The building blocks of good detection and response services for the ICS environment

By:
Søren Egede Knudsen
Our objectives today are to give Gartner a better understanding of:

1. why do customers choose Ezenta MDR and what have we learned from our engagements
   - Sales cycle, industry, customer size, decision makers, implementation honeymoon
   - Recap – why do customers say yes

2. How is Ezenta sales organised and what are our sales strategy on MDR going forward
Nobody wants managers, we want leaders!

Understanding the people’s value set is critical.

The leader

Team members

Practice as you preach!
Organisational priorities

- Staff
- Auditors
- You
- Value Chain
- Threats

Availability: 1 - 10
Remote control: 1 - 10
Casualties (H): 1 - 10
Define the needed technical level of the team
<table>
<thead>
<tr>
<th>Name</th>
<th>Skills</th>
<th>Personality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager</td>
<td>People, Business and Technical skills and experience. IT and OT.</td>
<td>Transformational leader Common purpose / goal Value based Honest</td>
</tr>
<tr>
<td>Security Network specialist/Analyst</td>
<td>FW, IDS, OT, IT, SIEM, Network</td>
<td>Team player Follow a list Communicative</td>
</tr>
<tr>
<td>OS Security specialist/Analyst</td>
<td>Windows, Linux, application, SIEM, OT</td>
<td></td>
</tr>
<tr>
<td>IR and forensics analyst</td>
<td>OS, Network, pen-test, forensics, OT</td>
<td>Plus: Analytic, Digger</td>
</tr>
<tr>
<td>SCADA specialist</td>
<td>IT, OT, SCADA processes and logic</td>
<td>Plus: Process Analytic</td>
</tr>
</tbody>
</table>

Pitfalls in selecting people

Selecting “do’ers”
IT not OT focused
Only technical knowledge
Not team player

Empower the team!
Integrated team (in-house & consultants)

Horizontal vs hierarchical team

Area level

Plant level

R=Responsible, A=Accountable, C=Consulted, I=Informed
Incident response plan

- Proactive services
- Regulation and rules
- Communication
- Agreements
- Priorities and stakeholders
- Easy to understand
- Roles
ICS visibility

LITTLE BOBBY

We don't see any threats so we're not going to invest in security.

ARE YOU LOOKING FOR THREATS IN YOUR NETWORKS?

NO-- WE'VE NO NEED FOR SECURITY TECHNOLOGIES.

IF YOU'RE NOT LOOKING, HOW WOULD YOU KNOW IF THREATS ARE THERE OR NOT?

EVERYTHING SEEMS TO BE WORKING FINE!

OKAY-- SO FAITH, JUST SAY BLIND FAITH.

by Robert M. Lee and Jeff Haas

APRIL 1, 2018
ICS visibility

NSM + Asset + Segmentation = visibility

Asset Communication Profile
(Assets, protocol, tags)
INCI\textit{DENT} readiness

Are you ready for an incident?

8 step for readiness

- Stakeholders and priorities
- Definition of IR types
- Members of the IR team
- Empowerment of the team
- Model (RACI)
- Network (segmentation)
- Assets
- Dataflow
Organisational priorities

leadership

Team members

Skills and experience

Visibility
THANK YOU!