YAKSHA: Implementing Honeypot as-a-Service

A. Kostopoulos, I. Chochliouros, C. Patsakis, M. Anastasiadis, A. Guarino

Infocom World 2020 – November 2020

Scope & objectives

- **YAKSHA builds an ecosystem of partners** around its solutions **that will contribute to enhancing cybersecurity skills in Europe and creating new positions for cybersecurity specialists in ASEAN.** Moreover, the **direct access to the important ASEAN market** will positively impact the competitiveness of European security industry.
- **The YAKSHA software solution will be validated in real-world pilot projects in both EU and ASEAN**, ***initially focusing on Vietnam and Greece,*** and with plans to expand the deployments to other countries.

Objectives

1. To assess the Cyber Security state of the art in the ASEAN area and future developments

2. To develop and validate a distributed, flexible, cybersecurity solution.

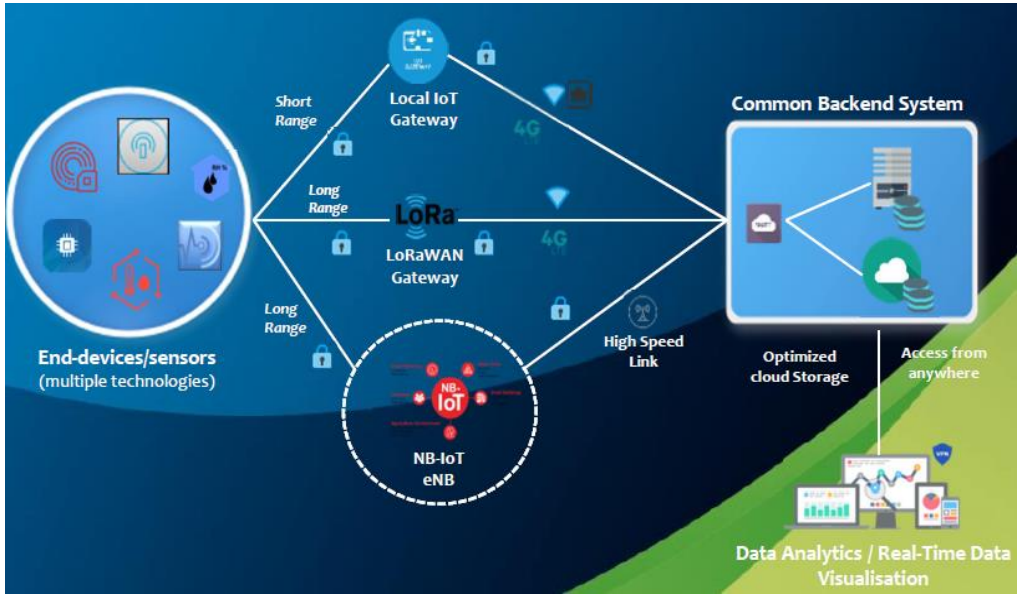
3. To enable the *sustainable* uptake of scientific, technical and economic results and foster cooperation and partnerships between EU-ASEAN.

Architectural Components

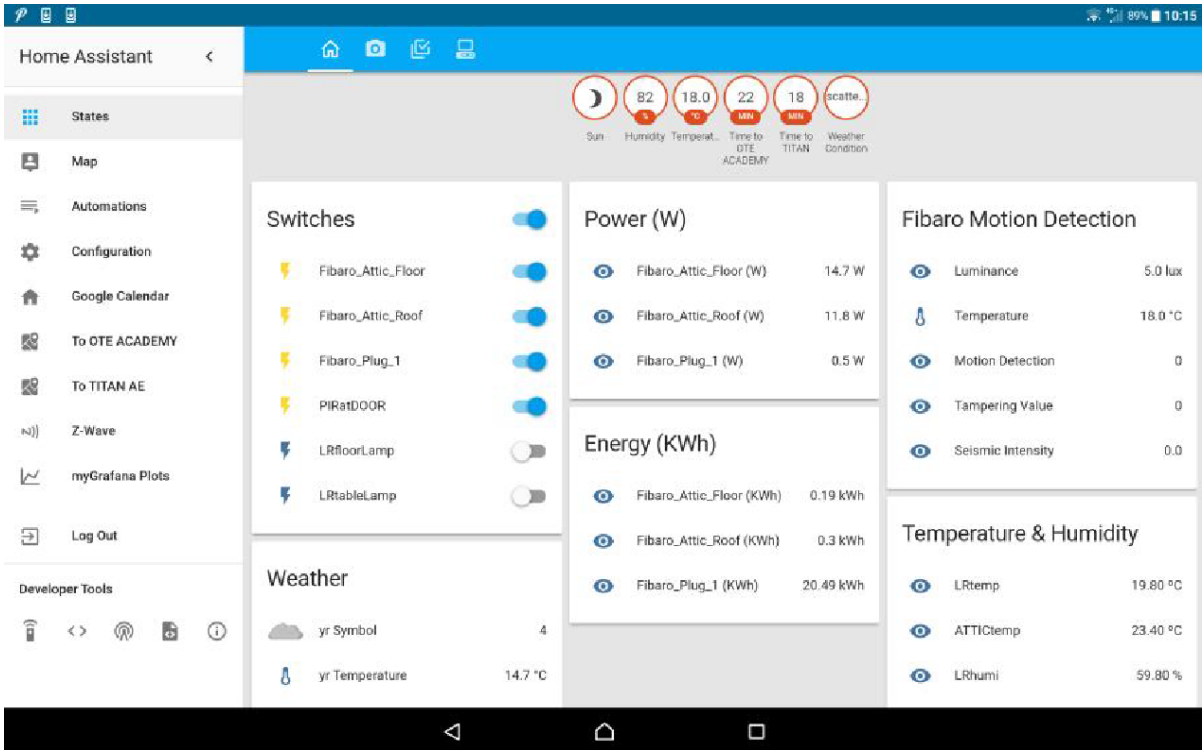
- **A YAKSHA Node:** *On top, the installed honeypots which are exposed to the Internet so that attackers will try to penetrate them.*
  - **Maintenance and Integration Engine:** *configuration of a new honeypot, uploading and exposing it to the Internet and data wipe.*
  - **Monitoring Engine:** *sanity checks to determine whether the honeypot is properly working*
  - **Correlation Engine:** *find how significant is the penetration and propagation of the sample, and it correlates the attack patterns with input from older samples.*
  - **Reporting Engine:** **presenting the information in a readable form**
  - **Connectivity and Sharing Engine:** *information exchange with other YAKSHA nodes (e.g., malware samples).*

Use Case: *IoT Platform Testbed*

- **Pre-commercial environment** (infrastructure and settings) **to collect real data** of potential attacks against the smart home IoT platform product.
- **YAKSHA analytics capability will be used to raise awareness and provide decision support** in strengthening the cybersecurity posture of the product.
- **Awareness of potential attacks in the wild against ICT products and services.**



OTE's IoT testbed (cont.)



Sensors' data

All the measurements received from five different sensors connected to OTE's IoT testbed platform:

- *power consumption,*
- *humidity,*
- *temperature,*
- *base stations sites,*
- *parking area.*

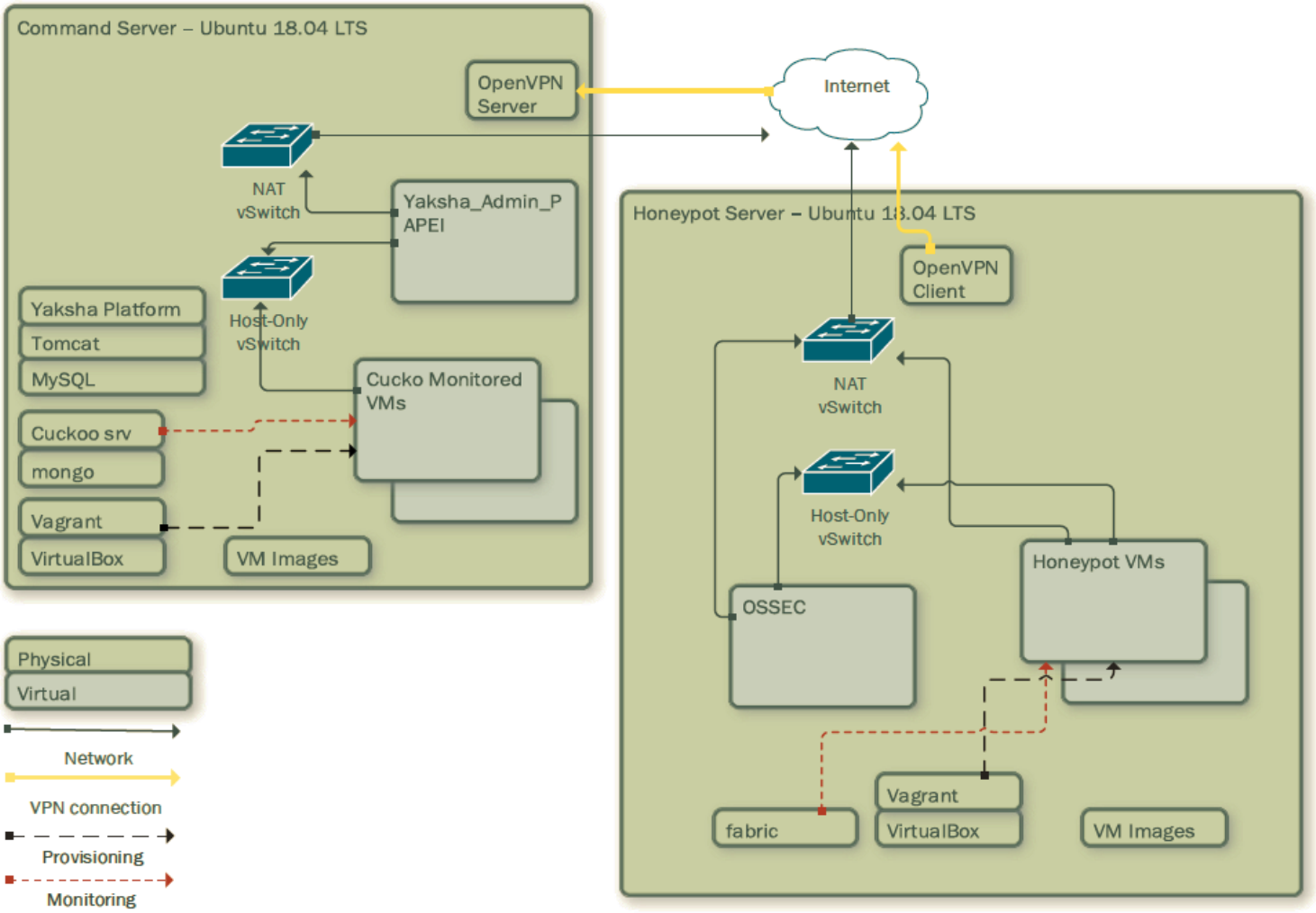
The measurements are visualised using the Grafana software.

YAKSHA Architecture

The YAKSHA pilot project installation for Greece will handle one end user node, OTE.

The figure provides a scheme of a typical YAKSHA node, constituted by:

- *a Command and Control Server and*
- *a Honeypot Server*

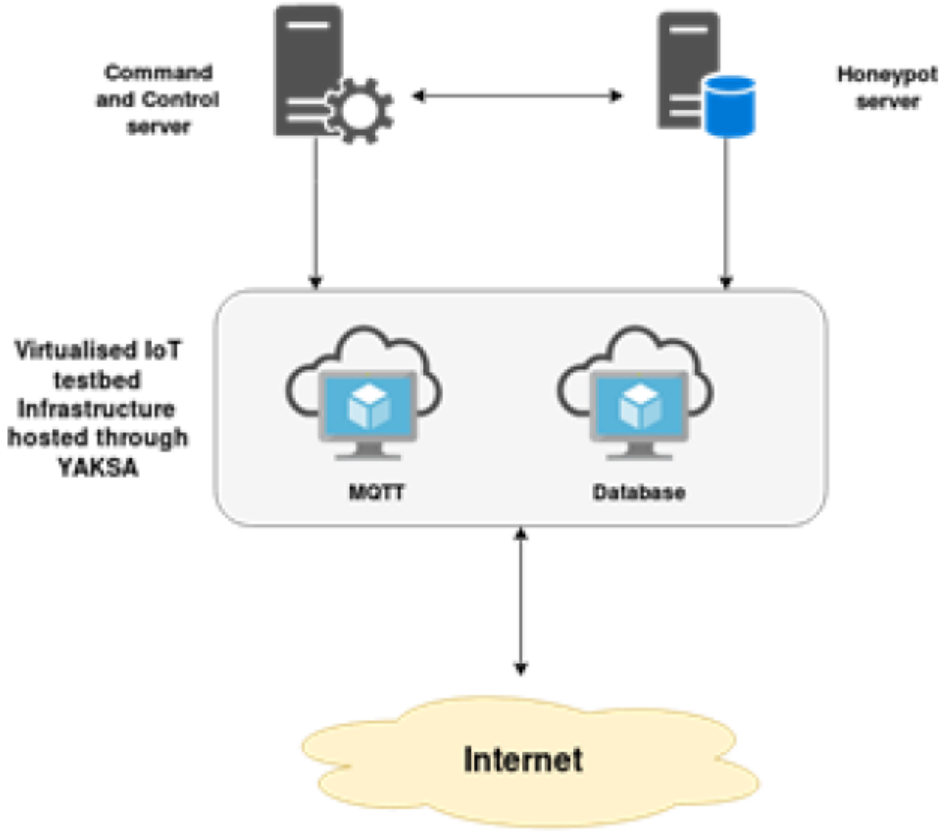


Installing YAKSHA in OTE's lab testbed

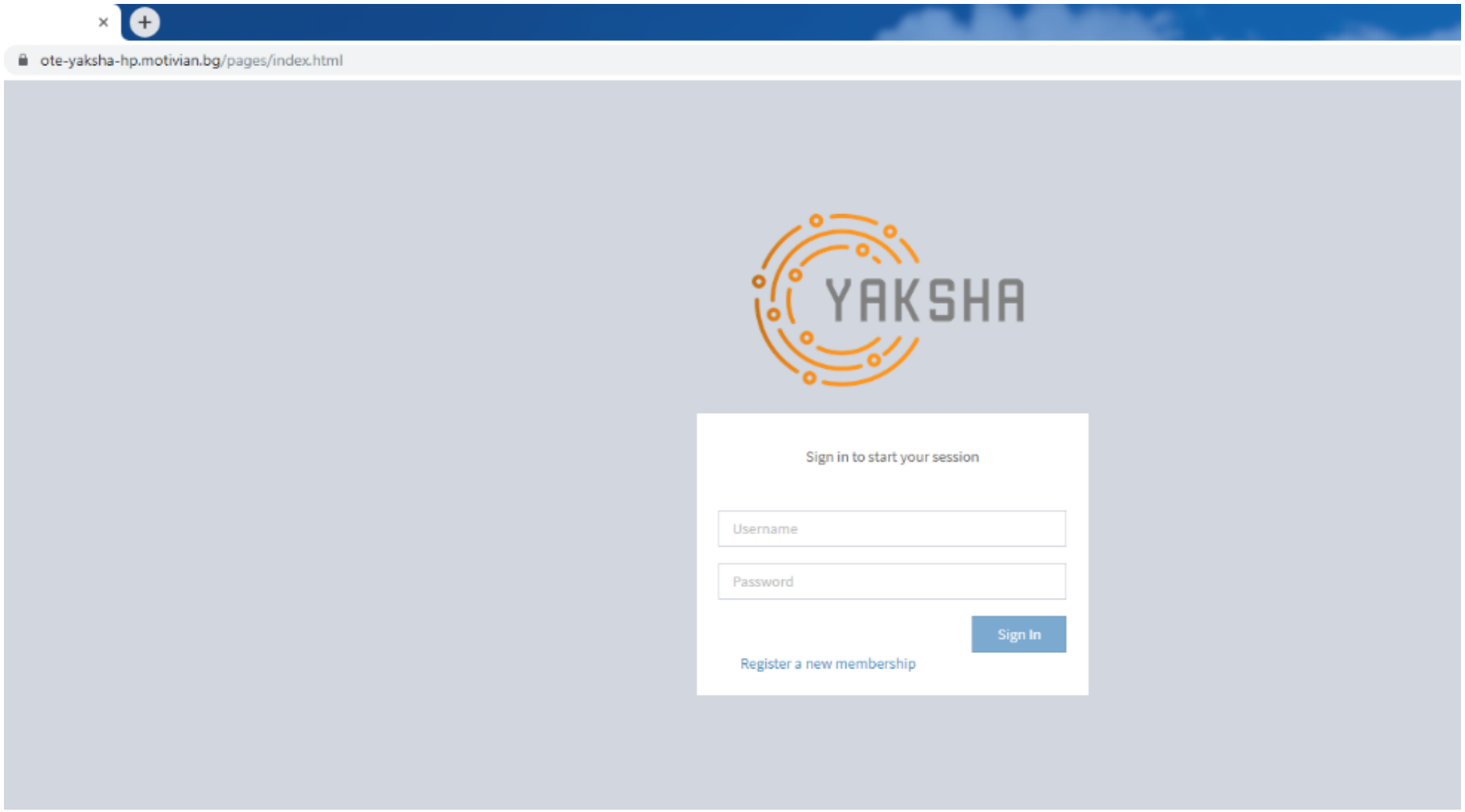
After YAKSHA installation:

- One physical machine for:
  - YAKSHA command and control server,
  - YAKSHA honeypot server.
- IoT testbest consists of:
  - MQTT broker
  - Database.

Each part is hosted on a dedicated virtual machine, which are part of OTE's cloud infrastructure.

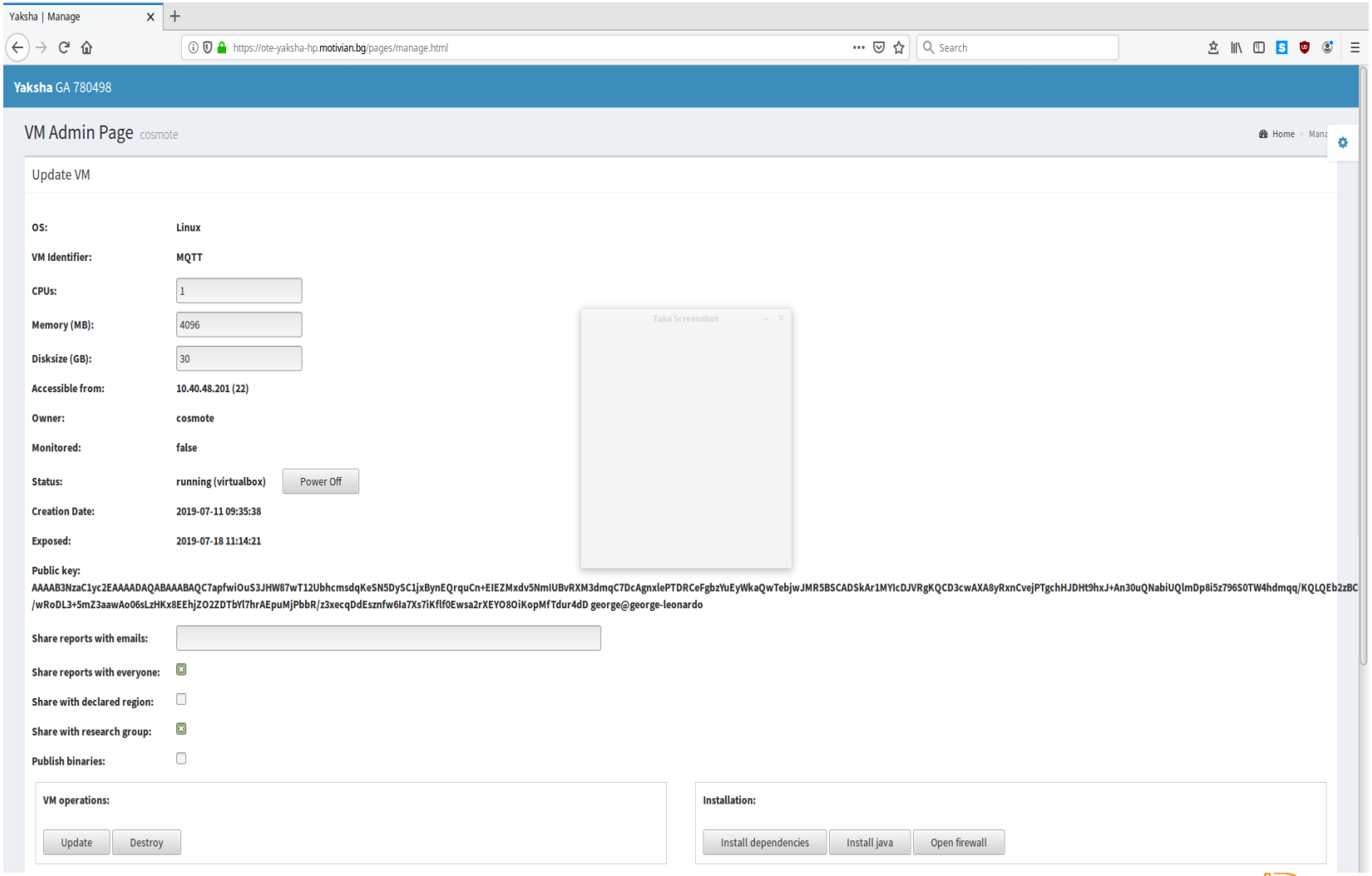


YAKSHA Dashboard



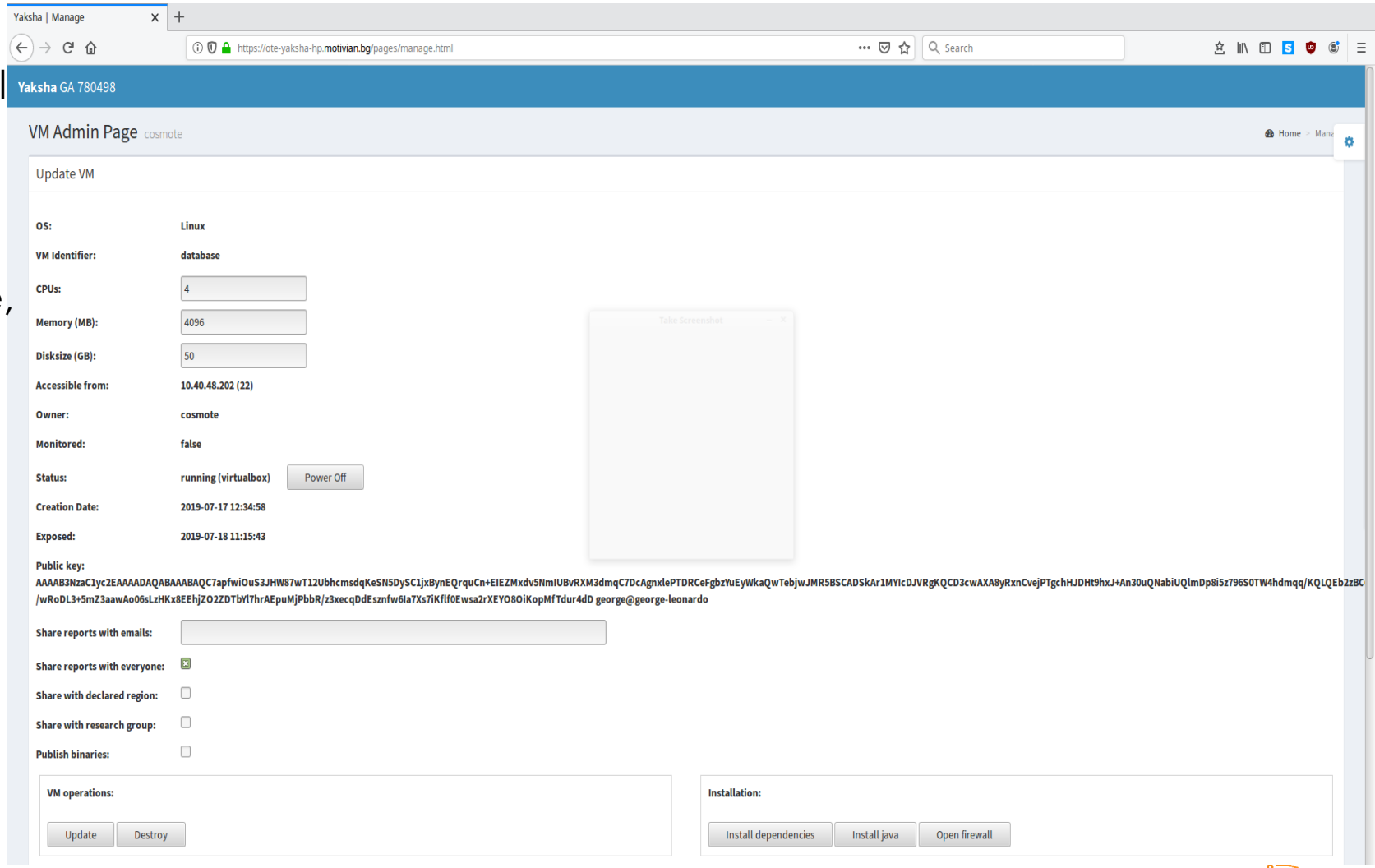
Virtual infrastructure

The virtual machine, which is deployed for the MQTT broker, for OTE's IoT platform.



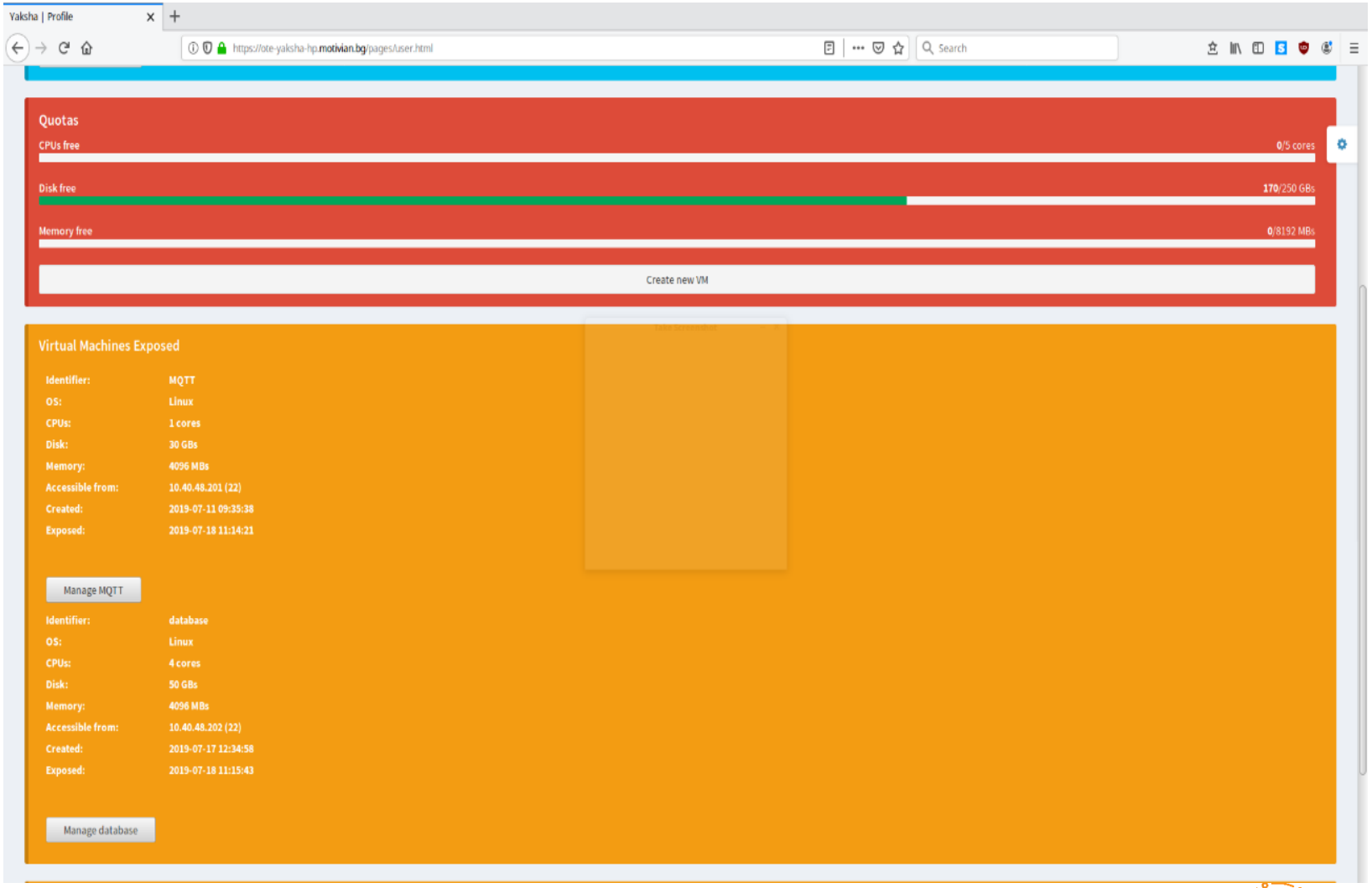
Virtual infrastructure (cont.)

The virtual machine, which is deployed for the database, for OTE's IoT platform.

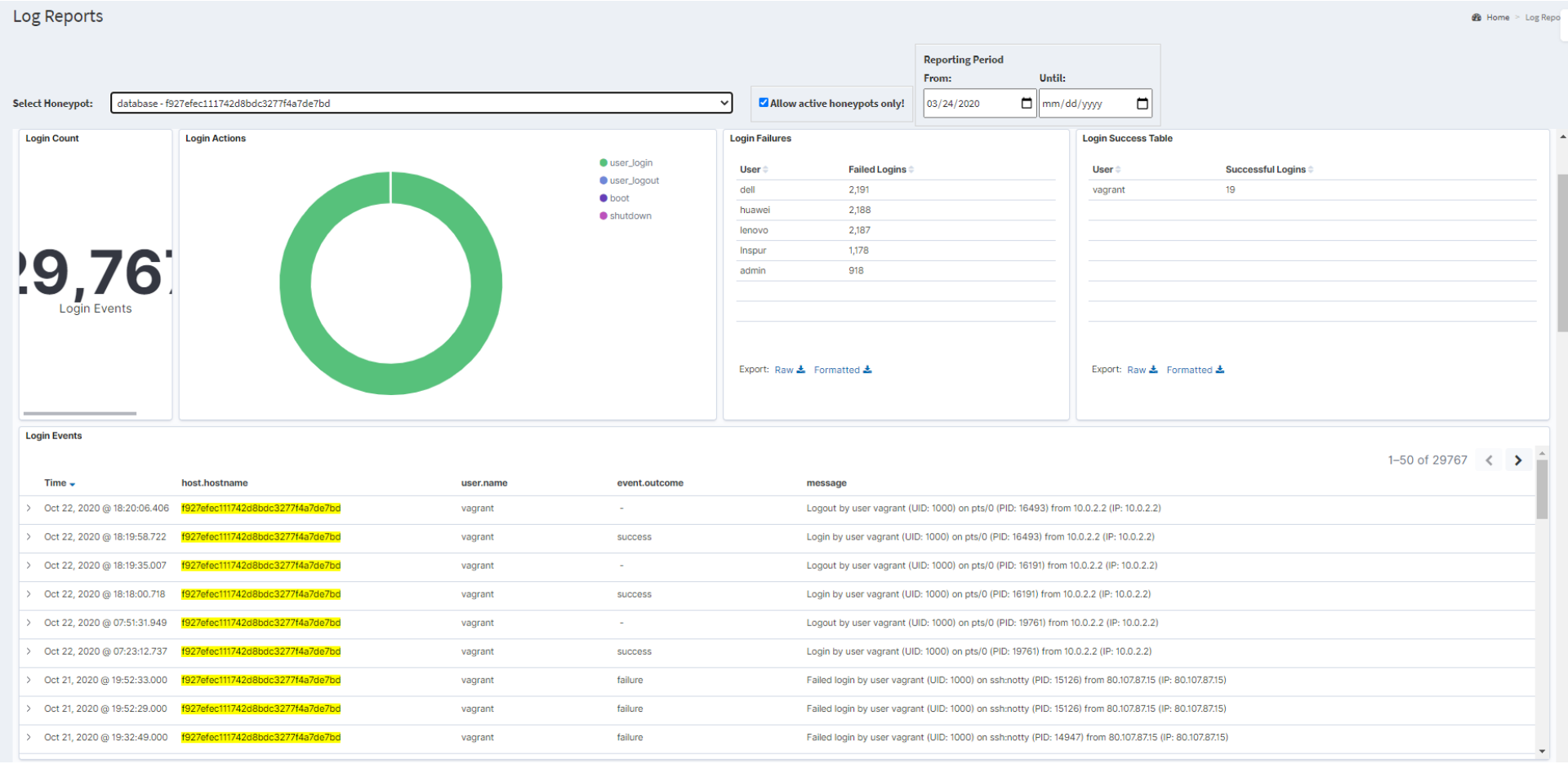


Virtual infrastructure (cont.)

The characte-ristics of the deployed VMs *(e.g., CPU, disk, memory, etc.)*.



Log Reports


Log Reports
Home > Log Repo
Reporting Period
From:
Until:
Select Honeypot:
database - f927efec111742d8bdc3277f4a7de7bd
Allow active honeypots only!
03/24/2020
mm/dd/yyyy
Login Count
9,76
Login Events
Login Actions
user_login
user_logout
boot
shutdown
Login Failures
User
Failed Logins
dell 2,191
huawei 2,188
lenovo 2,187
Inspur 1,178
admin 918
Export: Raw Formatted
Login Success Table
User
Successful Logins
vagrant 19
Export: Raw Formatted
Login Events
1–50 of 29767
Time
host.hostname
user.name
event.outcome
message
Oct 22, 2020 @ 18:20:06.406 f927efec111742d8bdc3277f4a7de7bd vagrant - Logout by user vagrant (UID: 1000) on pts/0 (PID: 16493) from 10.0.2.2 (IP: 10.0.2.2)
Oct 22, 2020 @ 18:19:58.722 f927efec111742d8bdc3277f4a7de7bd vagrant success Login by user vagrant (UID: 1000) on pts/0 (PID: 16493) from 10.0.2.2 (IP: 10.0.2.2)
Oct 22, 2020 @ 18:19:35.007 f927efec111742d8bdc3277f4a7de7bd vagrant - Logout by user vagrant (UID: 1000) on pts/0 (PID: 16191) from 10.0.2.2 (IP: 10.0.2.2)
Oct 22, 2020 @ 18:18:00.718 f927efec111742d8bdc3277f4a7de7bd vagrant success Login by user vagrant (UID: 1000) on pts/0 (PID: 16191) from 10.0.2.2 (IP: 10.0.2.2)
Oct 22, 2020 @ 07:51:31.949 f927efec111742d8bdc3277f4a7de7bd vagrant - Logout by user vagrant (UID: 1000) on pts/0 (PID: 19761) from 10.0.2.2 (IP: 10.0.2.2)
Oct 22, 2020 @ 07:23:12.737 f927efec111742d8bdc3277f4a7de7bd vagrant success Login by user vagrant (UID: 1000) on pts/0 (PID: 19761) from 10.0.2.2 (IP: 10.0.2.2)
Oct 21, 2020 @ 19:52:33.000 f927efec111742d8bdc3277f4a7de7bd vagrant failure Failed login by user vagrant (UID: 1000) on ssh:notty (PID: 15126) from 80.107.87.15 (IP: 80.107.87.15)
Oct 21, 2020 @ 19:52:29.000 f927efec111742d8bdc3277f4a7de7bd vagrant failure Failed login by user vagrant (UID: 1000) on ssh:notty (PID: 15126) from 80.107.87.15 (IP: 80.107.87.15)
Oct 21, 2020 @ 19:32:49.000 f927efec111742d8bdc3277f4a7de7bd vagrant failure Failed login by user vagrant (UID: 1000) on ssh:notty (PID: 14947) from 80.107.87.15 (IP: 80.107.87.15)

Log Reports (cont.)

User Changes

1
User Changes

User Count

35
Users

User Change Actions

Process Count

13,951
Processes

Process Starts

13,769
Started

Process Stops

13,776
Stopped

Process Events

>	Oct 26, 2020 @ 06:38:56.602	f927efec111742d8bdc3277f4a7de7bd	chronograf	existing_process	1047	chronograf
>	Oct 26, 2020 @ 06:38:56.602	f927efec111742d8bdc3277f4a7de7bd	grafana	existing_process	1177	grafana-server
>	Oct 26, 2020 @ 06:38:56.602	f927efec111742d8bdc3277f4a7de7bd	influxdb	existing_process	1185	influxd
>	Oct 26, 2020 @ 06:38:56.602	f927efec111742d8bdc3277f4a7de7bd	root	existing_process	1277	polkitd
>	Oct 26, 2020 @ 06:38:56.602	f927efec111742d8bdc3277f4a7de7bd	root	existing_process	16442	bash
>	Oct 26, 2020 @ 06:38:56.602	f927efec111742d8bdc3277f4a7de7bd	root	existing_process	16470	inotifywait
>	Oct 26, 2020 @ 06:38:56.602	f927efec111742d8bdc3277f4a7de7bd	root	process_error	32500	sshd

Process Names

Process	Count
sshd	24,634
apt.systemd.dai	638
bash	581
unattended-upgr	557
agetty	522
apt-get	323
http	237
accounts-daemon	234

Export: Raw Formatted

Process Users

Process	Count
root	20,993
sshd	11,520
_apt	637
systemd-network	261
influxdb	260
messagebus	260
systemd-resolve	260
chronograf	259

Export: Raw Formatted

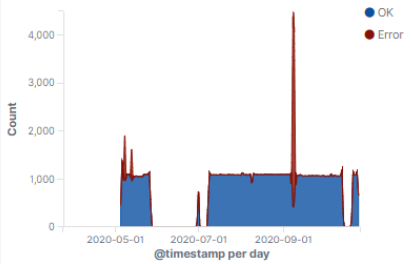
Process Executions

1–50 of 1102927

	Time	agent.hostname	process.args	auditd.summary.actor.primary	auditd.summary.actor.secondary	pro
>	Oct 26, 2020 @ 13:22:51.103	f927efec111742d8bdc3277f4a7de7bd	date, +%Y-%m-%d %H:%M:%S	unset	root	/bin
>	Oct 26, 2020 @ 13:22:51.099	f927efec111742d8bdc3277f4a7de7bd	stat, --format=%U, /var/lib/influxdb/data/_internal/monitor/488/00000000004-000000001.tsm	unset	root	/usr
>	Oct 26, 2020 @ 13:22:51.059	f927efec111742d8bdc3277f4a7de7bd	date, +%Y-%m-%d %H:%M:%S	unset	root	/bin
>	Oct 26, 2020 @ 13:22:51.055	f927efec111742d8bdc3	stat, --format=%U, /va	unset	root	/usr

Log Reports (cont.)

DNS Request Status Over Time [Packetbeat] ECS



DNS Query Summary [Packetbeat] ECS

145,067
Count

6.7MB
Client Bytes

12MB
Server Bytes

53.6
Avg Response Time (ns)

1–50 of 543

Time	dhcpv4.transaction_id	dhcpv4.op_code	dhcpv4.option.message_type	source.ip	destination.ip	dhcpv4.
Oct 26, 2020 @ 11:28:13.245	0x41bc249f	bootrequest	request	10.0.2.15	10.0.2.2	02:a1:18:
Oct 26, 2020 @ 11:28:13.245	0x41bc249f	bootreply	ack	10.0.2.2	10.0.2.15	02:a1:18:
Oct 25, 2020 @ 23:28:14.080	0x41bc249f	bootreply	ack	10.0.2.2	10.0.2.15	02:a1:18:
Oct 25, 2020 @ 23:28:14.079	0x41bc249f	bootrequest	request	10.0.2.15	10.0.2.2	02:a1:18:
Oct 25, 2020 @ 11:28:14.695	0x41bc249f	bootrequest	request	10.0.2.15	10.0.2.2	02:a1:18:
Oct 25, 2020 @ 11:28:14.695	0x41bc249f	bootreply	ack	10.0.2.2	10.0.2.15	02:a1:18:

Data Transfer [Packetbeat DHCPv4] ECS

83.6KB
Requests

145KB
Responses

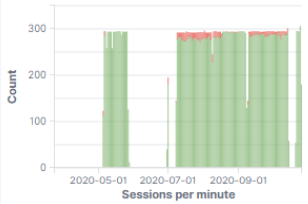
Total Number of TLS Sessions [Packetbeat] ECS

36,606
Count

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://10.40.48.23:5000/malwares	10,424
http://archive.ubuntu.com/ubuntu/dists/bionic-backports/InRelease	128
http://archive.ubuntu.com/ubuntu/dists/bionic-updates/InRelease	128
http://archive.ubuntu.com/ubuntu/dists/bionic/InRelease	128
http://security.ubuntu.com/ubuntu/dists/bionic-security/InRelease	128

TLS Sessions [Packetbeat] ECS



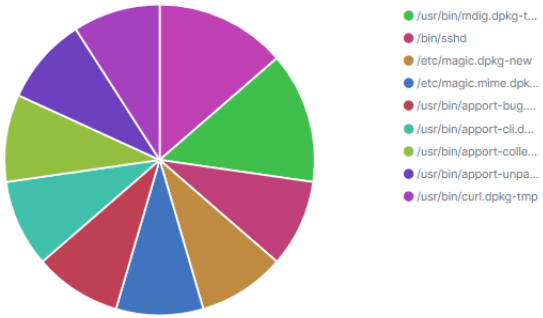
Total number of HTTP transactions [Packetbeat] ECS

21,051
Count

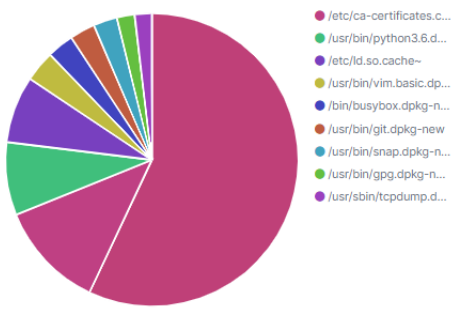
Top created [Auditbeat File Integrity] ECS

Log Reports (cont.)

Top deleted [Auditbeat File Integrity] ECS



Top updated [Auditbeat File Integrity] ECS



World Writable File Count [Auditbeat File Integrity] ECS

0

Actions [Auditbeat File Integrity] ECS

1,469	1,454	1,164	422
initial_scan - Count	updated - Count	created - Count	moved - Count

344
deleted - Count

File Integrity Events [Auditbeat File Integrity] ECS

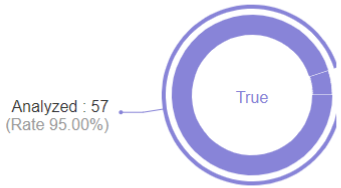
1–50 of 4914

Time	file.path	event.action
Oct 22, 2020 @ 09:53:28.185	/etc/ld.so.cache~	moved
Oct 22, 2020 @ 09:53:28.185	/etc/ld.so.cache~	attributes_modified
Oct 22, 2020 @ 09:53:28.185	/etc/ld.so.cache	created
Oct 22, 2020 @ 09:53:28.162	/etc/ld.so.cache~	updated
Oct 22, 2020 @ 09:53:28.160	/etc/ld.so.cache~	created
Oct 22, 2020 @ 09:53:28.160	/etc/ld.so.cache~	updated
Oct 15, 2020 @ 04:17:01.721	/bin/sshd	updated
Oct 15, 2020 @ 04:17:01.716	/bin/sshd	updated

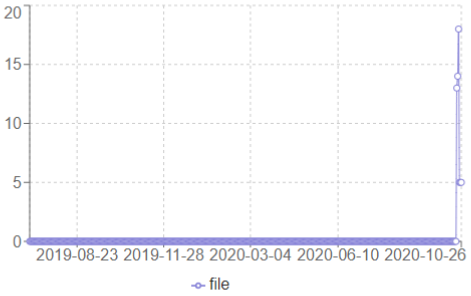
Malicious Files Collection

Malicious Files Collection

Total Files Analysed



Total Files over Time



Total Files per Honeypot

Malicious Files Static and Dynamic Analysis Reports (JSON Format)

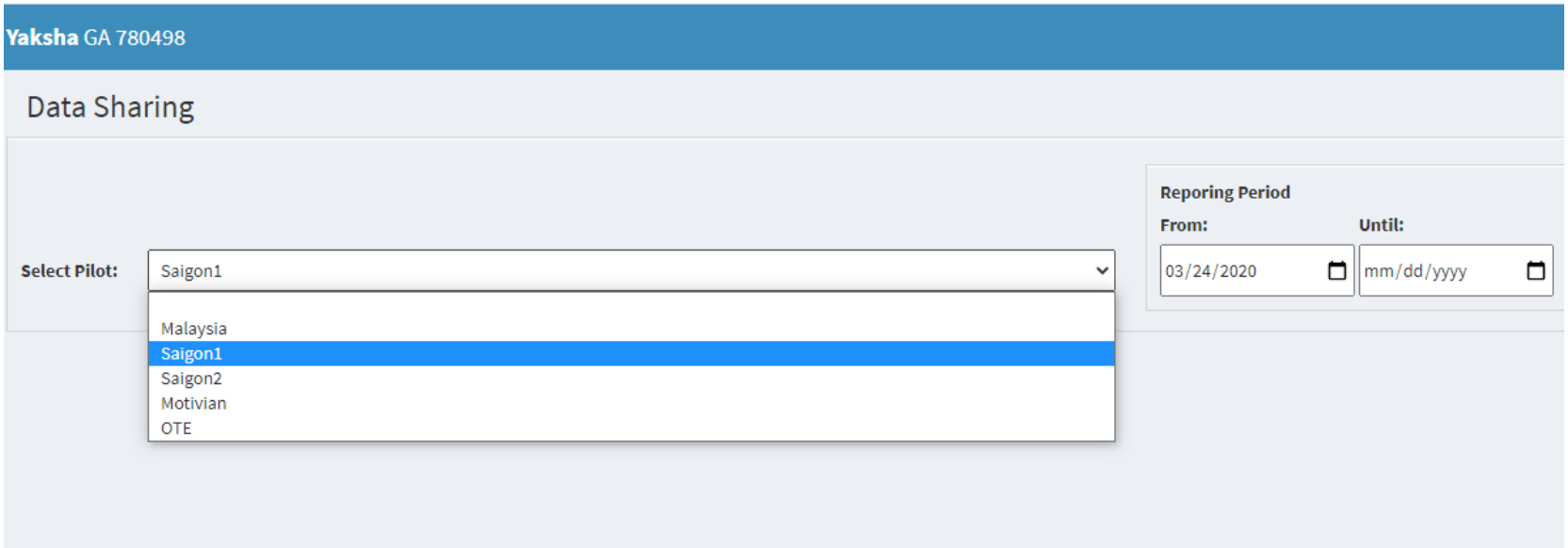
Analysis Reports List

Search

Download	Path	Honeypot	Exposed IP	OS	Size	Date
	/tmp/apt.conf.F5iHiV	database	94.70.239.216	linux-gnu	12277	2020-10-26
	/tmp/apt.conf.tFI8eJ	database	94.70.239.216	linux-gnu	12277	2020-10-26
	/tmp/apt.conf.YZuvc7	database	94.70.239.216	linux-gnu	12277	2020-10-26
	/tmp/apt.conf.qk4BAY	database	94.70.239.216	linux-gnu	12277	2020-10-26
	/tmp/apt.conf.dHVJWr	database	94.70.239.216	linux-gnu	12277	2020-10-26

6-10 of 60

Data Sharing



Conclusions

- YAKSHA automates a big part of this procedure and distribute this information to peers.
- Most companies and organizations are not able to create such analytics for their systems, so YAKSHA can become the first such system to automatically provide such features.
- The technological experience and knowhow of EU is matched with the wide deployments of ASEAN countries to develop and field test the solution.
- YAKSHA intends to provide an automated framework for deploying honeypots and correlating the collected information.

The essential goal is to enable end-users, whether they are governments, organisations or companies, to easily setup customised honeypots, which will allow them to understand how their systems are being attacked on the wild, in an autonomous way.


YAKSHA


spi


UNIVERSITY
OF PIRAEUS


OTE
GROUP OF COMPANIES


inno


MOTIVIAN


VTT


Atos


vinasa


CyberSecurity
MALAYSIA


NECTEC
a member of NSTDA


ACIOA
ASEAN Chief Information Officer Association


DISE

Thank you for your attention!

https://project-yaksha.eu/

For more information:

Dr. Ioannis P. Chochliouros
Head of Fixed Network R&D Programs Section
Research and Development Dept., Fixed & Mobile
E-Mail: ichochliouros@oteresearch.gr; ic152369@ote.gr;

Dr. Alexandros Kostopoulos
Research and Development Dept., Fixed & Mobile
E-Mail: alexkosto@oteresearch.gr;