IEC 62443: Using ntopng for creating a Software Defined Factory

Giacomo Tontini
(VEM Sistemi S.p.a.)
Agenda

• IEC 62443
• Sd-factorii
  • Basic concepts
  • Architecture
  • Ntopng integration
  • What’s next
IEC 62443

- A set of international standards for the security of industrial automation and control systems (IACS)
- Risk-based framework that helps organizations identify, assess, and mitigate cyber security risks
- Widely recognized as the leading standard for IACS security
- Flexible and scalable
- Involves a continuous process of review and update of security controls
IEC 62443

Made of four parts:

• General: This part provides an overview of the standard and defines common terms and concepts.

• Security for systems and networks: This part focuses on the technical aspects of IACS security, such as network security, device security, and security management.

• Security for components and systems engineering: This part focuses on the development and implementation of secure IACS components and systems.

• Security assessment and certification: This part provides guidance on how to assess and certify the security of IACS.
IEC 62443 – Cybersecurity within OT environment

- Identification of different security levels
- Subdivision of the various production lines into multiple isolated environments
- Segregation between environments enabled by firewall rules
OT hostilities

• OT devices are typically network endpoints whose traffic is "unknown"

• OT environments are typically offered off the shelf with the production pipeline and are not structurally governed

• IT skills necessary to manage production plants are mostly absent within organization

• Infrastructures elements are non-homogeneous and lack minimum network level requirements

• OT environments mostly lack security governance and are therefore highly vulnerable spaces
Sd-factorii fundamental
SD-Factorii
Software-Defined Factory Intelligent Infrastructure

- Zero trust approach
- OT traffic learning and visibility
- Infrastructure discovery and inventory
- No IP address change upon OT devices relocation and network segmentation
- Mostly based on open-source solutions
- Microservices architecture
  Cloud native by design
Operative flow

- Discovery
- Zoning
- Host Relocation
- Contract & Policies
- Monitoring & Operation
Conceptual model: zones

- Any device connected to IT or OT network that must be collocated into a «zone»
- **Parent Zones**: represent a specific broadcast domain where originally endpoint belong.
- **Child Zone**: a new broadcast domain, separate from the other zone’s BD, where endpoints could be placed

- Parent Zone can have multiple Child Zones
- An endpoint can move from a Parent zone to one Child Zone and vice-versa.
- An endpoint can move freely from each child zone of the same Parent Zone
Endpoint and zones

Child1 zone

Child2 zone

Child3 zone
Conceptual model: contract

- Security Zone A
- Host Y
- Host X is able to communicate with Host Y, while not with Host Z
- Host X
- A and B zones are children of a parent zone C, not represented
- Security Zone B
- «contract» between A and B is needed
Contracts and policies

• Represents a communication relationship between zones

• Unique for each pair of zones and communication direction

• Contracts cannot exist between parent zones

• Each contract is made up of its atomic components called Policies

• Two types of policies: those provided by the user and those proposed by a sensor/probe

• A policy defines which traffic originating from a source zone can cross the boundaries towards a destination zone (parent zones or sister zones). Source ip / Dest IP/ Ports / Protocols
Sd-factorii architecture

Control-Hub-UI

IBC – Intent Based Controller

Device Service Switch
Device Service Firewall
MAC address table Discovery Manager
Network State Monitor
Topology Discovery Manager

MongoDB

Authentication Manager

ntop

ntopConf'23

Sept, 21-22 · Pisa
Device service

Switch device service
- Provides an abstraction layer for different switch vendor interfaces (Cisco, HP)
- Restconf and SSH as South Bound API (will support Netconf and gNMI)

Firewall device service
- Provides an abstraction layer for different firewall vendor interfaces (Fortinet, Checkpoint and Pfsense)
- REST as South Bound API and North Bound API
Topology graph
Conversation graph
Parent Zone
Children Zone
Policy adaptation (nTop)
## Alerts and remediation

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Date: 9/21/2023</td>
<td>Remediation: nothing</td>
<td>Date: 9/21/2023</td>
<td>Remediation: ignore</td>
</tr>
<tr>
<td>Date: 9/21/2023</td>
<td>Remediation: ignore</td>
<td>Date: 9/21/2023</td>
<td>Remediation: nothing</td>
</tr>
<tr>
<td>Date: 9/21/2023</td>
<td>Remediation: nothing</td>
<td>Date: 9/21/2023</td>
<td>Remediation: nothing</td>
</tr>
</tbody>
</table>

**ntopConf23**

Sept, 21-22 · Pisa
What’s next

• Multi-site/Multitenancy

• Multi-sensor distributed in crucial network nodes

• Pro-active network segmentation suggestions in compliance with IEC 62443 standard

• Pro-active remediation upon events coming from probe or third-party sources

• Visualization widget of current compliance level to IEC 62443 standard
Thank you for the attention.

giacomo.tontini@vem.com