# Benefits of Network Automation in an OT Environment

Tom Goerke, Cisco
GM Innovations Centres ANZ

AOG March 2019

Innovation Central
A collaboration led by Cisco

woodside

DATA 61 | CSIRO

Curtin University

CISCO

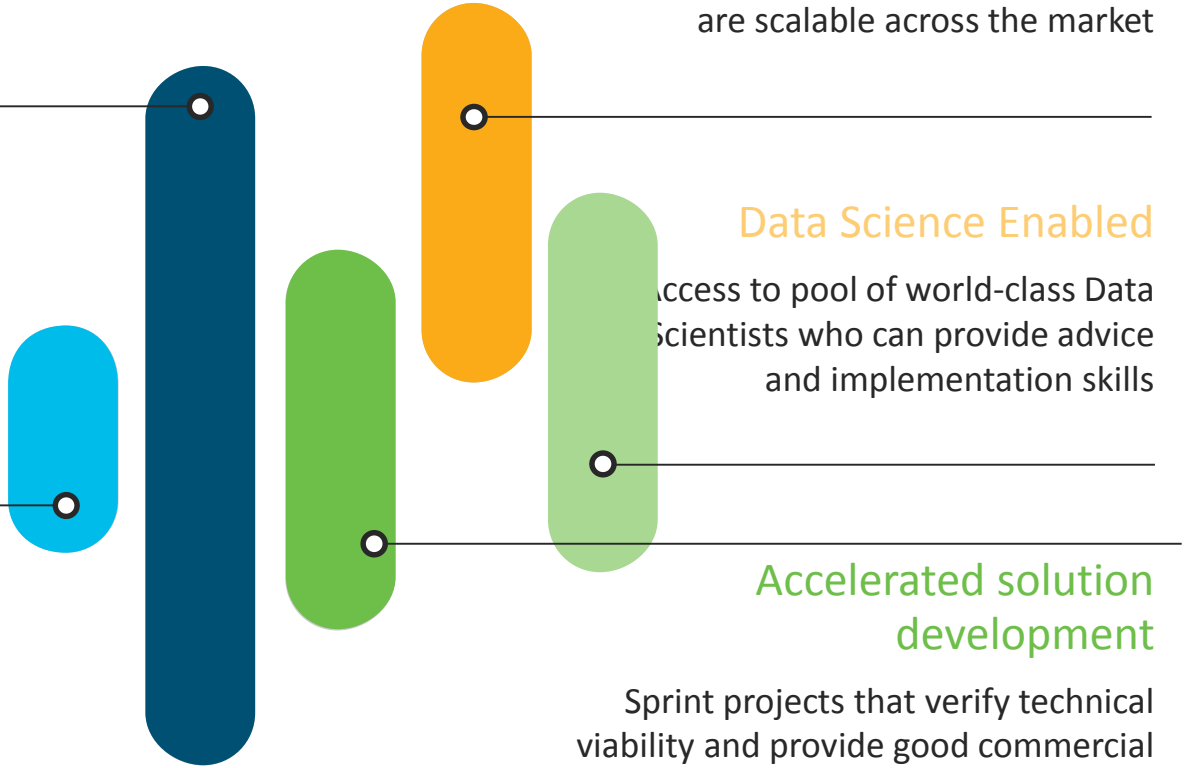
# Innovation Central

## Customer-centric

Prioritise projects, solutions with high customer impact and that are scalable across the market

## Proven Partnerships

Between corporate, SME, academic, research and government



## Data Science Enabled

Access to pool of world-class Data Scientists who can provide advice and implementation skills

## Foundational Technologies

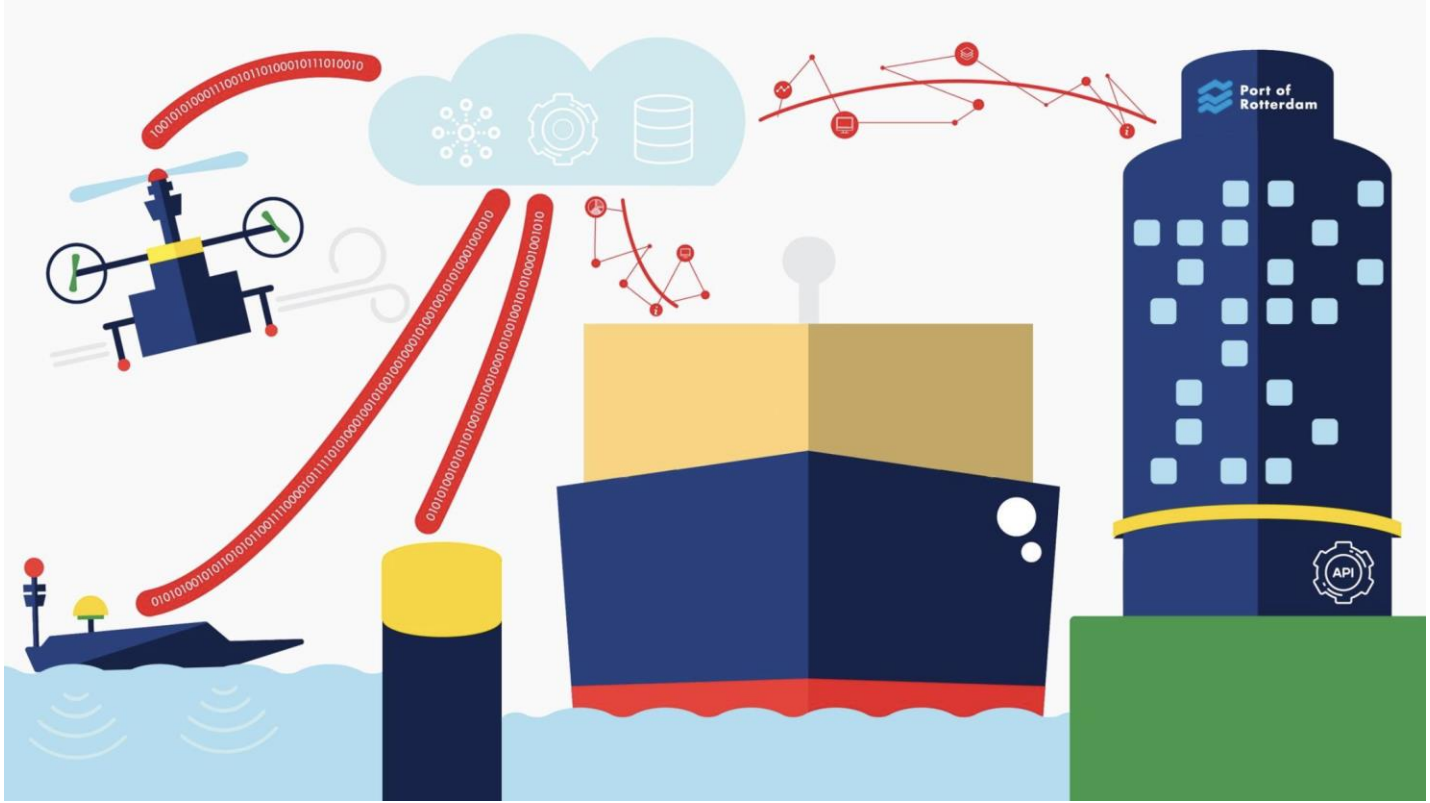
That enable secure IoT in agriculture, smart cities and transport

## Accelerated solution development

Sprint projects that verify technical viability and provide good commercial insight

# Port of Rotterdam

# Smart Infra

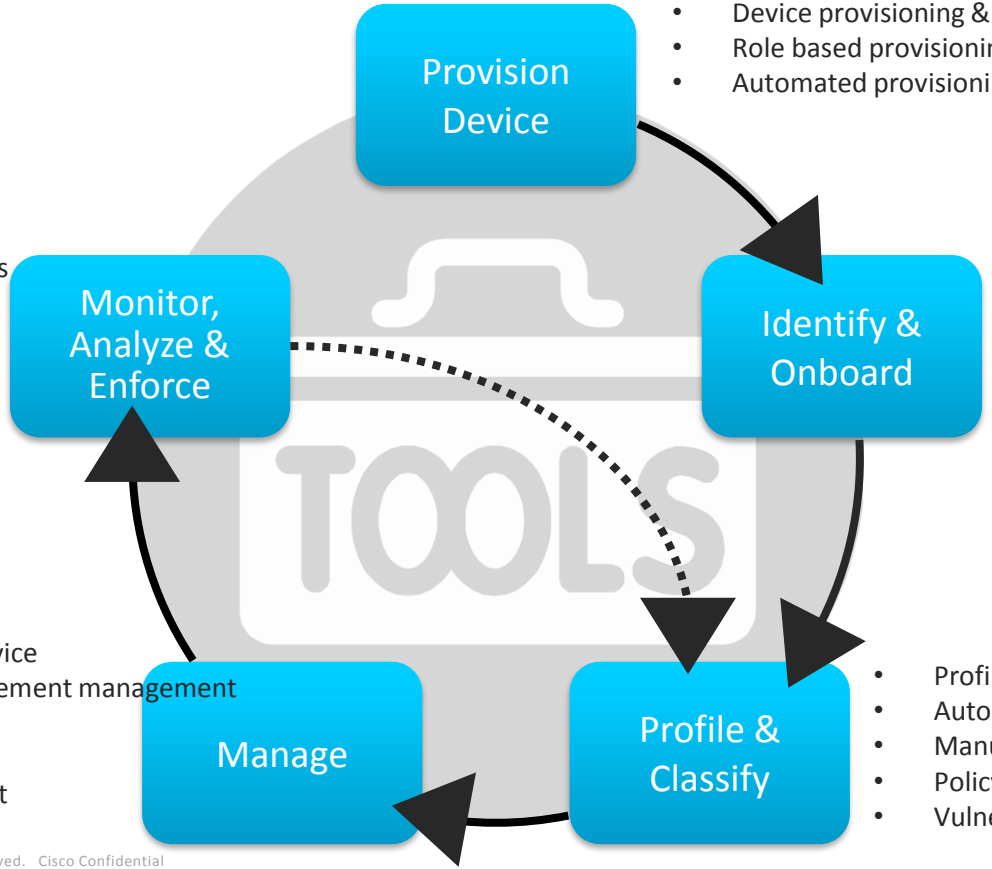


# IT and Operational Teams (OT) have different requirements

| IT | OT |
| --- | --- |
| What is this thing? | How do I connect this thing? |
| Does it belong to this network? | Is it working & connected? |
| Is its connection functional? | Does it need maintenance? |
| What network access does it need? | Is it communicating with its App? |
| Is it behaving as designed? | Is it sending and receiving the data? |

Everything is now a shade of grey

# IoT Operational Tools: Managing IoT Lifecycle




- Device provisioning & registration portal
- Role based provisioning of devices: App/Scanner
- Automated provisioning through Wi-Fi NAN

- Establishing trust between network and device
- Individual PSK or PKI
- Locally provisioned or manufacturer bootstrapped

- Profile and Classify the device
- Automated (device database)
- Manufacturer provided (MUD)
- Policy based
- Vulnerability assessment (Scoring)

- Role-based & policy based device entitlement/inventory management management
- 'My devices' portal
- Threat Management
- Advanced device management

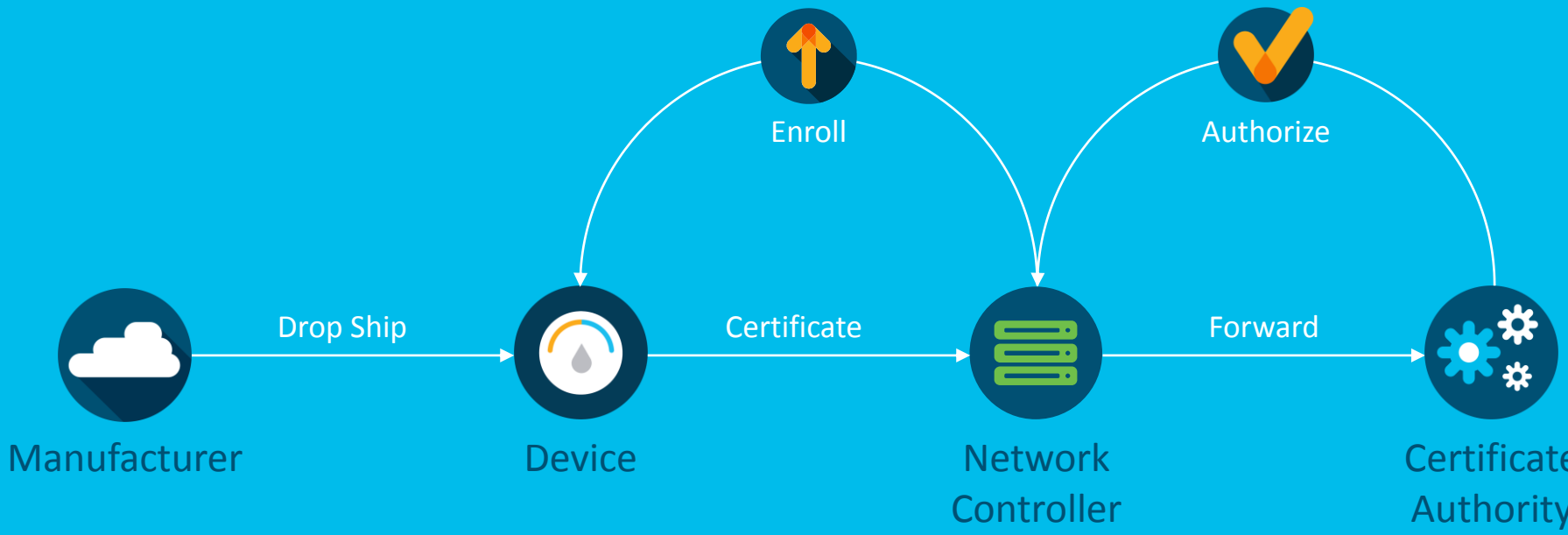
- Continuous behavioral analysis
- Threat scoring
- Automated Remediation

# Problem

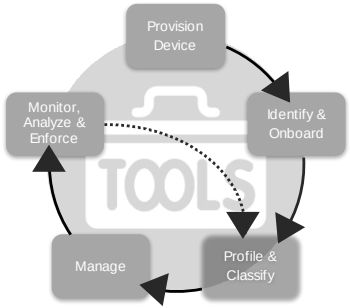
Scalable Autonomous onboarding with strong device identity

# Solution

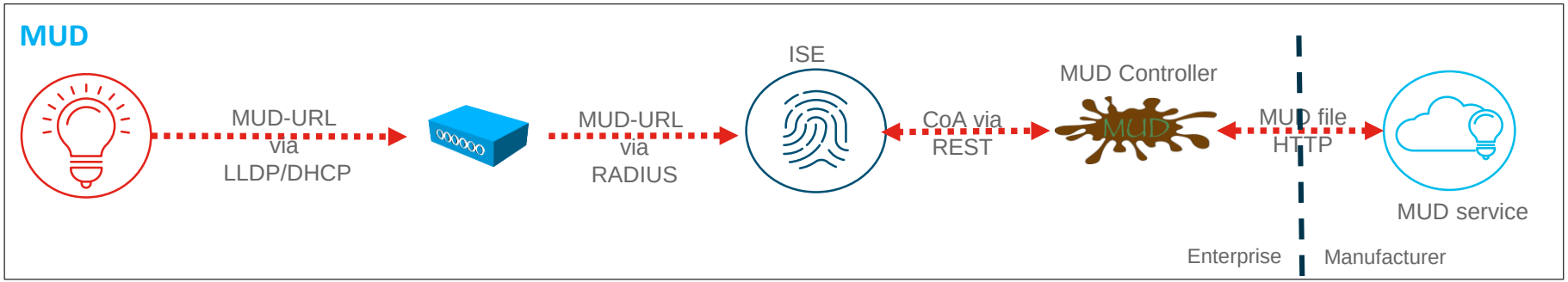
IETF Standards Bootstrap Remote Secure Key Infrastructure (BRSKI / ANIMA)



# What is behind it: Automated Profiling of IoT Devices




1. OUI (MAC address)
2. AAA
3. DHCP/LLDP
4. RF Fingerprinting
5. Behavioral analytics
6. Manufacturer Usage Description (MUD)

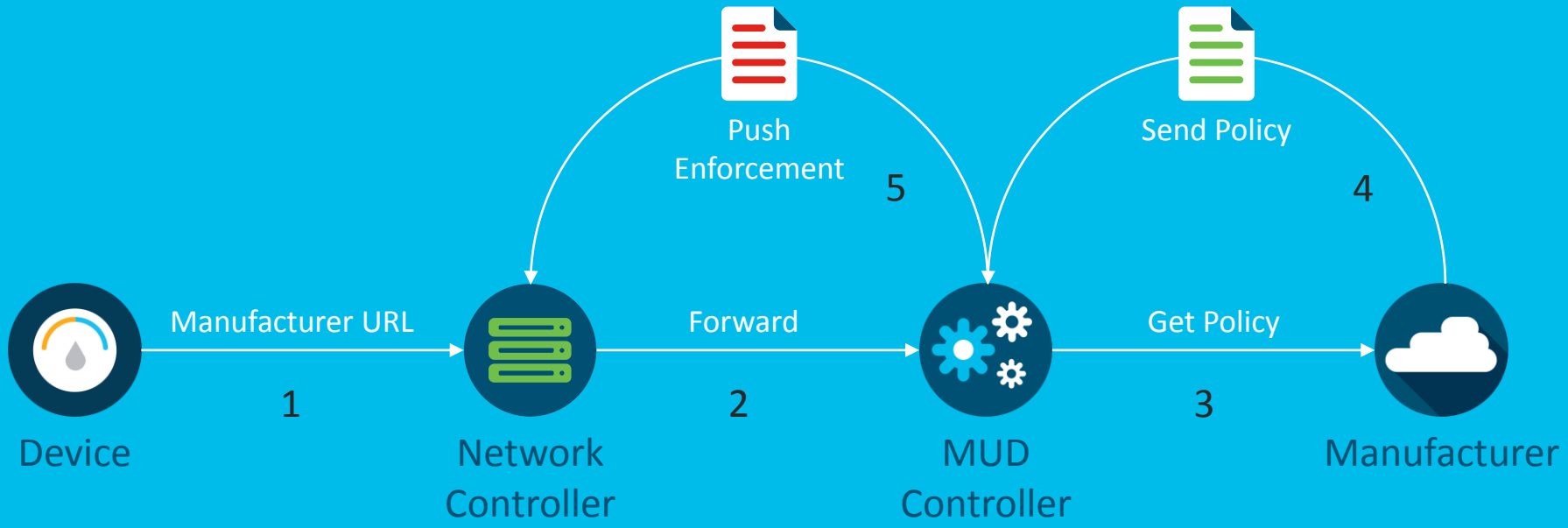


# Problem

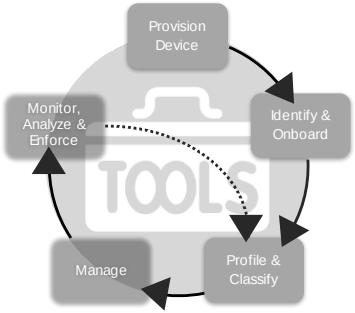
Understand expected device behavior and turn it into policy

# Solution

IETF Standard Manufacturer Usage Descriptions (MUD)



# What is behind it: Managing & Monitoring IoT Devices




1. Monitor
   - RF Fingerprinting
   - Traffic/Flow Inspection
   - Stealthwatch
   - Umbrella/Talos
2. Manage
   - DNA-C network policy management
   - DNA-C IoT policy manager
   - IoT Insights mobile management tools for IT and OT
3. Enforce
   - TrustSec

# Summary

# Summary

- Number of IoT devices will be exponentially higher than IT
- Manual approaches used in IT will NOT scale to IoT
- Industrial OT environments are in the process of increasing the number and types of sensors and devices
- IoT Security must be autonomous and simple
- Network teams need to be factoring in the Business requirements for IoT and starting the journey now
- Cisco is drafting these new standards and implementing them
- WISE Programme supporting this in ICP in Perth

# Wireless Industrial Sensor Environment
## An ICP Program

### Vision

Validate cost effective, alternative approaches to digitise industrial assets through the development and evaluation of battery powered sensors

### Approach

Build a low power access radio lab environment. Integrate the data acquisition platform. Stream sensor data into various historian and analytics platforms. Evaluate and drive the smart sensor market

### Outcome

Understanding of ideal sensor, connectivity and data acquisition solutions to support massively scalable industrial sensor networks


CISCO