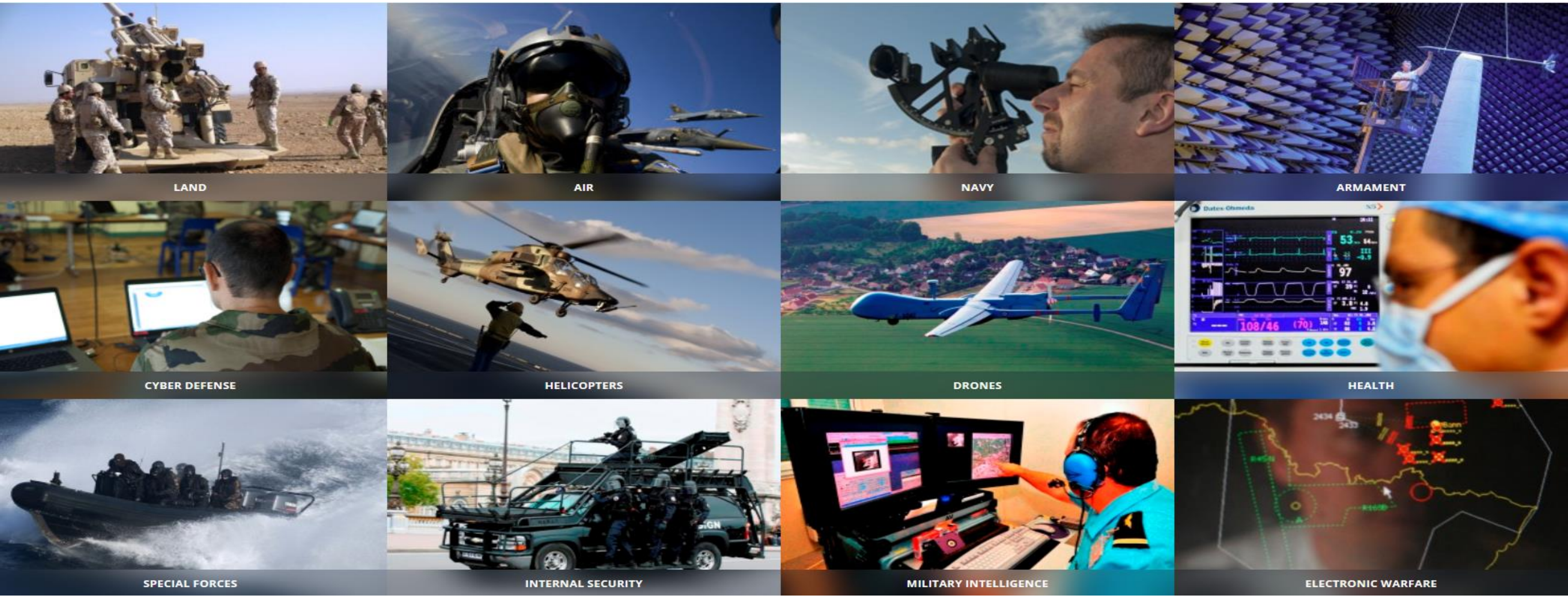
DCI MISSIONS

- Transferring the French Armed Forces know-how

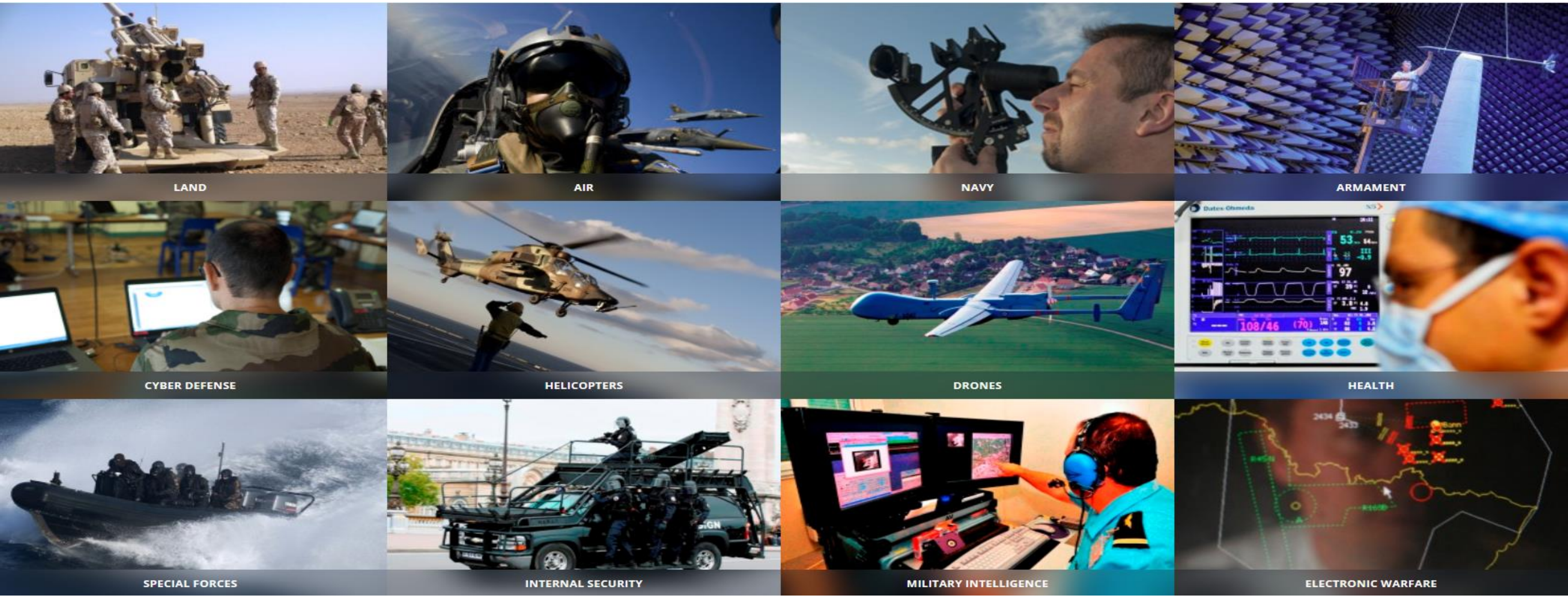


- Cyberdefence department 2013. Over 1,000 employees located in France, Middle East, Asia and South America

TRAININGS AND EXERCISES

HOW TO FOSTER CYBER-DETECTION ?

FEEDBACKS FROM 3 TRAININGS AND RELATED MEANS



CAPABILITIES ASSESSMENTS : compliance, governance & operational

CYBERDEFENSE CAPABILITIES HAVE TO BE ASSESSED in 3 LEVELS : COMPLIANCE, GOVERNANCE AND OPERATIONAL

Assessment Level

SOLUTIONS 1

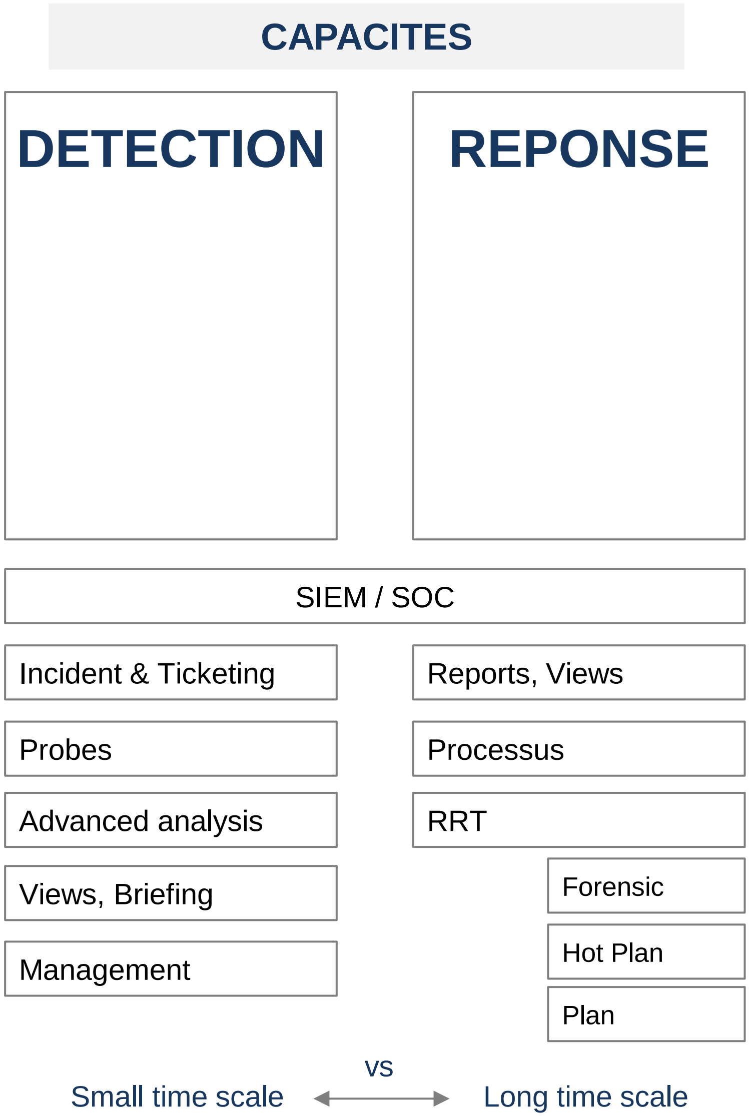
Compliance assessment with iso 2700n
Organization, Process, Procedures,
Risk evaluation and protection

GOVERNANCE 2

Assessment of organization, process and solutions implemented.
Consistency, overlap, synergy through Role playing, simulation.
Technical level not played

OPERATIONAL 3

Full assessment of the entire capability through exercise in realistic environment (events, staff, tools, view, etc.)



CAPACITES

DETECTION

REPONSE

SIEM / SOC

Incident & Ticketing

Probes

Advanced analysis

Views, Briefing

Management

Reports, Views

Processus

RRT

Forensic

Hot Plan

Plan

Small time scale vs Long time scale

Assessment Level

1 SOLUTIONS

Compliance assessment with doctrine, ISO for crisis, internal procedures.
Organization, Process, Procedures,
External relations

2 GOVERNANCE

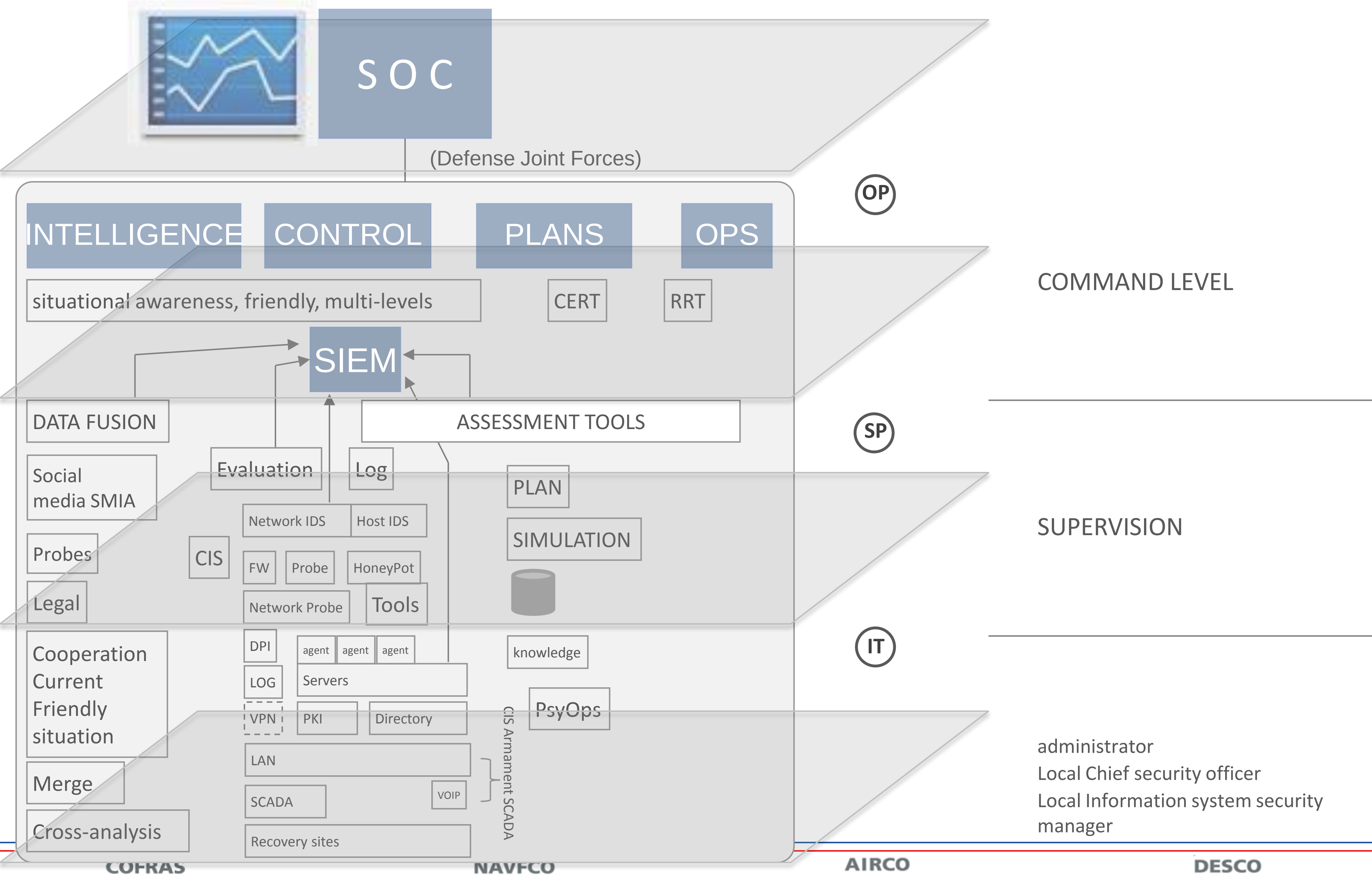
Assessment of organization, process and implemented procedures. Assessment of the consistency, synergy, with a large panel of key attendees (top executive & decision-makers) through Role Playing, Table Top game, serious, games, simulation. *Technical level not played*

3 OPERATIONAL

Full assessment of the entire capability through exercise in realistic environment (events, staff, tools, view, etc.)

Cyberdefence > MULTIDIMENTION

A SOC for Active Cyberdefense, cyberLab as a resource for evaluation, training, research, benchtest, complex use cases, options evaluation for plans, etc.



SOC

(Defense Joint Forces)

INTELLIGENCE

CONTROL

PLANS

OPS

situational awareness, friendly, multi-levels

CERT

RRT

SIEM

DATA FUSION

ASSESSMENT TOOLS

Social media SMIA

Evaluation

Log

PLAN

Network IDS

Host IDS

SIMULATION

Probes

CIS

FW

Probe

HoneyPot

Legal

Network Probe

Tools

DPI

agent

agent

agent

knowledge

Cooperation Current Friendly situation

LOG

Servers

PsyOps

VPN

PKI

Directory

LAN

CIS Armament SCADA

Merge

SCADA

VOIP

Cross-analysis

Recovery sites

OP

COMMAND LEVEL

SP

SUPERVISION

IT

administrator

Local Chief security officer

Local Information system security manager

Organization & processes

Functions held in the Chain of Command and Capability Resources

JFC

CYBERCOMMAND

J1 — HR

J2 — Intelligence

- Drives data collect from various sensors, databases, CIS, and other sources.
- Conduct further data collection for complementary information
- Cross-Analysis

J3 — Current OPERATION

- Collect technical reports
- Collaborate with Plan/J5
- Conduct operations (diagnosis, analysis, crisis tasks such hot plan, etc.)

J4 — Logistic

J5 — PLAN

- Leverages surveillance awareness and survey to develop long and short-term plans, tailored strategy, courses of action, and shape execution of Offensive, Defensive Cyberspace Operations.
- Cast information to authorities

J6 — CIS

- Provide all the necessary technical tools and environment.
- Platform, applications servers, links, secured networks, workshop platforms for evaluations, analysis, etc.

J3

Cyber Prevention

- Running cold plan
- Using local resources (HR & tech)

Cyber Detection

- Picture
- SIEM / Supervisor

Cyber Response

- Running response operations

J5

Cyber Prevention

- Design Cold plan
- Schedule Local Resources (HR & tech)

Cyber Detection

- Diagnosis Design
- Views performance

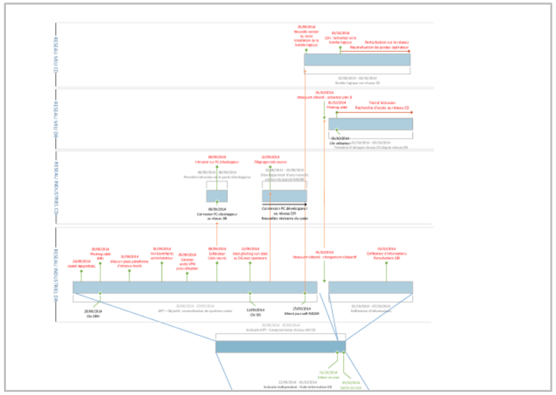
Cyber Response

- Plan design: forensic, RRT task

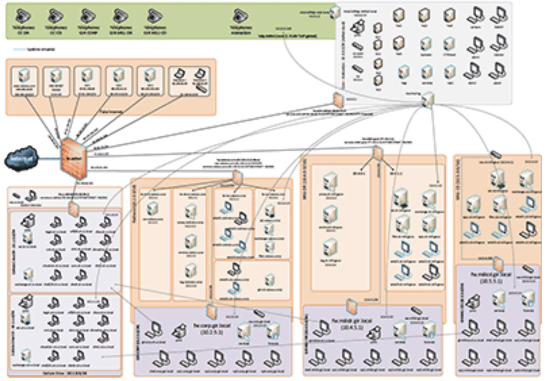
CYBERLAB : Comprehensive environment : technical & scenario

Comprehensive target architecture : servers, active network components, settings, failures, flaw, fake events

SCENARIO



ARCHITECTURE



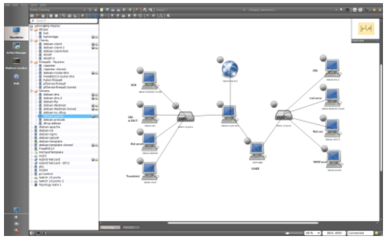
DOCUMENTS

ANIMATION TRAINING

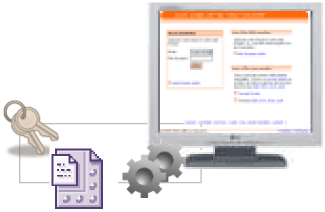
Direx

EQUIPEMENTS

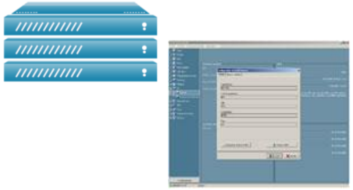
FRAMEWORK



SETTINGS



COMPONENTS



Virtual machines & Hybrid (scada)

TRAINING

administrator

TRAINING PLATFORM ARCHITECTURE

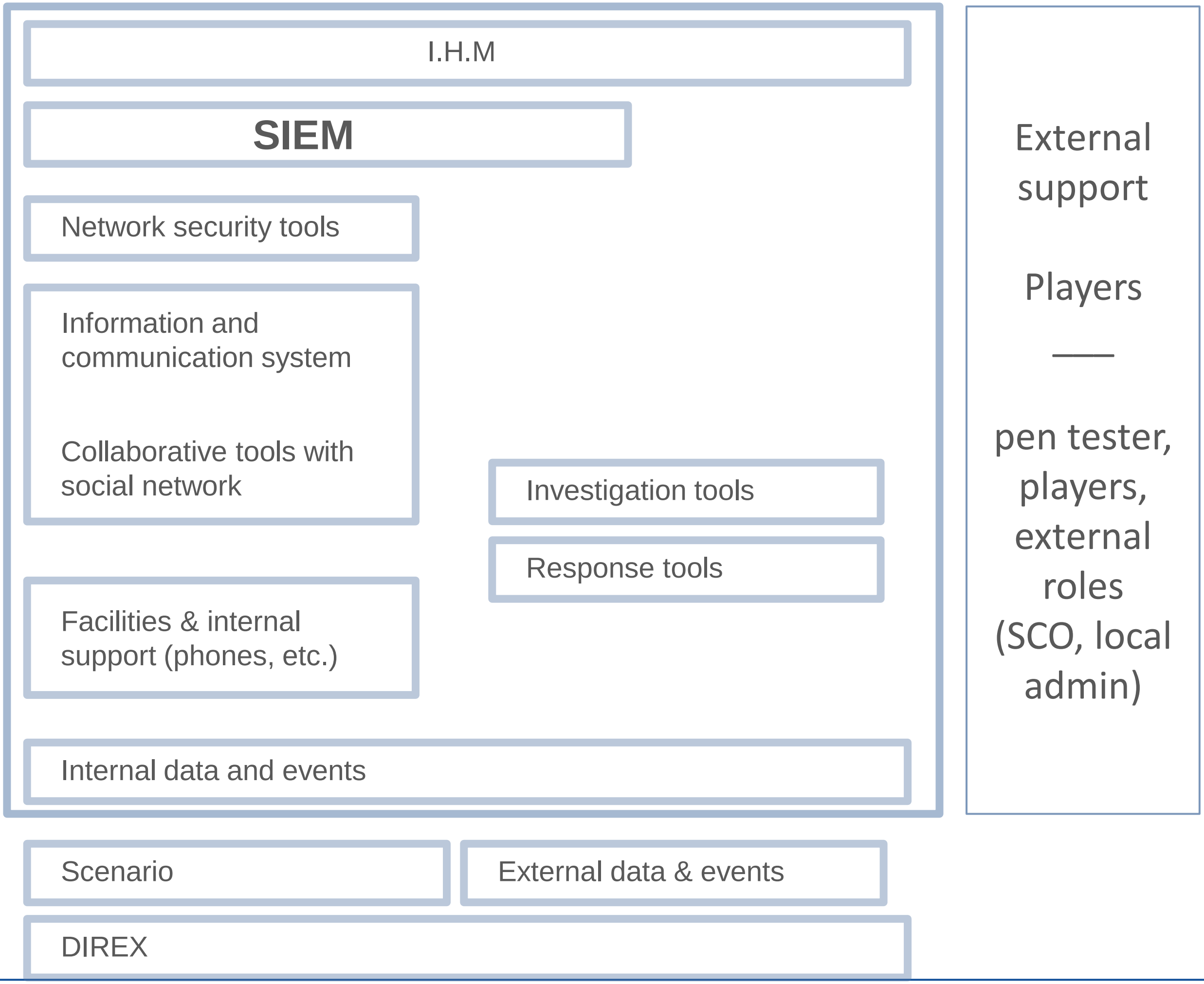
Main platform components and external resources

EXERCISE MEANS > OVERALL ARCHITECTURE > TO CONFIGURE FOR EACH SCENARIO

Technical support

Infrastructure Hosting

Intel, cooperation



I.H.M

SIEM

Network security tools

Information and communication system

Collaborative tools with social network

Investigation tools

Response tools

Facilities & internal support (phones, etc.)

Internal data and events

Scenario

External data & events

DIREX

External support

Players

pen tester, players, external roles (SCO, local admin)

PLATFORM #1

COMPLEXITY OF THE ORGANIZATION + BRIDGING ISSUE

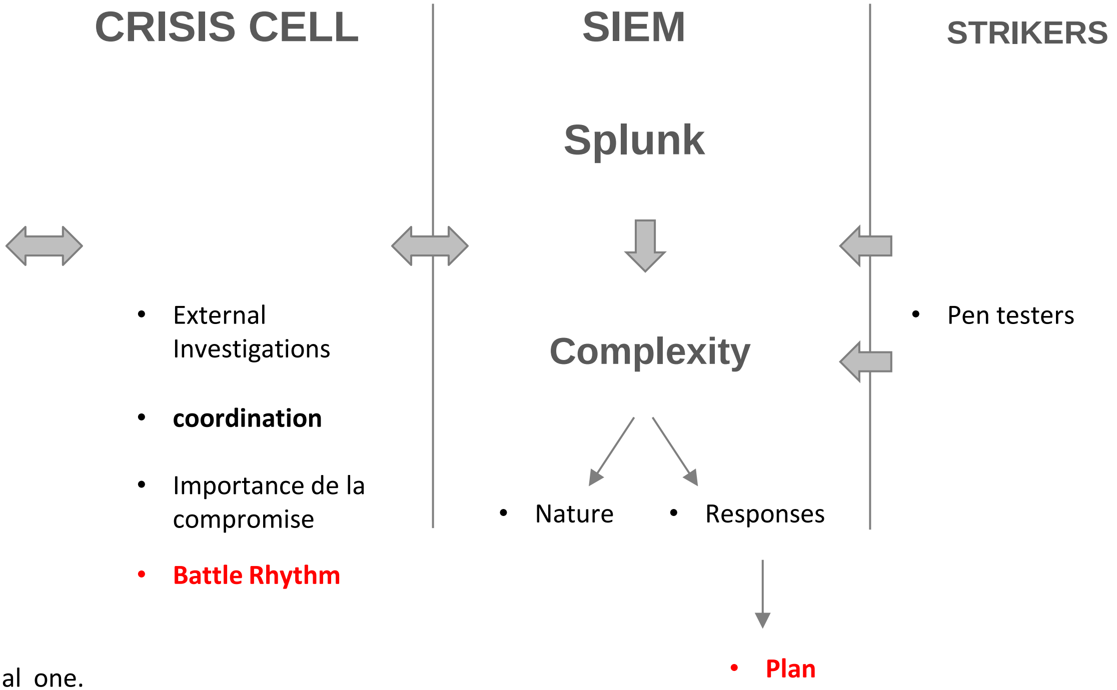
DETECTION > EXTERNAL (internet) AND INTERNAL (ioc)

CASE #1

SUB CONTRACTOR WORKING FOR MoD

EMAIL : MALWARE WITHIN THE ATTACHED FILE

CLASSIFIED FILE FOUND ON INTERNET



CRISIS CELL

- External Investigations
- **coordination**
- Importance de la compromise
- **Battle Rhythm**

SIEM

Splunk

Complexity

- Nature
- Responses

- **Plan**

STRIKERS

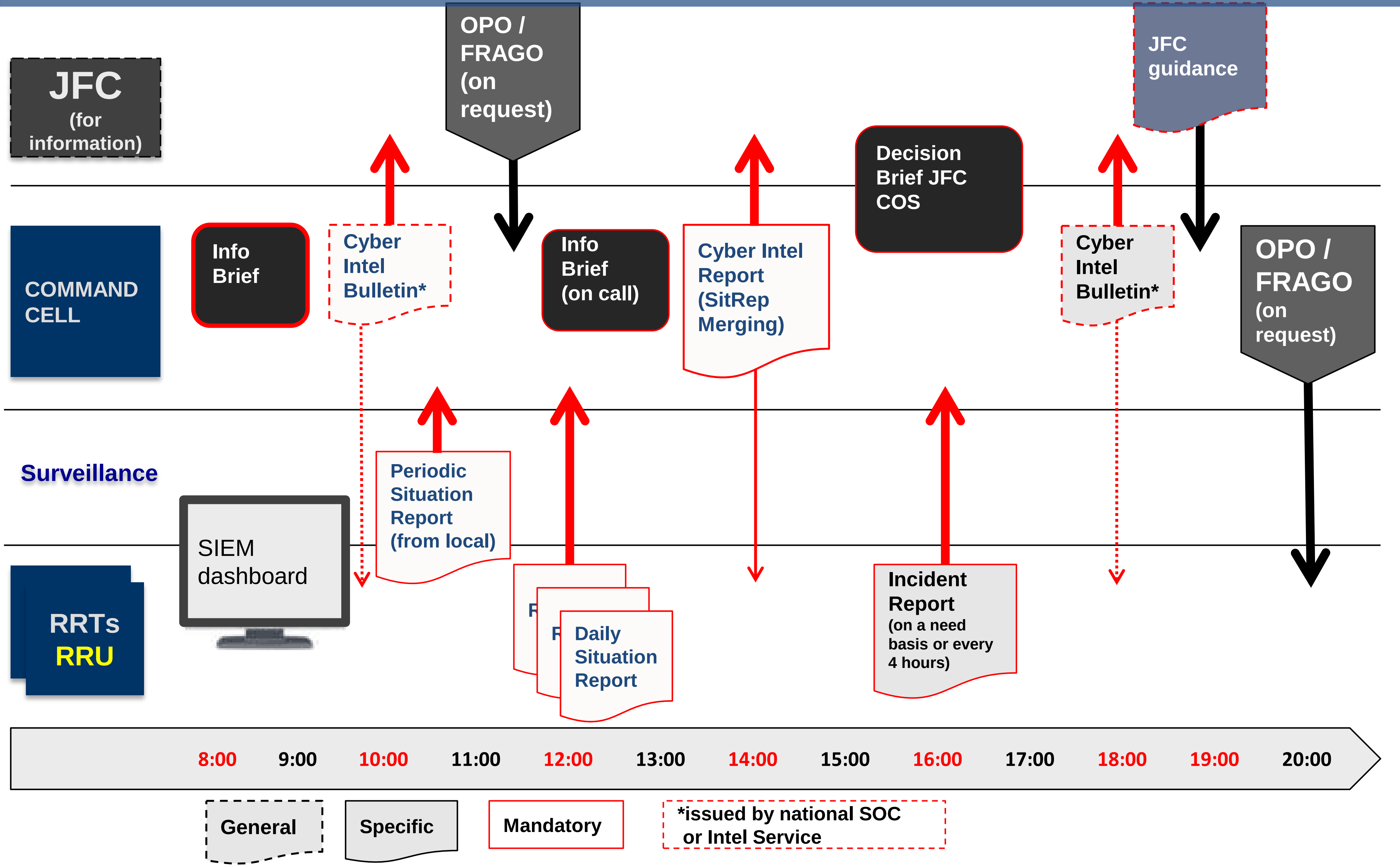
- Pen testers

DIFFICULTIES

Players are facing 2 ways of detection: external one and internal one. Further more, the additional external conditions (attacks from pen testers) make process more difficult

BATTLE RHYTHM: simulation of 1 day representative

Typical day sequence played in exercise, different battle rhythm to converge



JFC (for information)

COMMAND CELL

Surveillance

RRTs RRU

OPO / FRAGO (on request)

JFC guidance

Info Brief

Cyber Intel Bulletin*

Info Brief (on call)

Cyber Intel Report (SitRep Merging)

Decision Brief JFC COS

Cyber Intel Bulletin*

OPO / FRAGO (on request)

Periodic Situation Report (from local)

SIEM dashboard

Daily Situation Report

Incident Report (on a need basis or every 4 hours)

8:00 9:00 10:00 11:00 12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 20:00

General

Specific

Mandatory

*issued by national SOC or Intel Service

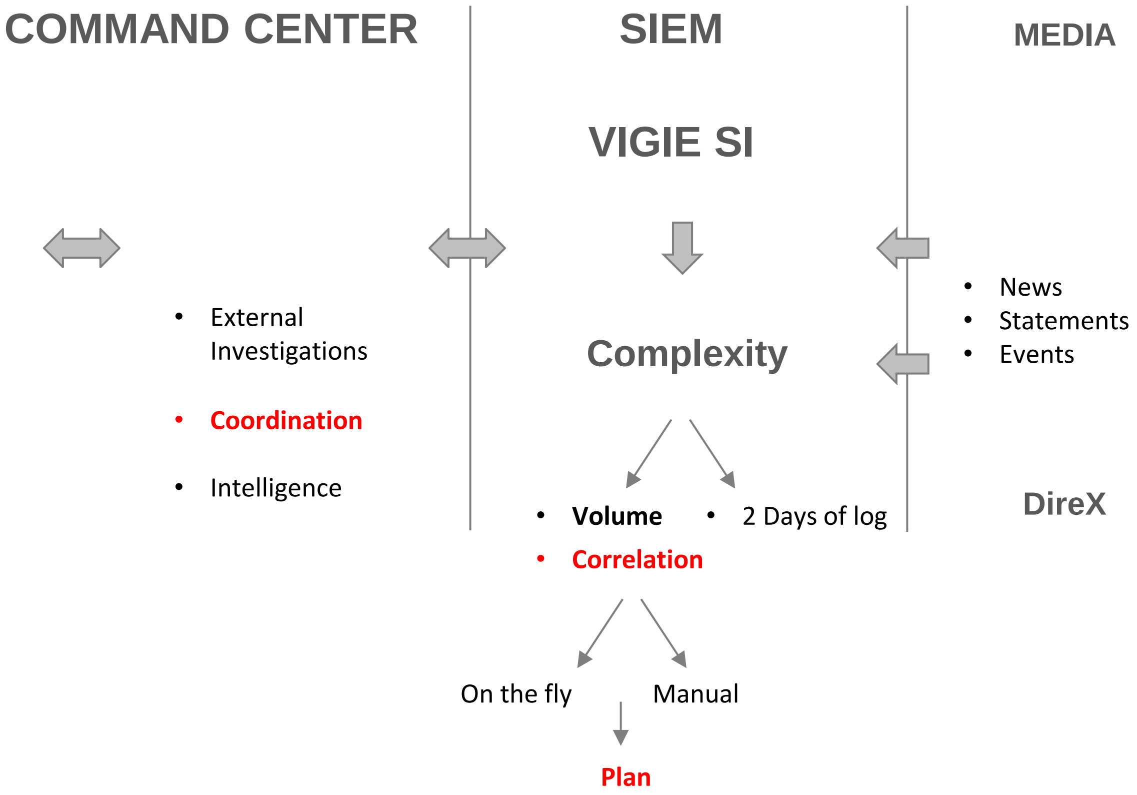
PLATFORM #2

COMPLEXITY OF THE ANALYSIS + CORRELATION

DETECTION > INTERNAL (SIEM Alerts)

CASE #2

CRITICAL INFRASTRUCTURE OPERATOR
SEVERAL ALERTS
RECONSTRUCTIONS OF EVENTS & CORRELATION



COMMAND CENTER

- External Investigations
- **Coordination**
- Intelligence

SIEM

VIGIE SI

Complexity

- **Volume**
- 2 Days of log
- **Correlation**

On the fly

Manual

Plan

MEDIA

- News
- Statements
- Events

DirEX

DIFFICULTIES

Players are facing 2 days of log data
Bridging with the command center

- Briefing, reports (infra, Biz, Strikes)
- Plan
- Operations

PLATFORM #3

COMPLEXITY OF PREVENTION, DETECTION BEFORE FAILURE (NEW SOURCE LOG AND ANALYSER)

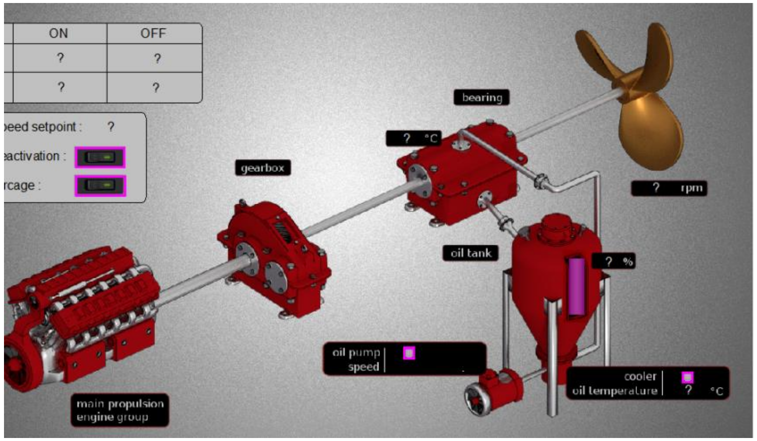
DETECTION > VISUAL (SUPERVISOR, TOOL or HUMAN- TOO LATE) OR PROBE SUPERVISOR

CASE #3

CRITICAL INFRASTRUCTURE OPERATOR

ATTACK ON THE FIRMWARE

RECONSTRUCTIONS OF EVENTS & CORRELATION



	ON	OFF
	?	?
	?	?

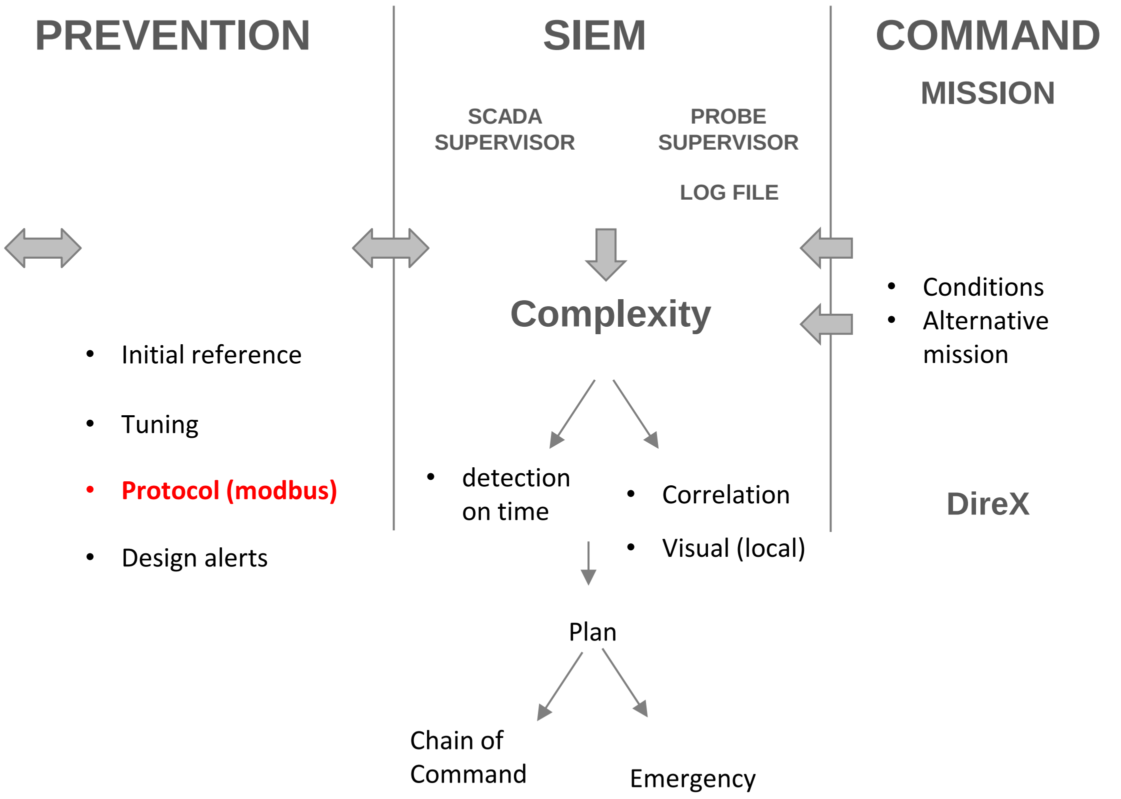
peed setpoint : ?

eactivation :

rcage :

Players are facing a failure with the oil pump and inconsistence temperature (local vs remote)

Short Loop with **extra source** (probe)



PREVENTION

- Initial reference
- Tuning
- **Protocol (modbus)**
- Design alerts

SIEM

SCADA SUPERVISOR

PROBE SUPERVISOR

LOG FILE

Complexity

- detection on time
- Correlation
- Visual (local)

Plan

Chain of Command

Emergency

COMMAND

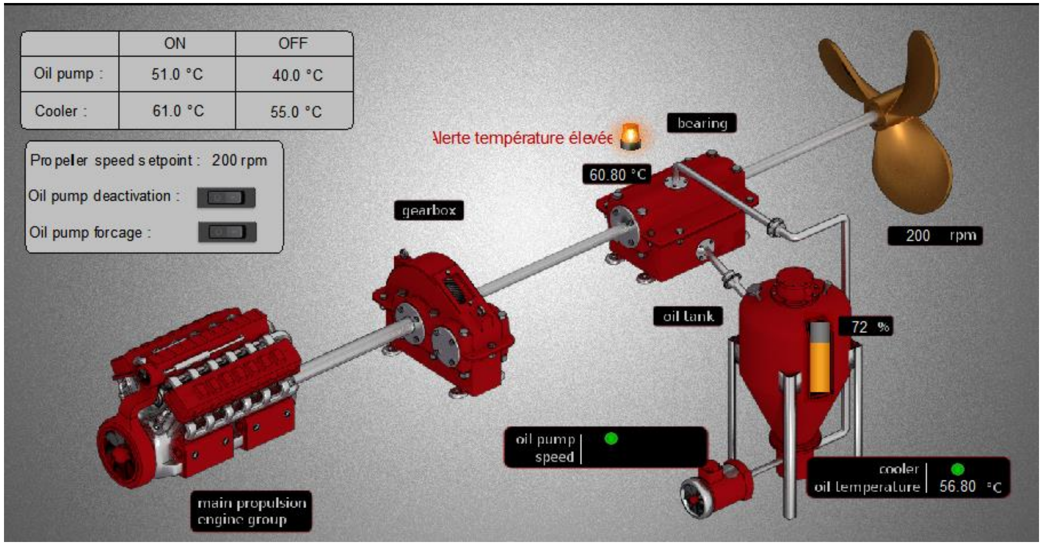
MISSION

- Conditions
- Alternative mission

DireX

DETECTION > COMPLEXITY > NEW SOURCES TO ANALYSE IN RISK MANAGEMENT

CASE #3



	ON	OFF
Oil pump :	51.0 °C	40.0 °C
Cooler :	61.0 °C	55.0 °C

Pro peler speed s etpoint : 200 rpm

Oil pump deactivation :

Oil pump forcage :

Alerte température élevée

bearing
60.80 °C
gearbox
200 rpm
oil tank
72 %
oil pump speed ●
cooler oil temperature ● 56.80 °C
main propulsion engine group

HYBRID INFORMATION :

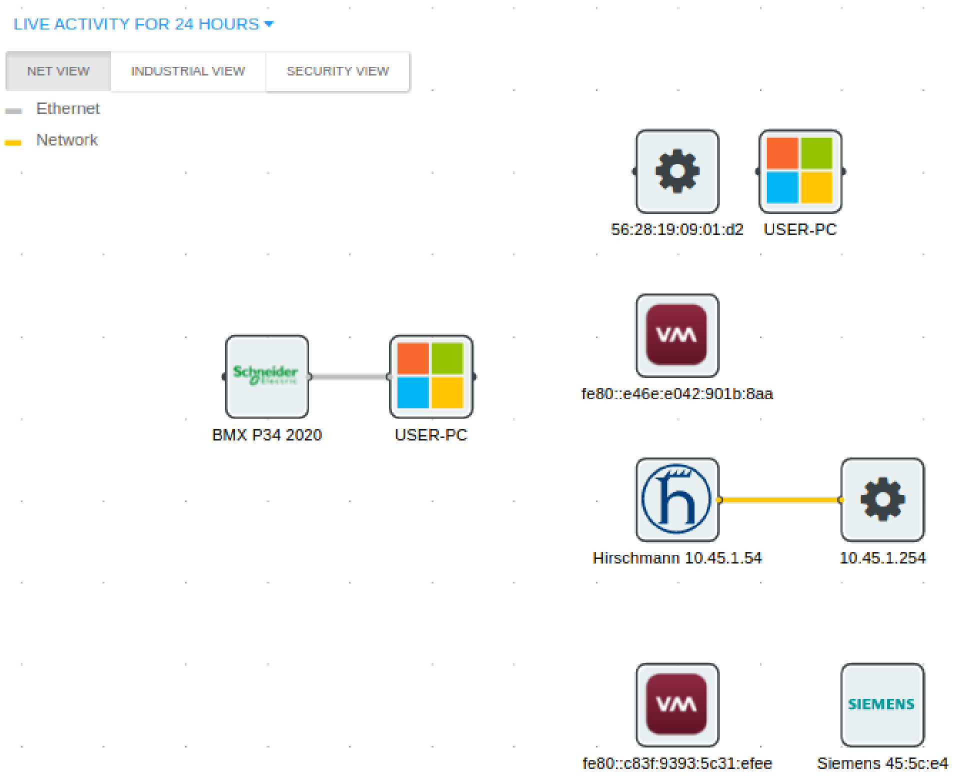
- **Temperature probe within the PLC**
- **Should the temperature be replaced by a dedicated probe**
- **How to add more information and sources ?**

PLATFORM #3

NEW IDS: DEDICATED PROBE. NEW SOURCE : LOG AND ANALYSER

DETECTION > COMPLEXITY > DISCOVERING NODES AND TRAFFIC

CASE #3



NEW IDS :

- **What's going on ?**
- **Correlation with others information**

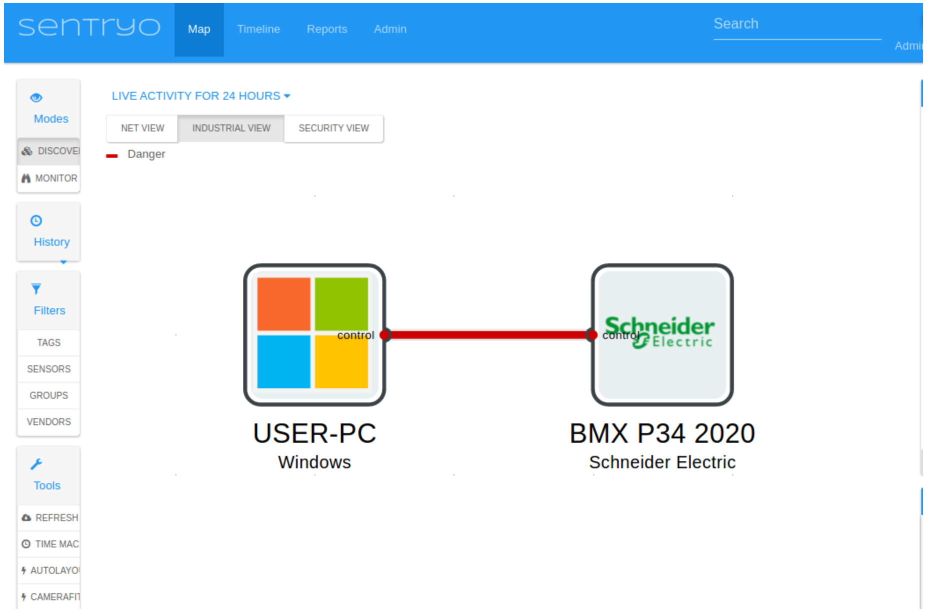
PLATFORM #3

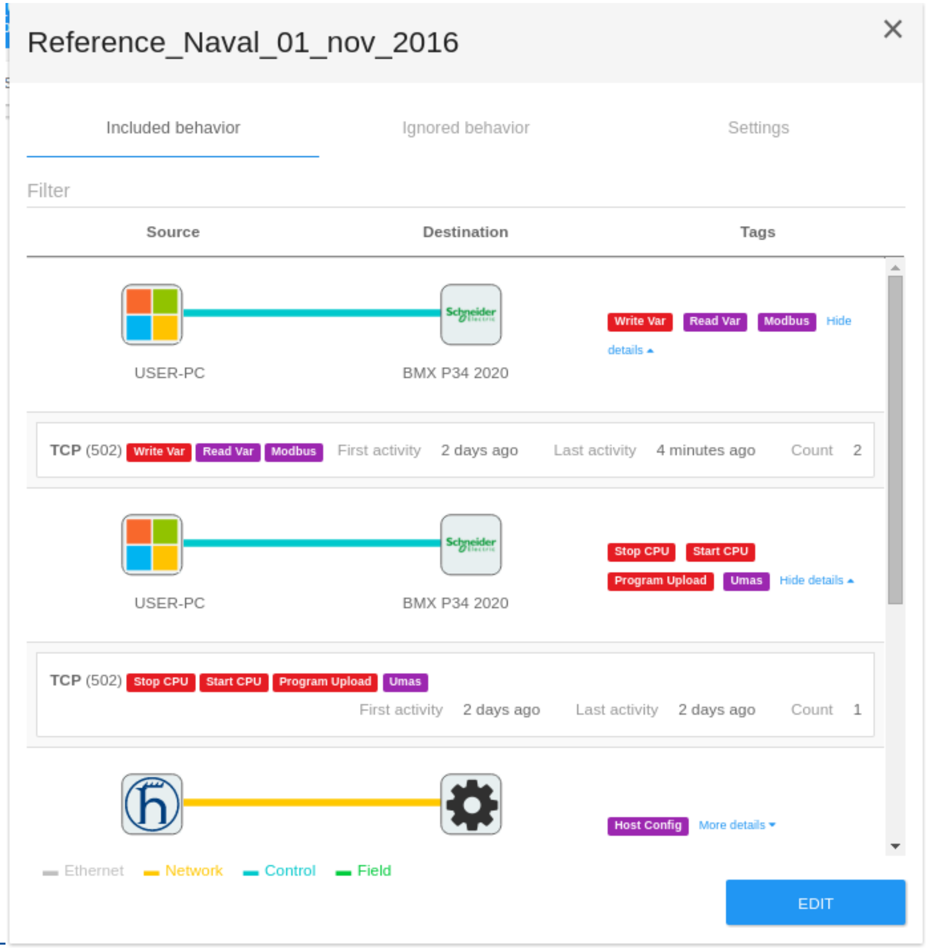
COMPLEXITY OF DETECTION. PROBE WITH REFERENCE SETTING BEFORE OPERATION,

DETECTION > COMPLEXITY IN UPSTREAM PHASE (PROBE CONFIGURATION)

CASE #3

Using a traffic reference to compare the log traffic





Reference_Naval_01_nov_2016 ×

Included behavior | Ignored behavior | Settings

Filter

Source	Destination	Tags
USER-PC	BMX P34 2020	Write Var, Read Var, Modbus, Hide details ▴

TCP (502) Write Var Read Var Modbus First activity 2 days ago Last activity 4 minutes ago Count 2

Source	Destination	Tags
USER-PC	BMX P34 2020	Stop CPU, Start CPU, Program Upload, Umas, Hide details ▴

TCP (502) Stop CPU Start CPU Program Upload Umas First activity 2 days ago Last activity 2 days ago Count 1

Source	Destination	Tags
		Host Config, More details ▾

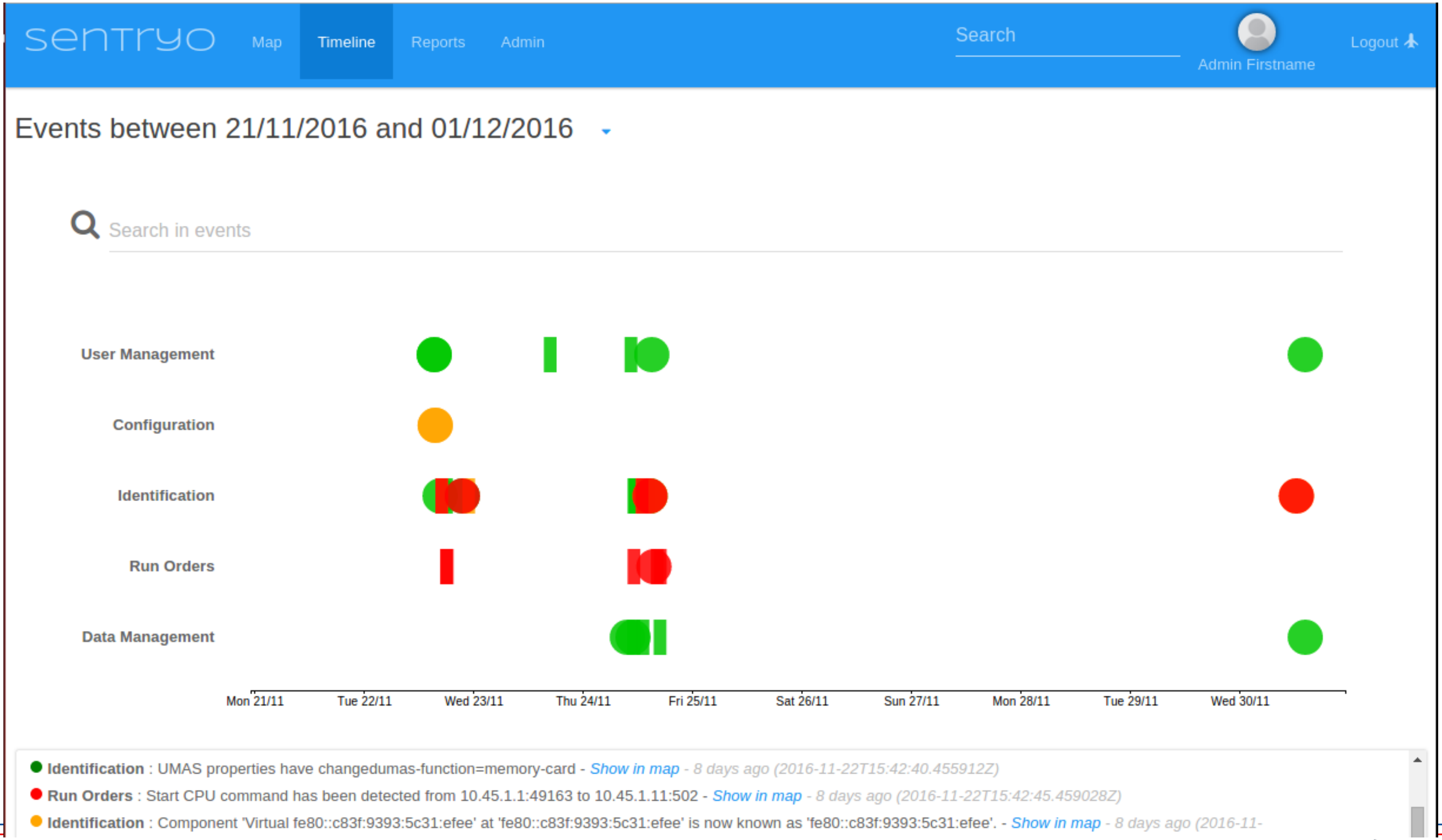
PLATFORM #3

COMPLEXITY OF PREVENTION, DETECTION BEFORE FAILURE (NEW SOURCE LOG AND ANALYSER)

DETECTION > COMPLEXITY > UNDERSTANDING THE SEQUENCE OF EVENTS

CASE #3

Reconstitution of the sequence of events



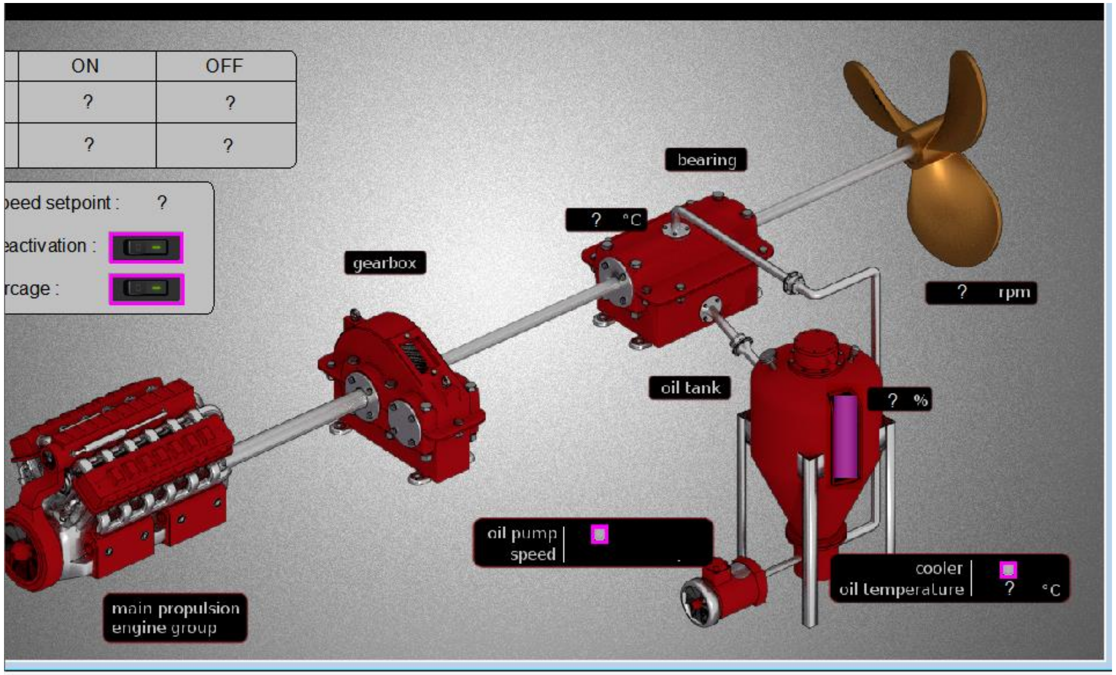
● **Identification** : UMAS properties have changedumas-function=memory-card - *Show in map - 8 days ago (2016-11-22T15:42:40.455912Z)*

● **Run Orders** : Start CPU command has been detected from 10.45.1.1:49163 to 10.45.1.11:502 - *Show in map - 8 days ago (2016-11-22T15:42:45.459028Z)*

● **Identification** : Component 'Virtual fe80::c83f:9393:5c31:efee' at 'fe80::c83f:9393:5c31:efee' is now known as 'fe80::c83f:9393:5c31:efee'. - *Show in map - 8 days ago (2016-11-*

DETECTION > COMPLEXITY IN UPSTREAM PHASE (CONFIGURATION OF THE PROBE)

CASE #3



	ON	OFF
	?	?
	?	?

peed setpoint : ?

eactivation :

rcage :

HOW TO CONFIGURE THE PROBE BEFORE THE MISSION

WHAT ARE THE COLD PLAN ?

- **Restore firmware: when, why ?**
- **Investigation to confirm diagnosis, How To ?**
  - **Comparing the “Reference” of traffic and behaviour**
  - **Correlation with other sources of information**
- **Emergency measures ?**

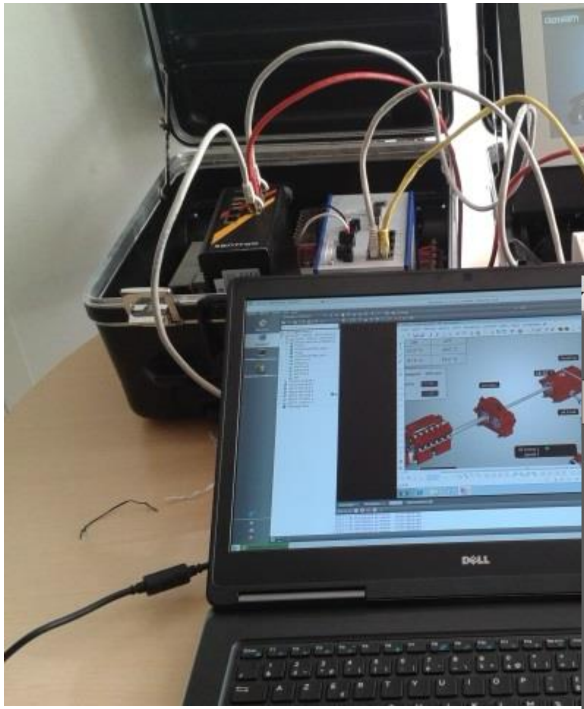
HOW TO BUILD HOT PLAN ?

- **Multiply the scenario operation conditions**

- **Enhance the Exercise with several type of scenario**
- **Investigation to confirm diagnosis, How To ?**
  - **Comparing the “Reference” of traffic and the going on/past behaviour**
  - **Correlation with other sources of information**
- **Set of emergency measures (Response sheets and forms)?**

DETECTION > DESIGN MODULAR ARCHITECTURE WITH A CYLAB

CASE #3

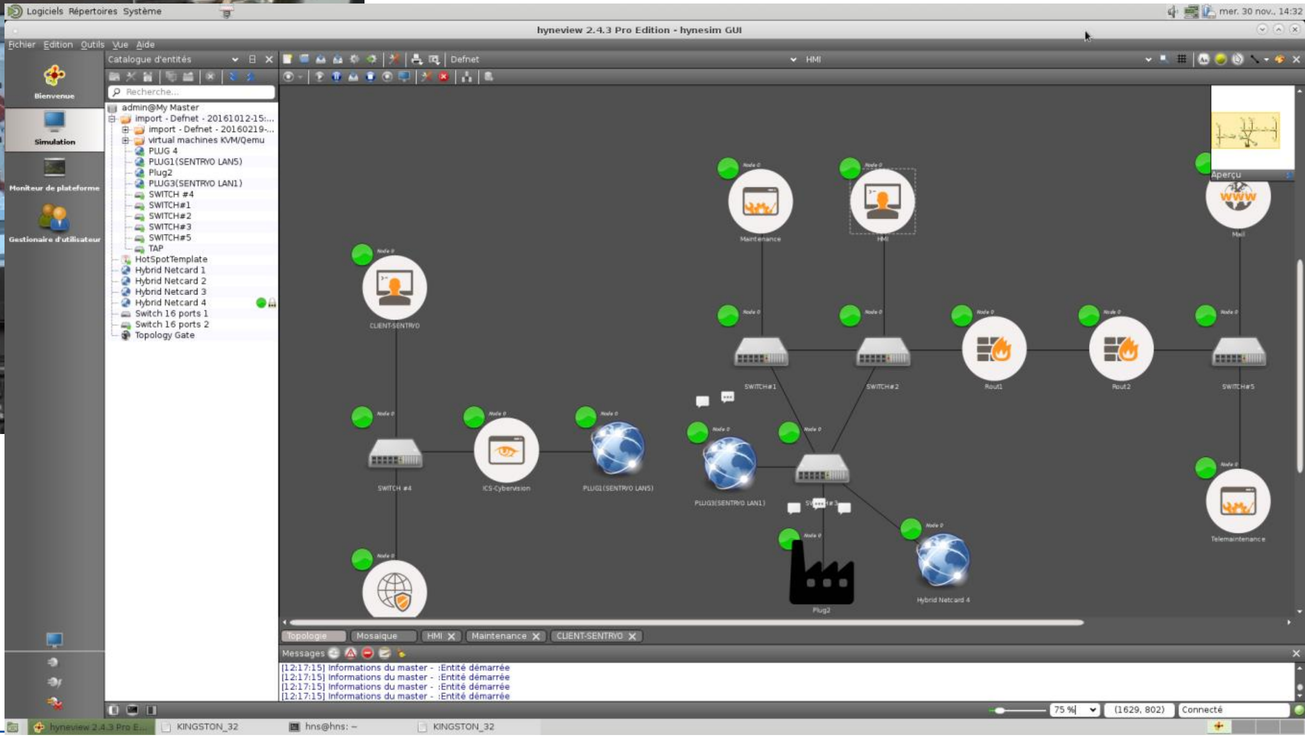


USING A CYLAB TO BUILD MORE SCENARIO

SAVE TIME

ISSUING REALISTIC CONFIGURATION CLOSE TO USERS NEEDS AND OPERATIONS (beyond open source assets)

MIXING VM and physical nodes



```
[12:17:15] Informations du master -  :Entité démarrée
[12:17:15] Informations du master -  :Entité démarrée
[12:17:15] Informations du master -  :Entité démarrée
[12:17:15] Informations du master -  :Entité démarrée
```

D C I

QUESTIONS