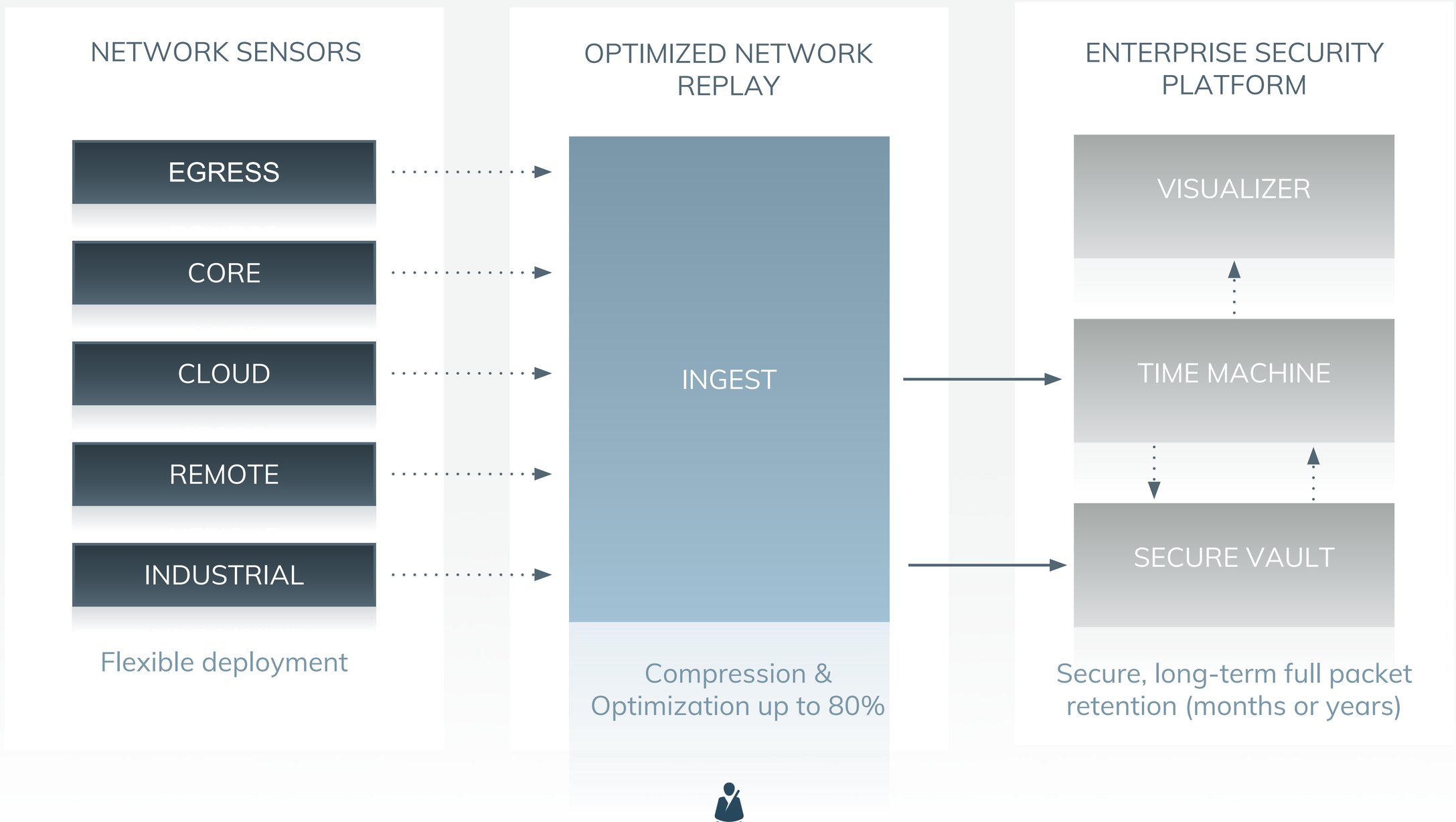
PROTECTWISE™

Industrial Control Systems (In)Security
&
Suricata

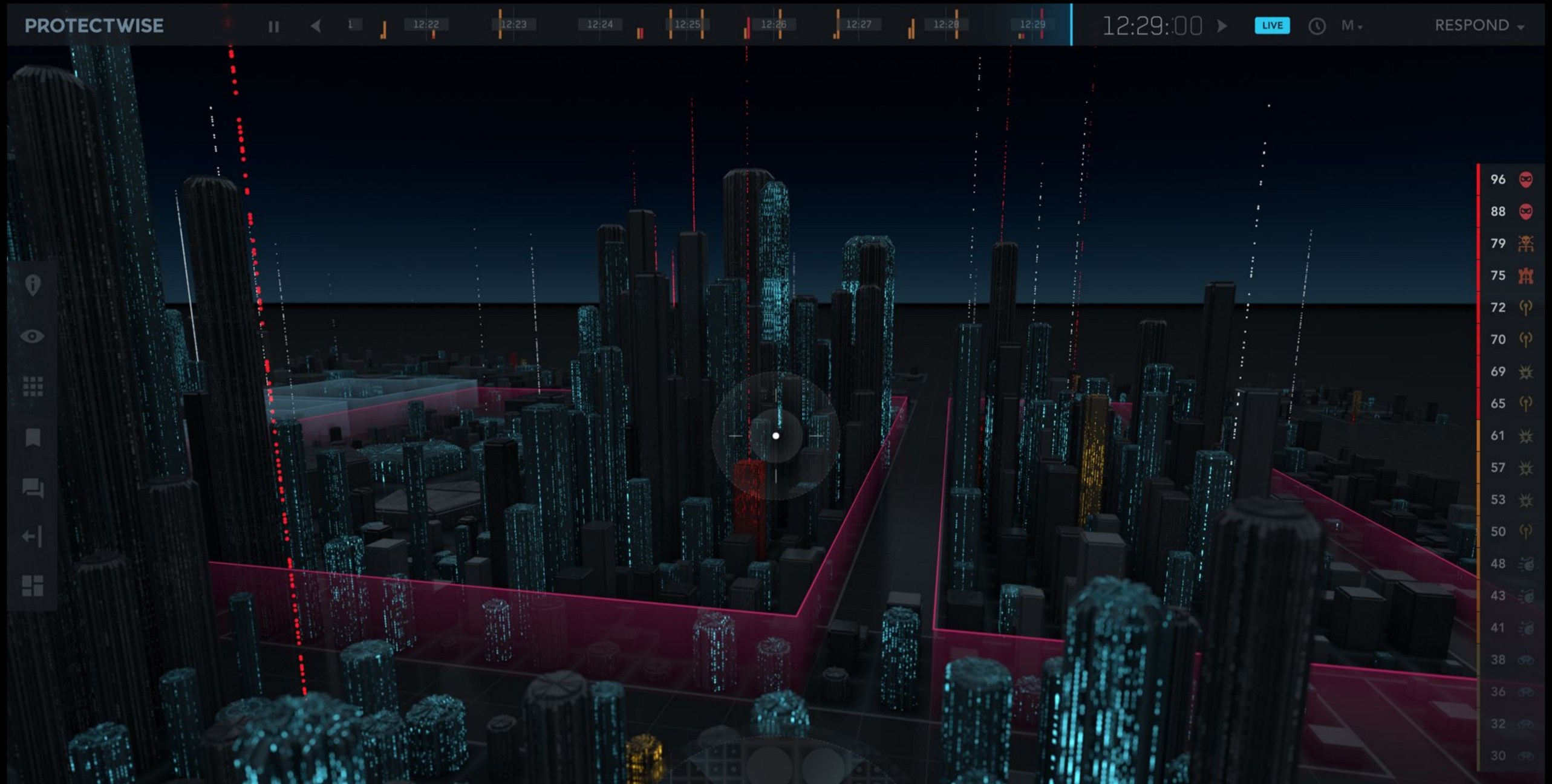
PROTECTWISE™

- Founded in 2013
- Headquartered in Denver, Colorado, U.S.
- Leadership — industry veterans from McAfee, Palo Alto Networks, Symantec
- More than $70 million in VC funding raised to date
- Customers span virtually every industry — oil & gas, utilities, manufacturing, healthcare, finance, entertainment, government
- Hundreds of deployments globally — 35+ deployed across upstream, downstream and wind farm environments at major oil & gas company

HOW IT WORKS


NETWORK SENSORS
OPTIMIZED NETWORK REPLAY
ENTERPRISE SECURITY PLATFORM
EGRESS
CORE
CLOUD
REMOTE
INDUSTRIAL
INGEST
VISUALIZER
TIME MACHINE
SECURE VAULT
Flexible deployment
Compression & Optimization up to 80%
Secure, long-term full packet retention (months or years)

IMMERSIVE SECURITY



INDUSTRIAL CONTROL SYSTEMS

WIDE RANGE OF SYSTEMS

SCADA, PLC, RTU, DCS, HMI, and others that provide an interface to a specific industrial process.

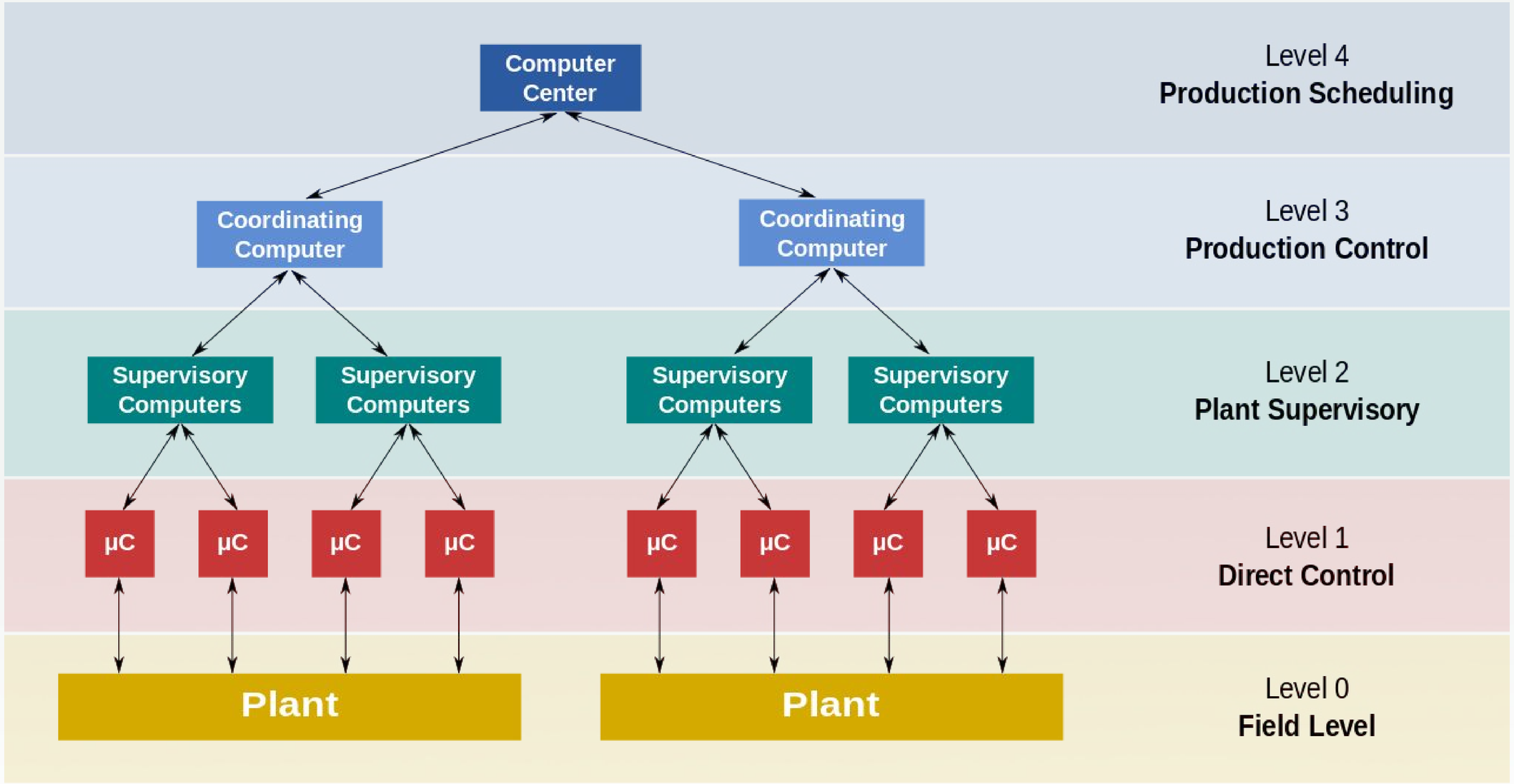
HIGH LEVEL OF SYSTEM CONTROL

ICS systems expose a large attack surface since they have various levels of programmability to enable controllers to adjust the specific industrial process.

HIGH LEVEL OF IMPACT

Specific industrial process means a specific level of control. Traffic light timing, water distribution, even nuclear power plant turbines are all controlled by ICS

Industrial Control Systems



HIGH SECURITY IN INDUSTRIAL CONTROL SYSTEMS

RESTRICTING PHYSICAL ACCESS TO THE ICS NETWORK AND DEVICES.

Yep, no physical access to 1000 oil rigs

RESTRICTING LOGICAL ACCESS TO THE ICS NETWORK AND NETWORK ACTIVITY

Network configurations are *always* correct

PROTECTING INDIVIDUAL ICS COMPONENTS FROM EXPLOITATION

Patches, audit trails, security software. Nothing a little helicopter fuel can’t fix

RESTRICTING UNAUTHORIZED MODIFICATION OF DATA

Oh, let me just turn on that feature

DETECTING SECURITY EVENTS AND INCIDENTS

And that’s why we’re here

RESTRICTING LOGICAL AND PHYSICAL ACCESS

DEVICES HAVE NO ACCESS TO THE INTERNET OR COMPUTERS THAT HAVE ACCESS TO THE INTERNET

- Searching for a specific device: OccupyTheWeb's Hacker Training Camp
- Metasploit module to find modbus devices: Modbus Unit ID and Station ID Enumerator
- Supply Chain Attack

WE ALL KNOW HOW WELL SINGLE FACTOR AUTHENTICATION WORKS

```
content:"ENTER USER NAME|3a|";
```

ICS INSECURITY

Duqu/Stuxnet - S7, ProfiBus

- Iran: Uranium Enrichment Facility

Slammer - SCADA DoS

- USA: Nuclear Power Plant
- Bypassed firewalls due to unknown connections

Havex - OPC, Modbus, S7, ENIP

- France: Industrial Machine Producer
- Germany: Industrial Application and Machine Manufacture

ICS DETECTION IN SURICATA

EXISTING PROTOCOLS

DNP3 (3.2)

- https://redmine.openinfosecfoundation.org/issues/1745

CIP OVER ETHERNET (ETHERNET/IP) (3.2)

- http://ieeexplore.ieee.org/document/7946818/
- https://redmine.openinfosecfoundation.org/issues/1495

MODBUS (2.1)

- http://www.ssi.gouv.fr/agence/publication/detection-dintrusion-dans-les-systemes-industriels-suricata-et-le-cas-modbus/
- https://redmine.openinfosecfoundation.org/issues/1310

ADD YOUR OWN

app-layer-x, detect(-engine)-x

GET ON THE MODBUS

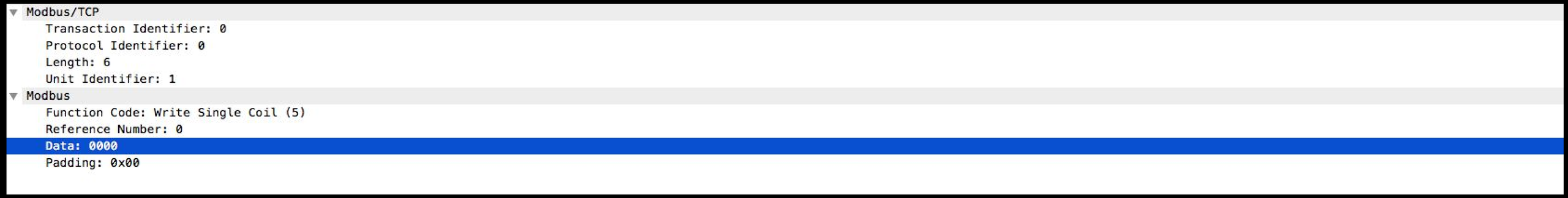
SETUP SURICATA

- TCP Streams may be ***very*** long lived
- Unlimited stream depth
- Long TCP timeouts
- app-layer.protocols.modbus.detection-ports.dp = 502
- vars.address-groups (protocol_CLIENT and protocol_SERVER)

FIND SOME CAPTURES

- https://github.com/ITI/ICS-Security-Tools/tree/master/pcaps

Basic Detections



Modbus Signature Format

- modbus: function <value>
- modbus: function <value>, subfunction <value>
- Modbus: function [!] <assigned | unassigned | public | user | reserved | all>

DETECTING A WRITE

SIGNATURE

```
alert modbus !$MODBUS_CLIENT any -> $MODBUS_SERVER 502 (modbus: function 0x05; msg:"Modbus
Write Single Coil"; sid: 2;)
```

ALERT


```
{"timestamp":"2004-08-26T06:01:34.214335-0600","flow_id":1773133511107067,"pcap_cnt":10,"eve
 nt_type":"alert","src_ip":"10.0.0.57","src_port":2578,"dest_ip":"10.0.0.3","dest_port":502,
 "proto":"TCP","tx_id":1,"alert":{"action":"allowed","gid":1,"signature_id":2,"rev":0,"signa
     ture":"Modbus Write Single Coil","category":"","severity":3},"app_proto":"modbus"}
```


DNP3 DETECTION

SIGNATURE

```
alert dnp3 !$DNP3_CLIENT any -> $DNP3_SERVER 20000 (dnp3_func: write; msg: "DNP3 Write"; sid: 4;)
```

ALERT


```
{"timestamp":"2015-01-28T13:15:40.964537-0700","flow_id":724467624748480,"pcap_cnt":7,"event
 _type":"alert","src_ip":"192.168.60.1","src_port":50616,"dest_ip":"192.168.60.130","dest_po
 rt":20000,"proto":"TCP","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":4,"rev
        ":0,"signature":"DNP3 Write","category":"","severity":3},"app_proto":"dnp3"}
```


CIP OVER ETHERNET (ETHERNET/IP)

SIGNATURE

```
alert enip !$ENIP_CLIENT any -> $ENIP_SERVER 44818 (cip_service: 0x4c; msg: "CIP Service"; sid: 7;)
```

ALERT

CIP OVER ETHERNET (ETHERNET/IP)

SIGNATURE

```
alert enip !$ENIP_CLIENT any -> $ENIP_SERVER 44818 (cip_service: 76; msg: "CIP Service
Decimal"; sid: 9;)
```

ALERT


```
{"timestamp":"2012-11-12T04:03:00.277922-0700","flow_id":1669874013441192,"pcap_cnt":10,"event
_type":"alert","src_ip":"141.81.0.10","src_port":52593,"dest_ip":"141.81.0.63","dest_port":4
4818,"proto":"TCP","tx_id":1,"alert":{"action":"allowed","gid":1,"signature_id":9,"rev":0,"s
ignature":"CIP Service Decimal","category":"","severity":3},"app_proto":"enip"}
```


TCP VS MODBUS DETECTION

TCP SIGNATURE

```
pcre:"/[\S\s]{3}(\x05|\x06|\x0F|\x10|\x15|\x16)/iR";
```

MODBUS SIGNATURE

```
alert modbus !$MODBUS_CLIENT any -> $MODBUS_SERVER 502 (modbus: access write; msg:"Modbus Write Request";)
```

A SIGNATURE ABOUT NOTHING

MODBUS SIGNATURES

```
alert modbus !$MODBUS_CLIENT any -> $MODBUS_SERVER 502 (modbus: function 0x05; msg:"Modbus Write Single Coil
  First"; sid:11; xbits:set,modbus,track ip_src;)
alert modbus !$MODBUS_CLIENT any -> $MODBUS_SERVER 502 (modbus: function 0x07; msg:"Modbus Read Exception After
  Write"; sid:12; xbits:isset,modbus,track ip_src;)
```

ALERT

SURICATA IS TERRIBLE FOR ICS

DID YOU CHECK YOUR VARIABLES?

- Make sure you actually set <protocol>_SERVER and <protocol>_CLIENT

DID YOU CHECK YOUR SIGNATURES?

- Make sure you’re checking in versus out of the variables

DID YOU CHECK YOUR DETECTION PORTS?

- Signatures don’t automatically define detection ports

ASK ON IRC

TARGETED SURICATA IMPROVEMENTS

MODBUS SHOULD DISTINGUISH BETWEEN REQUEST AND RESPONSE

- https://redmine.openinfosecfoundation.org/issues/1904
- https://redmine.openinfosecfoundation.org/issues/1574

```
alert modbus !$MODBUS_CLIENT any -> $MODBUS_SERVER 502 (modbus: function 0x05; msg:"Modbus Write Single Coil"; sid: 2;)
alert modbus $MODBUS_SERVER 502 -> !$MODBUS_CLIENT any (modbus: function 0x05; msg:"Modbus Write Single Coil Reversed"; sid: 3;)
```


```
{"timestamp":"2006-07-21T08:24:52.781795-0600","flow_id":429225671086147,"pcap_cnt":8,"event_type":"alert","src_ip":"166.161.16.230","src_por
  t":502,"dest_ip":"192.168.66.235","dest_port":2582,"proto":"TCP","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":3,"rev":0,"s
  ignature":"Modbus Write Single Coil Reversed","category":"","severity":3},"app_proto":"modbus"}
{"timestamp":"2006-07-21T08:24:52.903252-0600","flow_id":429225671086147,"pcap_cnt":10,"event_type":"alert","src_ip":"192.168.66.235","src_po
  rt":2582,"dest_ip":"166.161.16.230","dest_port":502,"proto":"TCP","app_proto":"modbus","tx_id":0,"alert":{"action":"allowed","gid":1,"sign
  ature_id":2,"rev":0,"signature":"Modbus Write Single Coil","category":"","severity":3}}
```


No.	Time	Source	Destination	Protocol	Length	Info
20	15.747464	192.168.66.235	166.161.16.230	Modb…	66	Query: Trans: 0; Unit: 1, Func: 5: Wri…
21	16.221932	166.161.16.230	192.168.66.235	Modb…	66	Response: Trans: 0; Unit: 1, Func: 5: Wri…

TARGETED SURICATA IMPROVEMENTS

IMPROVING ICS SIGNATURE WRITING

- Similar to existing signatures with keywords to do “advanced” matches
- Detect malformed requests
- Pipelining support and pipelining matches

TARGETED SURICATA IMPROVEMENTS

ADDITIONAL FLOW TIMEOUT PROTOCOLS

- Allow timeouts for any protocol specified in app-layer?

ADDITIONAL ICS PROTOCOLS

- PCCC
- OPC Classic
- Others?

LARGER SURICATA EFFORTS

SURICATA RESTARTS

- Serialize state

FLOW CHARACTERIZATION

- Roll up false positives as mischaracterization

PROTOCOL UPGRADES

- Upgrade (e.g. ENIP to PCCC), retain and detect against original protocol

BRING YOUR OWN PROTOCOL

- Easily plug in libraries with more robust detections

PROTECTWISE™

ACKNOWLEDGEMENTS

- Suricata Contributors
  - #suricata on IRC
- Protectwise ICS Team
- Protectwise 401 TRG
  - https://401trg.pw/

PROTECTWISE™

Questions?

PROTECTWISE™

THANK YOU