



ICAO MID

# CYBER SECURITY AND RESILIENCE SYMPOSIUM

TOWARDS A RESILIENT AVIATION CYBERSPACE

AMMAN, JORDAN | 15-17 OCTOBER 2019

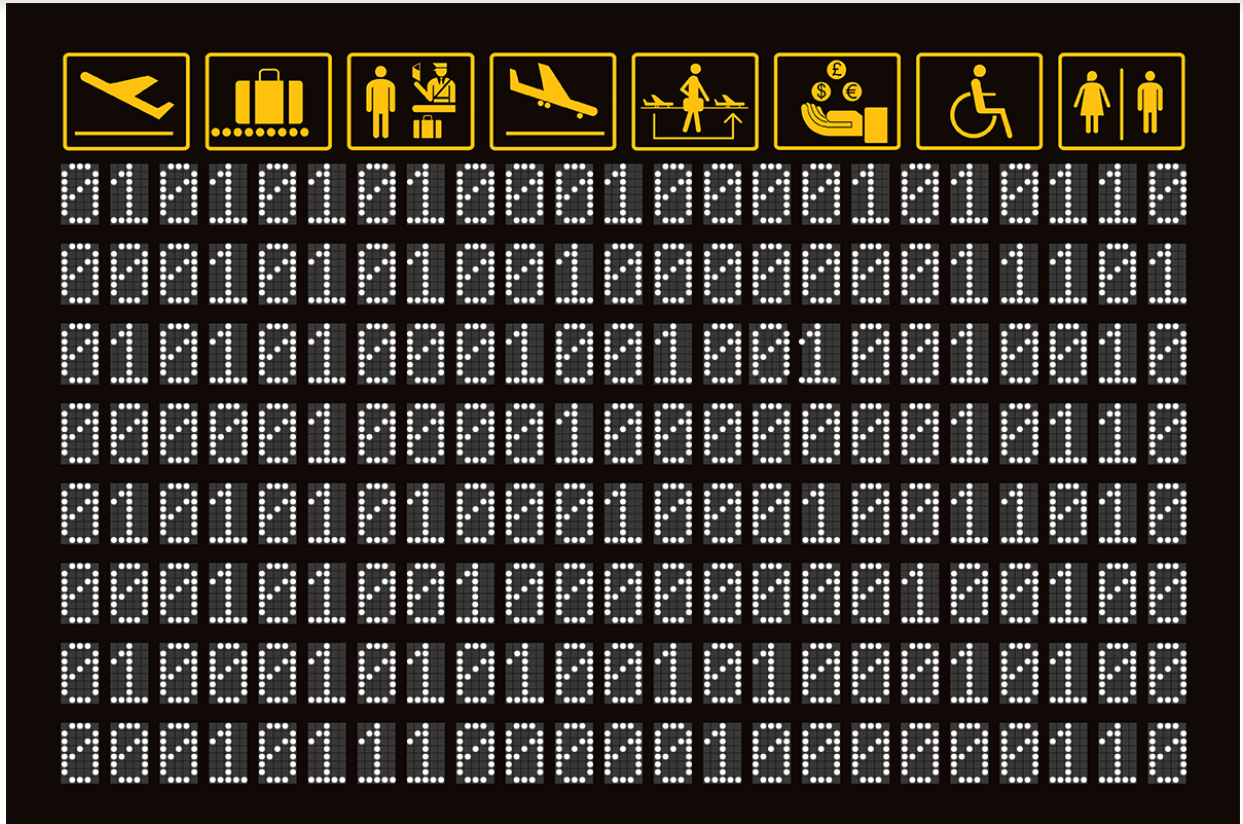


ICAO 2019

75 YEARS OF CONNECTING THE WORLD

## Omar Sherin

*Cyber Analytics in Aviation*





ICAO MID

**CYBER SECURITY AND  
RESILIENCE SYMPOSIUM**

TOWARDS A RESILIENT AVIATION CYBERSPACE

AMMAN, JORDAN | 15-17 OCTOBER 2019



ICAO 2019

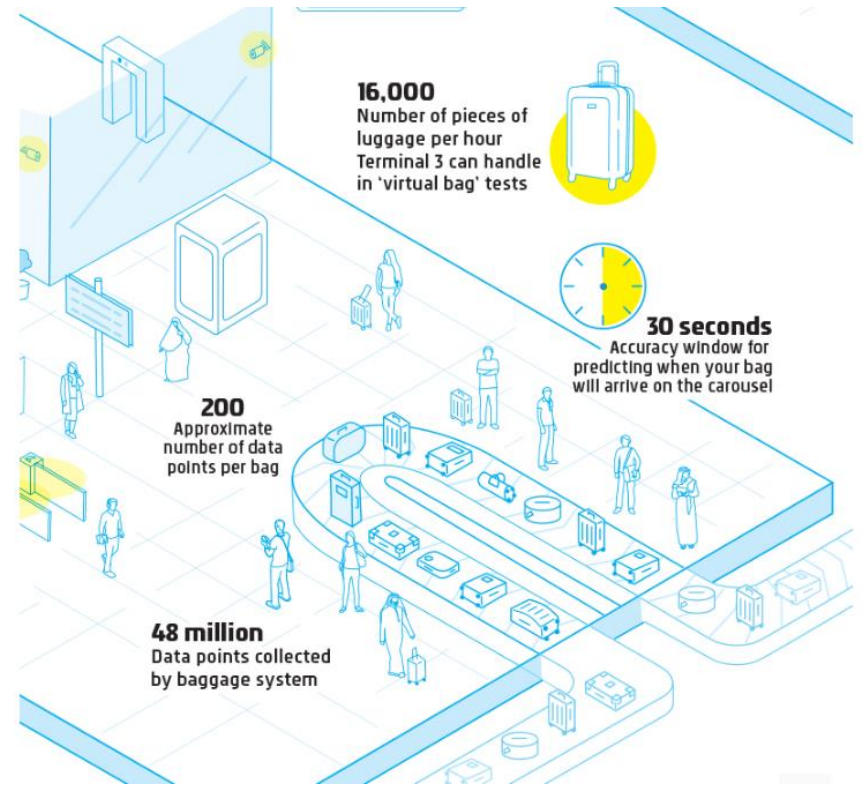
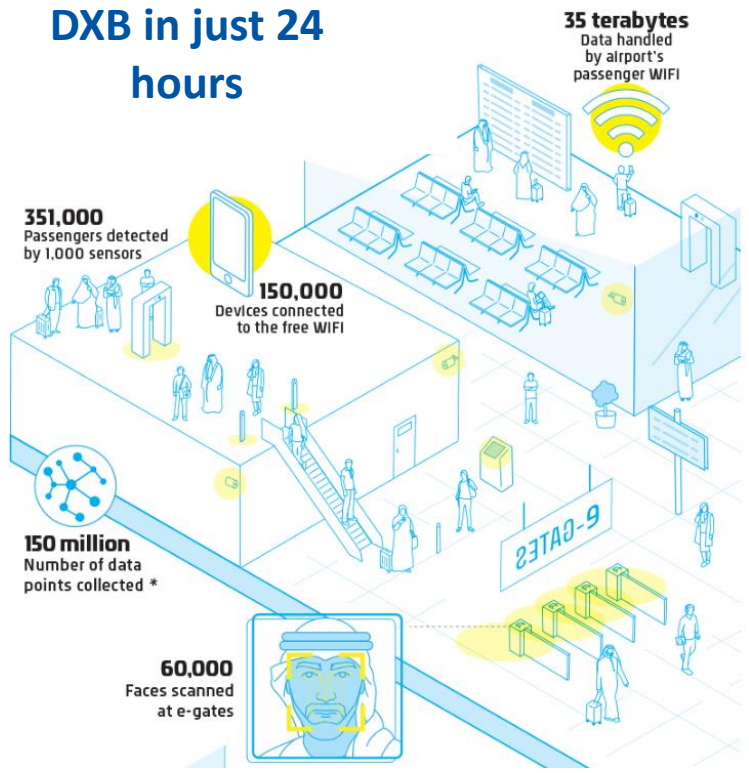
75 YEARS OF  
CONNECTING  
THE WORLD

How many data records are created  
each month in DXB ?

**5 Billion** (Records)



## DXB in just 24 hours





ICAO MID

# CYBER SECURITY AND RESILIENCE SYMPOSIUM

TOWARDS A RESILIENT AVIATION CYBERSPACE

AMMAN, JORDAN | 15-17 OCTOBER 2019



ICAO 2019

75 YEARS OF CONNECTING THE WORLD

# Eid Holiday (1 day) 2019

How things will look like  
with 5G ?

**280,000**

Passengers moved through the airport



**194**

Number of passengers a minute



**120,000**

Staff working at the airport



**1,100**

Flights to/from 220 destinations



**240,000**

Number of checked bags handled



**255,373**

Items sold in Dubai Duty Free



**20,000**

Cups of coffee served







ICAO MID

# CYBER SECURITY AND RESILIENCE SYMPOSIUM

TOWARDS A RESILIENT AVIATION CYBERSPACE

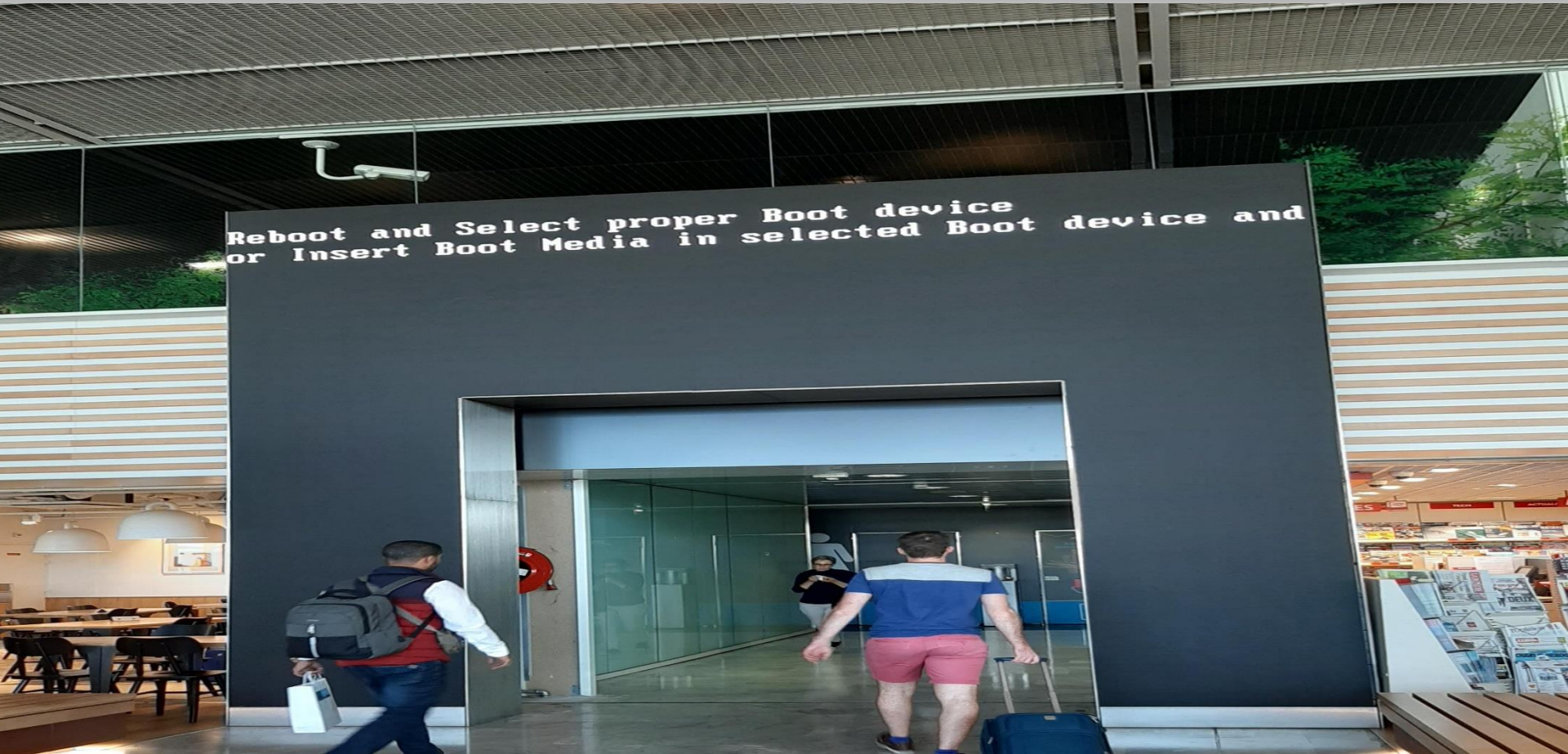
AMMAN, JORDAN | 15-17 OCTOBER 2019



ICAO 2019

75 YEARS OF  
CONNECTING  
THE WORLD

Reboot and Select proper Boot device  
or Insert Boot Media in selected Boot device and





## 24 Servers

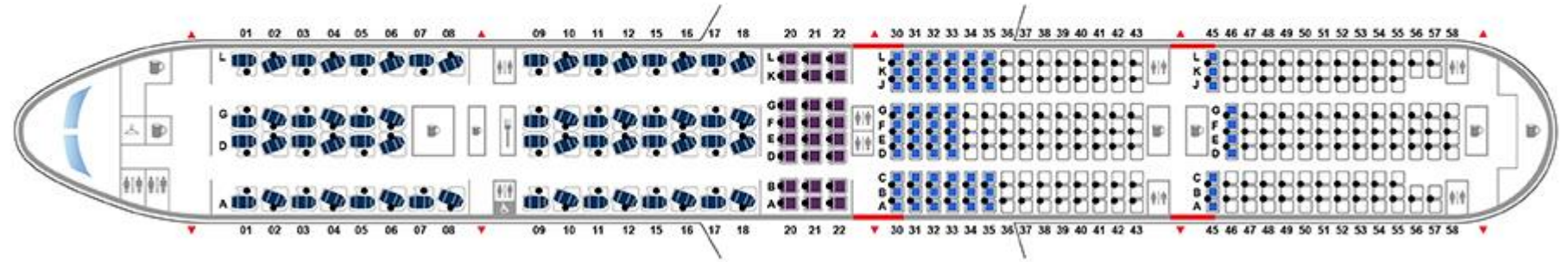
12 CCTVs , 6 TB storage, 1K Meters of  
Fiber cabling, AD, DNS, DHCP, Wireless APs

- A. Data center of a local airport
- B. Data center of a medium business
- C. Data center of an international airport



# Boeing 777 - 300

- United Polaris® business
- United® Premium Plus
- Economy Plus®
- Economy
- In Seat Power
- Exit Row
- Exit Doors
- Lavatory
- Accessible Lavatories
- Closet
- Galley
- Midflight hospitality area



A flying data center





**BOEING SMARTCABIN**

SMART BINS

WIRELESS PASSENGER SERVICES

SMART LAVATORY

ORCHESTRATED CABIN ENVIRONMENT

SMART WINDOW

WIRELESS CABIN NETWORK

SMART DEVICES

HEALTH MONITORING

# Welcome to the Smart Cabin

- Passengers health monitoring !!
- Access your Netflix and Spotify (2022)





Seat: 30B

Name: SVDU30B, IP: 172.17.34.136, MAC: 00:06:CF:03:E0:A6

SVDU serial number: K1002270

AVP SEB: QSEB29ABC, Port: 2

PCU SEB: QSEB29ABC, Port: 2

Database DESC:      "A321 I5 CONFIG"

Database PN: 625694-13\_00

VA Area: 2, PA Area: 2

Primary server: D1P1-V111

Secondary server: D2P1-V118

## My Airbus A321 Trip

- My Seat IP  
172.17.34.136
- My Seat MAC address:  
00:06:CF:03:E0:A6
- The Ent. Server name:  
D2P1-V111



ICAO MID

## CYBER SECURITY AND RESILIENCE SYMPOSIUM

TOWARDS A RESILIENT AVIATION CYBERSPACE

AMMAN, JORDAN | 15-17 OCTOBER 2019



ICAO 2019

75 YEARS OF  
CONNECTING  
THE WORLD

So how can we put all this data to  
good use ?

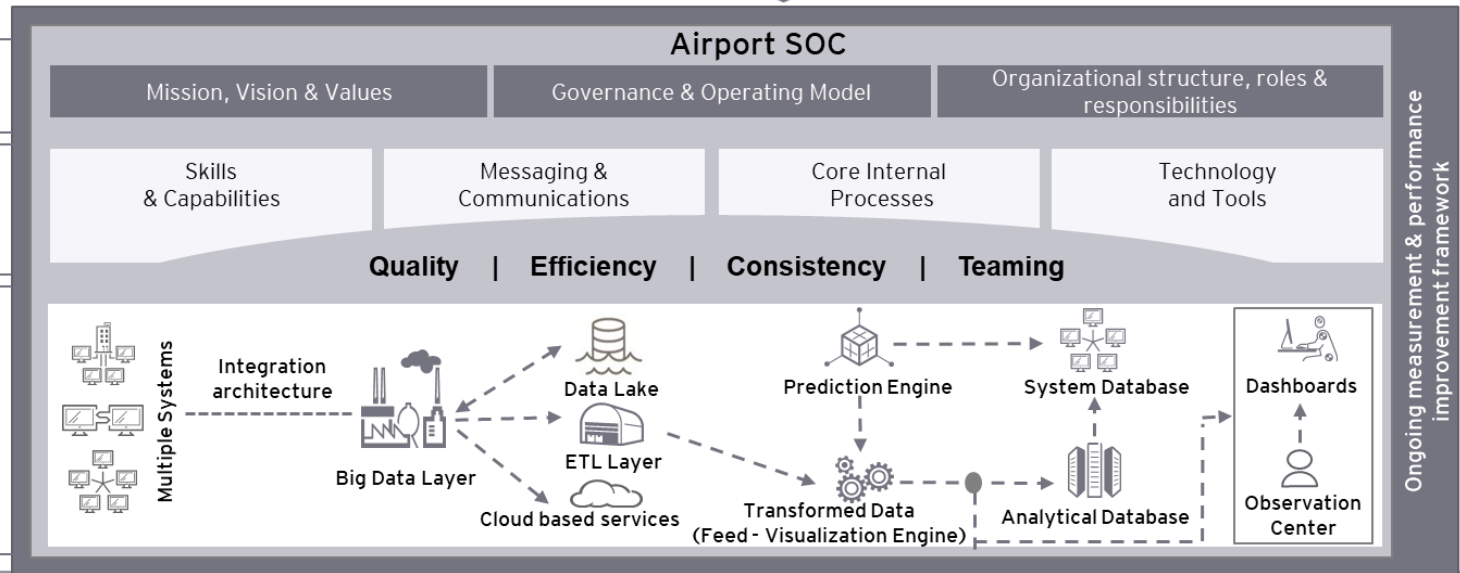


#### Threat Intelligence & External Awareness

Open source Intelligence (OSINT)	Signal Intelligence (SIGINT)	Human Intelligence (HUMINT)	Traveler Experience	Sector & Geographic Reach	
Business Context			Enterprise Event Data		
Policies & Standards	Risk Framework	Business Strategy	Incident Data	Testing Results	Heuristics
Compliance Requirements	Asset Inventory	IoT & OT Security Strategy	Forensic Data	Vulnerability Data	Baselines



Who we are  
How we work  
What we intend to do



Ongoing measurement & performance improvement framework







# ICAO MID

## CYBER SECURITY AND RESILIENCE SYMPOSIUM

TOWARDS A RESILIENT AVIATION CYBERSPACE

AMMAN, JORDAN | 15-17 OCTOBER 2019



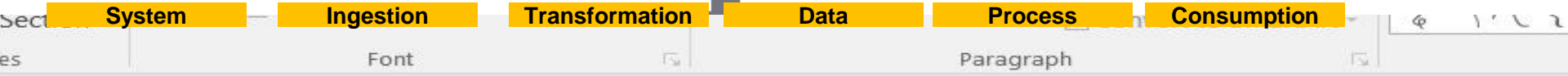
ICAO 2019

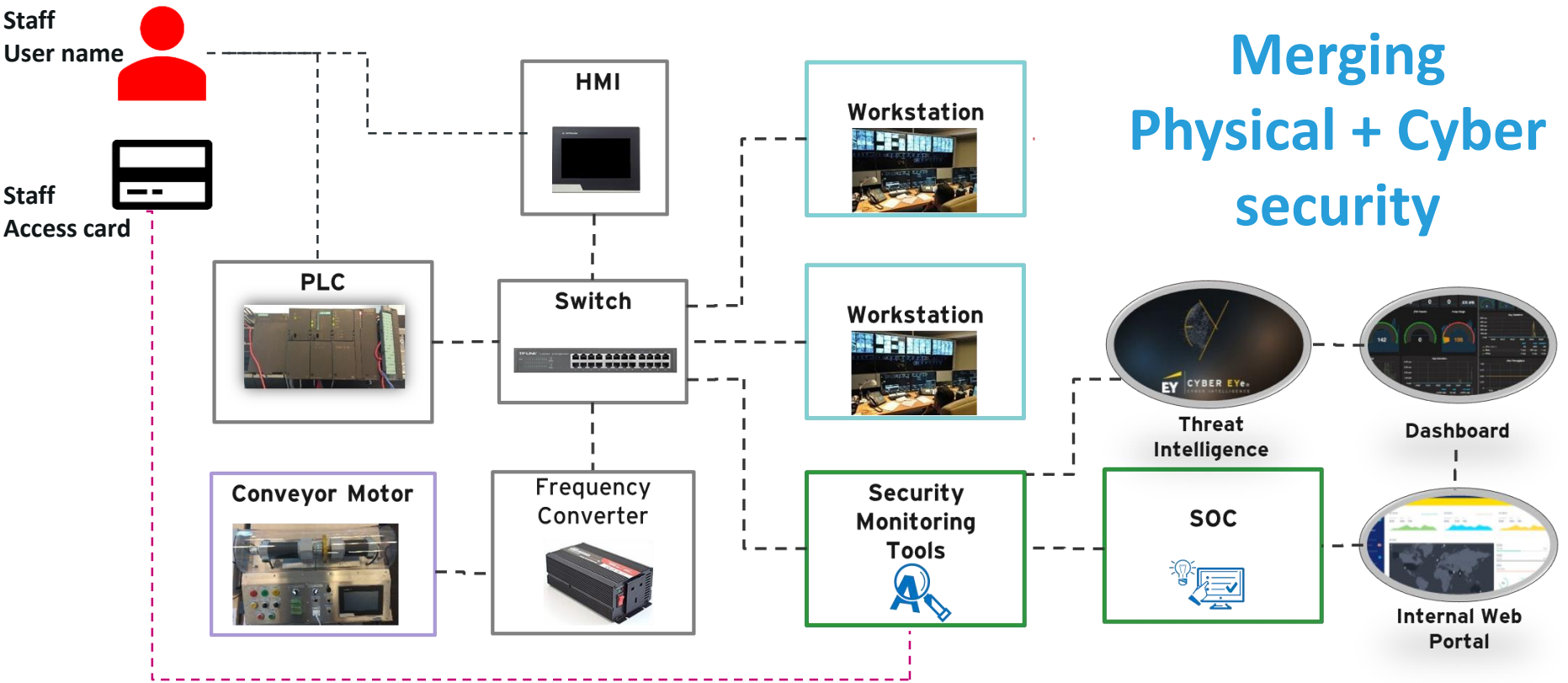
75 YEARS OF CONNECTING THE WORLD

### Threat Intelligence & External Awareness

Open source Intelligence (OSINT)	Signal Intelligence (SIGINT)	Human Intelligence (HUMINT)	Traveler Experience	Sector & Geographic Reach
----------------------------------	------------------------------	-----------------------------	---------------------	---------------------------

Business Context			Enterprise Event Data		
Policies & Standards	Risk Framework	Business Strategy	Incident Data	Testing Results	Heuristics
Compliance Requirements	Asset Inventory	IoT & OT Security Strategy	Forensic Data	Vulnerability Data	Baselines





# Merging Physical + Cyber security



# Baggage Handling Analytics

### Current State

	Status
Reactive strategies undertaken once an alarm has been flagged against a baggage	✓
Proactive or predictive Capabilities to identify threat	✗
Streamline no. of bags for manual checking	✗

### Input Data

Incidence data
TOD/DOY/DOM
Origin of Travel
Destination
Weather data
Special events
Employee data
Name
Age
Employment duration
Work profile
Past history
Education
Passenger data
Name, Age
Demographic information
Citizenship
Employment information

### Methodology

$$y_{i^*}(t+1) = f\left(\sum_{j=1}^N w_{i^*j} y_j(t) + I_{i^*}(t)\right)$$

$$y_i(t+1) = y_i(t), \quad i \neq i^*$$

Hidden Layer

Threat Score

### Outcome

Passenger	Risk Score	Risk Profile
A	87	High
B	10	Safe
C	18	Safe
D	32	Safe
E	65	Low
F	46	Low
G	63	Low
H	80	Moderate
I	33	Safe
J	78	Moderate
K	53	Low
L	10	Safe

VARIATION IN RISK WITH TIME

RISK SCORING: HIGH (85-100) MODERATE (65-85) LOW (40-65) SAFE (0-40)

\* TOD : Time of Day, DOY: Date of Year, DOM: Date of Month





ICAO MID

# CYBER SECURITY AND RESILIENCE SYMPOSIUM

TOWARDS A RESILIENT AVIATION CYBERSPACE

AMMAN, JORDAN | 15-17 OCTOBER 2019



ICAO 2019

75 YEARS OF  
CONNECTING  
THE WORLD



الهيئة العامة للطيران المدني  
CIVIL AVIATION AUTHORITY

وزارة المواصلات والاتصالات  
MINISTRY OF TRANSPORT  
AND COMMUNICATIONS



# Aviation Cyber Security Guidelines



# A regional 1st



ICAO MID

# CYBER SECURITY AND RESILIENCE SYMPOSIUM

TOWARDS A RESILIENT AVIATION CYBERSPACE

AMMAN, JORDAN | 15-17 OCTOBER 2019



ICAO 2019

75 YEARS OF  
CONNECTING  
THE WORLD

# Questions?





# ICAO MID

## CYBER SECURITY AND RESILIENCE SYMPOSIUM

TOWARDS A RESILIENT AVIATION CYBERSPACE

AMMAN, JORDAN | 15-17 OCTOBER 2019



ICAO 2019

75 YEARS OF CONNECTING THE WORLD



# ICAO

North American  
Central American  
and Caribbean  
[NACC] Office  
Mexico City

South American  
[SAM] Office  
Lima

ICAO  
Headquarters  
Montréal

Western and  
Central African  
[WACAF] Office  
Dakar

European and  
North Atlantic  
[EUR/NAT] Office  
Paris

Middle East  
[MID] Office  
Cairo

Eastern and  
Southern African  
[ESAF] Office  
Nairobi

Asia and Pacific  
[APAC] Sub-office  
Beijing

Asia and Pacific  
[APAC] Office  
Bangkok



## THANK YOU



ICAO 2019

75 YEARS OF CONNECTING THE WORLD

الإيكاو ٢٠١٩

٧٥ عاماً  
من الربط بين أرجاء العالم