Using AI for OT Security

InnoTech summit

Ilan Barda

Taiwan, August 2018

Securing the Operational Networks

Definitions

OT (operational technology) is hardware and software that detects or causes a change, through the direct monitoring and/or control of physical devices, processes and events.

OT security is the process, technology and services used to secure industrial (and commercial) automation and control systems as a life cycle to create a safe and resilient environment for physical devices, processes and events.

5

Gartner

radiflow
Secure your Assets

About Radiflow

Empower users to maintain visibility and control of their operational network in the Industrial IoT era

- Focus on OT Security since 2014
- Tier-1 customers and partners
- Validation by 3rd-party labs

Recent success-stories


Case Study

Case Study:
Midwestern Electric Utility Deployment

The Challenge

Several requirements needed to be met to support the network project:

- Mechanism to control and monitor access to sub-station assets, according to NERC CIP v6 requirements
- Mechanism for creating specific firewall rules at BES Asset Boundaries for a variety of substation topologies, as per new CIP requirements
- Compliance with upcoming NERC CIP requirements for transient assets
- Serial connectivity, which is still required at several substations for legacy applications


SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS
Subscribe (Free) | CISO Forum 20

Home › SCADA / ICS

Cryptocurrency Mining Malware Hits Monitoring Systems at European Water Utility

By Mike Lennon on February 08, 2018

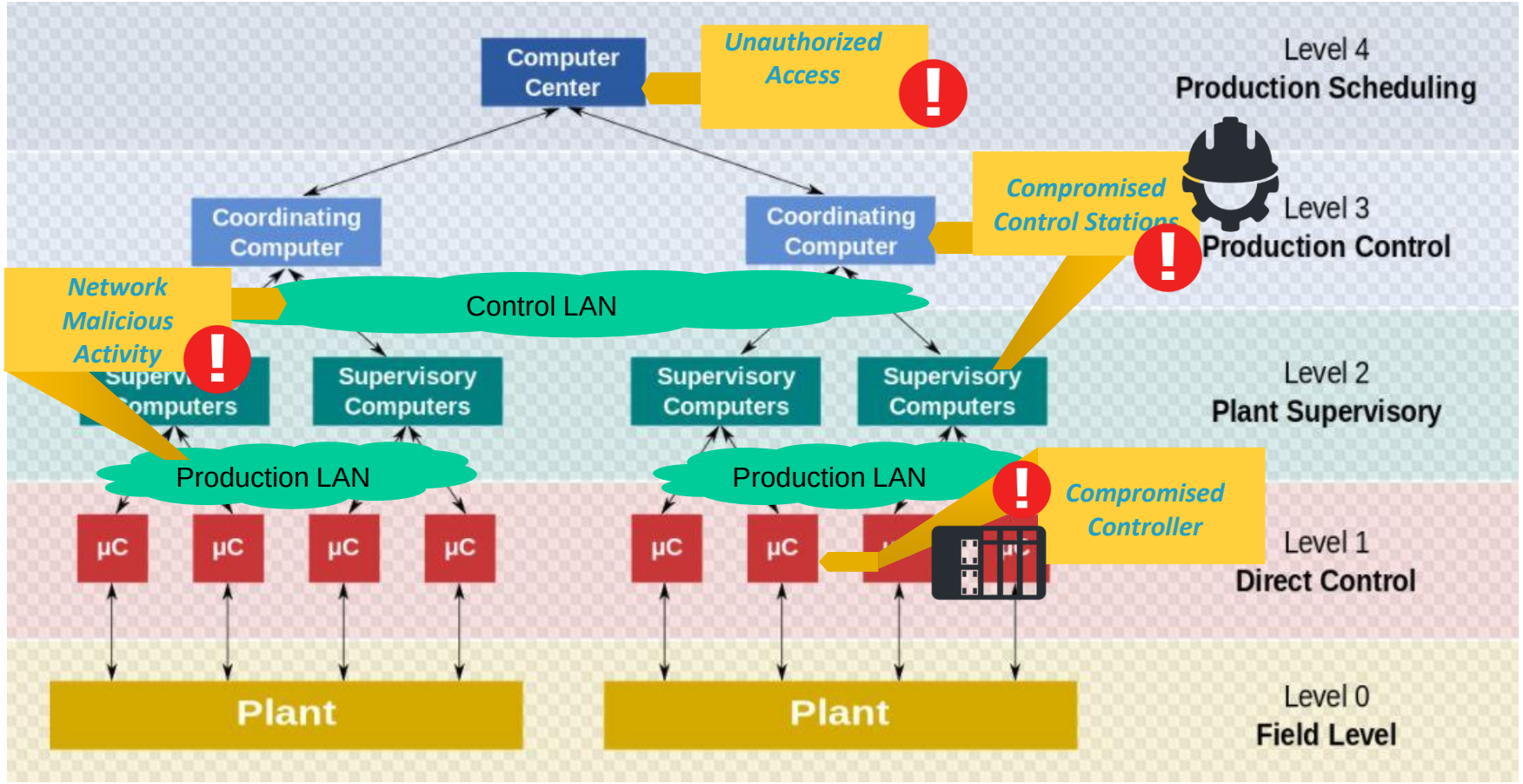
Share G+ Tweet Recommend 31 RSS

Malware Chewed Up CPU of HMI at Wastewater Facility

Cryptocurrency mining malware worked its way onto four servers connected to an operational technology (OT) network at a wastewater facility in Europe, industrial cybersecurity firm Radiflow told *SecurityWeek* Wednesday.

radiflow
Secure your Assets

Security Vulnerabilities in an Industrial Network

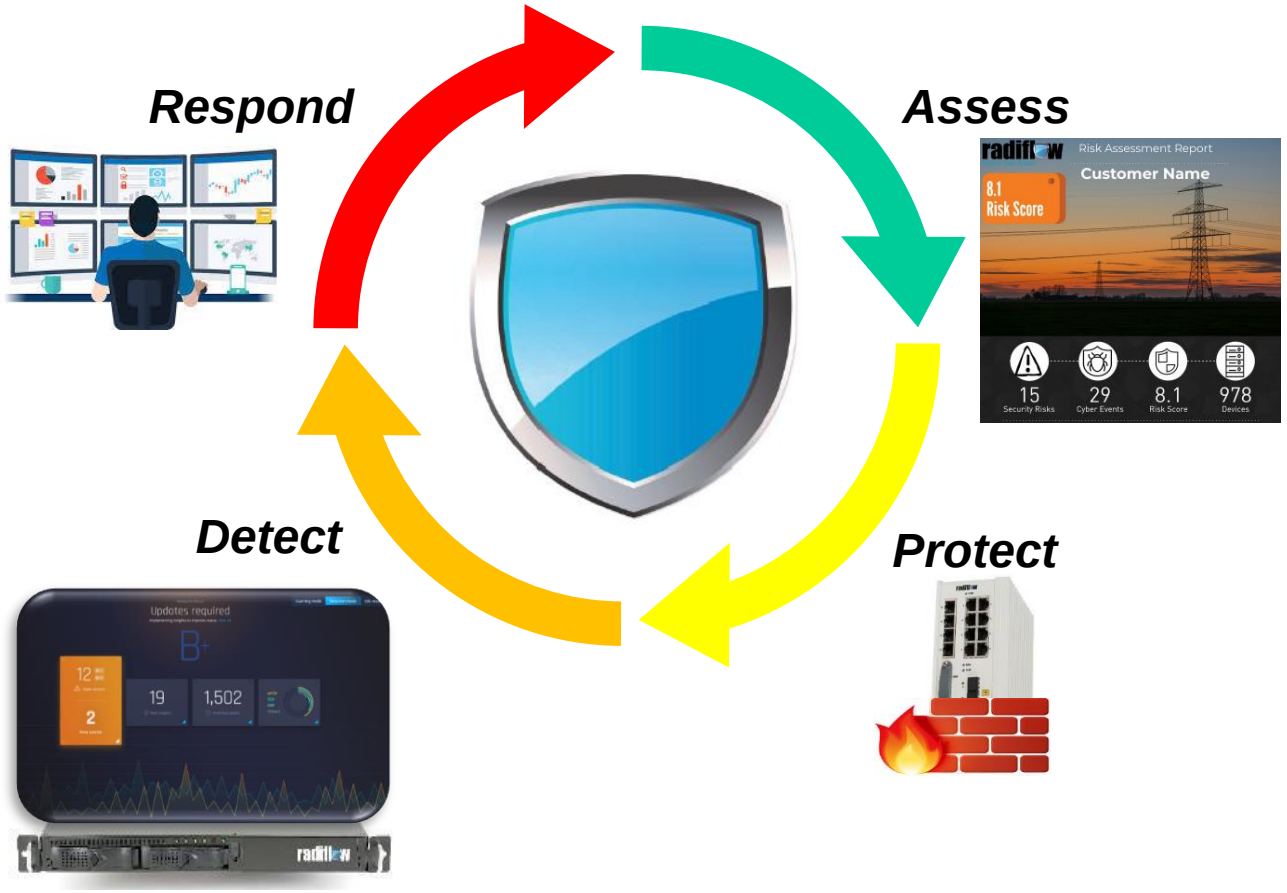


radiflow
Secure your Assets

Differences between IT and OT

Attribute	IT Systems	OT Systems
C- Confidentiality	High	Most cases - Low
I - Integrity	Low-Medium	Very High
A - Availability	Medium	Very High
Authentication	Medium to High	High
System Lifetime	3-5 years	10-15 Years
Typically Utilized OS	Windows/Linux	Windows/Linux/Embedded
Security patching	Standard/Frequent	Strongly Tested/Rare

Target – Ease the deployment of OT Security (1)



radiflow
Secure your Assets

Target – Ease the deployment of OT Security (2)

Op Center HMI

Security Center

- **Asset Inventory**
- **Risk mapping**
- **Anomaly detection**

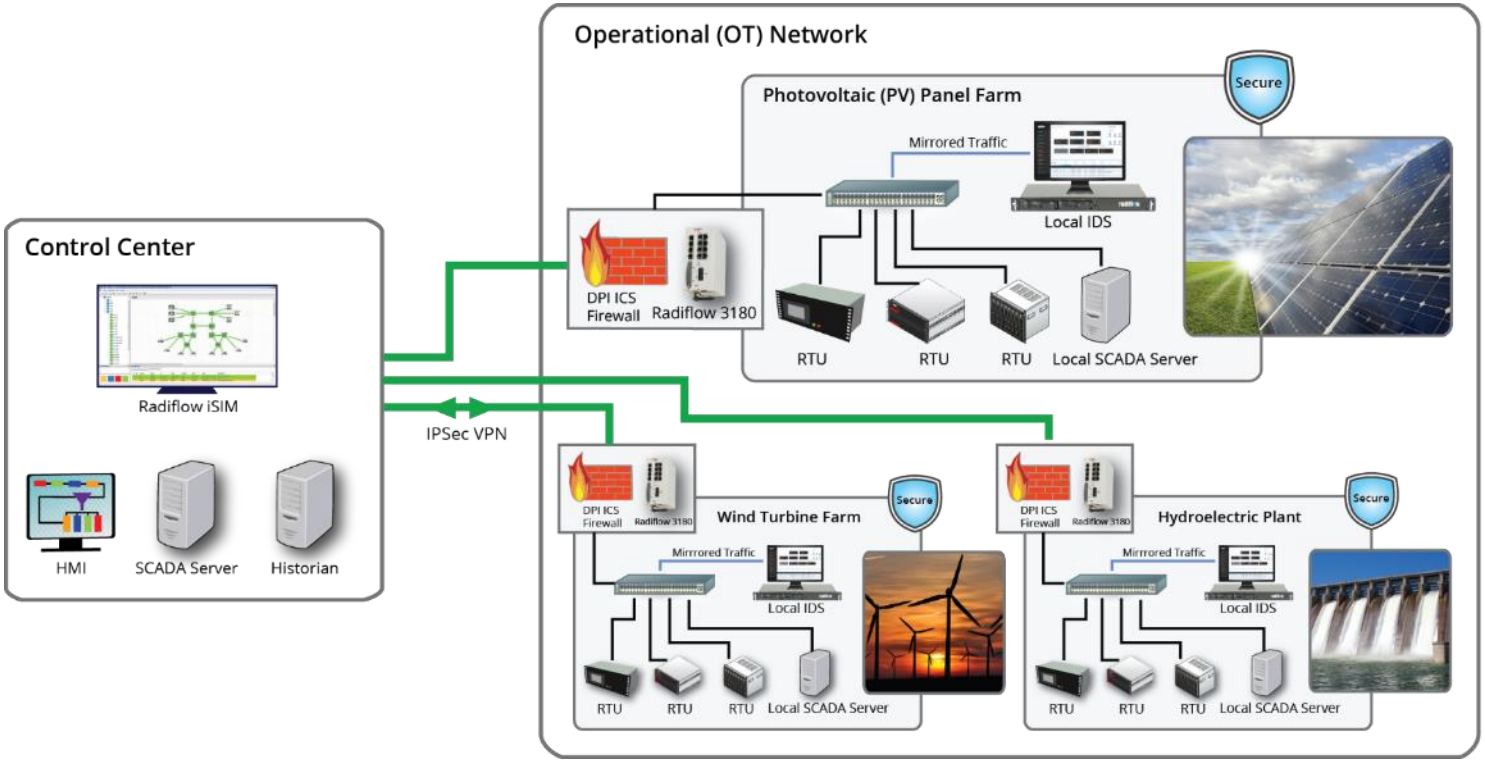
Network Firewalls

Smart Probes

radiflow
Secure your Assets

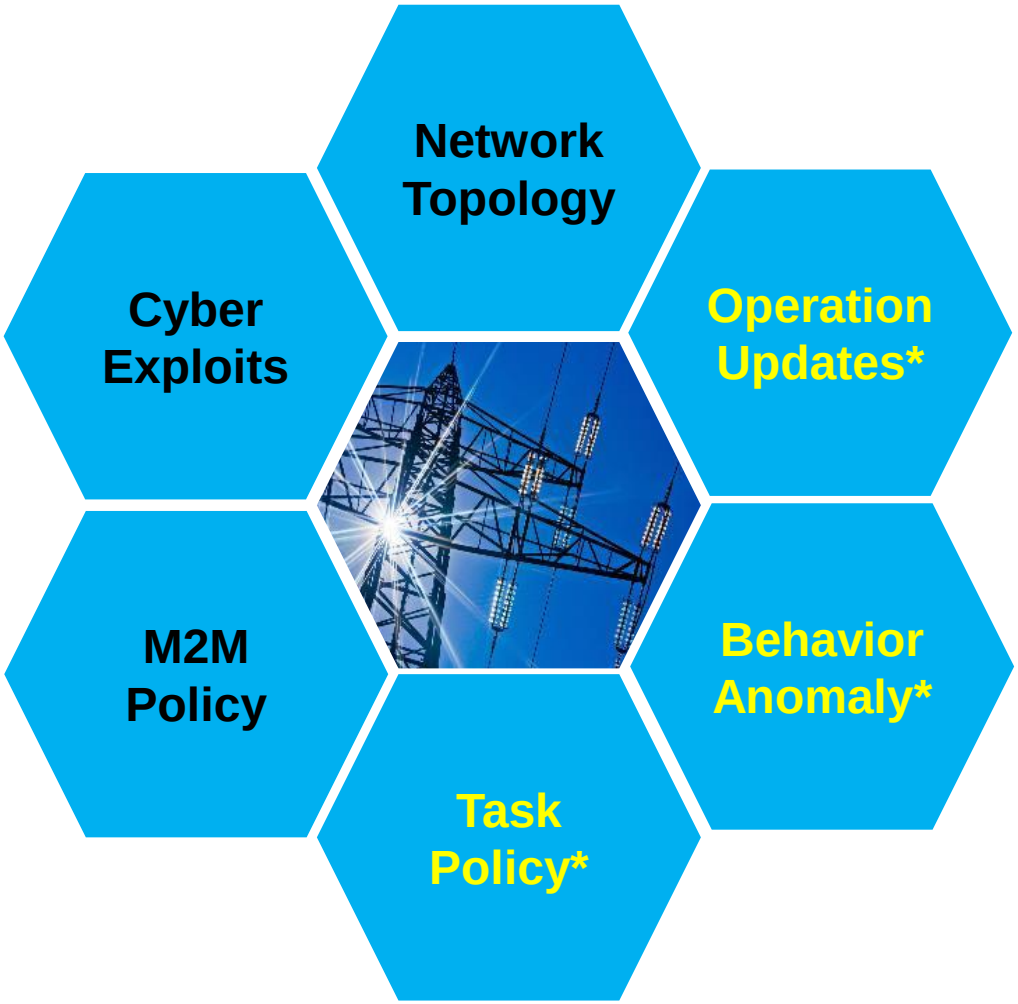
Case study – Securing Renewable power plants

- Site Threat Detection
- Secure remote access
- Integration with SCADA/SIEM



radiflow
Secure your Assets

OT Security Engines



*** AI Potential**

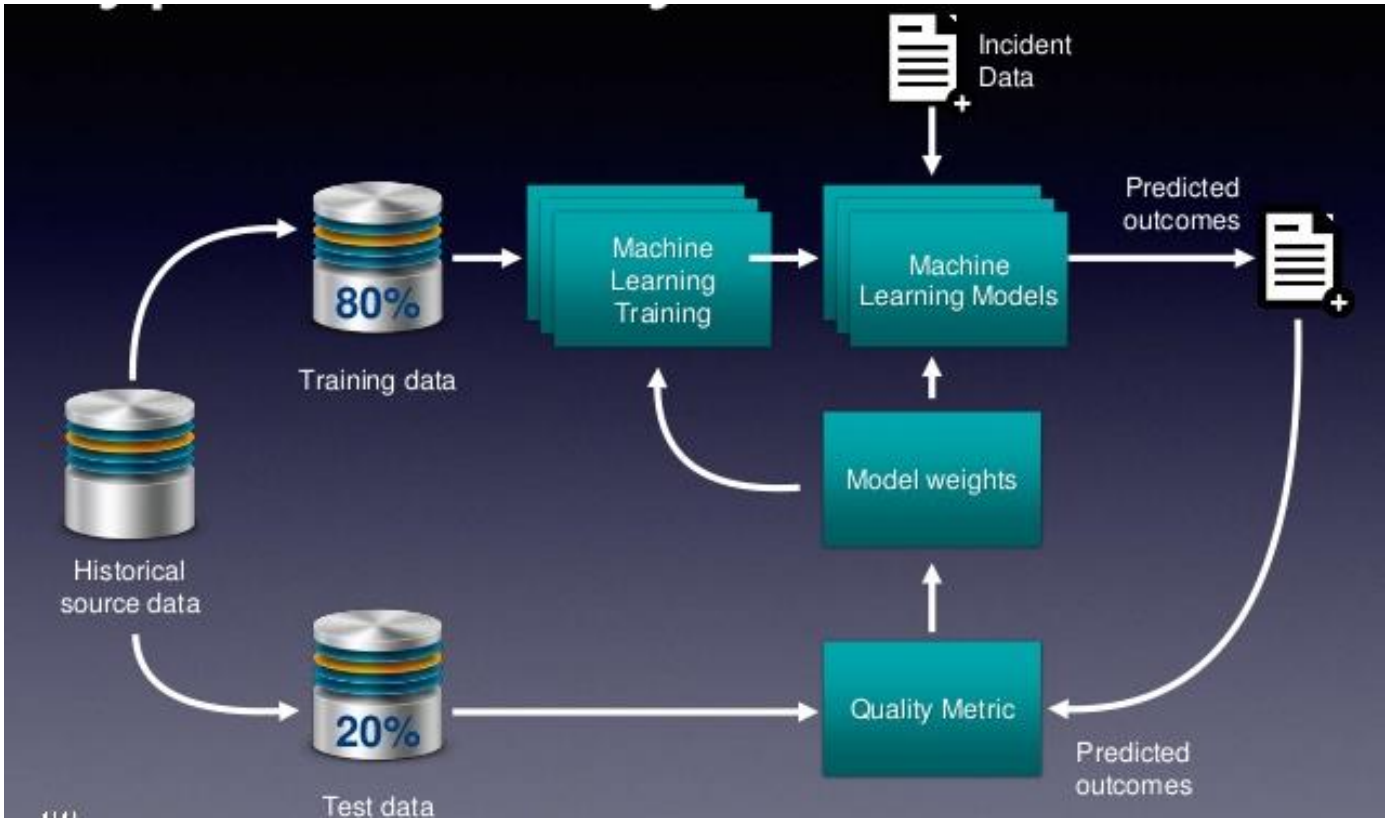
radiflow
Secure your Assets

What is AI

AI is technology that appears to emulate human analytics performance by learning, processing complex data and reaching its own conclusions

radiflow
Secure your Assets

AI Machine Learning Overview



Source: CFML

Status of AI today

Source: XKCD

The challenge for using AI in Security systems is not around the algorithms implementation but rather about applying them with a high degree of confidence

AI in OT Security – Issues to consider

- Value of AI for Industrial Networks
- Explaining the AI results
- Industrial Data for training AI Engines

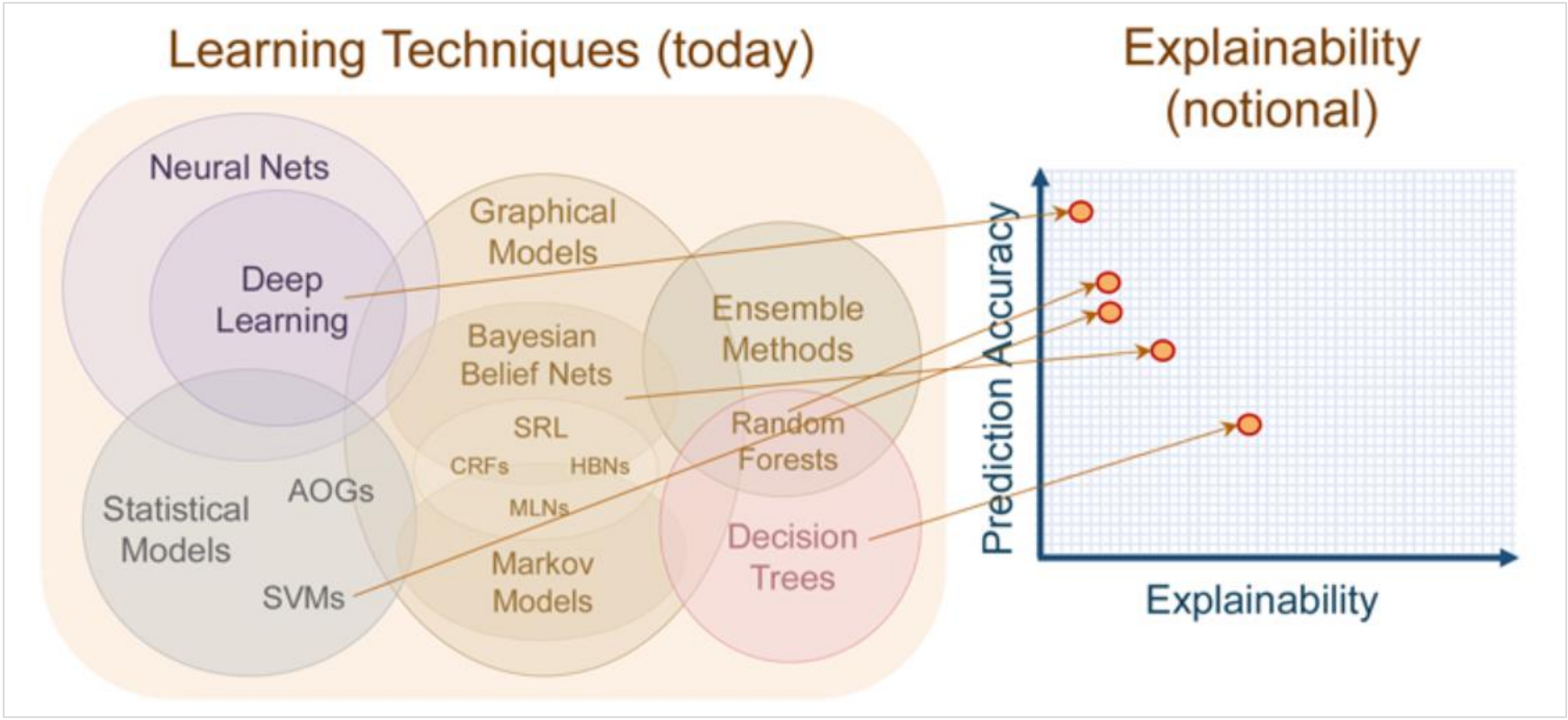
radiflow
Secure your Assets

Use-cases for AI in OT Security

- M2M sessions
  - OT Assets
    - Well-defined behavior → Rule-based Policy monitoring
    - Many vendors, Types & Protocols → AI for modeling
  - OT Processes – Many variations → AI for modeling?
    - Multiple sources of information – Sensors, Network, Servers
    - Process Anomaly alarms should be explainable

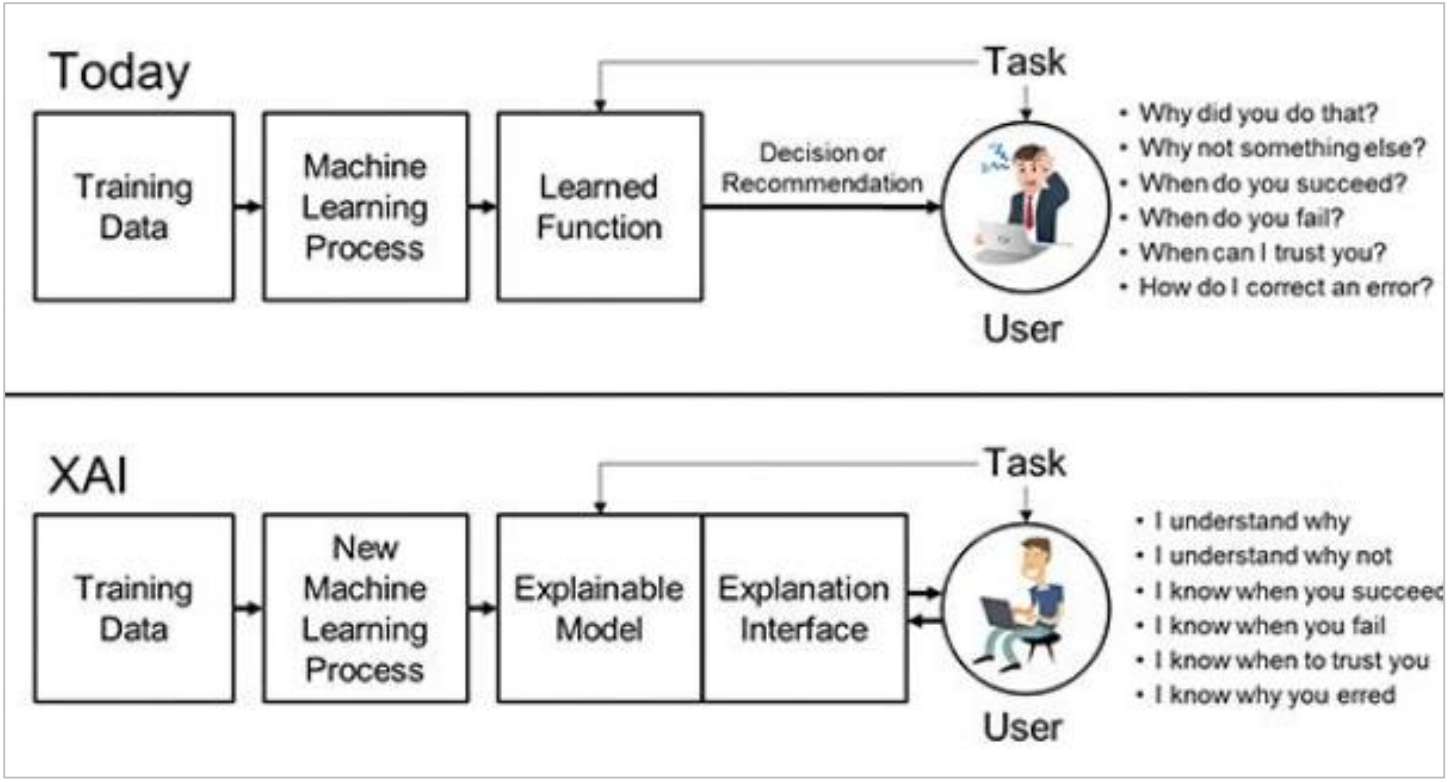
- H2M sessions
  - Restricted access → Rule-based task monitoring
  - Malicious actors → AI for Behavioral analysis?
  - Firmware & Logic updates → AI for impact analysis?

Status of AI Explainability



Source: DARPA

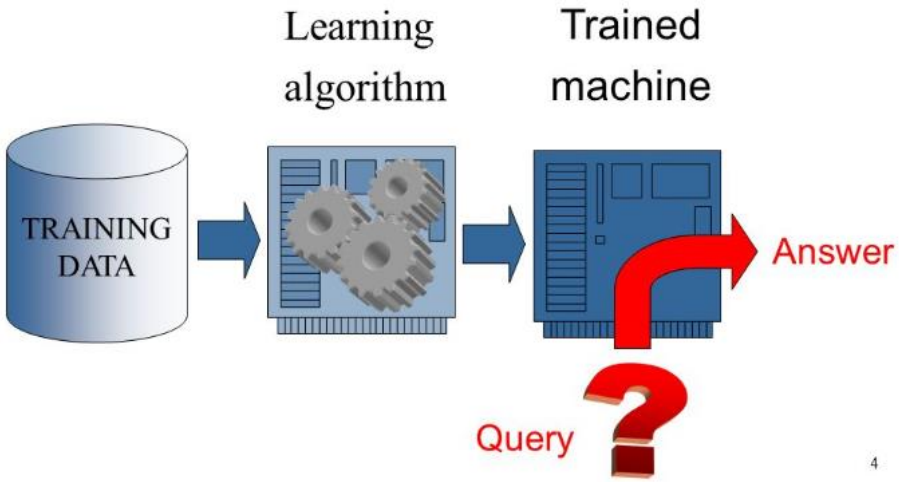
XAI model



Source: DARPA

Training Data for ML

- Effective ML algorithms require high amount of training data
- Such data is not easily-available for OT networks
  - Collecting such data requires the customer approval
  - Structuring the data requires the operator support



radiflow
Secure your Assets

AI in OT Security – Recommended Roadmap

- Current Use of AI
  - Automation – Parse new protocols and new types of devices
- Future Use of AI
  - Gather Data for Training AI algorithms
  - Decouple explainability from ML models

THANK YOU

For more details:
ilan_b@radiflow.com
www.radiflow.com