



# Securing complex cyber/physical systems

## Clinical environments IAM case studies

(aka. "Security Policy Automation")

(aka. "let's talk better access control")

**Ulrich Lang, PhD**

Founder & CEO

# Overview

- ▶ About
  - ▶ Cyber-physical
  - ▶ Smart healthcare
  - ▶ 3 case studies, incl. IoT Security Policy Automation
  - ▶ Conclusion
- 
- ▶ Slides: [objectsecurity.com/cis2017](http://objectsecurity.com/cis2017)

# Ulrich Lang, PhD



- ▶ ObjectSecurity® CEO/founder
  - ▶ Access control & security policy automation experts since 2000
- ▶ PhD (access policies) Cambridge
- ▶ Master's Infosec
- ▶ Author, patents, ...
- ▶ OpenPMF™ co-inventor
  - ▶ powerful access policies, effortless management
  - ▶ Many verticals, incl. gov./mil., transport, police/intel, hospitals...

# Why Cyber-Physical Systems?

▶ 'co-engineered interacting networks of physical and computational components'

- ▶ Critical infrastructure foundation
- ▶ Emerging/future smart services foundation
- ▶ Improve quality of life in many areas

▶ Examples: 'Smart' city, transport, hospital, grid... IoT (IIoT!)

▶ Cybersecurity impacts physical safety!

# 'Smart' healthcare (partly IIoT)

- ▶ Why?  
improve,  
patient care  
and efficiency
  - ▶ Networked, smart, semi-autonomous devices
  - ▶ Clinical, business, building systems communicate
  - ▶ Real-time analytics, tracking etc.
  - ▶ Automation
- 
- ▶ Huge potential,  
but hospitals need better cybersecurity to be safe

# The 'top down': Hospital IAM Roadmap

## ▶ Why did we do it?

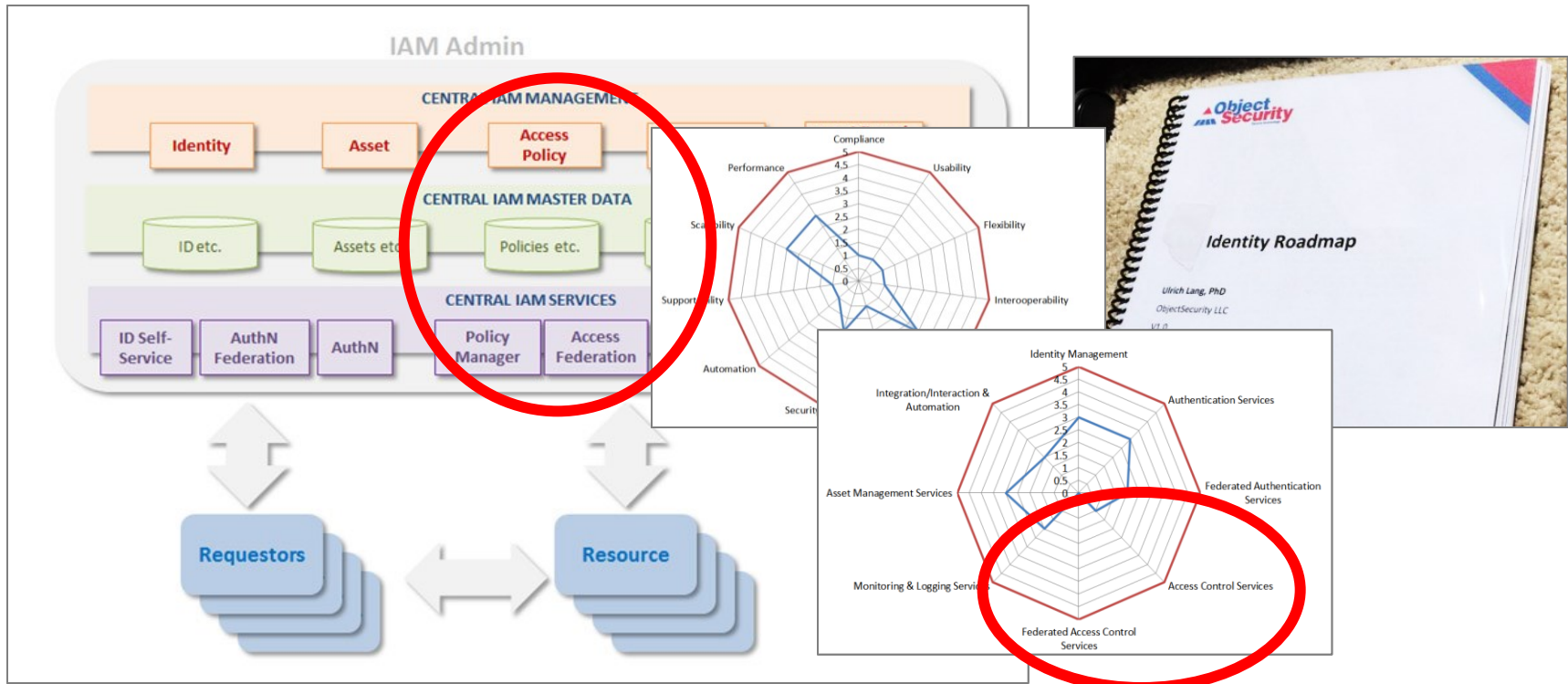
- ▶ To educate/explain need to them:

Security policy automation, fine-grained access

## ▶ Complexities

- ▶ IAM distributed (main IAM and numerous sub-IAMs)
- ▶ Custom batch processes
- ▶ Onboarding/Offboarding manual processes, limited checks
- ▶ Almost no workflow automation
- ▶ Flat network, little isolation (incl. cyber-physical)
- ▶ Fine-grained access control?  
Non-existent.

# A few weeks, 150+ pages and numerous meetings later...



The main challenges were political...

# Close-up on access control

## ▶ not good enough

- ▶ Unauthorized access: 25% → 1+
- ▶ Overprovisioned access
- ▶ Mirai, WannaCry etc.
- ▶ too simplistic: IBAC, RBAC, fragmented, siloed

## ▶ Better access control needed

- ▶ Prevent damage/fines: HIPAA \$4.8M
- ▶ Enable “smart business”: \$8.5M

## ▶ Attribute based Access Control

- ▶ part of solution (70% in 2020; Gartner)
- ▶ often too hard to: **1** manage/author **2** implement & integrate **3** audit

RBAC → ABAC

*“Nurses can only access medical records of patients*

+

...whose current **treating physician** is the **same physician** who the **nurse** is currently assigned to assist, and only if the **nurse** is currently badged into the same **physical building** as the one the **patient** is”

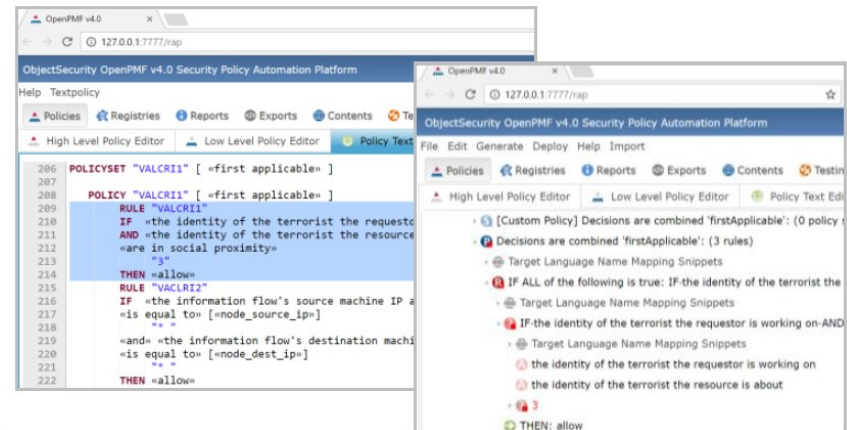
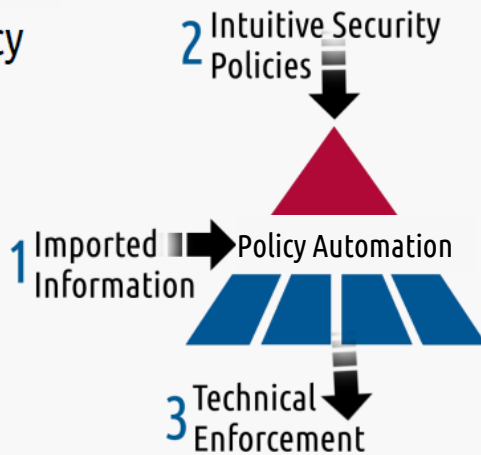


# Close-up on security policy automation (aka MDS)

- ▶ powerful security policies
- ▶ intuitive, generic to author
- ▶ effortless to manage
- ▶ consistent, testable

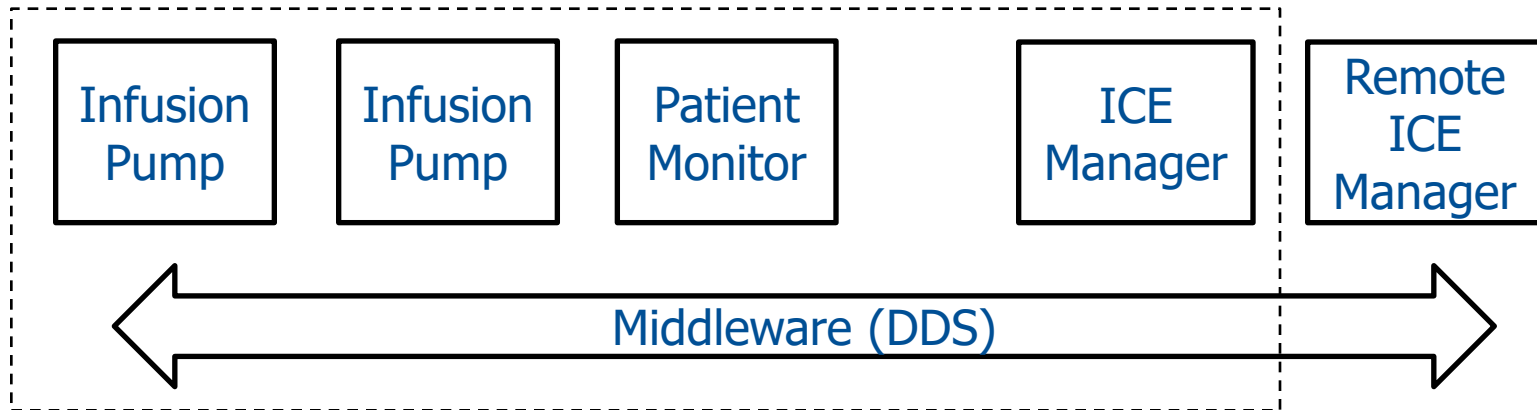


How security policy automation works:



# IIoT: Smart ICE

(DARPA SBIR subcontract for RTI)

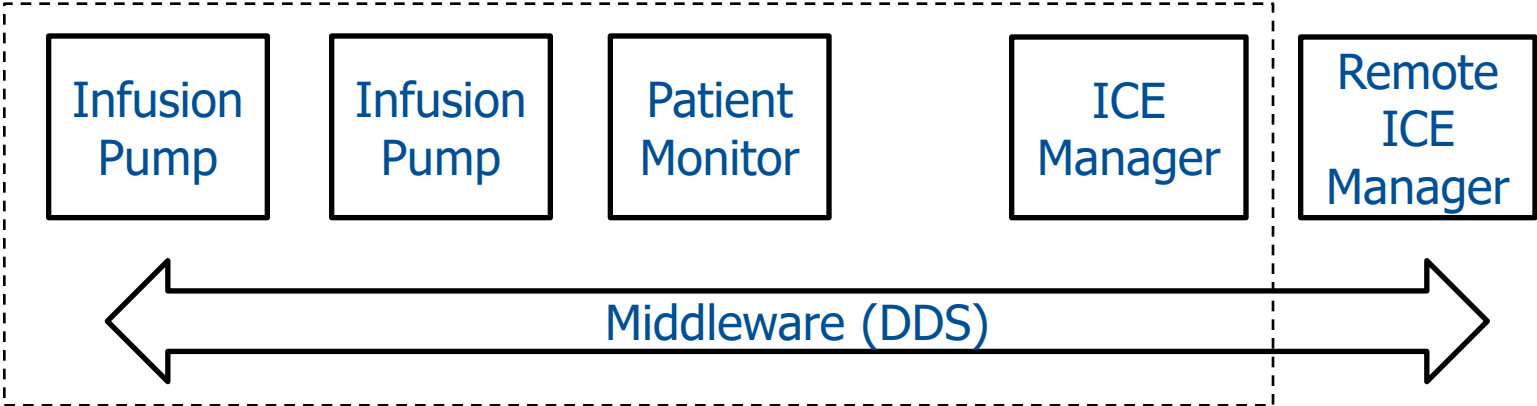


# IIoT: Smart ICE

(DARPA SBIR subcontract for RTI)

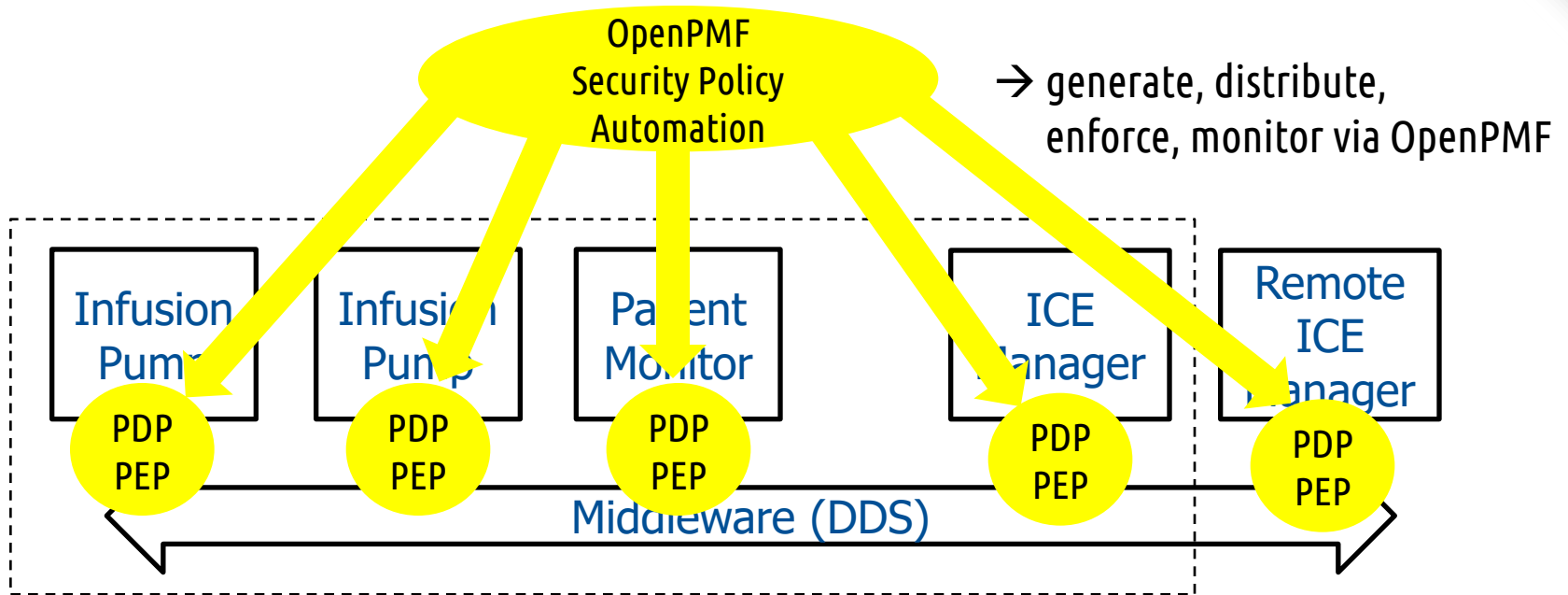
OpenPMF  
Security Policy  
Automation

→ author, test, document



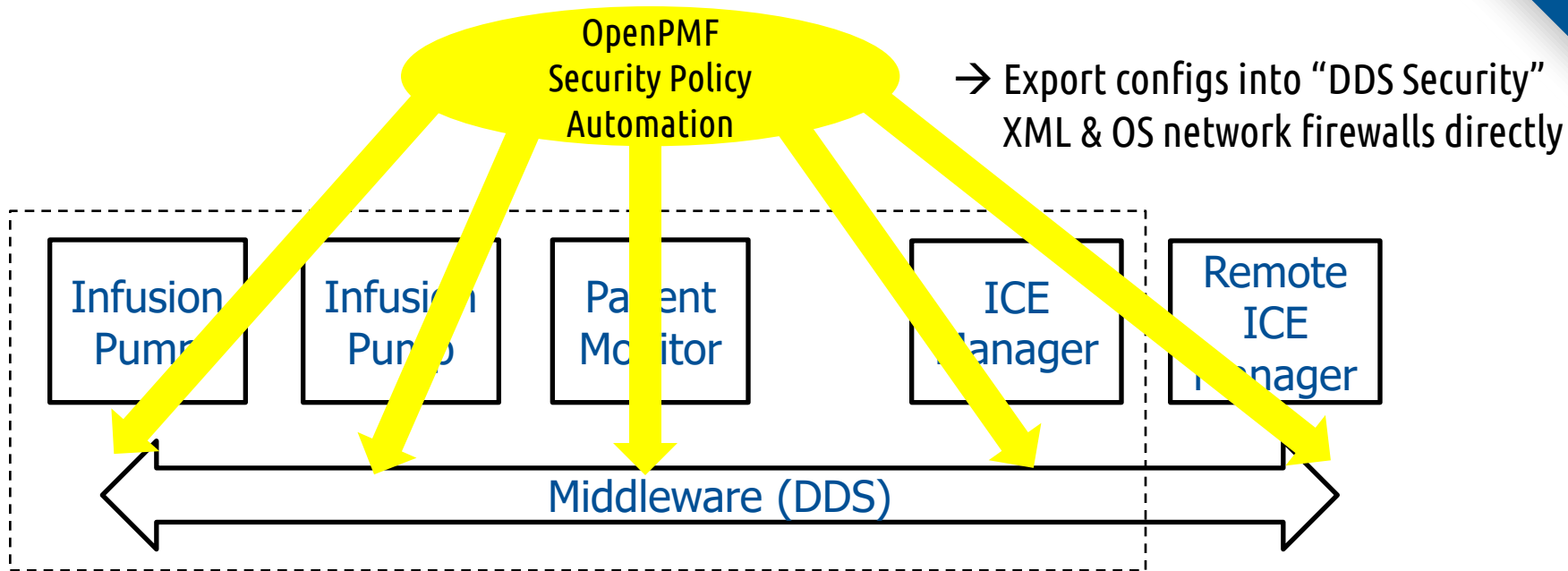
# IIoT: Smart ICE

(DARPA SBIR subcontract for RTI)



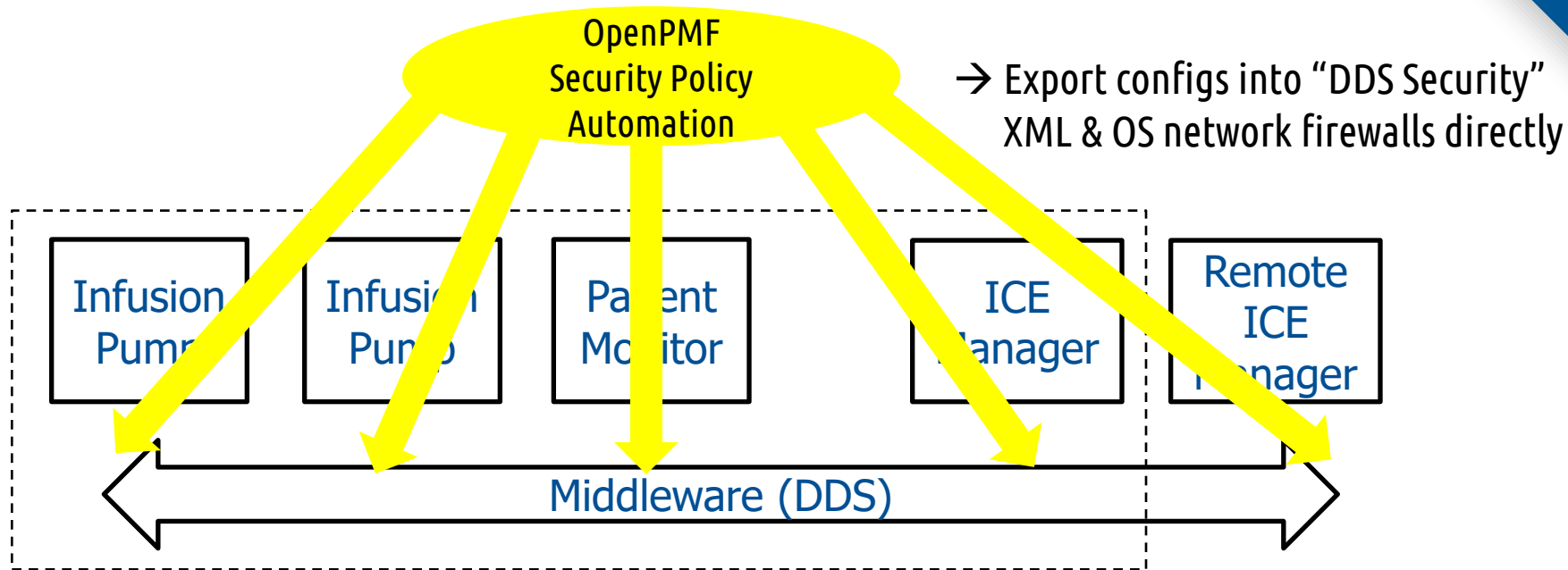
# IIoT: Smart ICE

(DARPA SBIR subcontract for RTI)



# IIoT: Smart ICE

(DARPA SBIR subcontract for RTI)



## Challenges in this SBIR scenario:

- ▶ process to determine policy?
- ▶ dynamic changes (devices move around)
- ▶ HIPAA
- ▶ How to wrap legacy devices
- ▶ seL4 microkernel
- ▶ manually specified application ‘model’ for security policy automation



# Smart operating room

## OpenICE DHP SBIR (subcontract for RTI)



- ▶ Continue “case study 2” work
- ▶ Integrate into OpenICE
- ▶ ‘Real’ access policies, data, apps
- ▶ formal policy testing, automatic detection and ingestion →



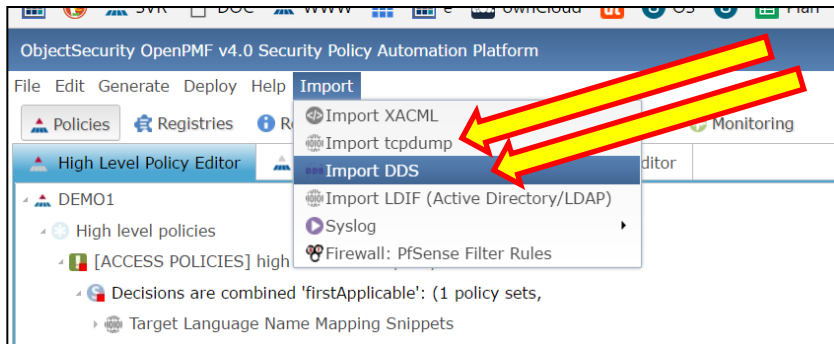
# Feature examples:



# SBIR PI/II work

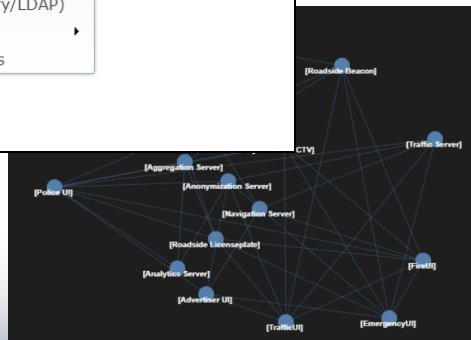
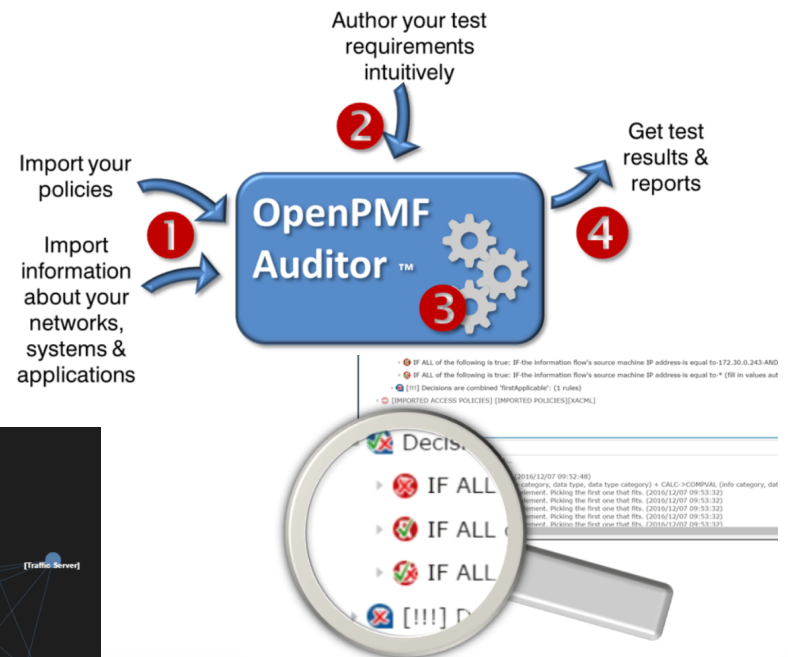
## Ingestion

- ▶ Import + smart merge traffic (net + DDS etc., also from NetPEPs)
- ▶ Import existing IdM
- ▶ Import existing policies



## Formal Testing

- ▶ Based on NIST ACPT
- ▶ Symbolic model checking



info@objectsecurity.com  
 www.objectsecurity.com  
**CONFIDENTIAL**

# Conclusion

- ▶ Security policy automation
  - ▶ Powerful technical security policy implementation...
  - ▶ users, devices, applications etc. → not just users
  - ▶ ..while easy to manage (intuitive policies, round-tripping)
  - ▶ consistent, testable, documented, robust, repeatable, ...
- ▶ Cyber-physical systems (IIoT) → great use-case
- ▶ Currently customers need education/understanding
  - ▶ consulting/integration partners needed
- ▶ The industry needs to move this way, we cannot manually manage technical policies for cyber-physical IIoT

© 2000-2017 ObjectSecurity Ltd. All rights reserved.

This entire document is copyright protected and may not be published in any form in other works without expressly written permission from ObjectSecurity Ltd. This document contains commercially confidential information and therefore this document does not constitute public disclosure (for patenting purposes). This is not a public document. Any distribution or exploitation without permission will be considered breach of contract.

**No re-selling permitted without prior explicit permission. No patenting of any of any of the described aspects permitted.**

Intellectual property: This document describes internals of OpenPMF, which are the intellectual property (background IPR) of ObjectSecurity Ltd., for which patents are pending. ObjectSecurity is the inventor of several of the described concepts, and any exploitation of these without permission will be considered as infringement of ObjectSecurity's legal rights.

Copyright, author rights, trademarks and other intellectual property rights: Some names are protected by trademarks which are the property of ObjectSecurity Ltd. or other third parties whether a specific mention in that respect is made or not. In particular (but not limited to): The ObjectSecurity logo, ObjectSecurity, the OpenPMF logo, OpenPMF, the ObjectWall logo, ObjectWall, TrustWand, the TrustWand Logo, SecureMDA, the SecureMDA logo, TrustedSOA, the TrustedSOA logo, SecureMiddleware, the SecureMiddleware logo, Security Management Ecosystem, SimulateWorld, and the SimulateWorld logo are trademarks or registered trademarks of ObjectSecurity.

This document and its contents are protected by copyright, author rights and/or other intellectual property rights which are the property of OBJECTSECURITY or third parties. Reproduction and use of the materials (or any information incorporated thereto such as but not limited to articles, graphical images, pictures, diagrams, video materials...) published in this document are hereby authorized provided that :

- (a) reproduction and use are solely for informational and non commercial use within your organisation in support of your better knowledge of Model Driven Security; and
- (b) any reproduction retains all original notices including proprietary or copyright notices ; and
- (c) materials are not modified, in whole or in part, in any way whatsoever.

No other use of the materials and of any information incorporated thereto is hereby authorized.

All concepts described may be protected by one or more patents or pending applications.

No part of this document may be reproduced in any form by any means without prior written authorisation of ObjectSecurity Ltd.

#### **Disclaimers**

This document is provided for general information only and should not be relied upon or used as the basis for making any transactions of any kind whatsoever.

All the information and any part thereof provided in this document are provided « AS IS » without warranty of any kind either expressed or implied including, without limitation, warranties of merchantability, fitness for a particular purpose or non infringement of intellectual property rights.

OBJECTSECURITY makes no representations or warranties as to the accuracy or completeness of any materials and information incorporated thereto and contained in this document.

OBJECTSECURITY makes no representations or warranties that this document will be free of harmful components.

The use of the materials (or any information incorporated thereto), in whole or in part, contained in this document is your sole responsibility. OBJECTSECURITY disclaims any liability for any damages whatsoever including without limitation direct, indirect, incidental and/or consequential damages resulting from access to the document and use of the materials provided therein.

This document may contain links to third party sites. The links are provided to you only as a convenience and the inclusion of any link does not imply neither an endorsement by OBJECTSECURITY of the linked sites nor any warranty from OBJECTSECURITY on said sites. Access to said linked sites is at your own risk.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS.