, as well as their geographical locations.

For more information, visit us at pledger-project.eu and welcometo.netcompany-intrasoft.com

Dr. Olga Segou

Netcompany-Intrasoft

Olga.SEGOU@netcompany-intrasoft.com

This project has received funding from the European Union’s Horizon 2020 Research and Innovation Programme under the Grant Agreement No 871536