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

info@objectsecurity.com
www.objectsecurity.com

Overview

- About
- Cyber-physical
- Smart healthcare
- 3 case studies, incl. IoT Security Policy Automation
- Conclusion

- Slides: 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

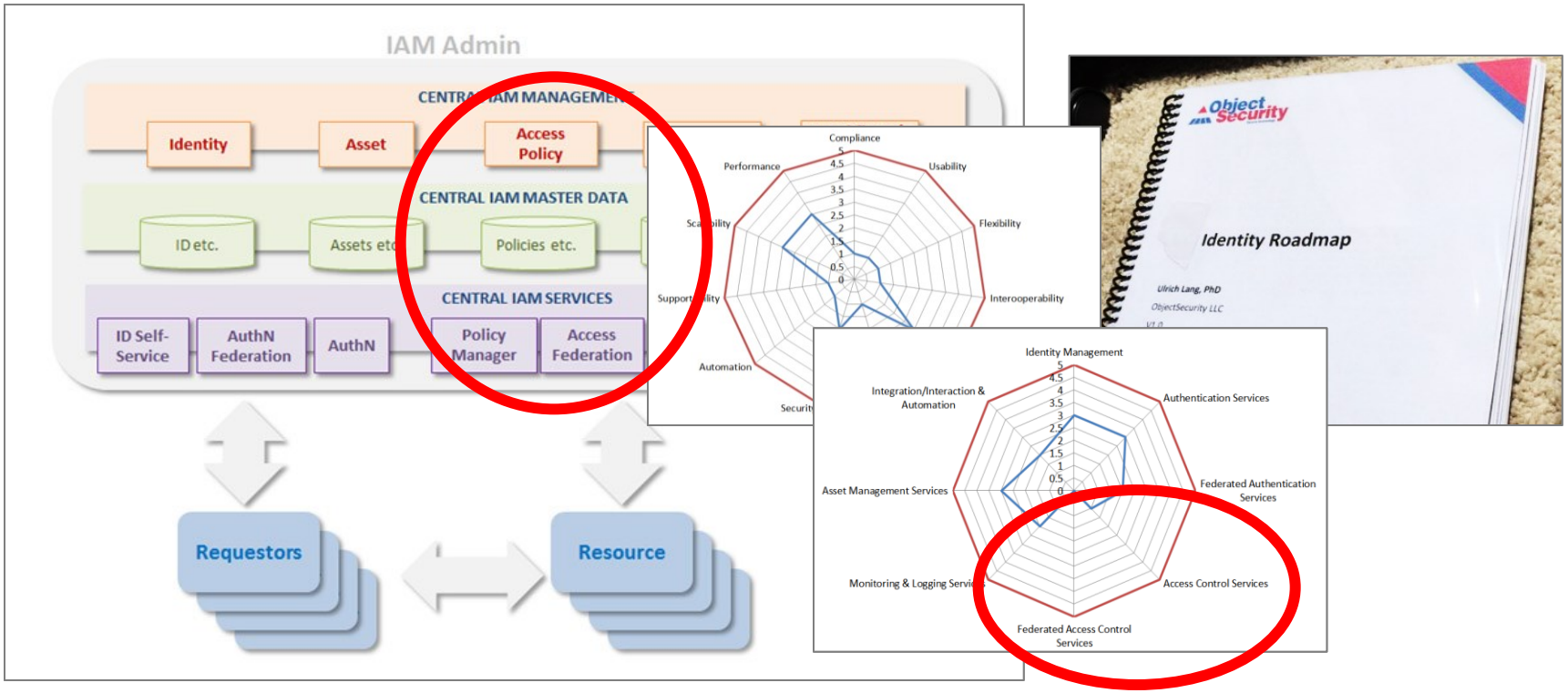
- Why did we do it?

- 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

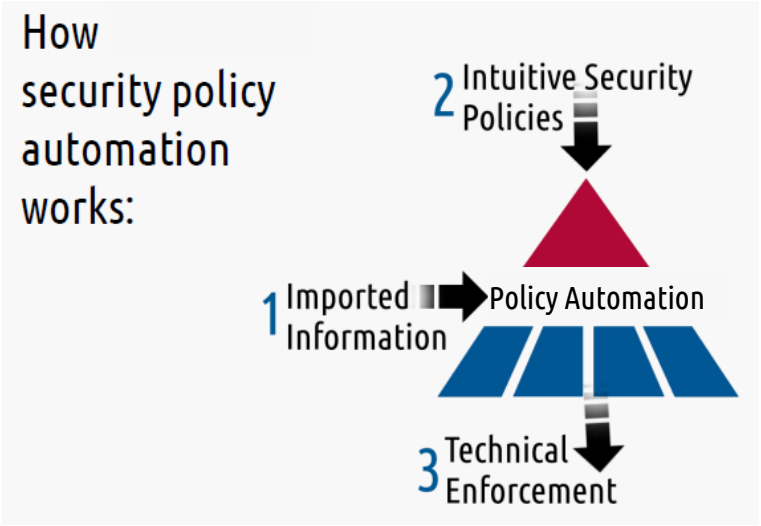
- not good enough
  - Unauthorized access: 25% →1+
  - Overprovisioned access
  - Mirai, WannaCry etc.
  - too simplistic: IBAC, RBAC, fragmented, siloed
- Better access control needed
  - Prevent damage/fines: HIPAA $4.8M
  - Enable "smart business": $8.5M
- Attribute based Access Control
  - part of solution (70% in 2020; Gartner)
  - often too hard to: **1** manage/author **2** implement & integrate **3** audit

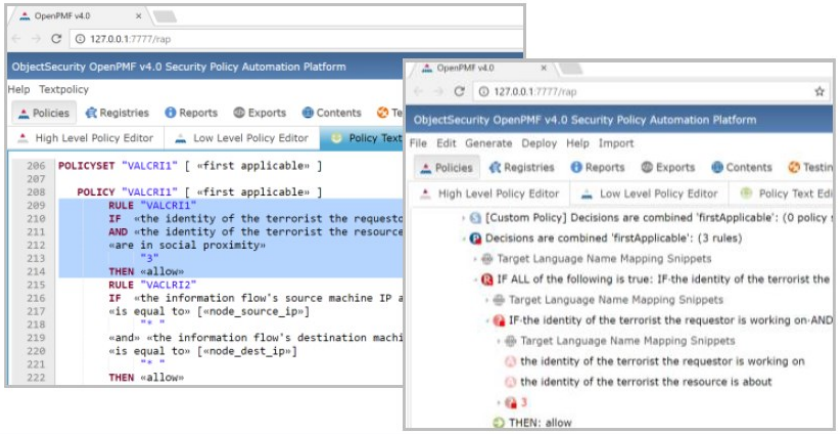
RBAC → ABAC

"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

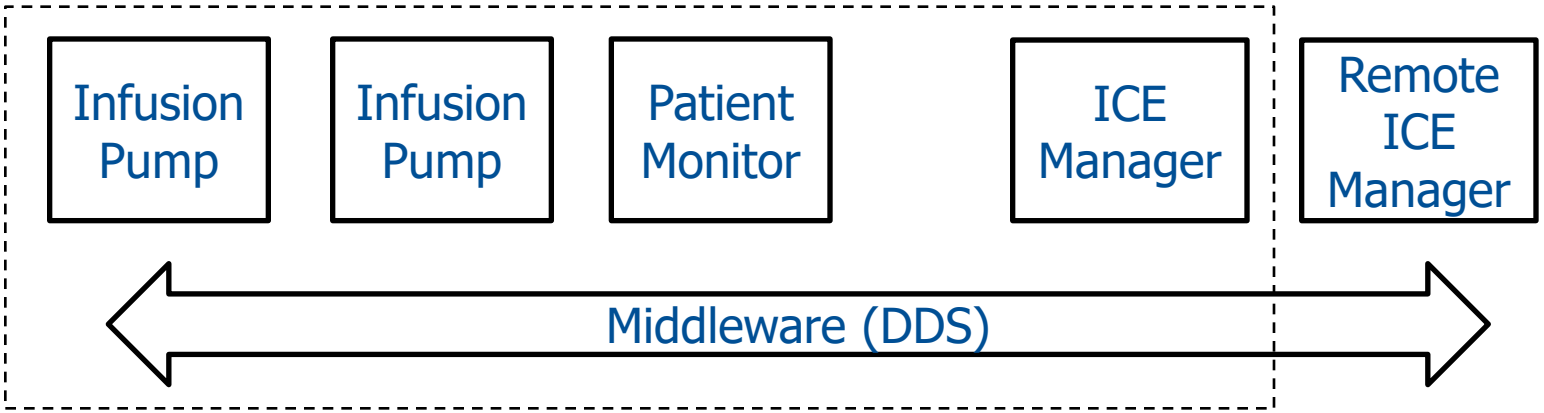




info@objectsecurity.com
www.objectsecurity.com

IIoT: Smart ICE

(DARPA SBIR subcontract for RTI)



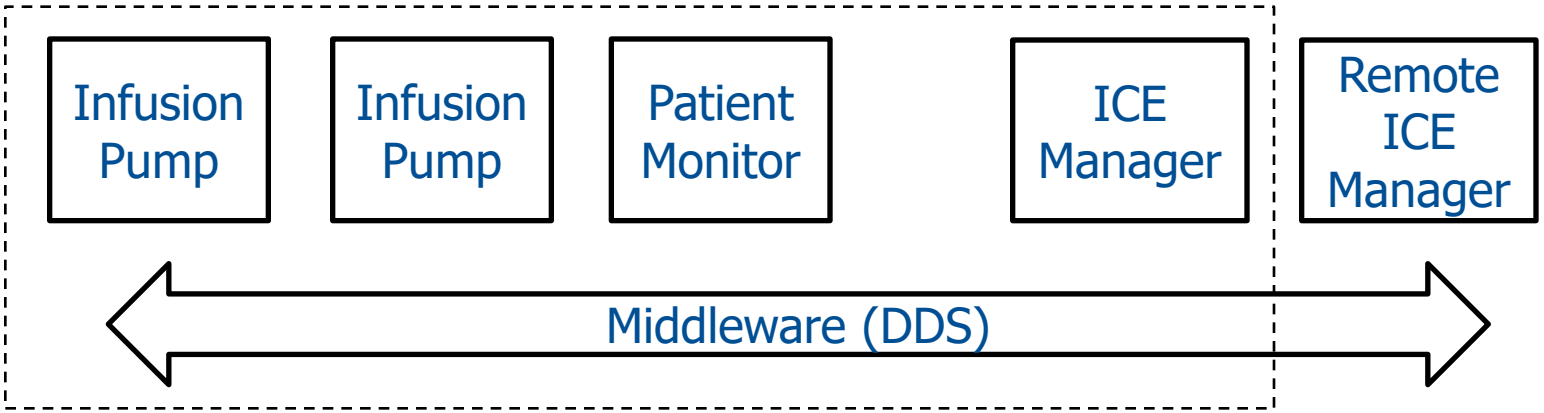
info@objectsecurity.com
www.objectsecurity.com

IIoT: Smart ICE

(DARPA SBIR subcontract for RTI)

OpenPMF Security Policy Automation

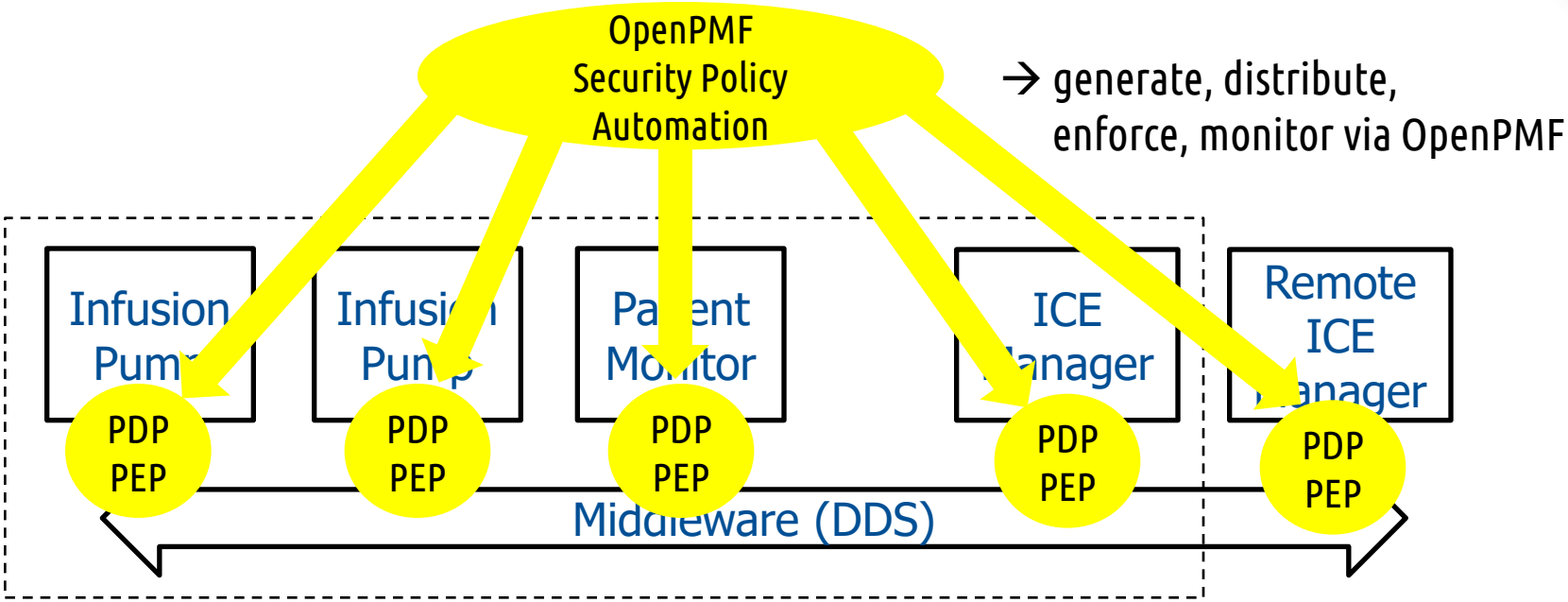
→ author, test, document



info@objectsecurity.com
www.objectsecurity.com

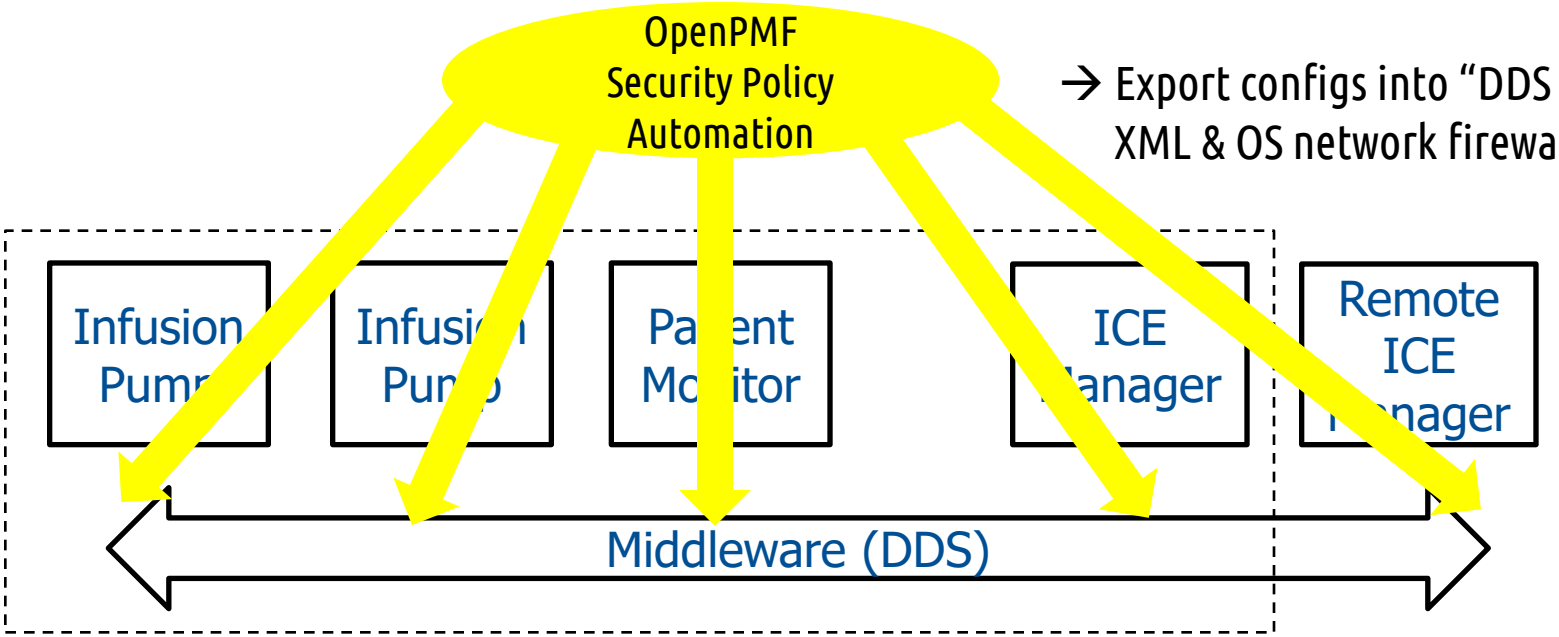
IIoT: Smart ICE

(DARPA SBIR subcontract for RTI)



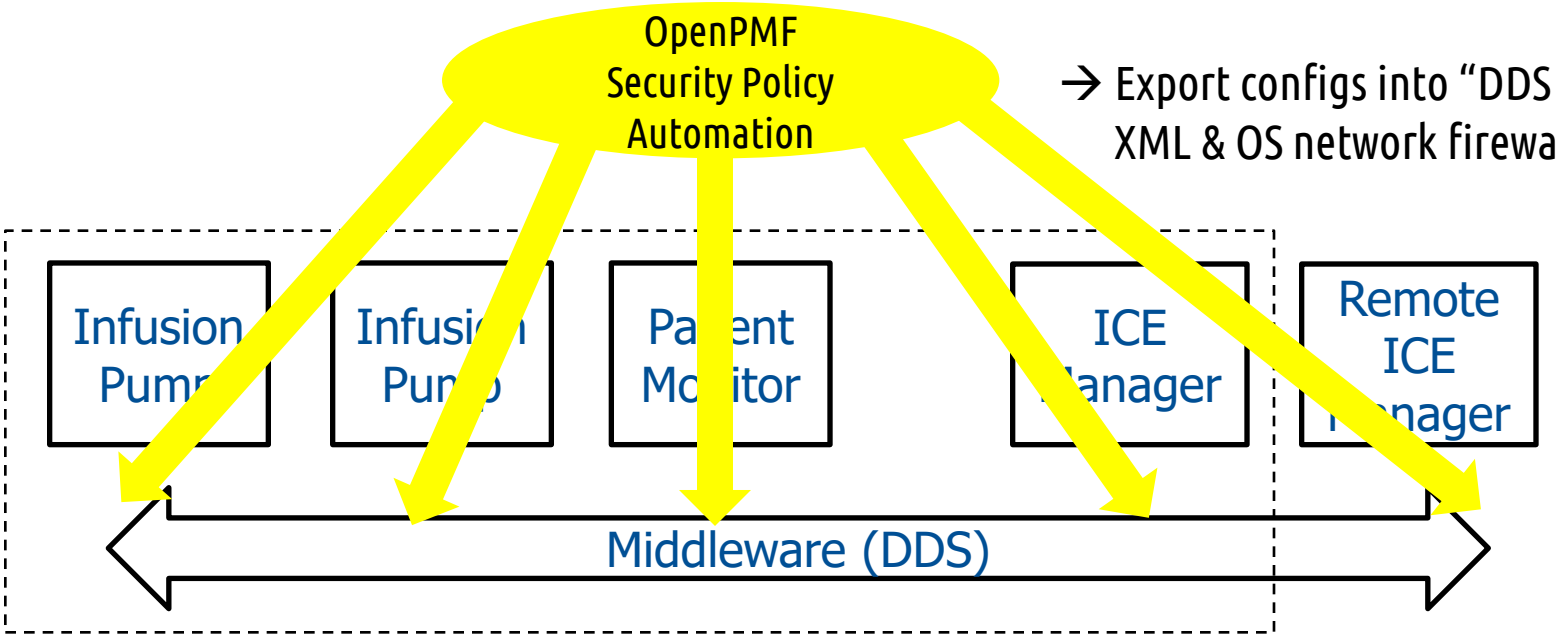
IIoT: Smart ICE

(DARPA SBIR subcontract for RTI)



IIoT: Smart ICE

(DARPA SBIR subcontract for RTI)



Challenges in this SBIR scenario:

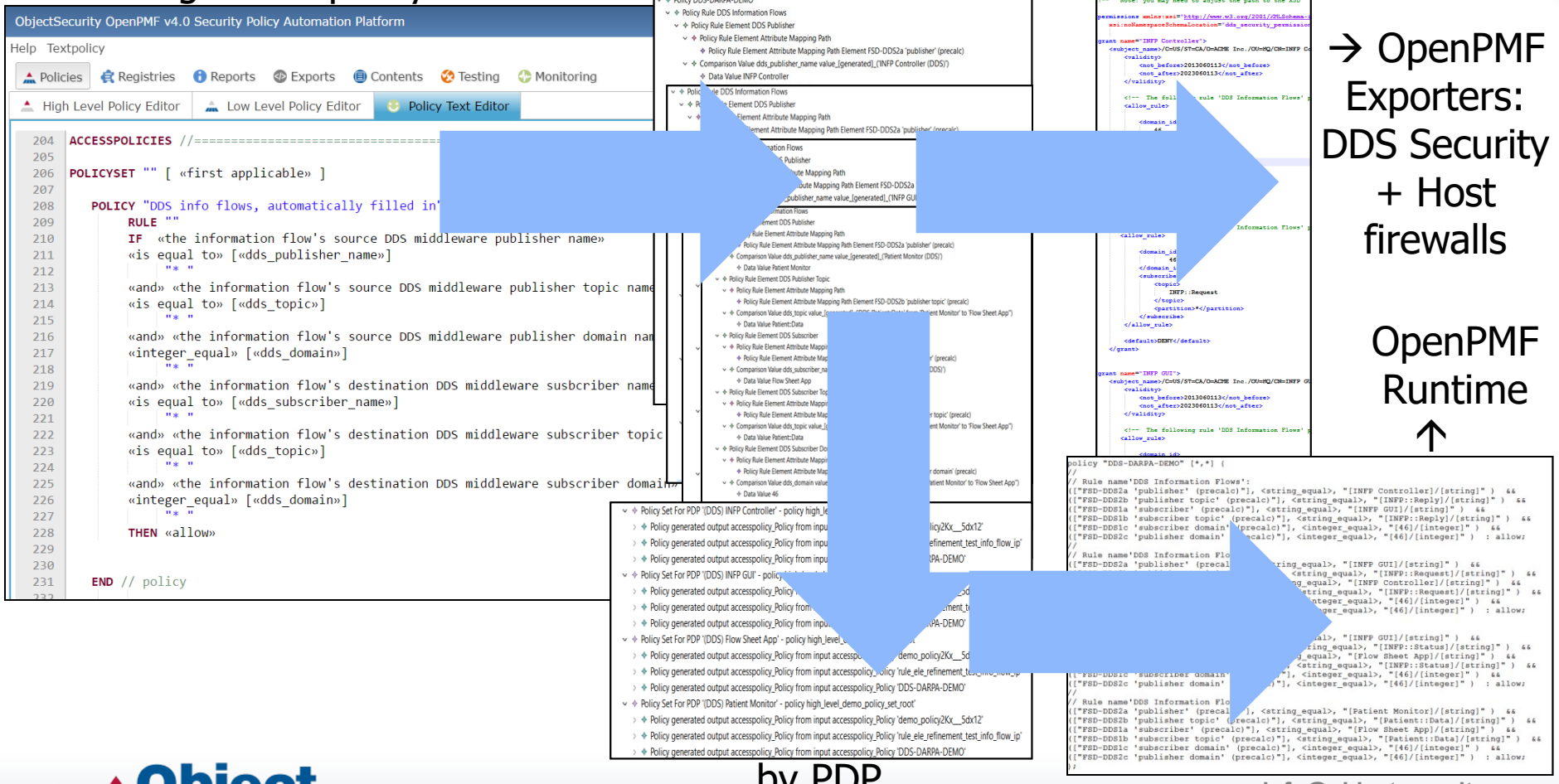
- process to determine policy?
- dynamic changes (devices move around)
- HIPAA

- How to wrap legacy devices
- seL4 microkernel
- manually specified application 'model' for security policy automation

Smart ICE
very/too simple policy automation example

High-level policy

Low-level policy



...by PDP

→ OpenPMF Exporters: DDS Security + Host firewalls

OpenPMF Runtime ↑

info@objectsecurity.com
www.objectsecurity.com

Smart operating room
OpenICE DHP SBIR (subcontract for RTI)

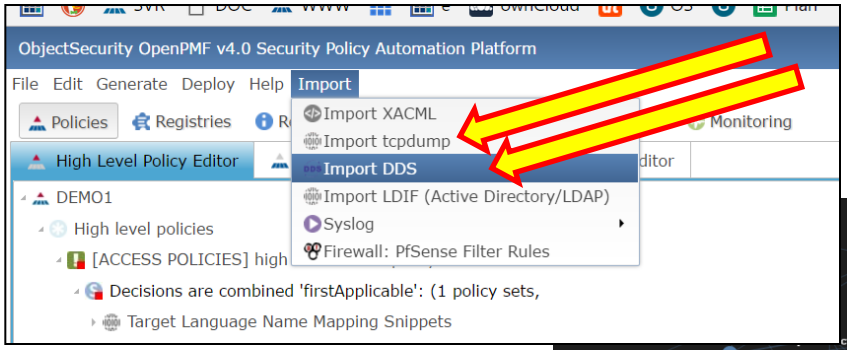
- Continue “case study 2” work
- Integrate into OpenICE
- ‘Real’ access policies, data, apps
- formal policy testing, automatic detection and ingestion →

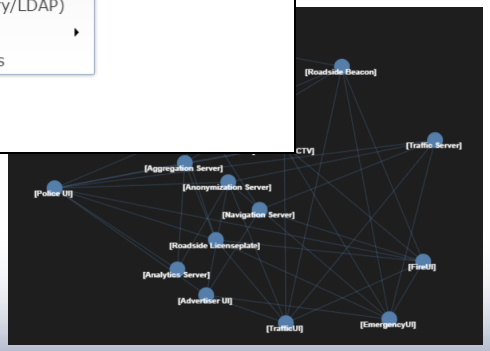
info@objectsecurity.com
www.objectsecurity.com

Feature examples: NIST National Institute of Standards and Technology SBIR PI/II work

Ingestion

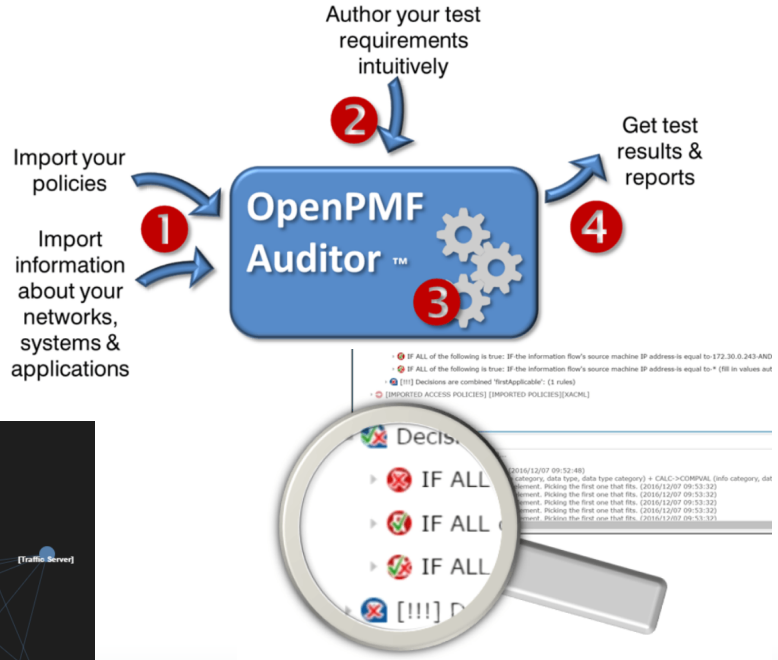
- Import + smart merge traffic (net + DDS etc., also from NetPEPs)
- Import existing IdM
- Import existing policies





Formal Testing

- Based on NIST ACPT
- Symbolic model checking



info@objectsecurity.com
www.objectsecurity.com

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