LOMOS: Runtime Security Monitoring Fit for the Cloud Continuum

Joao Pita Costa, **Hrvoje Ratkajec**, Daniel Vladušič, Tomaž Martinčič, Aleš Černivec, Justin Činkelj, Rosalia Davi, Simone Favrin, Lorenzo Gorza, Gilda di Marco

30th International European Conference on Parallel and Distributed Computing

IECCONT workshop, 26 - 30 August 2024, Madrid, Spain

Benefits of Runtime Security

DEPLOY SECURITY AGENTS (AUTOMATICALLY)

Deploy **security monitoring agents**, integrated into the monitoring mechanisms at runtime

AUTOMATE DETECTION AND INCIDENT RESPONSE

Notify about security threats according to pre-defined security policies, and using **NLP for undefined threats**

COMPLEMENT EXISTING SIEM PROCESSES

Tackle unexpected situations that may affect the **correct performance and underlying environment** (i.e. infrastructure failures, deterioration in the response time)

A Runtime Security Context

XLAB

INNOVATION

Using a powerful event and incident management, adapted to new functionalities, and an AI engine with features for future self-learning and self-healing capabilities

PROBLEM

Need for monitoring stack for the run-time conditions so that the security surveillance can be fed, taking into consideration yet unknown threads
that cannot be identified w/ patterns

SOLUTION

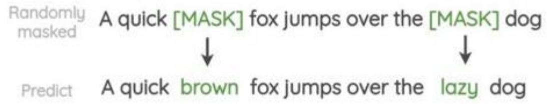
Monitoring system capable of detecting security-related events and incidents in the deployed application's environment. It is (to the extent possible) deployable automatically and notifies users about security alerts

VALUE

This monitoring system allows to create informative metrics/variables with significant discriminative power

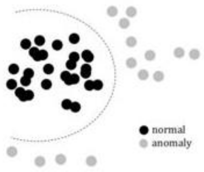
Anomaly Detection in Logs

- Use of Masked Language Modeling (MLM)
  - Common in self-supervised NLP



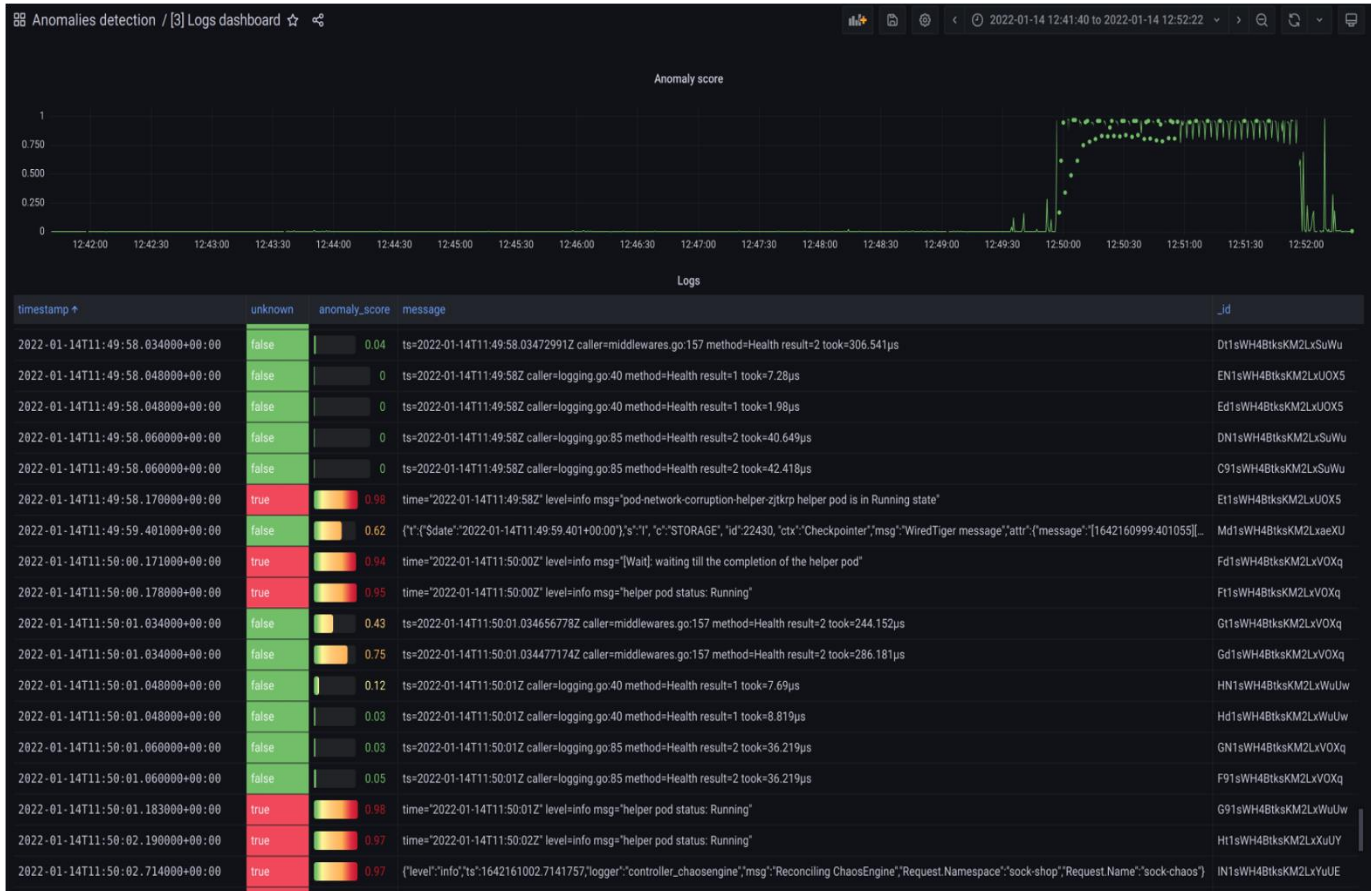
Randomly masked A quick [MASK] fox jumps over the [MASK] dog

Predict A quick brown fox jumps over the lazy dog



- Hypersphere Volume Minimization (HVM)
  - Hypothesis that ‘normal’ samples can be mapped to close representations.

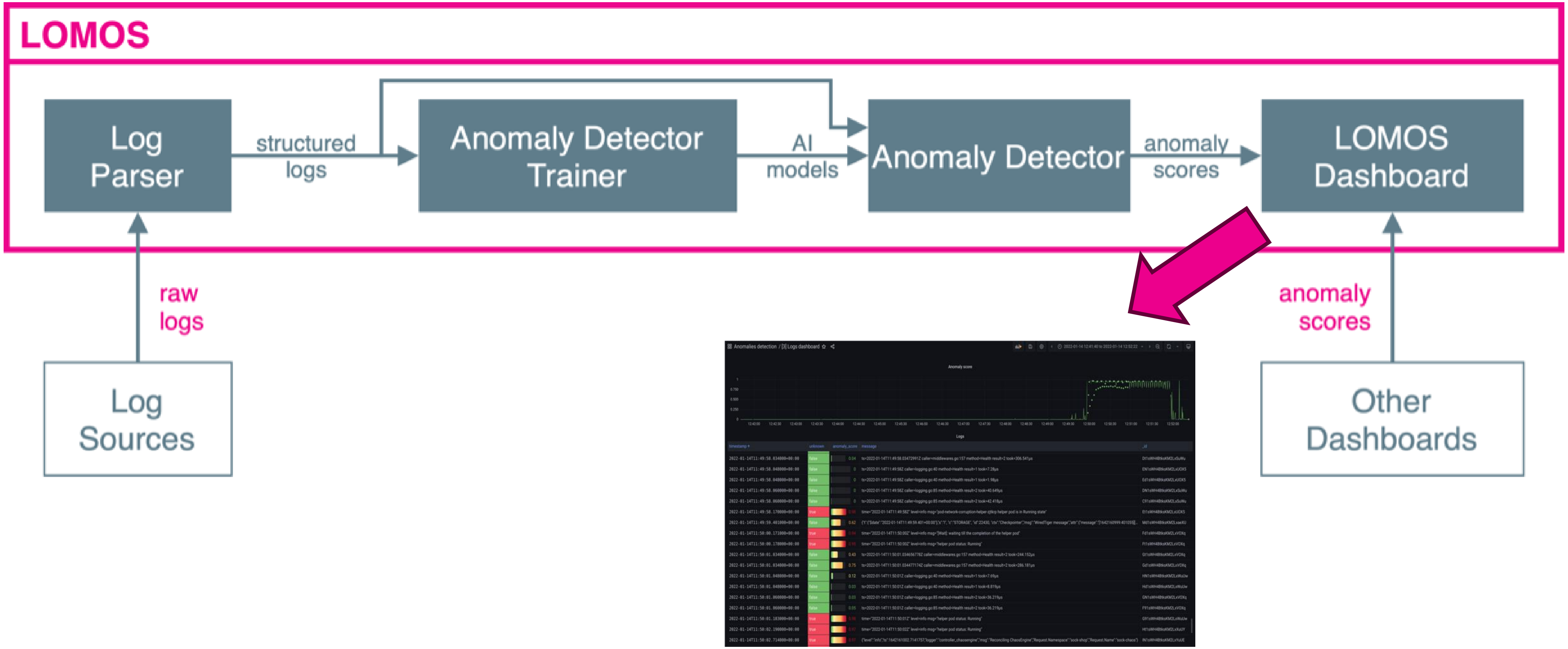
- When is an unseen log sequence anomalous?
  1. Randomly mask some its logs.
  2. Use our trained model to generate predictions.
  3. For every mask, our model provides some candidates.
  4. Is the true log within the candidate set?
     a) Yes: this is a normal log
     b) No: this log is anomalous
  5. If there are too many anomalous logs in the sequence > raise alarm!



Logs

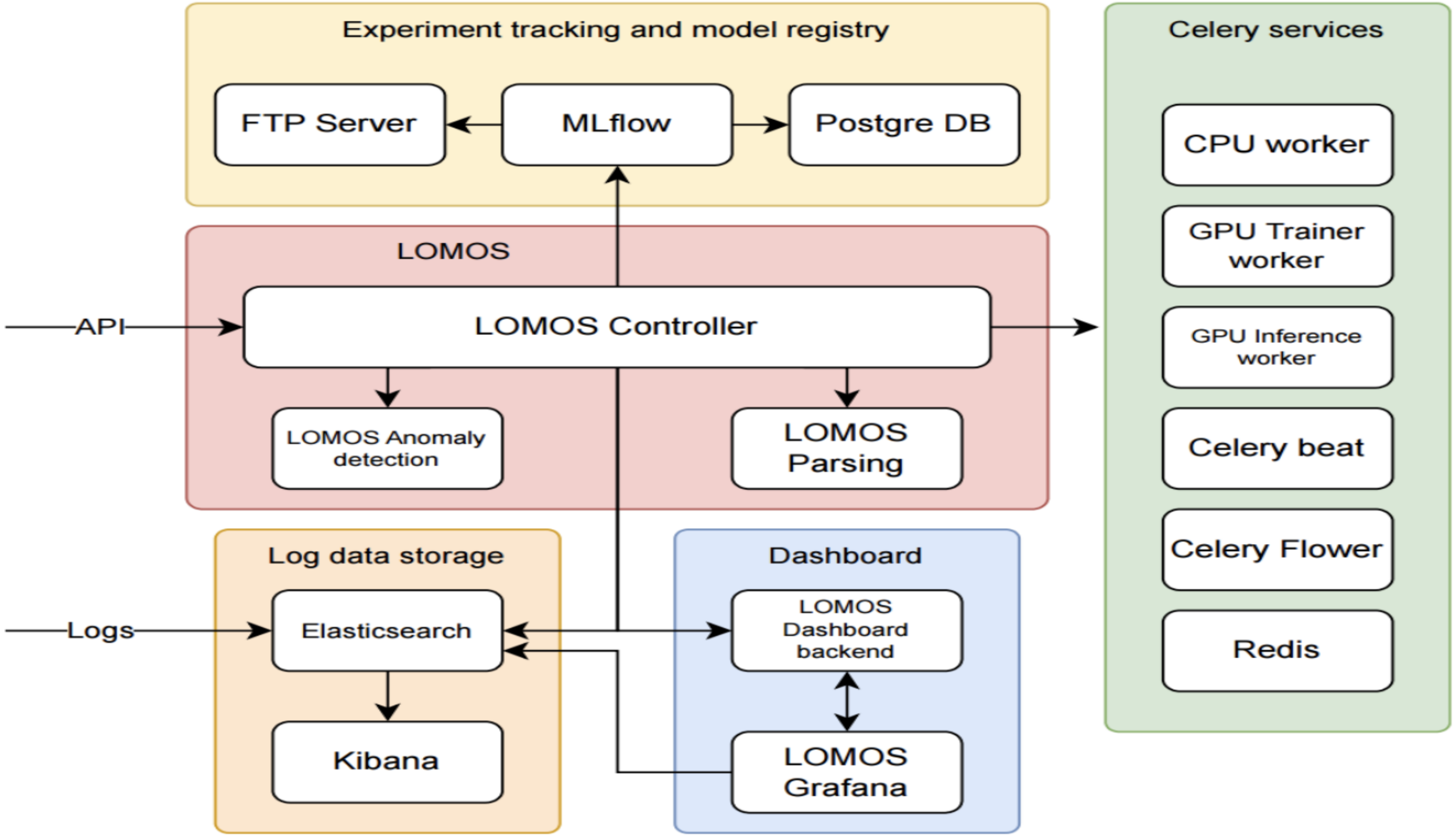
timestamp ↑	unknown	anomaly_score	message	_id
2022-01-14T11:49:58.034000+00:00	false	0.04	ts=2022-01-14T11:49:58.03472991Z caller=middlewares.go:157 method=Health result=2 took=306.541µs	Dt1sWH4BtksKM2LxSuWu
2022-01-14T11:49:58.048000+00:00	false	0	ts=2022-01-14T11:49:58Z caller=logging.go:40 method=Health result=1 took=7.28µs	EN1sWH4BtksKM2LxUOX5
2022-01-14T11:49:58.048000+00:00	false	0	ts=2022-01-14T11:49:58Z caller=logging.go:40 method=Health result=1 took=1.98µs	Ed1sWH4BtksKM2LxUOX5
2022-01-14T11:49:58.060000+00:00	false	0	ts=2022-01-14T11:49:58Z caller=logging.go:85 method=Health result=2 took=40.649µs	DN1sWH4BtksKM2LxSuWu
2022-01-14T11:49:58.060000+00:00	false	0	ts=2022-01-14T11:49:58Z caller=logging.go:85 method=Health result=2 took=42.418µs	C91sWH4BtksKM2LxSuWu
2022-01-14T11:49:58.170000+00:00	true	0.98	time="2022-01-14T11:49:58Z" level=info msg="pod-network-corruption-helper-zjtkrp helper pod is in Running state"	Et1sWH4BtksKM2LxUOX5
2022-01-14T11:49:59.401000+00:00	false	0.62	{"t":{"$date":"2022-01-14T11:49:59.401+00:00"},"s":"I", "c":"STORAGE", "id":22430, "ctx":"Checkpointer","msg":"WiredTiger message","attr":{"message":"[1642160999:401055][...	Md1sWH4BtksKM2LxaeXU
2022-01-14T11:50:00.171000+00:00	true	0.94	time="2022-01-14T11:50:00Z" level=info msg="[Wait]: waiting till the completion of the helper pod"	Fd1sWH4BtksKM2LxVOXq
2022-01-14T11:50:00.178000+00:00	true	0.95	time="2022-01-14T11:50:00Z" level=info msg="helper pod status: Running"	Ft1sWH4BtksKM2LxVOXq
2022-01-14T11:50:01.034000+00:00	false	0.43	ts=2022-01-14T11:50:01.034656778Z caller=middlewares.go:157 method=Health result=2 took=244.152µs	Gt1sWH4BtksKM2LxVOXq
2022-01-14T11:50:01.034000+00:00	false	0.75	ts=2022-01-14T11:50:01.034477174Z caller=middlewares.go:157 method=Health result=2 took=286.181µs	Gd1sWH4BtksKM2LxVOXq
2022-01-14T11:50:01.048000+00:00	false	0.12	ts=2022-01-14T11:50:01Z caller=logging.go:40 method=Health result=1 took=7.69µs	HN1sWH4BtksKM2LxWuUw
2022-01-14T11:50:01.048000+00:00	false	0.03	ts=2022-01-14T11:50:01Z caller=logging.go:40 method=Health result=1 took=8.819µs	Hd1sWH4BtksKM2LxWuUw
2022-01-14T11:50:01.060000+00:00	false	0.03	ts=2022-01-14T11:50:01Z caller=logging.go:85 method=Health result=2 took=36.219µs	GN1sWH4BtksKM2LxVOXq
2022-01-14T11:50:01.060000+00:00	false	0.05	ts=2022-01-14T11:50:01Z caller=logging.go:85 method=Health result=2 took=36.219µs	F91sWH4BtksKM2LxVOXq
2022-01-14T11:50:01.183000+00:00	true	0.98	time="2022-01-14T11:50:01Z" level=info msg="helper pod status: Running"	G91sWH4BtksKM2LxWuUw
2022-01-14T11:50:02.190000+00:00	true	0.97	time="2022-01-14T11:50:02Z" level=info msg="helper pod status: Running"	Ht1sWH4BtksKM2LxXuUY
2022-01-14T11:50:02.714000+00:00	true	0.97	{"level":"info","ts":1642161002.7141757,"logger":"controller_chaosengine","msg":"Reconciling ChaosEngine","Request.Namespace":"sock-shop","Request.Name":"sock-chaos"}	IN1sWH4BtksKM2LxYuUE

A General Context



timestamp ↓	unknown	anomaly_score	message	_id
2022-01-14T11:49:58.034000+00:00	false	0.04	ts=2022-01-14T11:49:58.03472991Z caller=middlewares.go:157 method=Health result=2 took=306.541µs	Dt1sWH4BtksKM2LxSuWu
2022-01-14T11:49:58.040000+00:00	false	0	ts=2022-01-14T11:49:58Z caller=logging.go:40 method=Health result=1 took=7.28µs	EN1sWH4BtksKM2LxUOX5
2022-01-14T11:49:58.040000+00:00	false	0	ts=2022-01-14T11:49:58Z caller=logging.go:40 method=Health result=1 took=1.98µs	Ed1sWH4BtksKM2LxUOX5
2022-01-14T11:49:58.060000+00:00	false	0	ts=2022-01-14T11:49:58Z caller=logging.go:85 method=Health result=2 took=40.649µs	DN1sWH4BtksKM2LxSuWu
2022-01-14T11:49:58.060000+00:00	false	0	ts=2022-01-14T11:49:58Z caller=logging.go:85 method=Health result=2 took=42.418µs	C91sWH4BtksKM2LxSuWu
2022-01-14T11:49:58.170000+00:00	true	0.98	time="2022-01-14T11:49:58Z" level=info msg="pod-network-corruption-helper-zjtkrp helper pod is in Running state"	Et1sWH4BtksKM2LxUOX5
2022-01-14T11:49:59.401000+00:00	false	0.62	{"t":{"$date":"2022-01-14T11:49:59.401+00:00"},"s":"I", "c":"STORAGE", "id":22430, "ctx":"Checkpointer","msg":"WiredTiger message","attr":{"message":"[1642160999:401055][...	Md1sWH4BtksKM2LxaeXU
2022-01-14T11:50:00.171000+00:00	true	0.94	time="2022-01-14T11:50:00Z" level=info msg="[Wait]: waiting till the completion of the helper pod"	Fd1sWH4BtksKM2LxVOXq
2022-01-14T11:50:00.178000+00:00	true	0.95	time="2022-01-14T11:50:00Z" level=info msg="helper pod status: Running"	Ft1sWH4BtksKM2LxVOXq
2022-01-14T11:50:01.034000+00:00	false	0.43	ts=2022-01-14T11:50:01.034656778Z caller=middlewares.go:157 method=Health result=2 took=244.152µs	Gt1sWH4BtksKM2LxVOXq
2022-01-14T11:50:01.034000+00:00	false	0.75	ts=2022-01-14T11:50:01.034477174Z caller=middlewares.go:157 method=Health result=2 took=286.181µs	Gd1sWH4BtksKM2LxVOXq
2022-01-14T11:50:01.040000+00:00	false	0.12	ts=2022-01-14T11:50:01Z caller=logging.go:40 method=Health result=1 took=7.69µs	HN1sWH4BtksKM2LxWuUw
2022-01-14T11:50:01.040000+00:00	false	0.03	ts=2022-01-14T11:50:01Z caller=logging.go:40 method=Health result=1 took=8.819µs	Hd1sWH4BtksKM2LxWuUw
2022-01-14T11:50:01.060000+00:00	false	0.03	ts=2022-01-14T11:50:01Z caller=logging.go:85 method=Health result=2 took=36.219µs	GN1sWH4BtksKM2LxVOXq
2022-01-14T11:50:01.060000+00:00	false	0.05	ts=2022-01-14T11:50:01Z caller=logging.go:85 method=Health result=2 took=36.219µs	F91sWH4BtksKM2LxVOXq
2022-01-14T11:50:01.183000+00:00	true	0.98	time="2022-01-14T11:50:01Z" level=info msg="helper pod status: Running"	G91sWH4BtksKM2LxWuUw
2022-01-14T11:50:02.190000+00:00	true	0.97	time="2022-01-14T11:50:02Z" level=info msg="helper pod status: Running"	Ht1sWH4BtksKM2LxXuUY
2022-01-14T11:50:02.714000+00:00	true	0.97	{"level":"info","ts":1642161002.7141757,"logger":"controller_chaosengine","msg":"Reconciling ChaosEngine","Request.Namespace":"sock-shop","Request.Name":"sock-chaos"}	IN1sWH4BtksKM2LxYuUE

A General Context



Energy Management and Decision Support System in Smart Homes

- ICOS employs machine learning (ML) models and environmentally sustainable practices to support data analysis from five smart homes, aiming to provide optimized energy management tailored to consumer needs.
- Privacy is provided by anonymizing data via the Data Management module, while data integrity is monitored by Wazuh and LOMOS, which also oversees infrastructure support and utilizes telemetry for log analysis to enhance model accuracy.
- The potential challenge of using it in such an environment could be scrambled information in the logs as the edge device will gather data from multiple IoT sources

smart home security

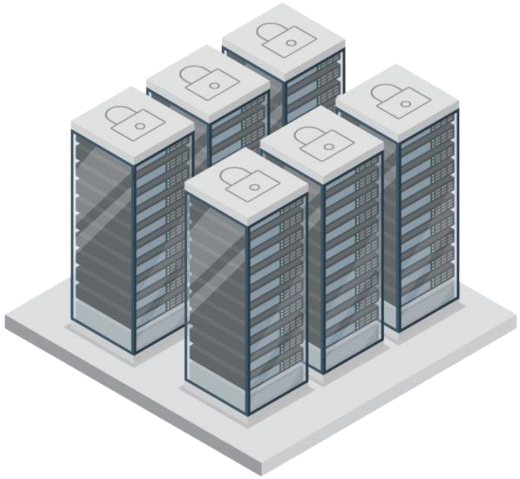
Real-time Security of Connected Medical Devices

- For real-time security of CMDs at CYLCOMED (i) LOMOS provides a mitigation barrier that helps making the digital health environment safer; and (ii) the ability to be deployed in such a complex framework, to adapt to different legal constraints
- CMDs Security Maintenance, providing the infrastructure for secure device management, including updates and configuration management, to reduce the attack surface.

Medical Device Monitoring

Electronic Health Records Datacentre Critical Infrastructure

- Ensure privacy, any potentially sensitive information within the logs was pseudonymized, supporting the integrity and reliability of our anomaly detection efforts.
- Engine benchmarking and quantitative performance measuring for the LOMOS engine; integration where the Cybersecurity Team maintain internally tools for Adversary Simulation and Red Team engagements.



Critical Infrastructure Resilience

Future Work

- ❑ The ability to aggregate logs from different applications and nodes could provide valuable insights and enable the creation of more accurate and comprehensive events and rules
- ❑ Comparing and tagging anomalies from different data sources, moving them to a training set, and converting them into events that can be integrated into the SIEM
- ❑ Deal with extensively regulated scenarios
- ❑ Heterogeneity and volatility of devices in IoT/Edge

HRVOJE.RATKAJEC@XLAB.SI

LinkedIn/company/xlab

WWW.XLAB.SI

Get IT done.