Industrial Cyber Security

DIGITAL TRUST CHALLENGE LAUNCH EVENT

FINLANDIA HALL, HELSINKI

INSTA

Henry Haverinen, 12 March 2020

ABOUT THE SPEAKER

- Dr. Henry Haverinen
- Cyber security leader who looks for the opportunity in every threat
- Fellow, Senior cyber security leader at Insta
- Cyber security architect, secure development lifecycle lead, technical product manager
- Connect with me on LinkedIn at https://www.linkedin.com/in/henryhaverinen/

AGENDA

- Cyber security challenges in industrial software powered solutions
- Differences between IT and OT security
- Two solution examples

Let’s calibrate our intuition for industrial cyber security

TYPICAL IMPORTANCE OF CIA TRIANGLE ELEMENTS

IT SECURITY

Confidentialty:	High
Data Integrity:	Medium
Availability:	Medium

OT SECURITY

Confidentialty:	Low
Data Integrity:	Very High
Availability:	Critical

STANDARDS

IT SECURITY

ISO 27001 Series

OT SECURITY

IEC 62443

ACCEPTABLE DOWNTIME

IT SECURITY

Often tolerated,
especially when maintenance
has been planned

OT SECURITY

Not acceptable,
or acceptable only during
infrequent maintenance windows

IMPORTANCE OF REAL TIME OPERATION

IT
SECURITY

Low

OT
SECURITY

Critical

RELEVANCE TO HUMAN OR ENVIRONMENTAL SAFETY

IT
SECURITY

Low

OT
SECURITY

High-Critical

SYSTEM LIFE CYCLE

IT SECURITY

Up to 5 years

OT SECURITY

Up to 25 years

AWARENESS AND SECURITY KNOWLEDGE

IT SECURITY

Usually OK

OT SECURITY

Varies a lot, often not good

ECOSYSTEM COMPLEXITY

IT SECURITY

Enterprise IT department is typically in control of suppliers.

OT SECURITY

Need to coordinate between customer IT, customer OT, vendor IT and vendor OT.

Multi-vendor systems

SCOPE OF SYSTEMS THAT NEED PROTECTION

IT SECURITY

Fixed and small number of systems

OT SECURITY

An industrial supplier may need to protect hundreds of new customer deliveries every year

SYSTEM OWNER'S SECURITY BUDGET

IT SECURITY

Usually planned based on risk

OT SECURITY

Often non-existent

CYBER SECURITY CHALLENGES IN INDUSTRIAL SOFTWARE-POWERED SOLUTIONS

Business challenges

How to enable cloud, mobile, analytics, remote operations?

How to gain competitive edge?

How to meet the increasing customer and compliance requirements in sales phase?

How to provide new profitable cyber security lifecycle services?

R&D challenges

How to save time and money by NOT having to build cyber security from scratch?

How to simplify cyber security in R&D?

Which cyber security technology has flexible enough licensing?

Underlying deeper challenges

How to achieve peace of mind that risks have truly been managed?

How to make the ethically right choices?

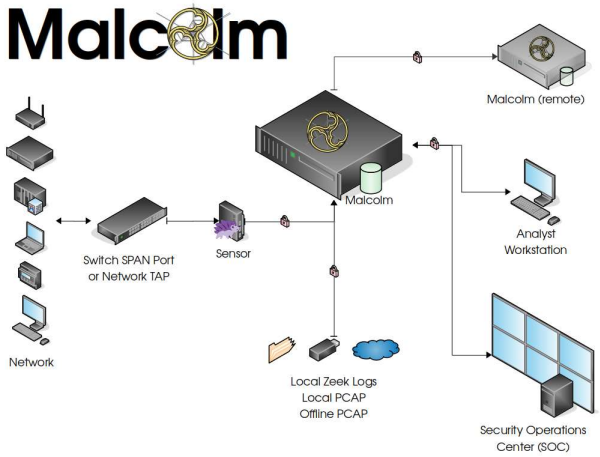
How to reduce stress?

Tackling these challenges

EXAMPLE SOLUTION:

OPEN SOURCE MALCOLM NETWORK TRAFFIC ANALYSIS TOOL SUITE

- Idaho National Laboratory of the U.S. Department of Energy has **integrated** a suite of **open source** network traffic analysis tools into an **easily deployable** package

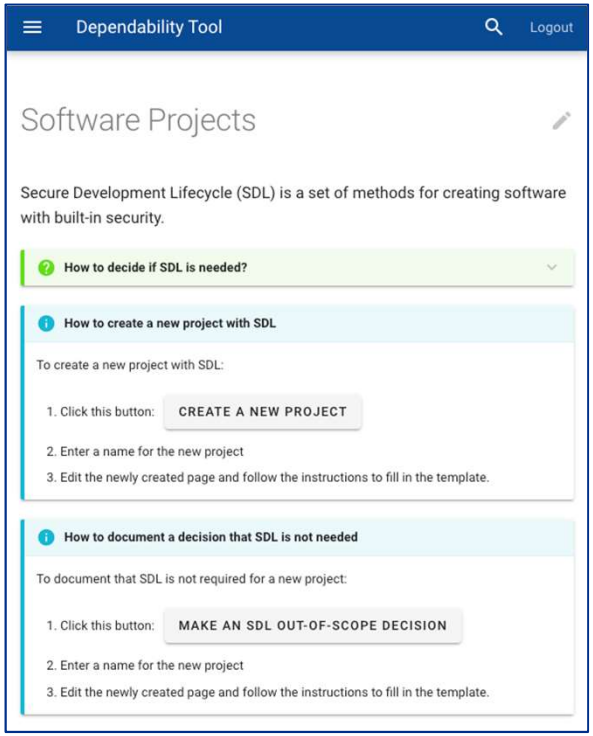


Source: https://github.com/idaholab/Malcolm

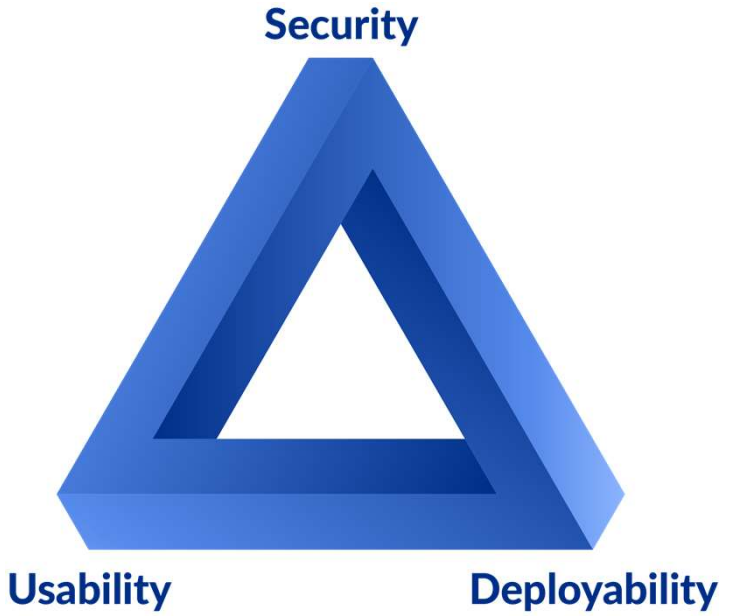
EXAMPLE SOLUTION:

AUTOMATING EXPERT KNOWLEDGE WITH INSTA'S SECURE SOFTWARE ENGINEERING SOLUTION

- Insta has **integrated** a secure software engineering solution that packages **IEC 62443 based** process blueprints, document templates, tasks and dashboards into an **easily deployable** web application
- The solution speeds up and **simplifies** the adoption of a secure software engineering process significantly



COMPLEX ENVIRONMENT CALLS FOR SIMPLE SOLUTIONS



ASOKAN'S TRIANGLE


INSTA
insta.fi
LUPA LUOTTAA