ACE NETWORK

Intercity Data Flow

- Adatgyűjtés és elemzés a terepről valós időben üzemeltetési és biztonsági célból.

Huszár Balázs
Senior IT Security Consultant
Ace Network Zrt.

INNOVATE TOGETHER

ICE NETWORK

OT Visibility Gap – Hol veszik el az adat?

- Zárt, legacy rendszerek (PLC, HMI, SCADA)
- Szabványok nélküli adatforrások, ipari protokollok
- Korlátozott hozzáférés – üzemidő > minden más

INNOVATE TOGETHER

ICE NETWORK

No Logs, No Alerts – Just Damage

- A vírus manipulálta a PLCket és irányította a centrifuga forgási frekvenciáját, hogy fizikai terhelést okozzon
- A HMI hibásan „OK”-t jelzett, mert a rendszer hamis adatokat mutatott vissza
- Nincs log, nincs riasztás ⇒ csak fizikai meghibásodás és üzemszünet tapasztalható

INNOVATE TOGETHER

ICE NETWORK

Understanding SIEMs

Mi is az a SIEM? - A Security Information and Event Management

Céljuk: láthatóság, összefüggések felismerése, gyors reagálás.

A Splunk nem csupán egy SIEM — egy adatplatform, amely minden típusú gépi adatot képes feldolgozni: biztonsági eseményeket, hálózati naplókat, szenzoradatokat vagy akár gyártási metrikákat is.

INNOVATE TOGETHER

ICE NETWORK

No Data Left Behind – Splunk Edge Hub

Hardveres peremhálózati eszköz, kimondottan OT környezetekhez

Közvetlen adatgyűjtés PLC-ből, szenzorokból, protokollokon keresztül (Modbus, MQTT, Syslog, REST, stb.)

Valós idejű adatfeldolgozás edge-en – még a továbbítás előtt

Biztonságos kapcsolat a Splunk központi rendszerhez (Enterprise / Cloud indexer vagy HEC)

INNOVATE TOGETHER

Splunk Edge Hub

Edge AI generates insights

Machine learning and deep learning are enabled on individual sensors to detect anomalies and other patterns at the edge - without sending data to the cloud.

Light · Vibration · Temperature · Humidity · Gyroscope · Pressure · Sound · Air Quality

Industrial protocols boost robustness

Natively supports MQTT, SNMP, ModBus and OPC UA protocols. Features an IP66 rating for durability.

OPC UA · MQTT · SNMP · Modbus

Connectivity keeps you in the know

Options include Power over Ethernet or Wifi 2.4/5ghz, LTE Cellular connectivity, and Bluetooth. Accessible through Splunk Connected Experiences including mobile, AR and TV.

Wifi · GPS · Cat M1

The **Splunk Edge Hub** enables expansion

Splunk Edge Hub containers

- Jelenleg elérhető:
  - Splunk UF
  - Litmus.IO
  - Node-Red
- Nemsokára elérhető:
  - Cyber Vision
  - Zeek
  - ThousandEyes
- Splunk Edge Hub SDK – Custom content

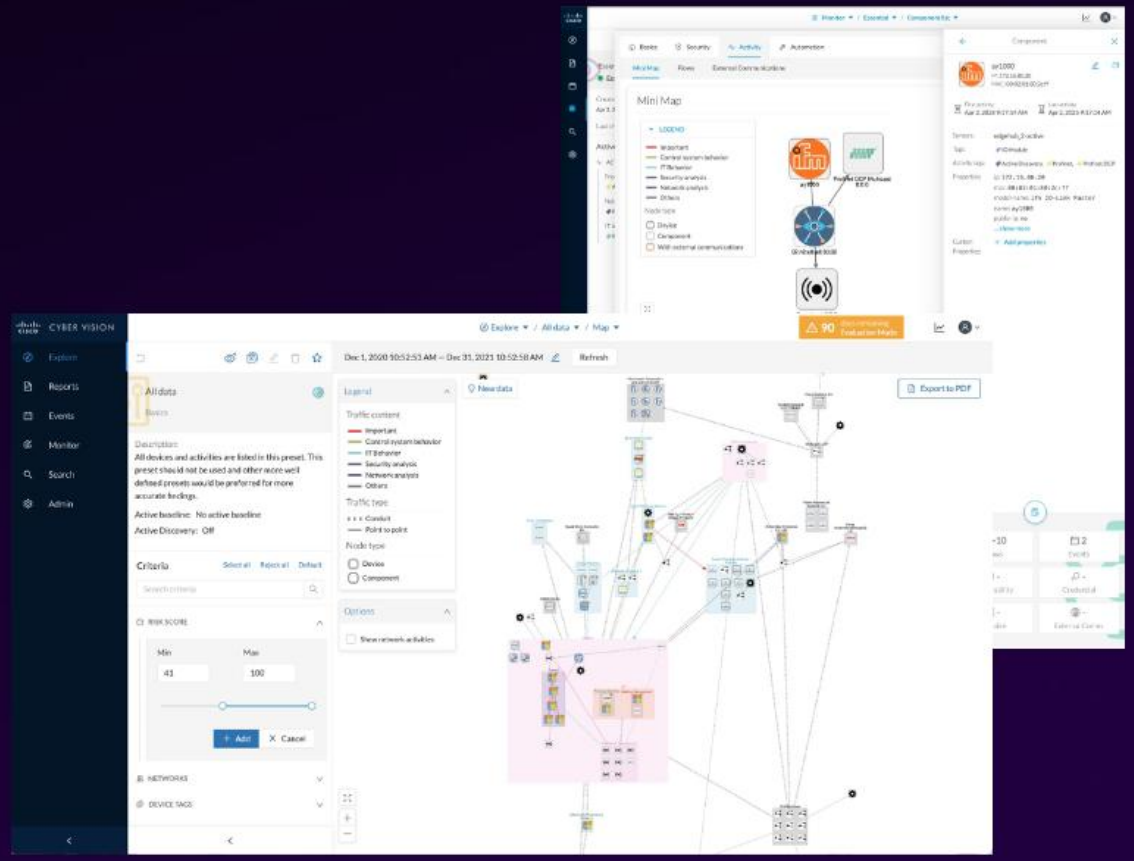
Cyber Vision Container

Splunk Edge Hub

A Cisco Cyber Vision container is available for the collection of OT security and vulnerability data sources on the edge.

Functionality:

- Dynamic asset inventory
- Passive and active discovery
- Vulnerability detection
- Risk scoring
- Splunk ES integration



Uses-cases:

- OT Security

  Cisco® Cyber Vision enables organizations to ensure the continuity, resilience, and safety of their industrial operations by providing continuous visibility into their Industrial Control Systems (ICS) to understand their security posture, improve their industrial networks efficiency, and extend IT security to their industrial operations.

Good to know:

- **Requires Cisco Cyber Vision license**
- **Data ingest via Add-on app**

Universal Forwarder Container

Splunk Edge Hub

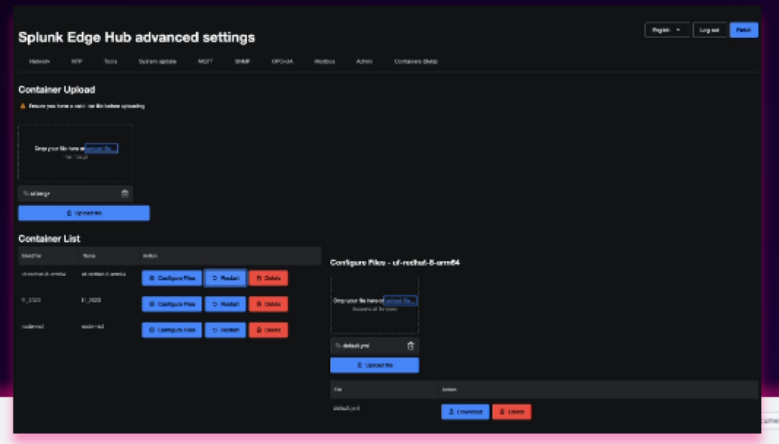
A Splunk Universal forwarder container is available for the collection of more traditional IT data sources on the edge.

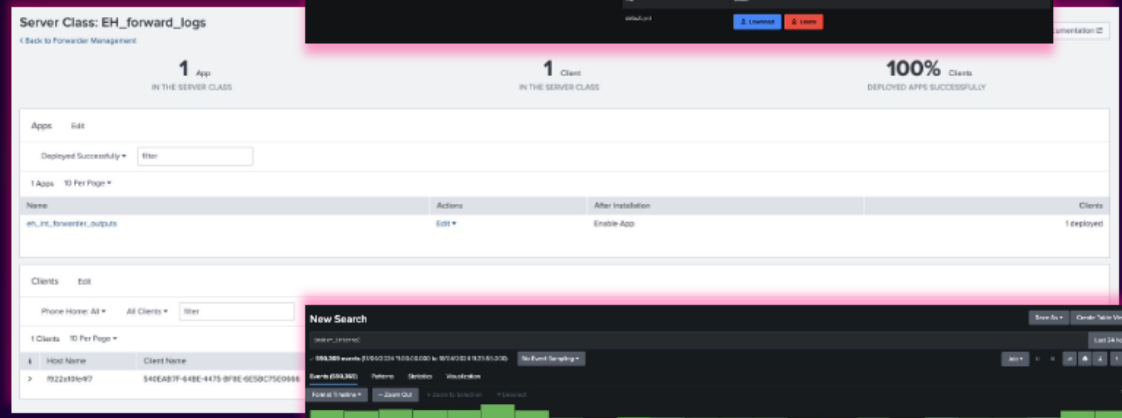
Functionality:

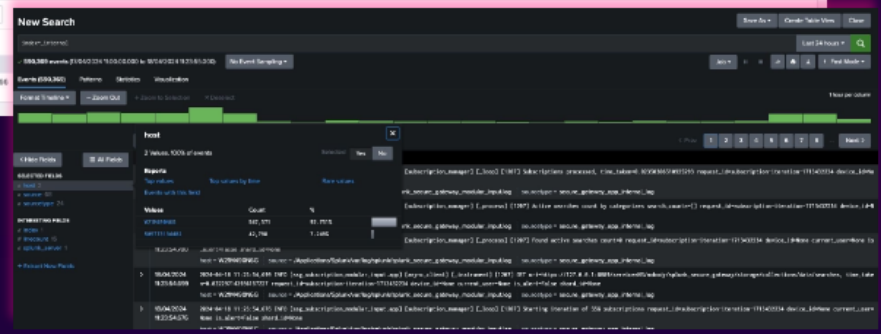
- Log collection via HEC port or TCP/UDP ports
- Act as an Intermediate forwarder via traditional S2S.
- Centralized Deployment Server
- Local container configuration via yaml upload (inputs, outputs, ports.)

Uses-cases:

- OT Security
  HMI monitoring - HMI's traditionally run older Windows versions and are very vulnerable due to a lack of patching. UF's on the HMI's can collect security logs to the Edge Hub UF as a extraction point.
  Network logs - O.T. network events can be collected from the local network and forwarded on to Splunk.
- OT Systems
  System logs from operational systems can be collected and forwarded. This allows for operational monitoring of control systems. etc.







Good to know:

- **Scalability limits (Not an IT data syslog replacement)**
- **Allows single device egress point of OT network**

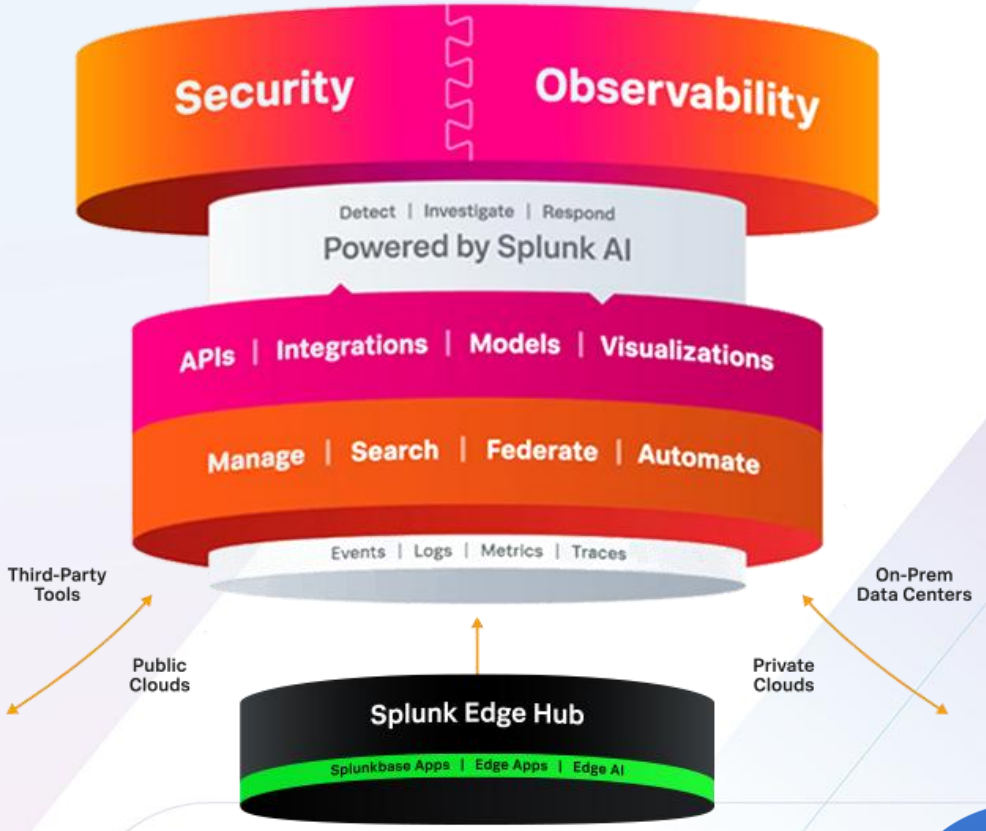
Beyond Logs – Adatból tudás

- Az Edge Hub adatai valós időben elérhetők a Splunkban
- Erős vizualizáció – interaktív dashboardokkal (pl. App for Industrial IoT)

- Automatikus korrelációk, outlier detection, prediktív elemzések

- Karbantartási, termelési és biztonsági szempontokat is lefed

- Mindez egy felületen, közös kontextusban



Factory Manufacturing Process

Download Display 98% Actions Edit

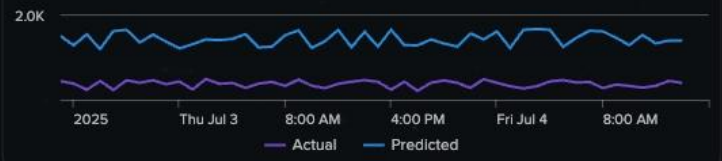
FACTORY STEPS 4 & 5 - BODY ASSEMBLY & TRIM AND GLASS

Overall Equipment Effectiveness (OEE) Metrics

OEE	Availability	Performance	Quality
72% ↓-10%	71% 0%	92% ↓-12%	96% ↑19%

Models Produced (Today)

5,465 ↓-40%



Business Operations Metrics

Unit: F | Edge Hub: JJ DVT Lab Wall

Energy	Production Cost	Operational Risk
1,456kWh ↑1%	$24,842 ↓-1%	12 ↓-68%

Body Assembly

Network Health 70%

Execution Rate

Overall Productivity Across Shifts Today

Body Assembly and Trim and Glass Systems

Shift 1	Shift 2	Shift 3
100%	70%	60%

Trim and Glass

Network Health 70%

Execution Rate

Body Assembly Detail

OEE 84%

INCIDENT REPORTS

ID	Device	Severity	Date
FM-2327	Welding Tool #1	High	2025-07-03

TEMP — Intake 89° Exhaust 89°

CO2 88ppm

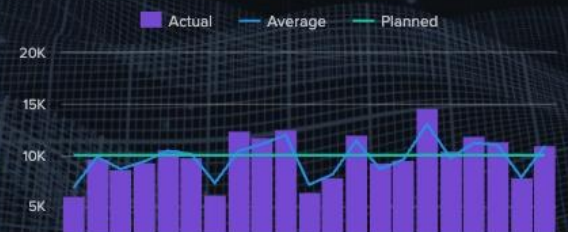
VIBRATION

VOC 87ppm

PRESSURE 938psi

IAQ 70IAQ

Production Planning (Last 10 Days)



Trim and Glass Detail

OEE 84%

INCIDENT REPORTS

ID	Device	Severity	Date
FM-2327	Paint Tool #2	Low	2025-07-03

TEMP — Intake 109° Exhaust 82°

CO2 80ppm

VIBRATION

VOC 83ppm

PRESSURE 938psi

IAQ 87IAQ

Welding booth - Station 1

FACTORY ANALYTICS - BODY ASSEMBLY

Edge Hub

SplunkEdgeHub-11a8

Data points analysed

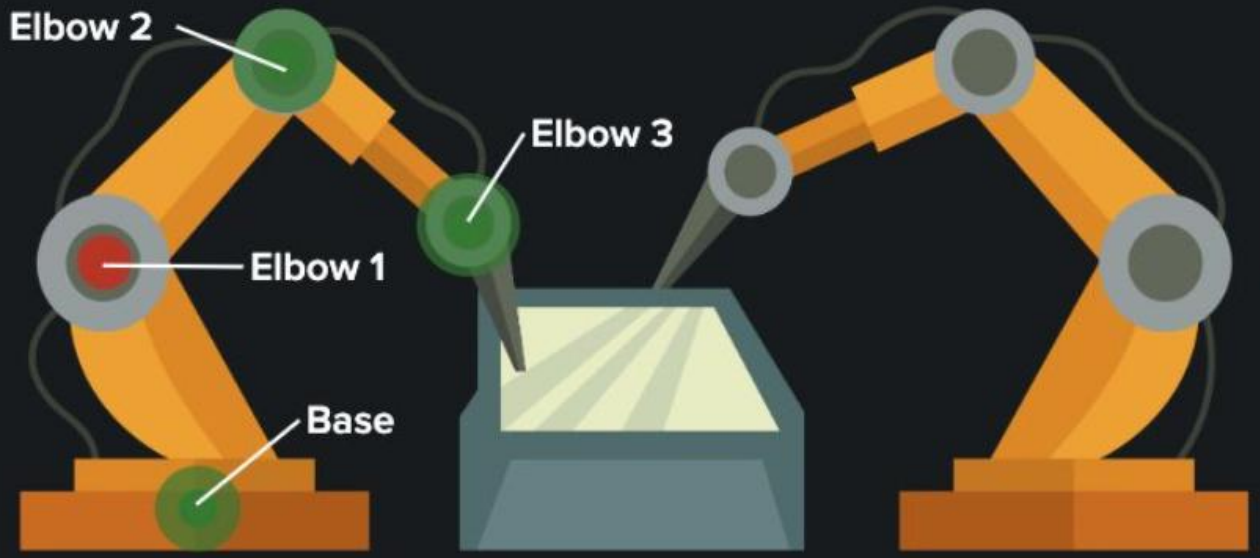
374

Vibration errors

3

Elbow 1 vibration anomaly detected

Elbow 1 vibration anomaly detected	16:57:20
Elbow 1 vibration anomaly detected	16:58:20
Elbow 1 vibration anomaly detected	16:58:30



CONSUMABLES

Contact tip		Welding wire	Welding gas	Cleaning Station
Temperature	Quality	Level	Level	Up time
872	82%	41%	95%	95%

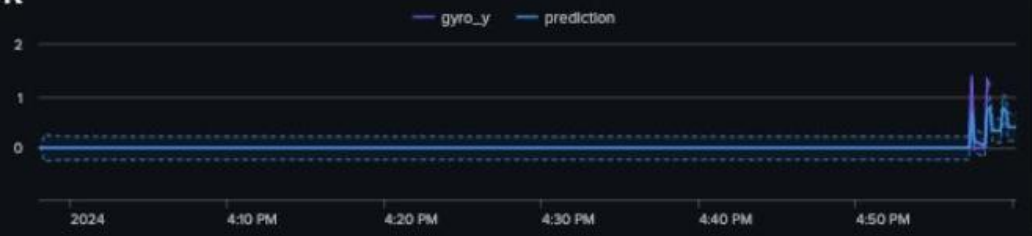
BASE MOTOR

Vibration level

0.0

Vibration trend

+1



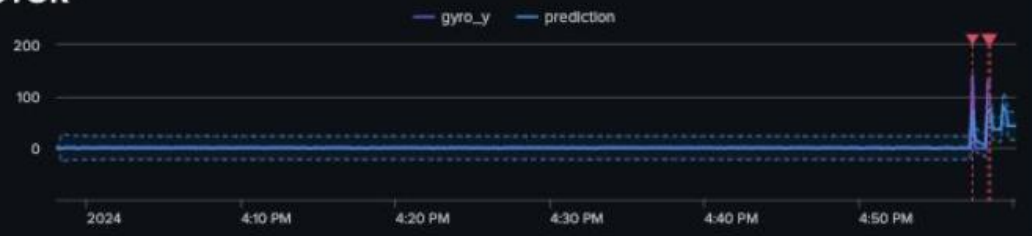
ELBOW 1 MOTOR

Vibration level

143.0

Vibration trend

+81



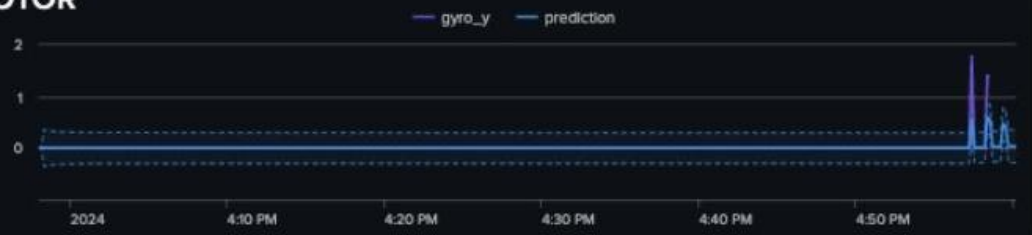
ELBOW 2 MOTOR

Vibration level

0.0

Vibration trend

+1



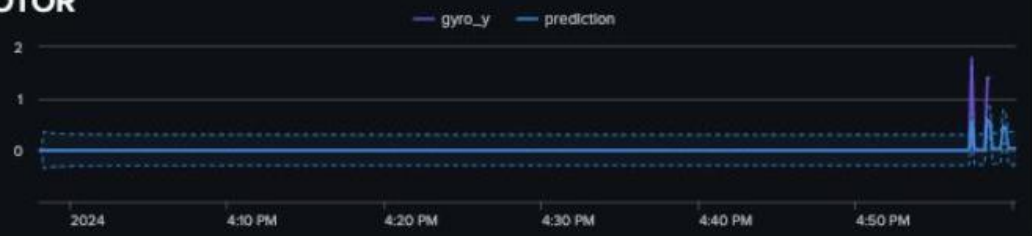
ELBOW 3 MOTOR

Vibration level

1.8

Vibration trend

+1



Datacenter Sensors

Global Time Range

Last 24 hours

Datacenter Sensors

Power Utilization

1,779 ↓ -56%

Water Capacity

44 ↓ -60%

Room Temperature

42° ↓ -79

Server Room Heatmap

Power Usage

Anomalies Detected

System	Rack	Devices	Value
Power	2	PDU-02	3400
Power	2	PDU-07	2375
Power	2	PDU-12	2245

Host	Priority	Rack	Row
mysql-02	High	2	A
storage_websever-02	Medium	2	A
storage_exchange-03	High	2	C
db-01	Critical	2	A
websphere-01	Medium	2	A

< Prev 1 2 Next >

Parc des Nations
CURRENT CROWD LEVELS

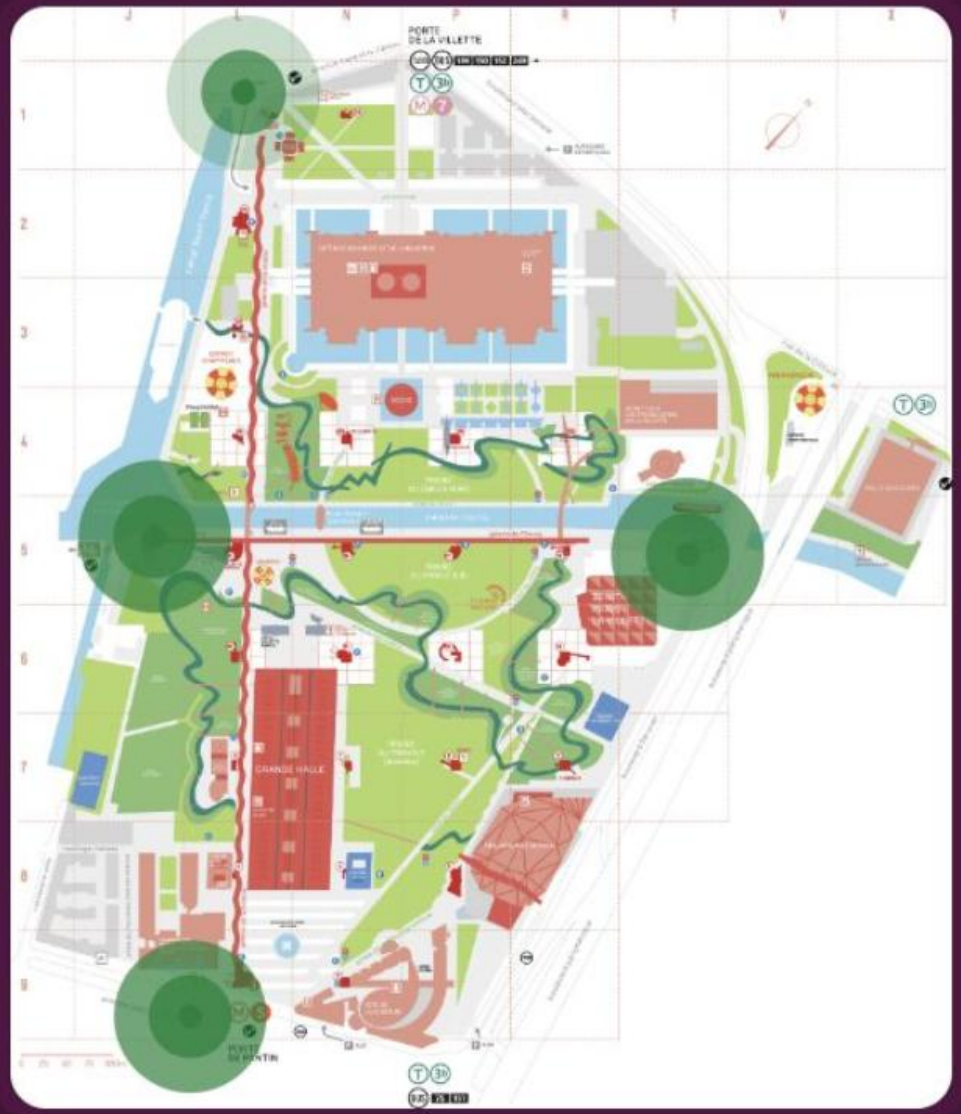
ESTIMATED OCCUPANCY

3,465 ↑22

TEMPERATURE	HUMIDITY	DESCRIPTION
13C 0	90% 0	broken clouds

METRO ARRIVALS

Station	Direction	Arrival time
Corentin-Cariou	Mairie d'Ivry • Villejuif - Louis Aragon	09:30:06
Porte de la Villette	Mairie d'Ivry • Villejuif - Louis Aragon	09:26:20
Delphine Seyrig	Porte Dauphine (Avenue Foch)	09:21:49
Porte de Pantin - Parc de la Villette	Porte Dauphine (Avenue Foch)	09:21:02



NORTH ENTRANCE
CONGESTION (People per min)

0 0

WEST ENTRANCE
CONGESTION (People per min)

14 ↑14

EAST ENTRANCE
CONGESTION (People per min)

2 ↓-11

SOUTH ENTRANCE
CONGESTION (People per min)

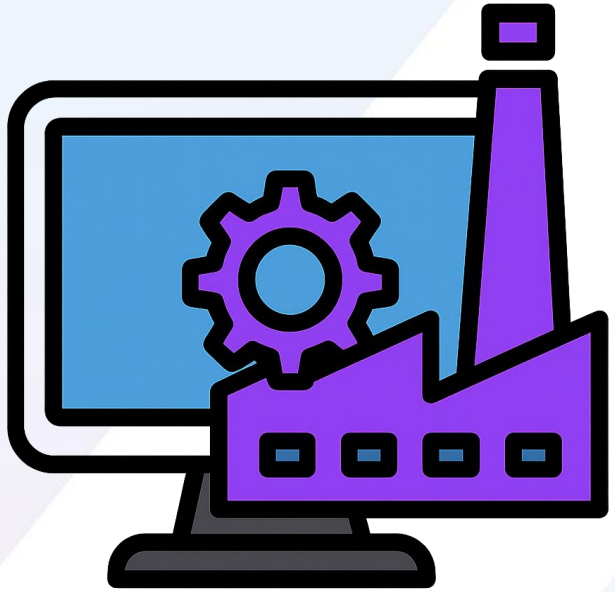
6 ↑6


Ctrl + F1
.conf
cisco
AI-driven industr
manufacturing
Industrial IoT

ICE NETWORK

One Platform, Two Worlds – IT és OT konvergencia

- Splunk egyedülállóan alkalmas IT és OT adatok integrálására
- Ugyanabban a környezetben:
  - gyártási adatok,
  - felhasználói viselkedés,
  - biztonsági események,
  - üzemeltetési naplók
- Konvergencia = gyorsabb válaszidő, hatékonyabb üzemeltetés, jobb biztonság



INNOVATE TOGETHER

ACE NETWORK

ACE Network Zrt.

huszar.balazs@acenetwork.hu

Tel.: +36 20 801 4000