



Industrial Cybersecurity

Opportunities and challenges
in Digital Transformation



MICHAEL WENG

Weng Security Consulting
Denmark

- More than 20 years' experience in IT
- NSM Evangelist, Threat Hunter and OT Incident Responder
- Holds a CISSP, the GIAC GICSP and the GIAC GRID (Analyst no. 47)

[linkedin.com/in/michael-weng-cissp-gicsp-grid-2306751/](https://www.linkedin.com/in/michael-weng-cissp-gicsp-grid-2306751/)



NSM/Threathunting in OT/ICS/SCADA environments

"... Know thy Network " (Rob Joyce, TAO, 2016)

"Defense is doable ..." (Rob. M. Lee, Dragos)

This presentation is *dedicated* to and in memory of our missed

Tina Petersen, KL Corporate Account Manager, Nordic
1969-2018 (30th July)



Rest in peace – You were always a big inspiration

About me ...

Rule `About_Michael_Weng`

{

meta:

date = "19. september 2018"

place= "Sochi, Russia"

author = "Michael Weng, CISSP, GICSP, GRID (Analyst no. 47), Danish"

description = "Owner of **ics2secure.com** & Senior OT/ICS Cyber Security Advisor"

strings:

\$a="Working for Novo Nordisk A/S for 16+ years, in manufacturing" ascii wide

\$b="Solution Design, Project Management, Validation, Operation & Maintenance, Infrastructure, Cyber Security" ascii wide

\$c="Specialized in NSM/Threat hunting in ICS/OT/SCADA environments" ascii wide

\$d="Threathunter, NSM, OT/ICS/SCADA Incident Response" ascii wide

\$d="SANS ICS410, SANS ICS515, SANS SEC 511" ascii wide

\$e="Weng Security Consulting, DK-2900 Hellerup, +45 3029 3079, info@ics2secure.com"

condition:

all of the above

}

Thanks and acknowledgment to


- Kaspersky Labs (KL) for inviting us all and hosting this 6th ICS Conference
- Chris Sistrunk (Mandiant) for inspiration (DEF CON 23 NSM 101 for ICS)
- Doug Burks (Security Onion) for pulling an awesome tool together
- Mikael Vingaard (Honeypot.dk) for supplying pcaps from his honeypot
- Robert M. Lee (SANS ICS515) for teaching an awesome class of IR & Active Defense in ICS
- Robert M. Lee (Dragos) for making "Little Booby – SCADA and Me"
- Eric Conrad (SANS SEC511) for teaching an awesome class of Continued Monitoring
- Richard Bejlich (Taosecurity) for writing awesome books about NSM
- You, the audience, for listening and (hopefully) asking good questions ...

Remember, it *is* possible to defend your ICS/OT/SCADA environment as ***Defense is doable...***

The next 20-30 min. ...

I will be (talking about)

- My background in the Pharma Industry
- NSM/Threathunting basics in OT/ICS/SCADA environments
- Open Source vs. Vendor based solutions (The actual only 'New' stuff to be found in my presentation)
- Generally be sharing my practical experience from the last 3 years as a Threathunter in OT/ICS/SCADA

- Q&A (if we have the time...) 

Working in the Pharma Industry

Then you're used to working with Regulatory Compliance (FDA) in Operations:

- Configuration Management, CIL's ... i.e. Asset Control
- GMP, GLP etc. : GxP ... a.o. written procedures for use of computer systems
- 21CFR Part 11 rules for the use of Electronic Records and Electronic Signatures
- And lately ... Data Integrity (ALCOA+)

... and when designing and building OT/ICS/SCADA installations (for Pharma) you use:

- The Purdue Reference Model i.e.
 - ISA88 Batch Control/Continued Manufacturing
 - ISA95 MoM – Manufacturing Operations Management (MES)
 - ISA99 (Now IEC62 443 – Cyber Security)

... and 'the bible':

- CPwE_D&IG from Cisco and Rockwell (Go read the first 2-300 pages)

Why is that relevant?

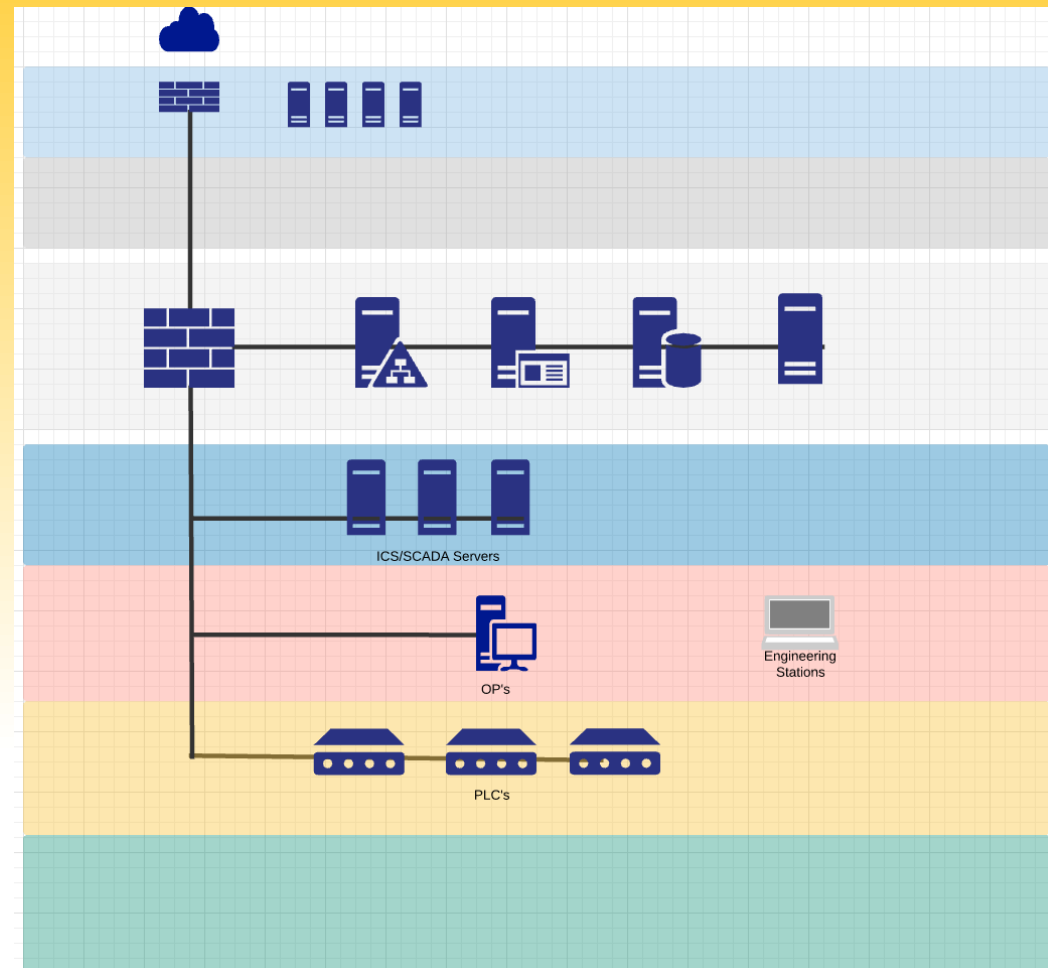


Cyber Security Architecture standard

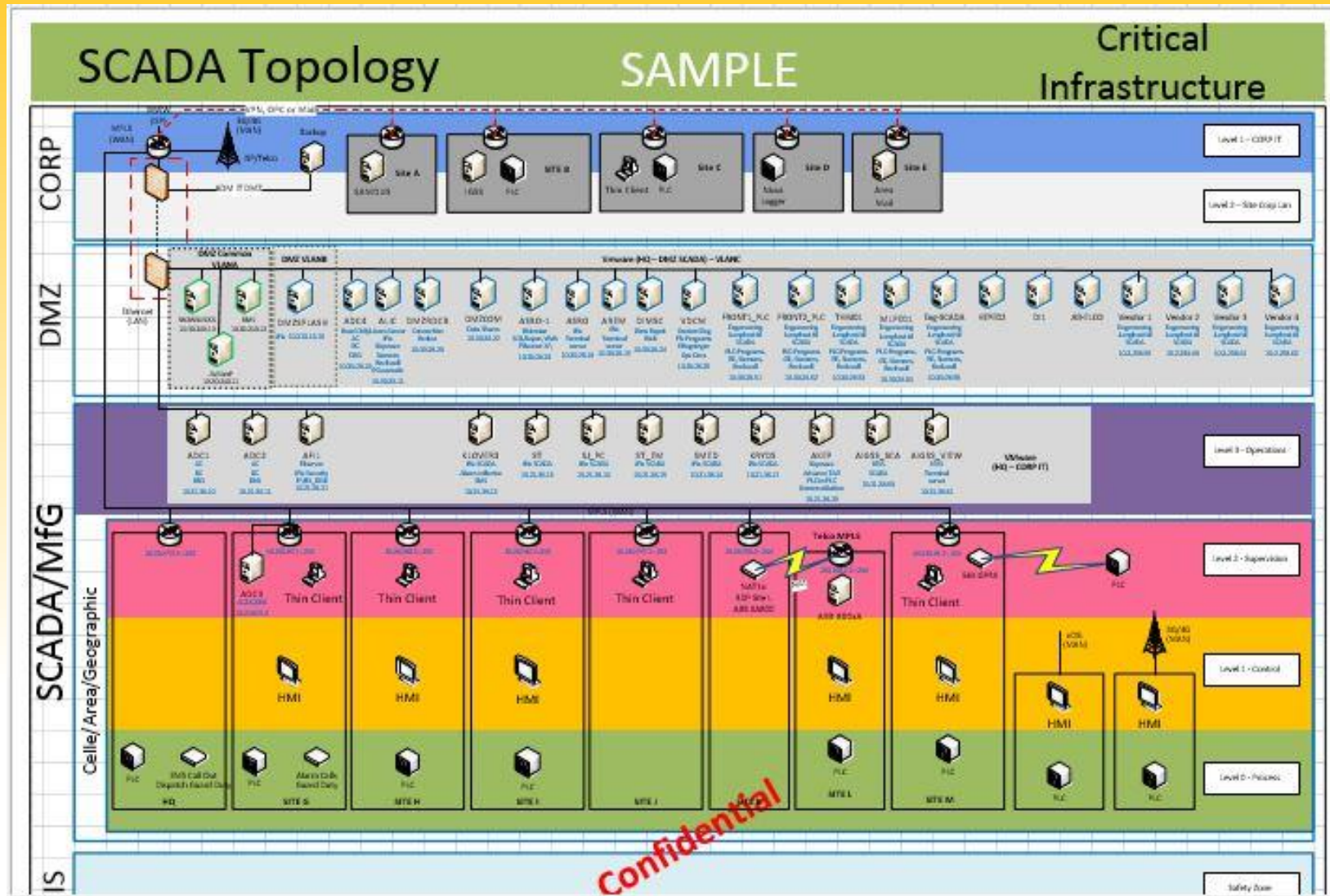
Most people knows it, fewer people knows it originates in the Purdue Reference Model

And even fewer people knows why it makes sense in the perspective of Cyber Security

Lets run through Why ...



A useful example of a Security Architecture



This is where the (only) hard work lies ...

... so do it right the first time ...

To gain success you need 98-99 % asset discovery ...

... did anyone say 'Defence-in-Depth'?

Why do we need NSM/Threathunting?

We know that prevention eventually will fail...

And adversaries will eventually get access to our networks and systems ...

We should not abandon the preventive controls, but extend our defense ...

We must add proactive network monitoring ... i.e. NSM and Threathunting

Network Security Monitoring/Threathunting ... Defense is doable

Be proactive ... ensure visibility ... go look for the adversaries in your networks

NSM/Threathunting in OT/ICS/SCADA

DO's

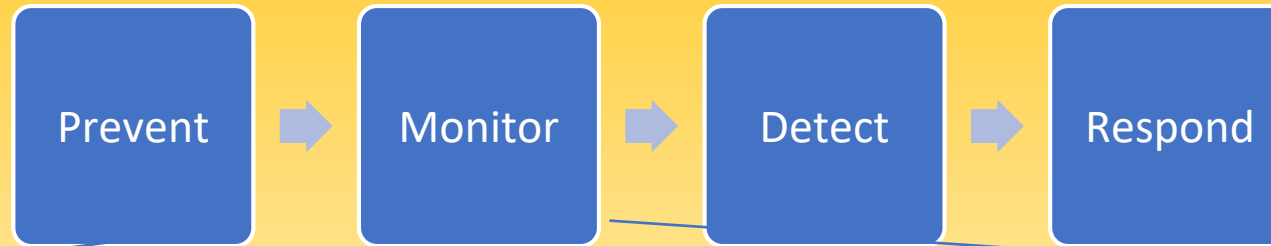
- **Know** thy Network – Work out a full OT asset inventory – and draw it ... (Rob Joyce)
- **Segregate** IT and OT (Purdue Reference Model and CPwE)
- Do proper and full **Segmentation** in the OT space (Purdue and CPwE)
- Place the Sensors in the natural **choke-points** called Conduits (Richard Bejlich)
- Do **Threat Modelling** Analysis as a basis for planning your Threathunting (Rob M. Lee)
- Combine with Sys/Event **log Collection** and **full Packet Capture** to the extent possible
- Utilize the **very static nature** of the OT environment (Gold Nugget)

Don't

- Assume you are in control of your own Network – You are not
- Think you are smarter than your adversaries – You are not
- Think your Network is of interest to you only – It is not
- Think you'll ever be done with Cyber Security – It will be endless

The Cyber Security Life cycle

Aim at Active Response and not Incident Response



| Data sources in OT/ICS/SCADA | |
|---|---|
| Netflows (IPFIX, Sflow, AppFlow, etc.) | Easy (requires a controlled infrastructure) |
| Network Traffic(pcap) | Easy (requires controlled switches) |
| Process Control logs (syslog) | Moderate (function must be available on controllers) |
| Process History | Moderate (Can require API access and integration) |
| Host based logs (Win & Nix supervisors) | Difficult (requires vendor approval) |
| ICS Software events and alarms | Difficult (requires API access and integration or central collection and integration with special analysis tools) |
| Special Equipment logs (digitale relays, CCTV/Video, physical access control) | Difficult (requires functionality on equipment/device and special integration with special analysis tools) |

One NSM Tool to rule them all ... SO



Open Source Linux Distro

SO the 'Old' way

Full packet capture – Tcpcap/Wireshark/NetworkMiner

Extracted – xplico/NetworkMiner

Session – BRO/FlowBAT

Transactional – BRO

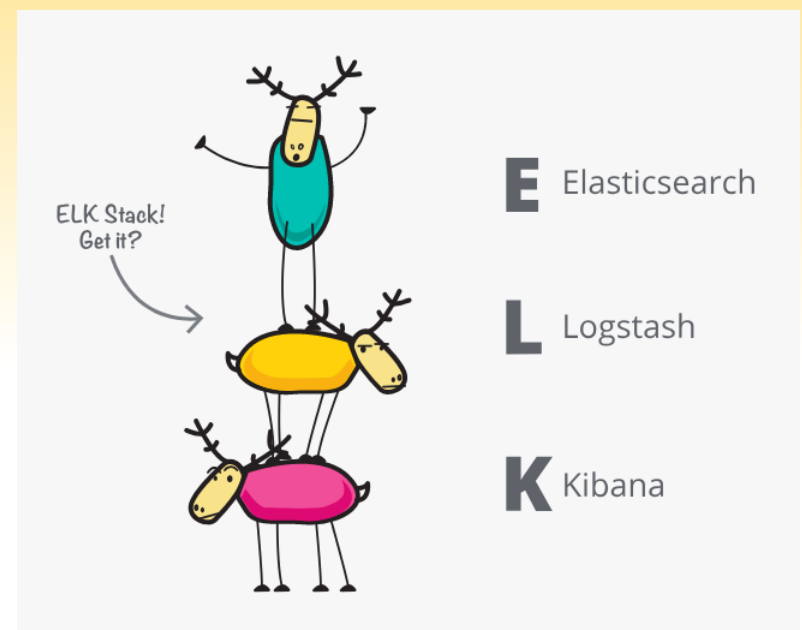
Statistical – capinfos/Wireshark

Meta – ELSA (and WHOIS)

Alerts – Snort/Suricata/squid, Snorby

Keyword: Pivot between data feeds based on IoC's

SO the 'New' way



Why buy a Vendor based solution?

Let's do a wild comparison to a completely random selected vendor product of a similar nature ... say, lets pick KICS for Networks® (yes, the NSM solution from KL)

Comparison:

Open source tools are free, takes approx. 15 min. to install and comes with plenty of resources on the Internet – But you have to dig in, to learn most of it ... and it sometimes has to be tweaked as well ... and sometimes it just doesn't work ...

A vendor based tool often takes a little longer to install and configure, and the tool might be free, but the license are normally not ... however, what you get in return is support from a huge user base and skilled technicians and supporters, and it always works ...

Open Source supports a few to a hundred sensors, Vendor based supports thousands of sensors and endpoints

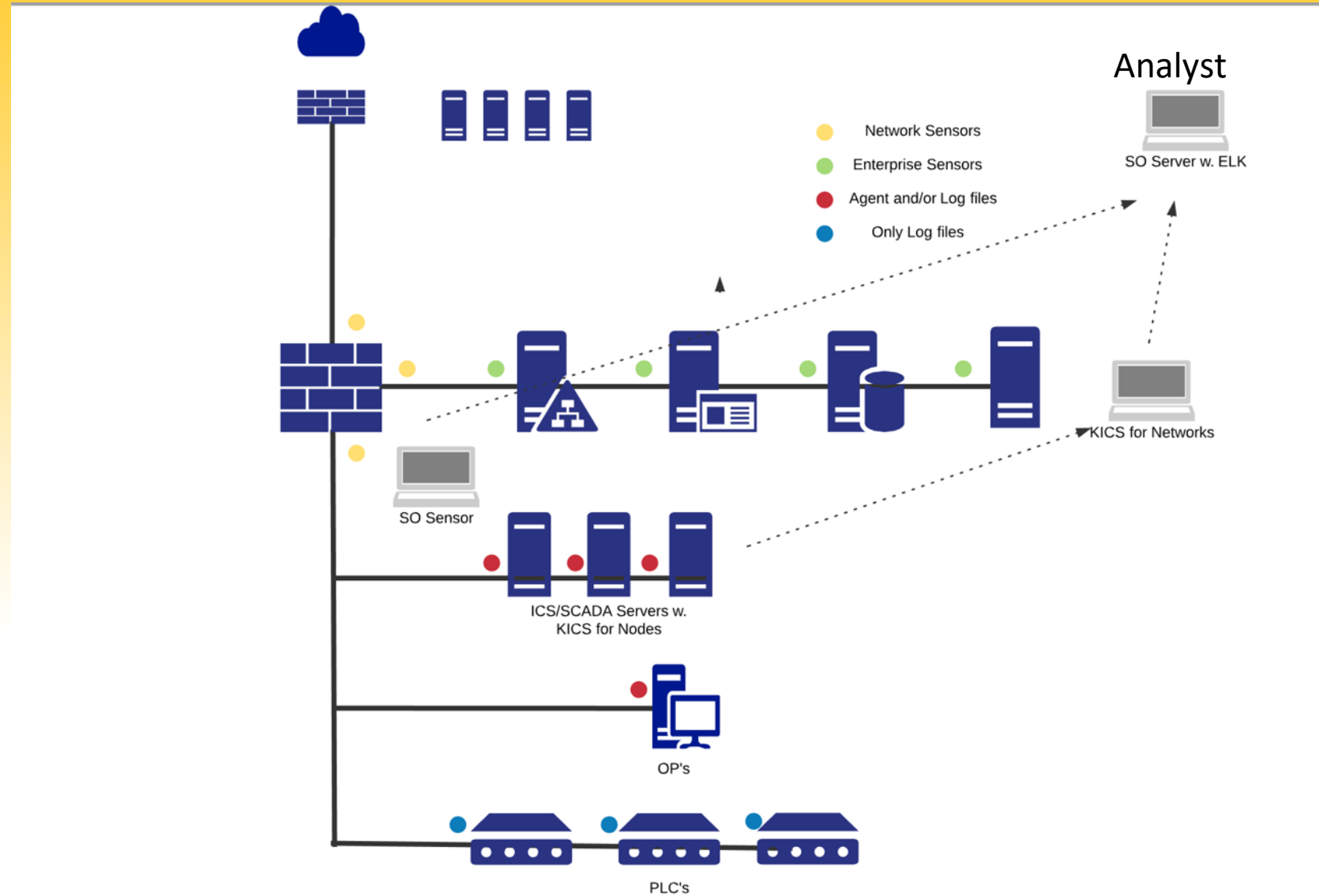
Easily integration ...

KICS is not a SIEM solution as-is, its part of an integrated security solution package from KL

KICS can easily be integrated into one (SIEM) ... and deliver important inputs for analysts

And as SO/ELK is 'kind of a' SIEM/Log Management solution, the two can actually integrate and compliment each other ... and especially in the OT/ICS/SCADA space the benefit of using KICS is, that KL has a vast knowledge and experience about the different environment types hence threats and vulnerabilities to OT/ICS/SCADA... and it speaks a lot of the 'native' dialects (protocols) ... so the two tools will integrated and support the analyst perfectly

The Lab model



ELK and Beats

The screenshot shows the Elastic.co/products website. At the top, there is a navigation bar with icons for Elasticsearch, Kibana, Logstash, Beats, ECE, Logging, Metrics, Site Search, Security, APM, and an 'All' button. Below this, the main content area is divided into sections for Kibana, Elasticsearch, and Beats/Logstash. A central vertical line with colored circles at the top, middle, and bottom connects the three main sections. The top circle is pink and green, the middle is yellow and blue, and the bottom is yellow and blue. Lines extend from these circles to the corresponding product descriptions.

Powering Data Search, Lo x

Secure | <https://www.elastic.co/products>

Elasticsearch Kibana Logstash Beats ECE Features Logging Metrics Site Search Security APM All

Kibana
Learn More Download
Kibana gives shape to your data and is the extensible user interface for configuring and managing all aspects of the Elastic Stack.

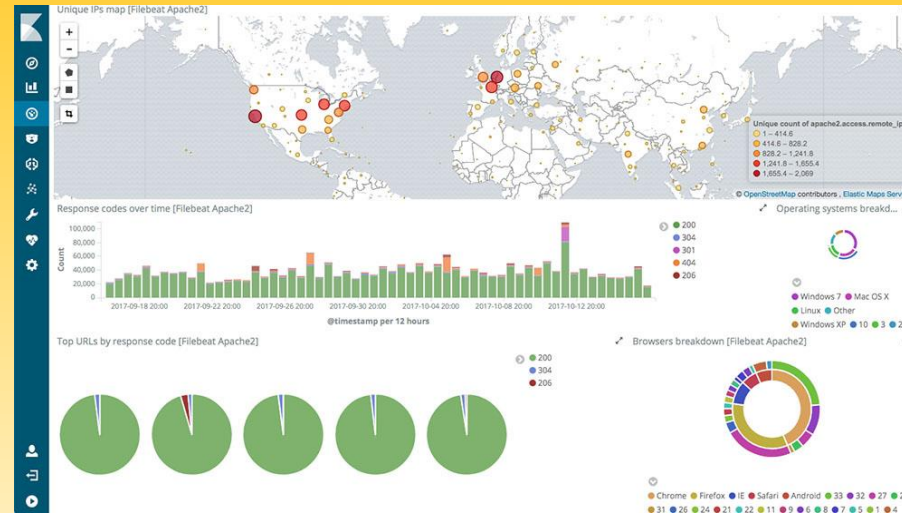
Search, analyze, and store your data.
Elasticsearch
Learn More Download
Elasticsearch is a distributed, JSON-based search and analytics engine designed for horizontal scalability, maximum reliability, and easy management.

Ingest any data, from any source, in any format.

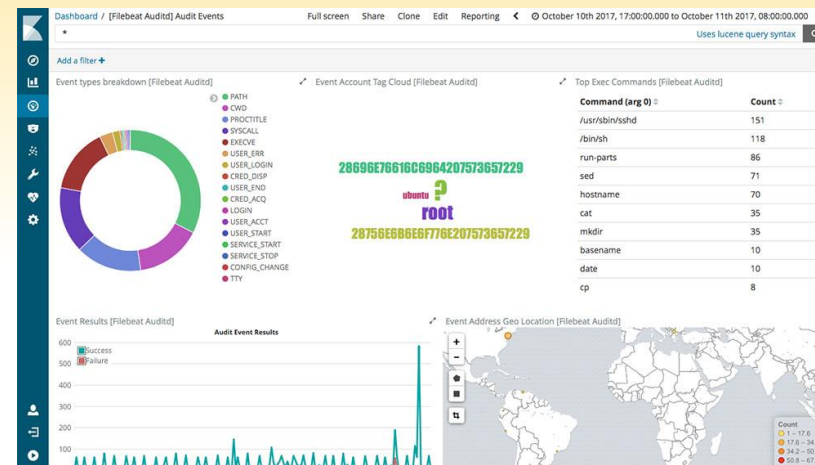
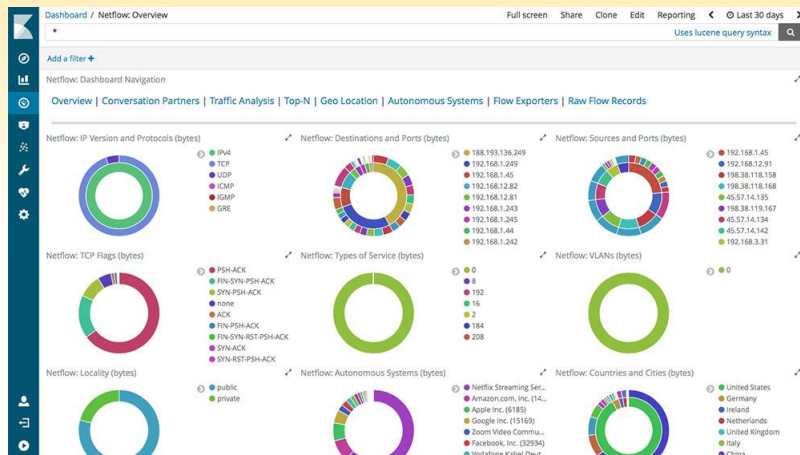
Beats Logstash

Using Beats to interact between SO and KICS

... FileBeats can do the job of integrating logfiles




... but try out PacketBeat or WinlogBeat as well....



Learn the trade of NSM ...

You can be up and running within 15-20 min. and start your proactive hunts after adversaries, on a free software platform and an old used Computer, basically ...

Later on, when you know the normal daily nature of your network operations, and have extended your skills, you can extent the setup with a vendor based solution that slowly can build up to a more professional 'SOC' like environment ... and you will quickly realise, that the very static nature of OT/ICS/SCADA will present abnormal patterns easily and visible to even an untrained eye ... and you will be actively defending your OT/ICS/SCADA environment with success ... before threats becomes Incidents

... you'll quickly have real business cases to show 'the money worth' to LoB management ... Happy hunting 

Q&A

Thank you for listening 

Remember... *Defense is doable* ... go look for threats in your OT environment

Michael Lehmann Weng, CISSP, GRID

ics2secure

Tuborgvej 56 1.Tv

2900 Hellerup

Denmark

+45 3029 3079

info@ics2secure.com

ics2secure consulting services within OT/ICS/SCADA:

- *NSM (Network Security Monitoring)*
- *Threat Hunting*
- *Active Defence & Incident Response*
- *Cyber Security Risk Assessment*
- *Network Assessment*
- *Project Management*
- *Solution Design & Implementation*

Backup

ics2secure

- Can help develop and implement/install NSM solutions based on KL KICS or SO (Sensor/Server solution)
- Can help implementing LAPS, AppLocker and centralized log-aggregation management of Event- and Syslogs
- Can help with Network Segmentation, DMZ design and cleaning of Firewall ACL's in that context
- Can help prepare for Incident Response/Forencis in OT/ICS/SCADA by implementing a strategy for collecting pcaps (Full Packet Captures) for a.o.t. Threathunting via Wireshark and/or NetworkMiner

All over the world ...