Risikoen med "ting"

Nils Roald
Cisco Advanced Threat Group – Northern Europe

Intelligence

Best of breed
Portfolio

Integrated
Architecture

All hackers targeting your infrastructure has one common goal..
ENDPOINTS

Why endpoints is in focus again?

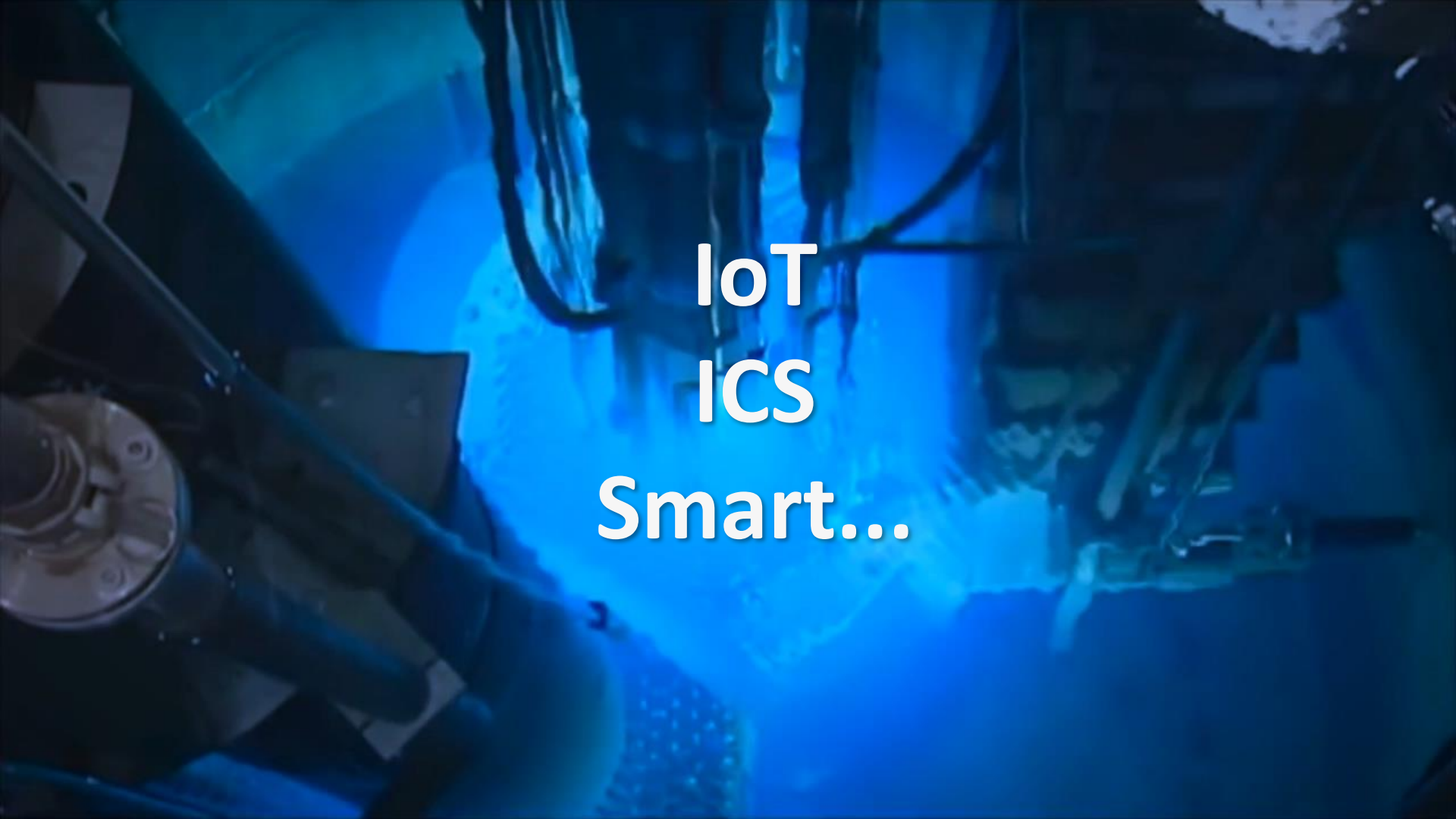
IoT exponential growth

Resource Hijacking

Growth in encrypted traffic

Requirement for visibility and traceability

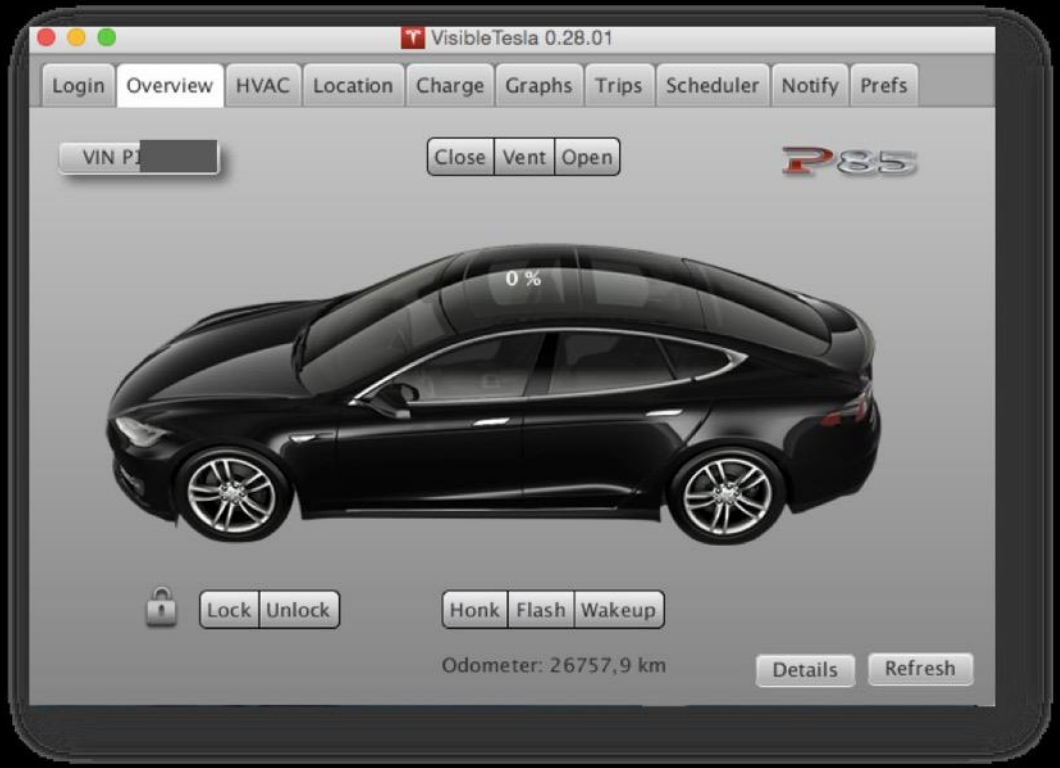
To few resources


IoT
ICS
Smart...

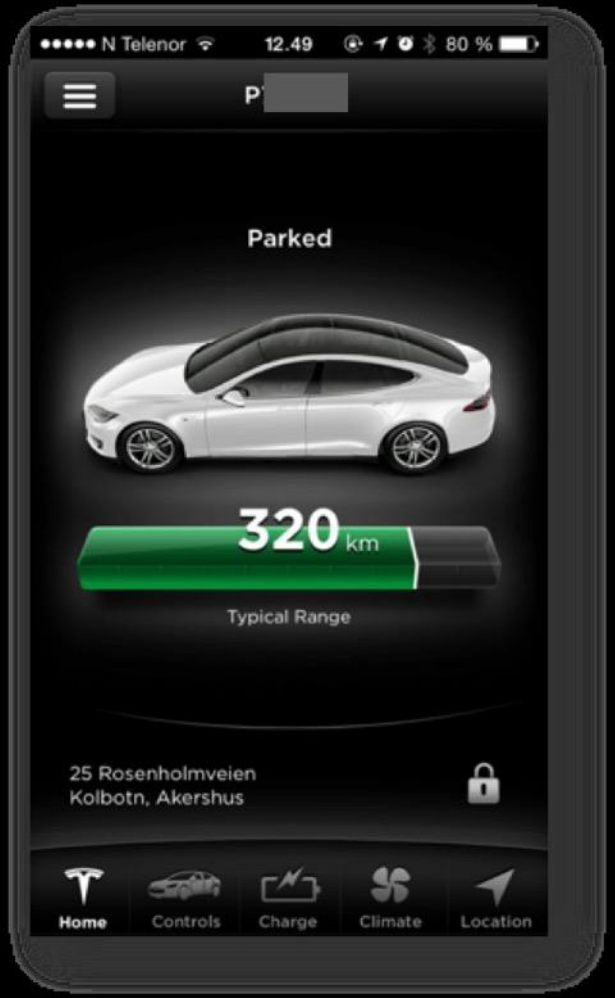
IoT attack surface

IoT Challenge

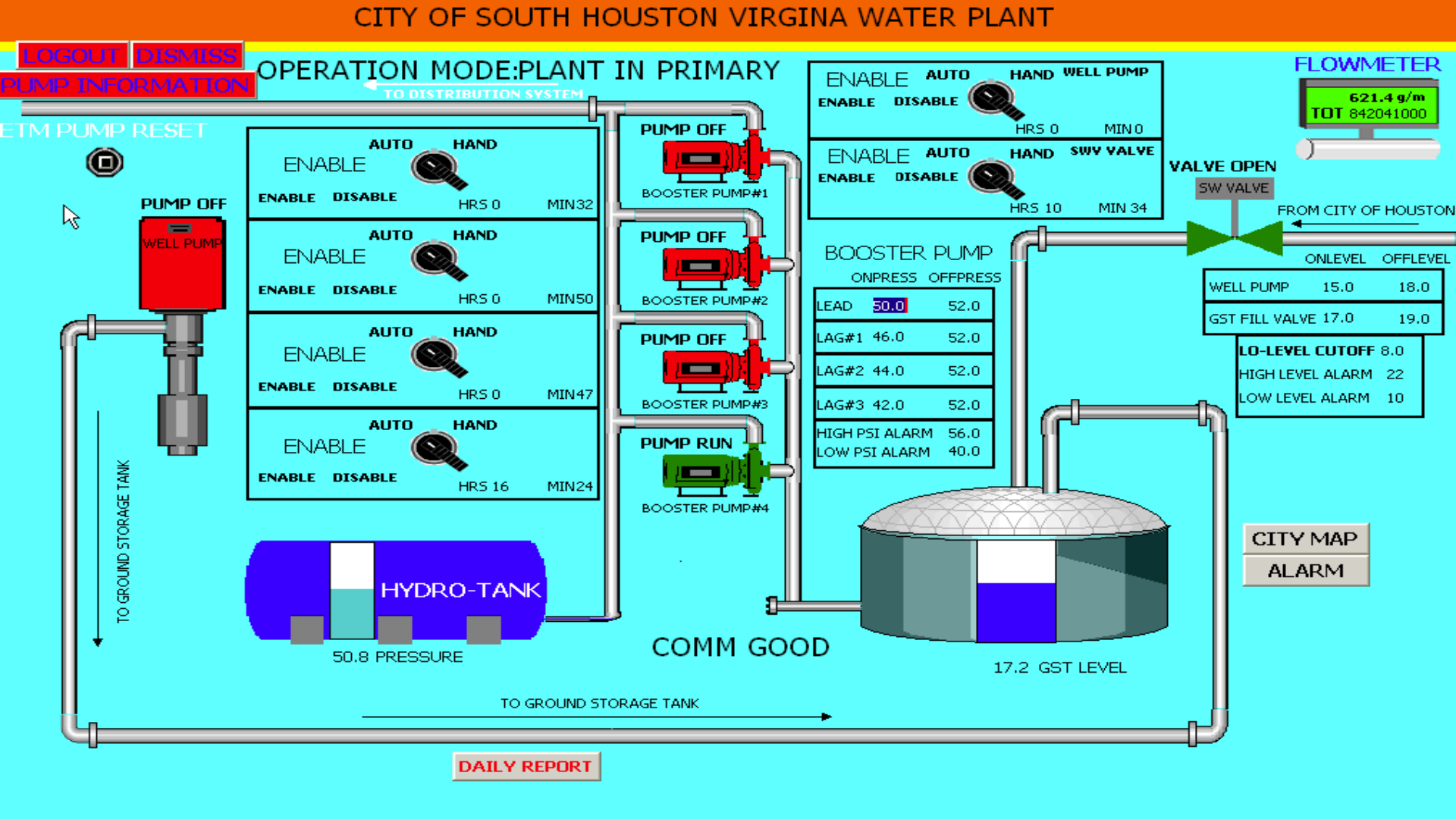
- Volume of Devices
- Operating Systems
- Designed to be (un)secure
- Protocols
- Immature usage

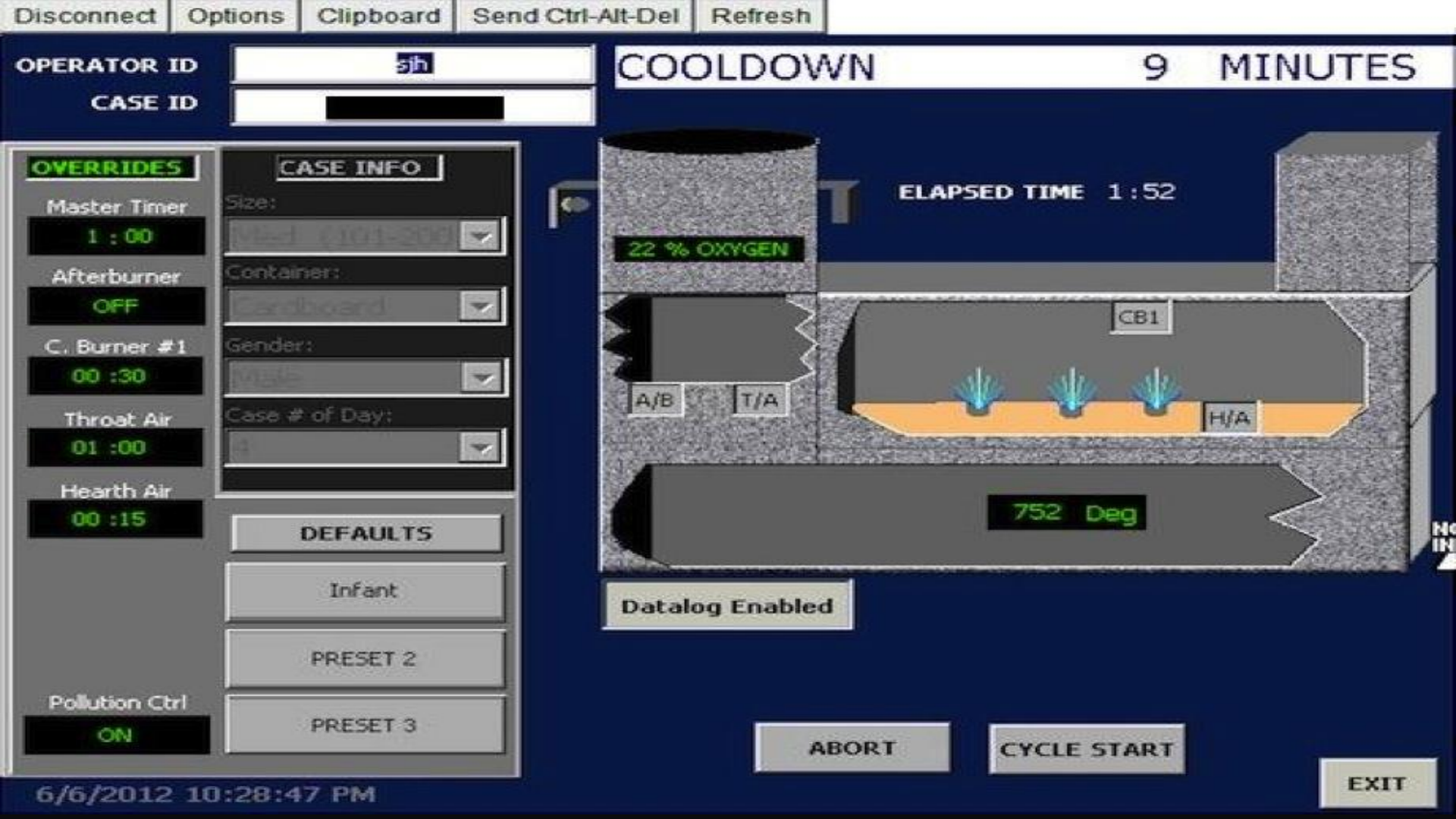


Tidligere bil i Visible Tesla



Ny bil i Teslas app


CITY OF SOUTH HOUSTON VIRGINA WATER PLANT
LOGOUT
DISMISS
PUMP INFORMATION
OPERATION MODE:PLANT IN PRIMARY
TO DISTRIBUTION SYSTEM
ETM PUMP RESET
PUMP OFF
WELL PUMP
ENABLE AUTO HAND
ENABLE DISABLE HRS 0 MIN32
ENABLE AUTO HAND
ENABLE DISABLE HRS 0 MIN50
ENABLE AUTO HAND
ENABLE DISABLE HRS 0 MIN47
ENABLE AUTO HAND
ENABLE DISABLE HRS 16 MIN24
PUMP OFF
BOOSTER PUMP#1
PUMP OFF
BOOSTER PUMP#2
PUMP OFF
BOOSTER PUMP#3
PUMP RUN
BOOSTER PUMP#4
ENABLE AUTO HAND WELL PUMP
ENABLE DISABLE HRS 0 MIN 0
ENABLE AUTO HAND SWV VALVE
ENABLE DISABLE HRS 10 MIN 34
BOOSTER PUMP
ONPRESS OFFPRESS
LEAD 50.0 52.0
LAG#1 46.0 52.0
LAG#2 44.0 52.0
LAG#3 42.0 52.0
HIGH PSI ALARM 56.0
LOW PSI ALARM 40.0
FLOWMETER
621.4 g/m
TOT 842041000
VALVE OPEN
SW VALVE
FROM CITY OF HOUSTON
ONLEVEL OFFLEVEL
WELL PUMP 15.0 18.0
GST FILL VALVE 17.0 19.0
LO-LEVEL CUTOFF 8.0
HIGH LEVEL ALARM 22
LOW LEVEL ALARM 10
TO GROUND STORAGE TANK
HYDRO-TANK
50.8 PRESSURE
COMM GOOD
17.2 GST LEVEL
CITY MAP
ALARM
TO GROUND STORAGE TANK
DAILY REPORT

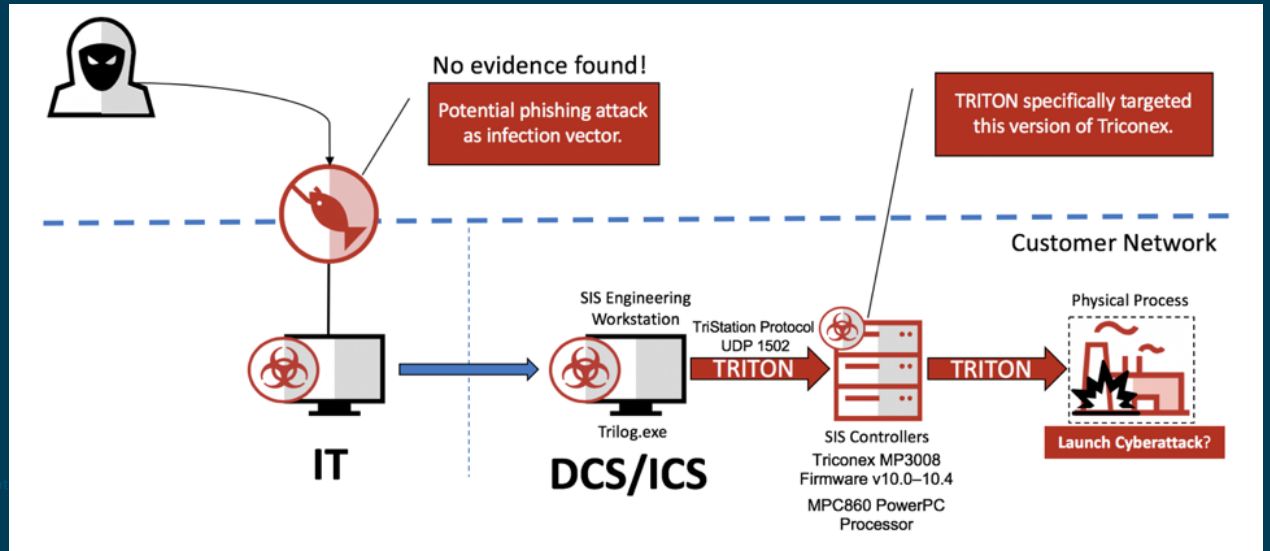

Disconnect
Options
Clipboard
Send Ctrl-Alt-Del
Refresh
OPERATOR ID
sh
CASE ID
COOLDOWN 9 MINUTES
OVERRIDES
Master Timer
1 : 00
Afterburner
OFF
C. Burner #1
00 :30
Throat Air
01 :00
Hearth Air
00 :15
Pollution Ctrl
ON
CASE INFO
Size:
Container:
Cardboard
Gender:
Case # of Day:
DEFAULTS
Infant
PRESET 2
PRESET 3
ELAPSED TIME 1:52
22 % OXYGEN
CB1
A/B
T/A
H/A
752 Deg
Datalog Enabled
ABORT
CYCLE START
EXIT
6/6/2012 10:28:47 PM

Some examples


CASINO

Triton

- Cause Operational Disruption to Critical Infrastructure
- Triconex Safety Instrumented System (SIS) controllers
- “The world’s most murderous malware”



```
Connection to 5.206.225.96 23 port [tcp/telnet] succeeded!

....
```

```
- A text-based MUD by Oscar P

No account? Register at www.elrooted.com
Enter user> yop
yop
Enter pass> yop
***

Disconnected by server. |
Press any key to exit.
```

Username	Password
admin	admin
root	default
support	support
admin	password
root	root
root	12345
root	password
service	service
guest	guest
root	user
tech	tech
mother	fucker

TECH • PHILIPS

Light Bulbs Flash "SOS" in Scary Internet of Things Attack

Mike Kemp—Rubberball/Getty Images

By JEFF JOHN ROBERTS November 3, 2016

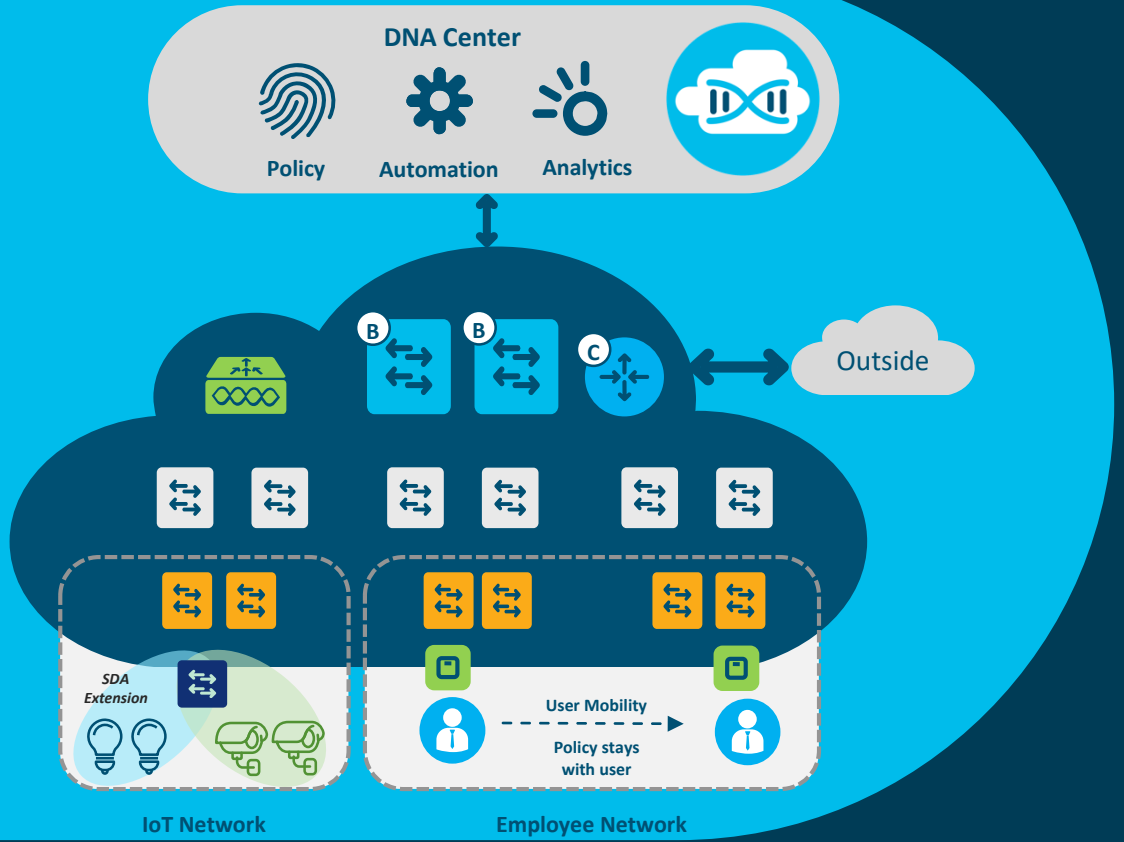
Hackers used a drone to target a set of Philips light bulbs in an office tower, infecting the bulbs with a virus that let the attackers turn the lights on and off, and flash an "SOS" message in Morse code.

IoT attack goals

- Denial of Service
- Destroy
- Botnet
- Beachhead
- Manipulate data
- Spionage

Cisco IoT Security

Segmentation

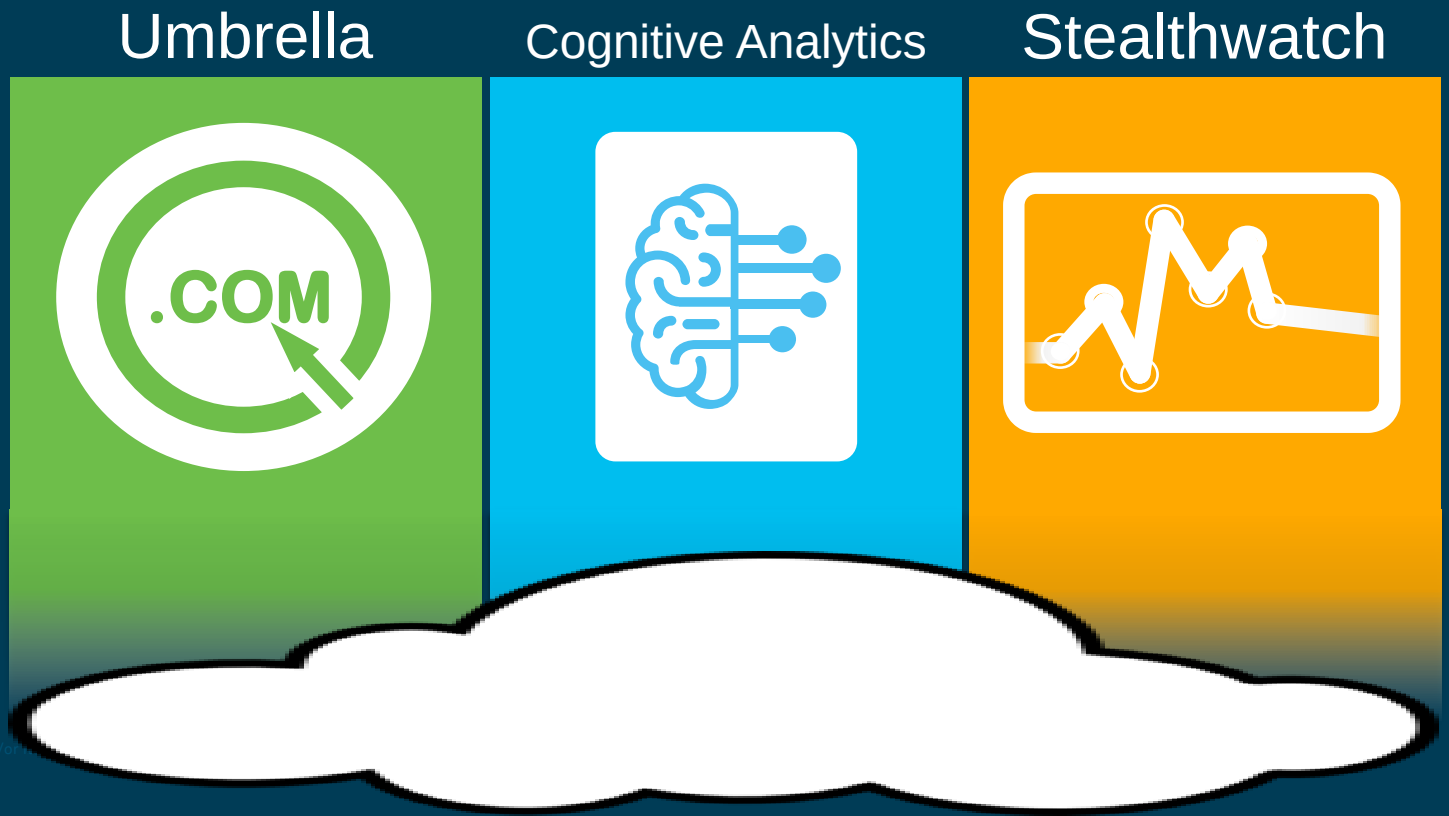


Identity-Based Policy & Segmentation

Automated Network Fabric

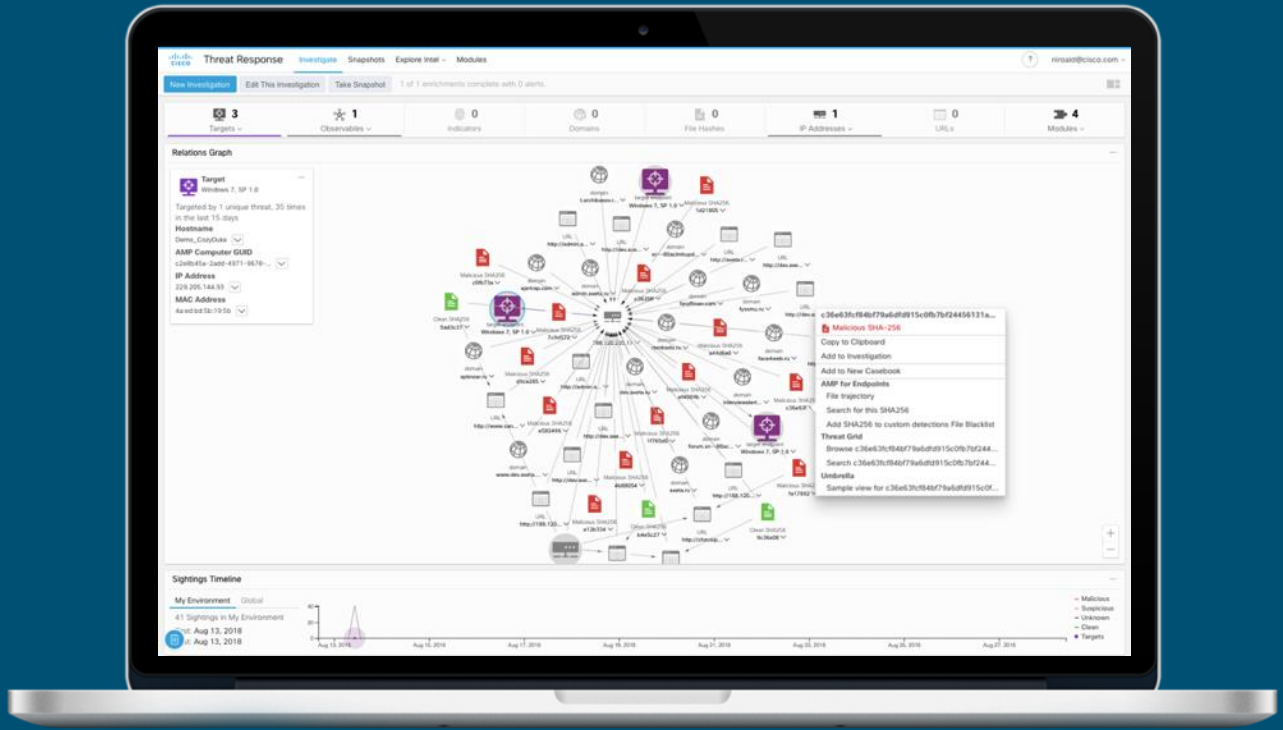
Insights & Telemetry

New detection methods



Agentless detection

Visibility



Threat Response | Investigate | Snapshots | Intelligence | Modules | Nils Roald

New Investigation | Snapshots ... | Stacked Layout

Investigation 48 of 48 enrichments complete

0 Targets | 48 Observables | 0 Indicators | 7 Domains | 27 File Hashes | 14 IP Addresses | 0 URLs | 4 Modules

Relations Graph Showing 200 nodes

Sightings Timeline

My Environment | Global

24 Sightings

st: Apr 1, 2013

st: Sep 24, 2018

VPNfilter


05.06.40
PERSONAL
NUTRITION
SUGGESTED ME
ANALYSIS


CISCO