Cyber-MAR Pilot 3

Cyber Range Modules:
L-ADS & XL-SIEM

ATOS

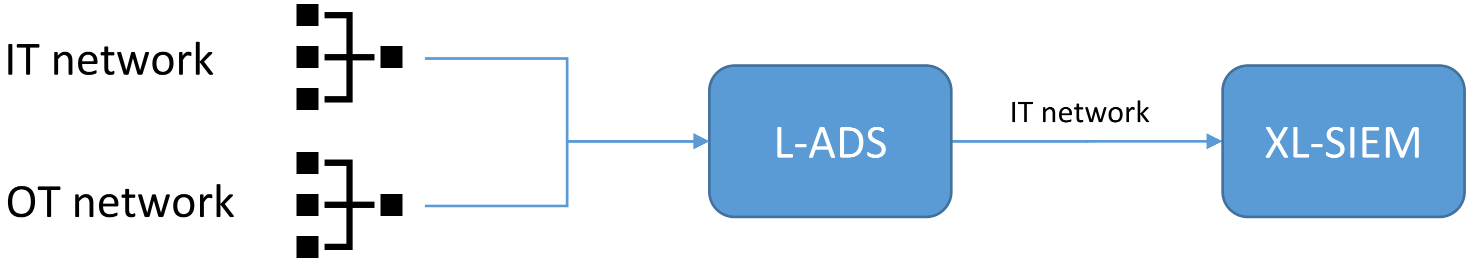
Alejandro García Bedoya

Jesús Villalobos Nieto

December 16th , Piraeus, Greece

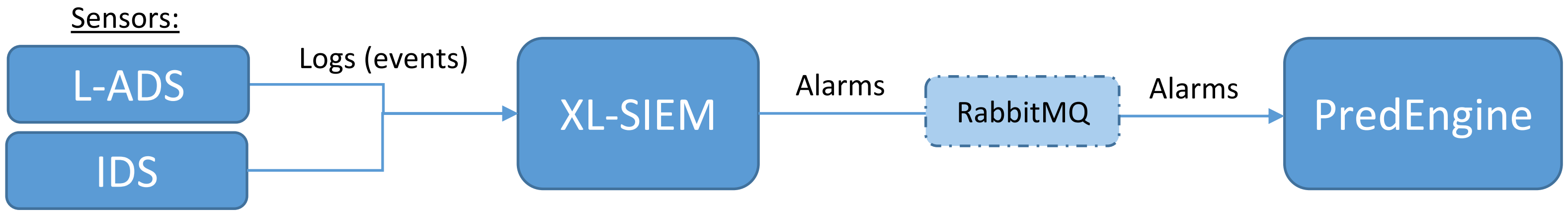
L-ADS

- Monitors and capture the network traffic in real-time
- Detects anomalies in the network using a Deep Learning algorithm
- The algorithm was trained using legit traffic
- Two instances deployed for improving the accuracy:
  - IT Network
  - OT Network
- Detected anomalies are sent to the XL-SIEM through Rsyslog

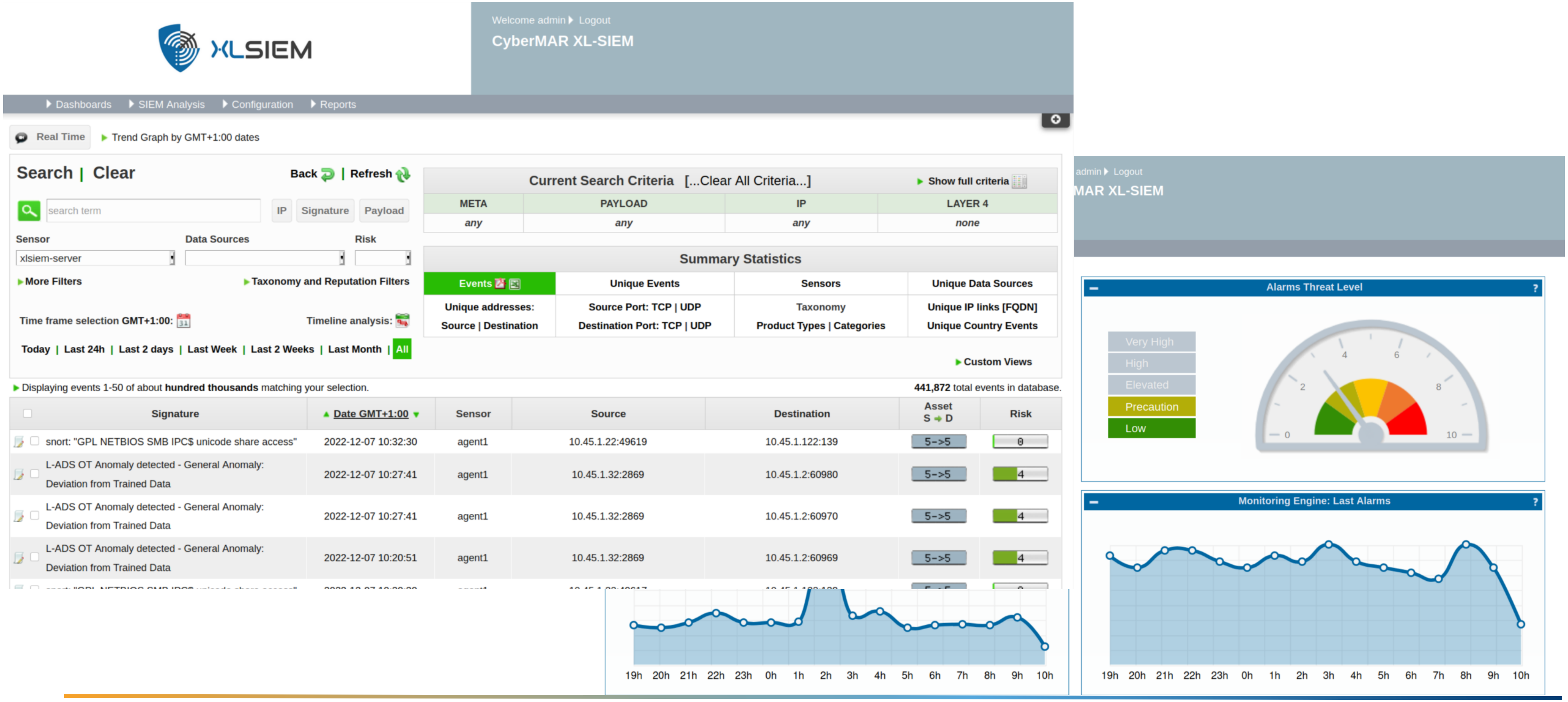


XL-SIEM

- Security information and event management system
- Logs received from different data sources are normalized into Events:
  - IDS (+HIDS)
  - L-ADS
- **Correlation engine ->** uses custom **correlation rules** -> generate **Alarms:**
  - Correlates sequences of Events / Alarms (cross-correlation)
- Alarms & Events are presented in the XL-SIEM GUI
- Alarms are forwarded to Prediction Engine through RabbitMQ
- XL-SIEM API for orchestration (stop, start and clean the services)



XL-SIEM



XLSIEM
Welcome admin ▸ Logout

CyberMAR XL-SIEM

▸ Dashboards ▸ SIEM Analysis ▸ Configuration ▸ Reports
Real Time
▸ Trend Graph by GMT+1:00 dates
Search | Clear
Back | Refresh
search term
IP
Signature
Payload

Sensor: xlsiem-server
Data Sources:
Risk:

▸ More Filters
▸ Taxonomy and Reputation Filters
Time frame selection GMT+1:00:
Timeline analysis:
Today | Last 24h | Last 2 days | Last Week | Last 2 Weeks | Last Month | All

Current Search Criteria [...Clear All Criteria...] ▸ Show full criteria

META	PAYLOAD	IP	LAYER 4
any	*any*	*any*	*none*

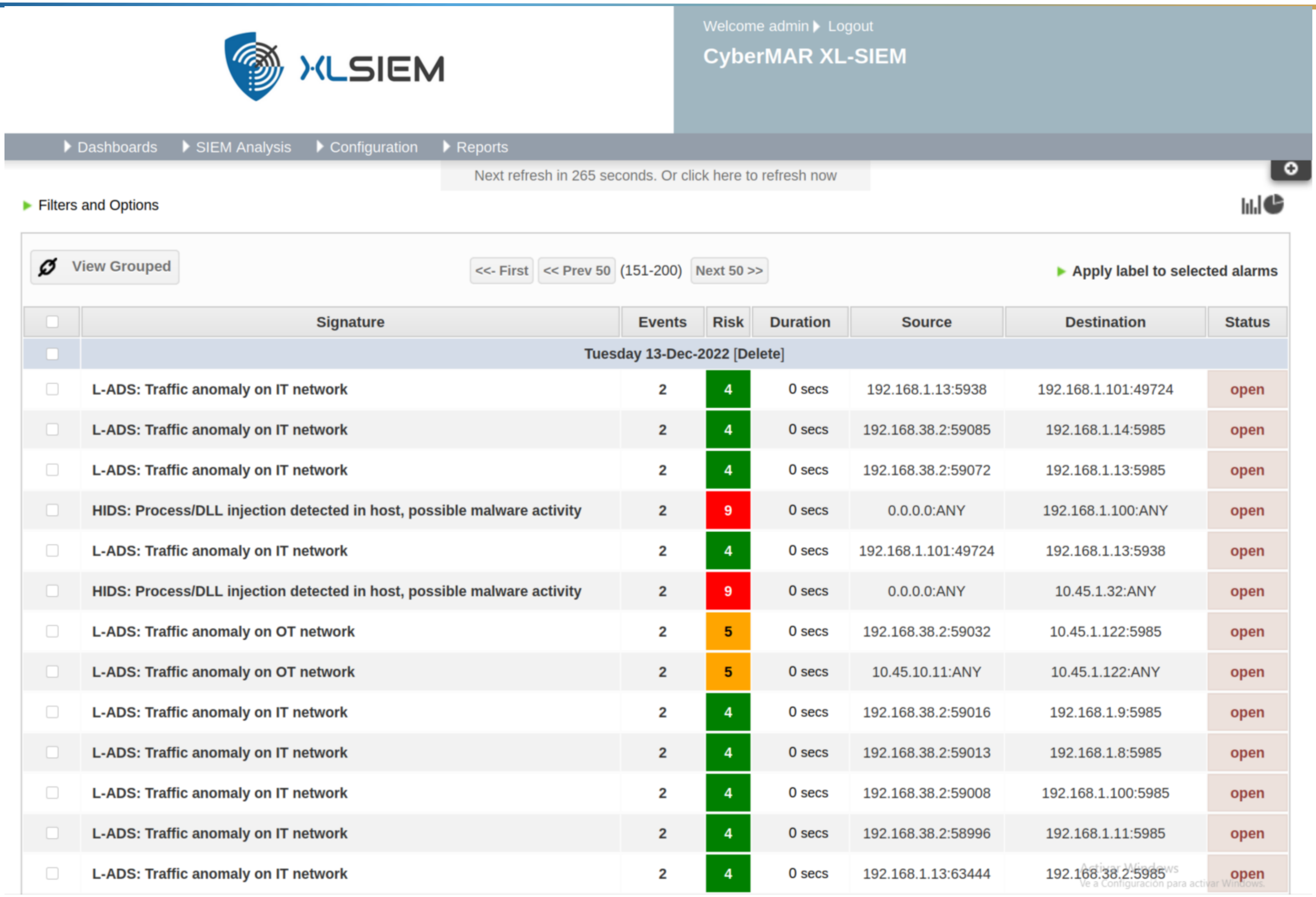
Summary Statistics

Events	Unique Events	Sensors	Unique Data Sources
Unique addresses: Source | Destination	Source Port: TCP | UDP Destination Port: TCP | UDP	Taxonomy Product Types | Categories	Unique IP links [FQDN] Unique Country Events

▸ Displaying events 1-50 of about **hundred thousands** matching your selection. **441,872** total events in database.

Signature	Date GMT+1:00	Sensor	Source	Destination	Asset S → D	Risk
snort: "GPL NETBIOS SMB IPC$ unicode share access"	2022-12-07 10:32:30	agent1	10.45.1.22:49619	10.45.1.122:139	5->5	0
L-ADS OT Anomaly detected - General Anomaly: Deviation from Trained Data	2022-12-07 10:27:41	agent1	10.45.1.32:2869	10.45.1.2:60980	5->5	4
L-ADS OT Anomaly detected - General Anomaly: Deviation from Trained Data	2022-12-07 10:27:41	agent1	10.45.1.32:2869	10.45.1.2:60970	5->5	4
L-ADS OT Anomaly detected - General Anomaly: Deviation from Trained Data	2022-12-07 10:20:51	agent1	10.45.1.32:2869	10.45.1.2:60969	5->5	4

XL-SIEM



CyberMAR XL-SIEM

Next refresh in 265 seconds. Or click here to refresh now

(151-200)

□	Signature	Events	Risk	Duration	Source	Destination	Status
□	Tuesday 13-Dec-2022 [Delete]						
□	L-ADS: Traffic anomaly on IT network	2	4	0 secs	192.168.1.13:5938	192.168.1.101:49724	open
□	L-ADS: Traffic anomaly on IT network	2	4	0 secs	192.168.38.2:59085	192.168.1.14:5985	open
□	L-ADS: Traffic anomaly on IT network	2	4	0 secs	192.168.38.2:59072	192.168.1.13:5985	open
□	HIDS: Process/DLL injection detected in host, possible malware activity	2	9	0 secs	0.0.0.0:ANY	192.168.1.100:ANY	open
□	L-ADS: Traffic anomaly on IT network	2	4	0 secs	192.168.1.101:49724	192.168.1.13:5938	open
□	HIDS: Process/DLL injection detected in host, possible malware activity	2	9	0 secs	0.0.0.0:ANY	10.45.1.32:ANY	open
□	L-ADS: Traffic anomaly on OT network	2	5	0 secs	192.168.38.2:59032	10.45.1.122:5985	open
□	L-ADS: Traffic anomaly on OT network	2	5	0 secs	10.45.10.11:ANY	10.45.1.122:ANY	open
□	L-ADS: Traffic anomaly on IT network	2	4	0 secs	192.168.38.2:59016	192.168.1.9:5985	open
□	L-ADS: Traffic anomaly on IT network	2	4	0 secs	192.168.38.2:59013	192.168.1.8:5985	open
□	L-ADS: Traffic anomaly on IT network	2	4	0 secs	192.168.38.2:59008	192.168.1.100:5985	open
□	L-ADS: Traffic anomaly on IT network	2	4	0 secs	192.168.38.2:58996	192.168.1.11:5985	open
□	L-ADS: Traffic anomaly on IT network	2	4	0 secs	192.168.1.13:63444	192.168.38.2:5985	open