Machine Learning applied to ICS Cybersecurity

Disruptive technologies in the fight against cyber attacks

Hannover, April 2019
Marcelo Branquinho, CEO & Founder

Marcelo Branquinho

CEO & Founder

marcelo@tisafe.com

Agenda

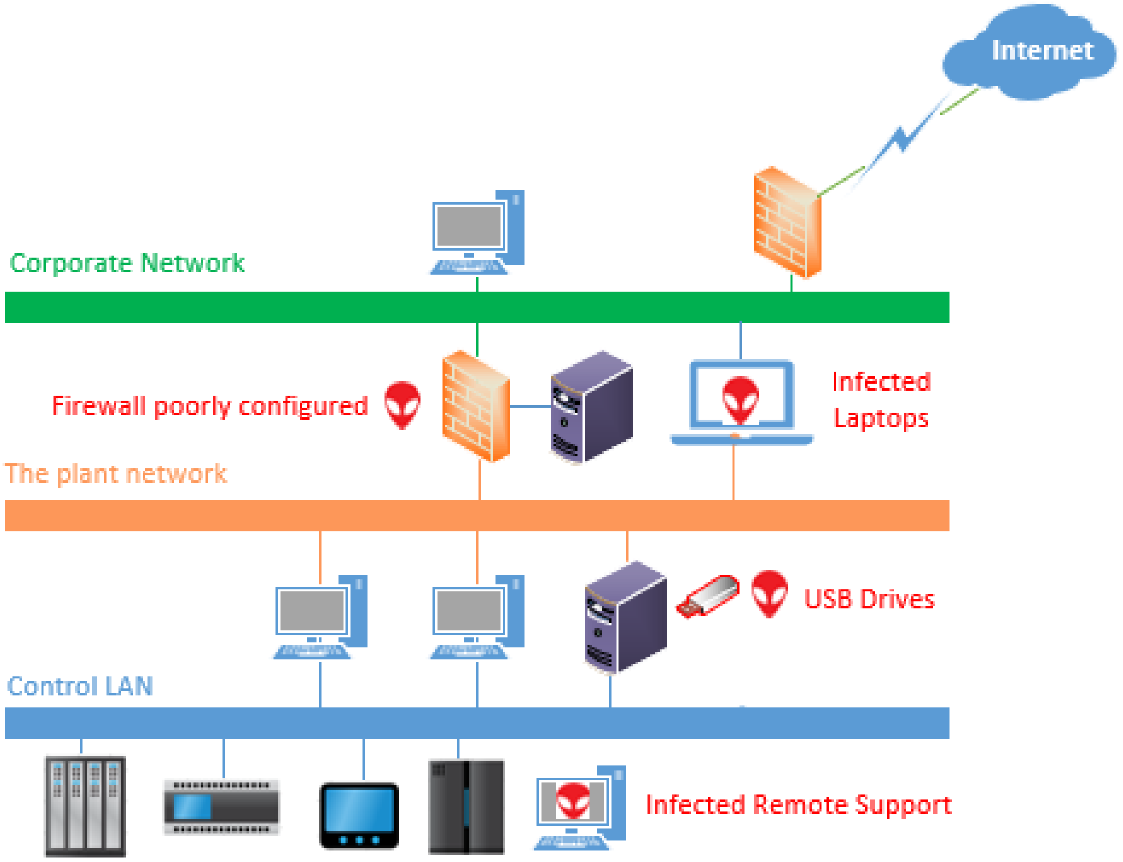
- What is Machine Learning?
- The use of Machine Learning in ICS Cybersecurity
- Using Machine Learning to Protect a Natural Gas Plant

Why security solutions fail?

- One popular solution used in ICS Cybersecurity is to install a firewall between business and control networks.
- Known as “**Bastion Model**” since it is based on a single point of security.
- Example: Chinese Wall

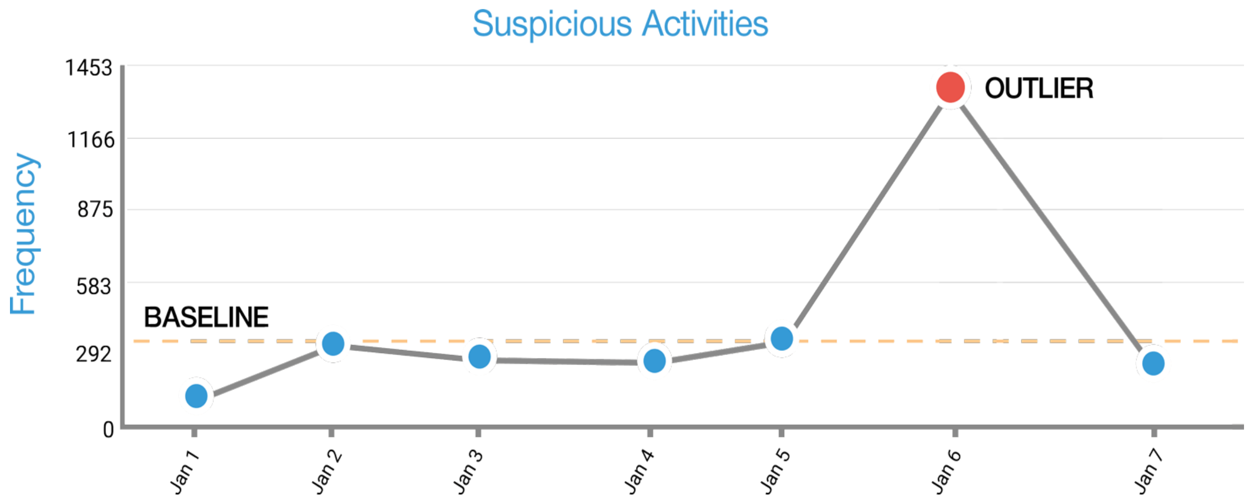
Pathways inside the control network

- Protecting only the perimeter of the OT network is not enough.
- A Worm infiltrated in:
  - A nuclear plant through a mobile 3G connection
  - A SCADA power system through a VPN
  - An Oil & Gas control system through the laptop of an outsourcer
- There were firewalls protecting the OT network perimeter in all these cases.
- It's necessary to protect the factory floor with modern and in-depth defense technologies.



What is Machine Learning?

- Machine learning is a method of data analysis that automates the construction of analytical models.
- It is an artificial intelligence strand that is based on the idea that systems can learn from data, identify patterns and make decisions with the least human intervention.
- It was born of pattern recognition and the theory that machines can learn without being programmed to perform specific tasks.
- The iterative aspect of machine learning is important because, as models are exposed to new data, they can adapt independently. They learn from previous calculations to produce reliable, repeatable decisions and results.

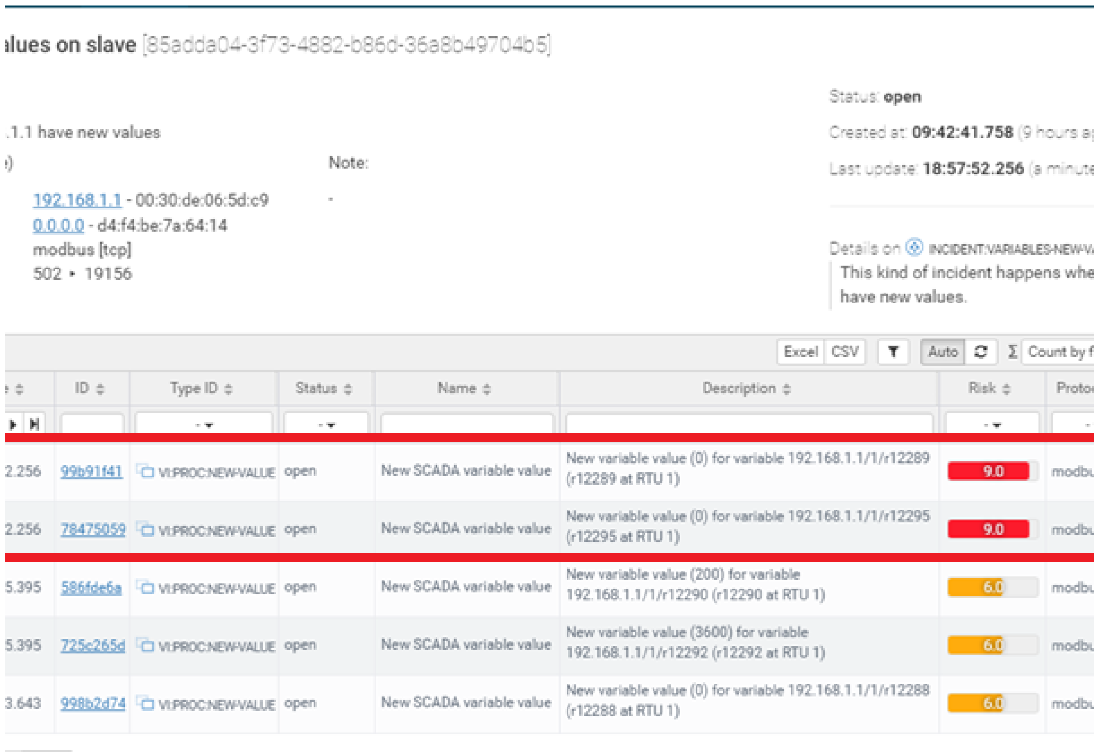


Where is Machine Learning used?

- Here are some well-known examples of machine learning applications:
  - Autonomous Google cars: the essence of machine learning;
  - Suggested offers such as Amazon and Netflix: daily machine learning applications;
  - Know what your customers are talking about you on Twitter: Machine learning associated with creating language rules;
  - Detection of undue behavior of equipment in automation systems (ICS): machine learning applied to industrial cyber security;

The use of Machine Learning in ICS Cybersecurity

- Machine Learning technology is implemented in the **Nozomi SCADA Guardian** solution, specific for ICS Cybersecurity
  - Detects cyber threats and process anomalies, providing unprecedented operational visibility.
  - Automatically discovers the industrial network assets, including its components, connections and topology.
  - Develops security and process profiles, as well as monitoring the system in real time for any change.



alues on slave [85adda04-3f73-4882-b86d-36a8b49704b5]

.1.1 have new values

)

192.168.1.1 - 00:30:de:06:5d:c9
0.0.0.0 - d4:f4:be:7a:64:14
modbus [tcp]
502 • 19156

Note:
-

Status: **open**
Created at: **09:42:41.758** (9 hours a
Last update: **18:57:52.256** (a minute

Details on INCIDENT:VARIABLES-NEW-V
This kind of incident happens whe
have new values.

e	ID	Type ID	Status	Name	Description	Risk	Proto
2.256	99b91f41	VI:PROC:NEW-VALUE	open	New SCADA variable value	New variable value (0) for variable 192.168.1.1/1/r12289 (r12289 at RTU 1)	9.0	modbu
2.256	78475059	VI:PROC:NEW-VALUE	open	New SCADA variable value	New variable value (0) for variable 192.168.1.1/1/r12295 (r12295 at RTU 1)	9.0	modbu
5.395	586fde6a	VI:PROC:NEW-VALUE	open	New SCADA variable value	New variable value (200) for variable 192.168.1.1/1/r12290 (r12290 at RTU 1)	6.0	modbu
5.395	725c265d	VI:PROC:NEW-VALUE	open	New SCADA variable value	New variable value (3600) for variable 192.168.1.1/1/r12292 (r12292 at RTU 1)	6.0	modbu
3.643	998b2d74	VI:PROC:NEW-VALUE	open	New SCADA variable value	New variable value (0) for variable 192.168.1.1/1/r12288 (r12288 at RTU 1)	6.0	modbu

Using Machine Learning to Protect a Natural Gas Plant

Technical demonstration that shows how Machine Learning technology can be applied in ICS Cybersecurity.

Check video at https://www.youtube.com/watch?v=j5k9CHI7K-Q

How will your company respond to an attack like this?

Are there cyber security specialists in the automation team?

Is your company's automation network really protected?

Thank You!

marcelo@tisafe.com

Want to know more, see Machine Learning live in our stand at Digital Factory.

Visit us: Hall 6, Stand C09

1–5 April 2019 • Hannover • Germany