xylem
Let's Solve Water

Smarter Together

Building cybersecurity through partnerships

xylem
Let's Solve Water

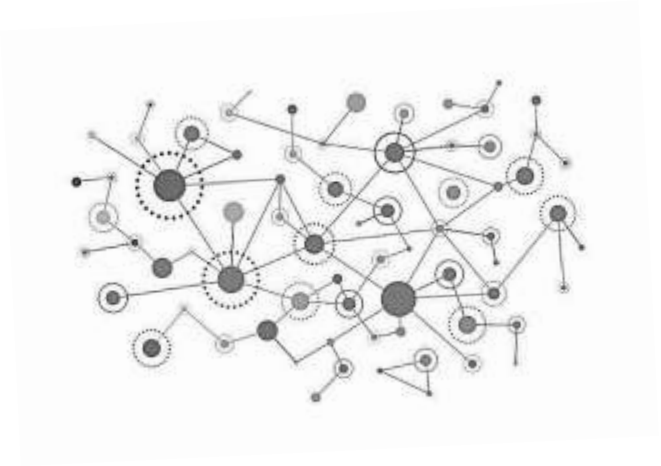
1

Connected, digital solutions create value for water infrastructure

South Bend Indiana’s Story - A Digital Transformation

Digital Solution

120 sensors for a real time monitoring system



Financial Savings

$1.5 Million savings in annual operating and maintenance

$500 Million in CAPEX savings

Environmental Improvements

1 Billion gallons / year reduction in sewer overflow

50% drop in E. Coli Concentrations in St. Joseph River

> ***“We spent 500 million dollars less than originally estimated, achieving the same environmental benefit and level of service, just by optimizing the existing system in the ground.”***
>
> **- Eric Horvath, Director of Public Works, City of South Bend**

https://www.xylem.com/en-us/support/case-studies-white-papers/south-bend-indiana-reduces-combined-sewer-overflow-70-percent-saves-500-million/

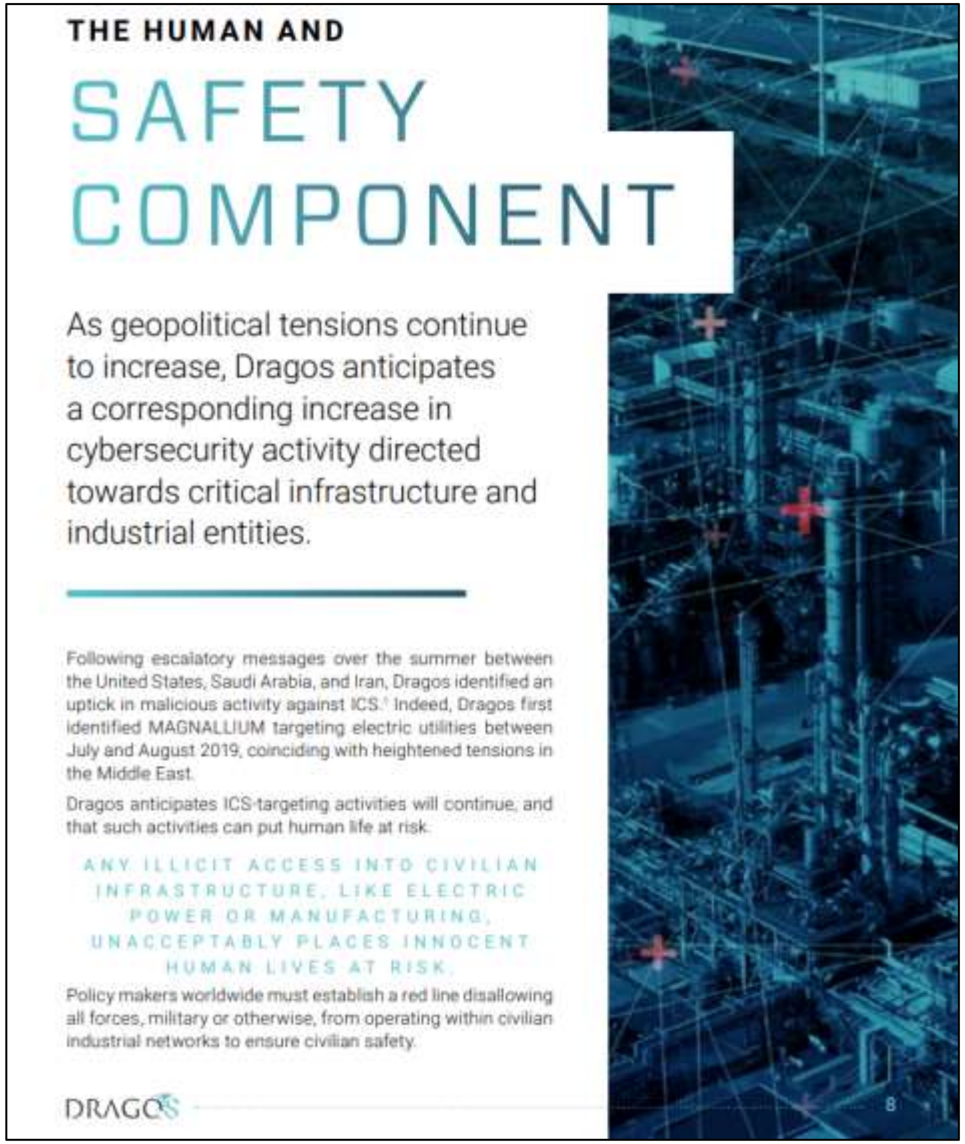
xylem
Let's Solve Water

Cyber threats are emerging against Water technologies

2

Cybersecurity can be a safety issue

Threat activity groups like MAGNALLIUM and RASPITE are specifically **targeting safety systems** and features to create disruptive events in critical infrastructure.



THE HUMAN AND

SAFETY COMPONENT

As geopolitical tensions continue to increase, Dragos anticipates a corresponding increase in cybersecurity activity directed towards critical infrastructure and industrial entities.

Following escalatory messages over the summer between the United States, Saudi Arabia, and Iran, Dragos identified an uptick in malicious activity against ICS.[1] Indeed, Dragos first identified MAGNALLIUM targeting electric utilities between July and August 2019, coinciding with heightened tensions in the Middle East.

Dragos anticipates ICS-targeting activities will continue, and that such activities can put human life at risk.

ANY ILLICIT ACCESS INTO CIVILIAN INFRASTRUCTURE, LIKE ELECTRIC POWER OR MANUFACTURING, UNACCEPTABLY PLACES INNOCENT HUMAN LIVES AT RISK.

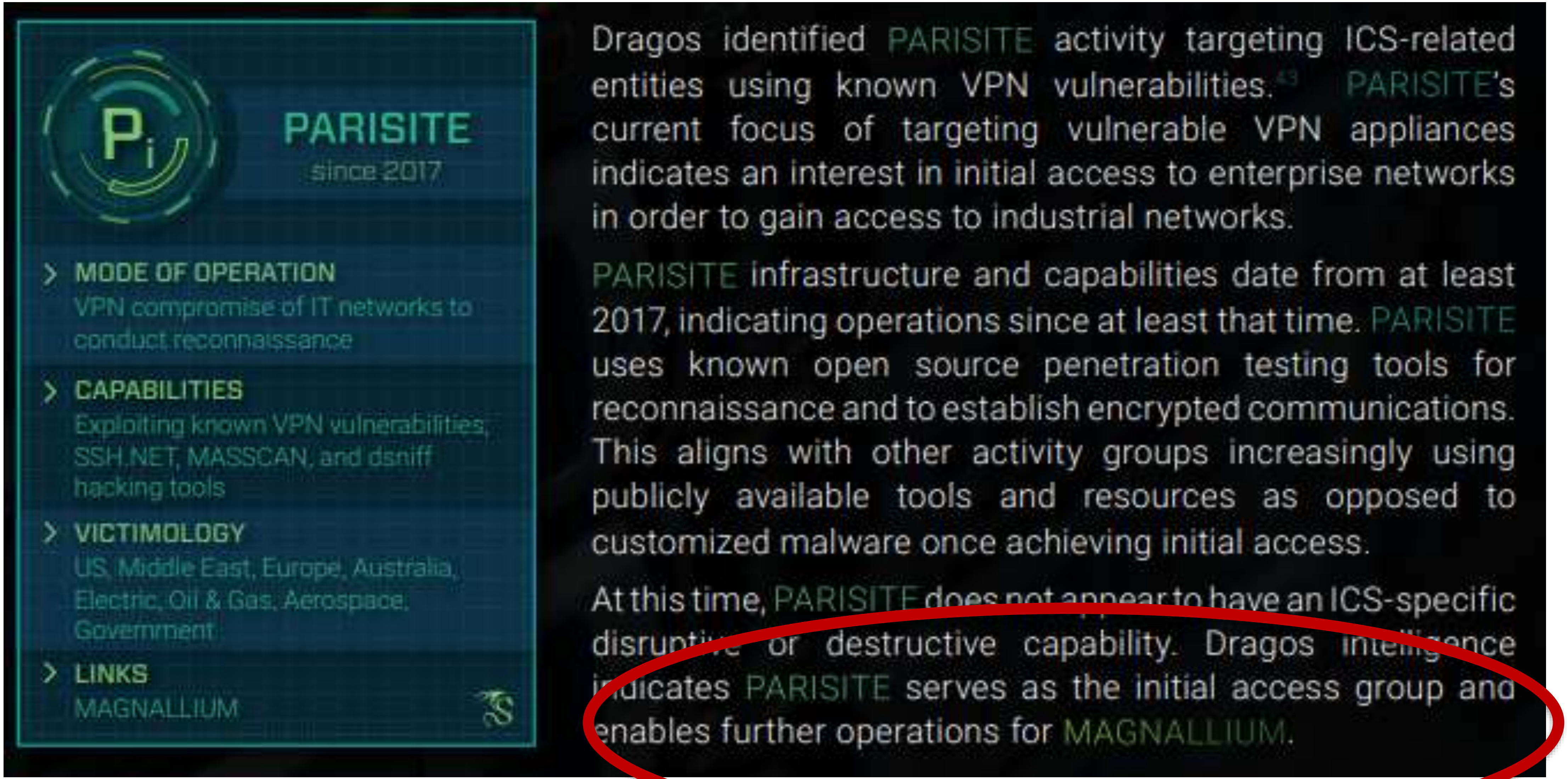
Policy makers worldwide must establish a red line disallowing all forces, military or otherwise, from operating within civilian industrial networks to ensure civilian safety.

DRAGOS

8

https://www.dragos.com/year-in-review/

Threat actors are pivoting to **targeting Water technology**



PARISITE

since 2017

MODE OF OPERATION
VPN compromise of IT networks to conduct reconnaissance

CAPABILITIES
Exploiting known VPN vulnerabilities, SSH.NET, MASSCAN, and dsniff hacking tools

VICTIMOLOGY
US, Middle East, Europe, Australia, Electric, Oil & Gas, Aerospace, Government

LINKS
MAGNALLIUM

Dragos identified PARISITE activity targeting ICS-related entities using known VPN vulnerabilities.[43] PARISITE's current focus of targeting vulnerable VPN appliances indicates an interest in initial access to enterprise networks in order to gain access to industrial networks.

PARISITE infrastructure and capabilities date from at least 2017, indicating operations since at least that time. PARISITE uses known open source penetration testing tools for reconnaissance and to establish encrypted communications. This aligns with other activity groups increasingly using publicly available tools and resources as opposed to customized malware once achieving initial access.

At this time, PARISITE does not appear to have an ICS-specific disruptive or destructive capability. Dragos intelligence indicates PARISITE serves as the initial access group and enables further operations for MAGNALLIUM.

Cyber attacks are costly to customers

Over $1 Trillion USD
In estimated global losses due to cyber crime in 2020 (average cost per incident over $500k USD)

Number of Threat Actors Increasing
Already 7 threat actors shown to specifically target water and wastewater infrastructure in the US and globally

150 Vulnerable Products
Used in water and wastewater systems in the US

20,000 Utility Employees
Say cyber threats are what they fear could have the biggest impact on operations

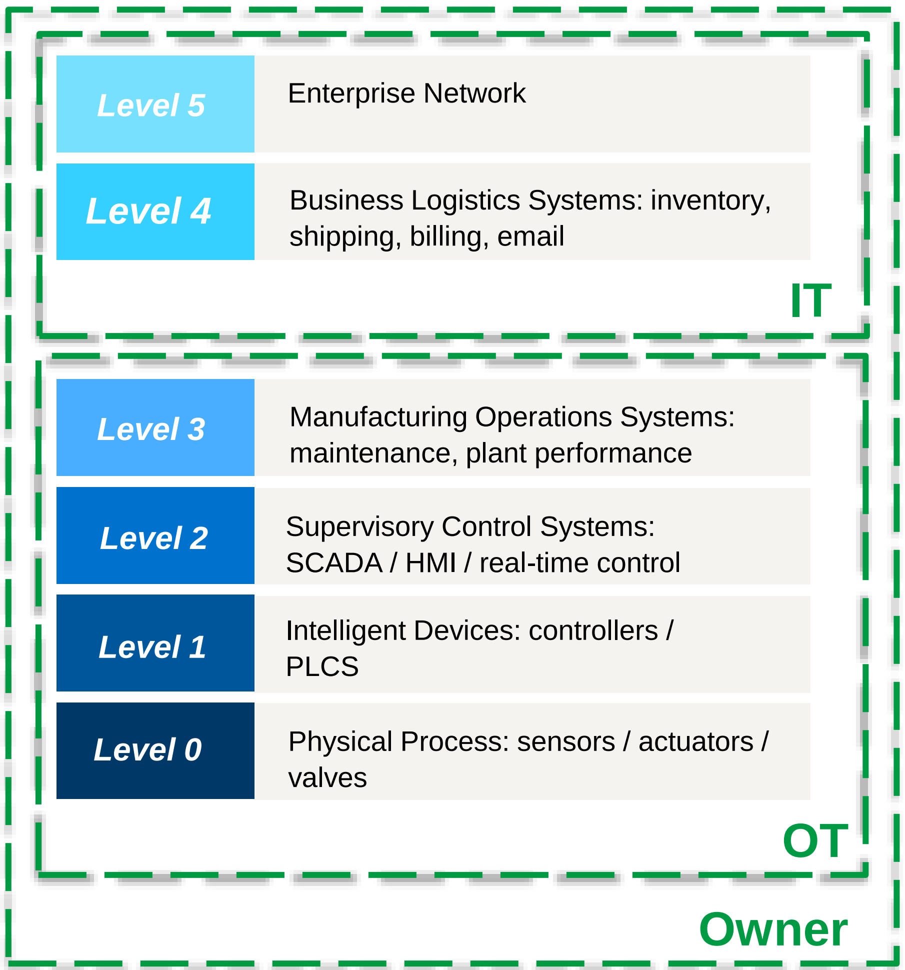
3rd Most Targeted Sector
When compared to other critical infrastructure in the US

$18.2 Million USD
In costs incurred due to a 2019 ransomware attack against a water utility in Maryland, US

Attacks on water infrastructure are already happening today.

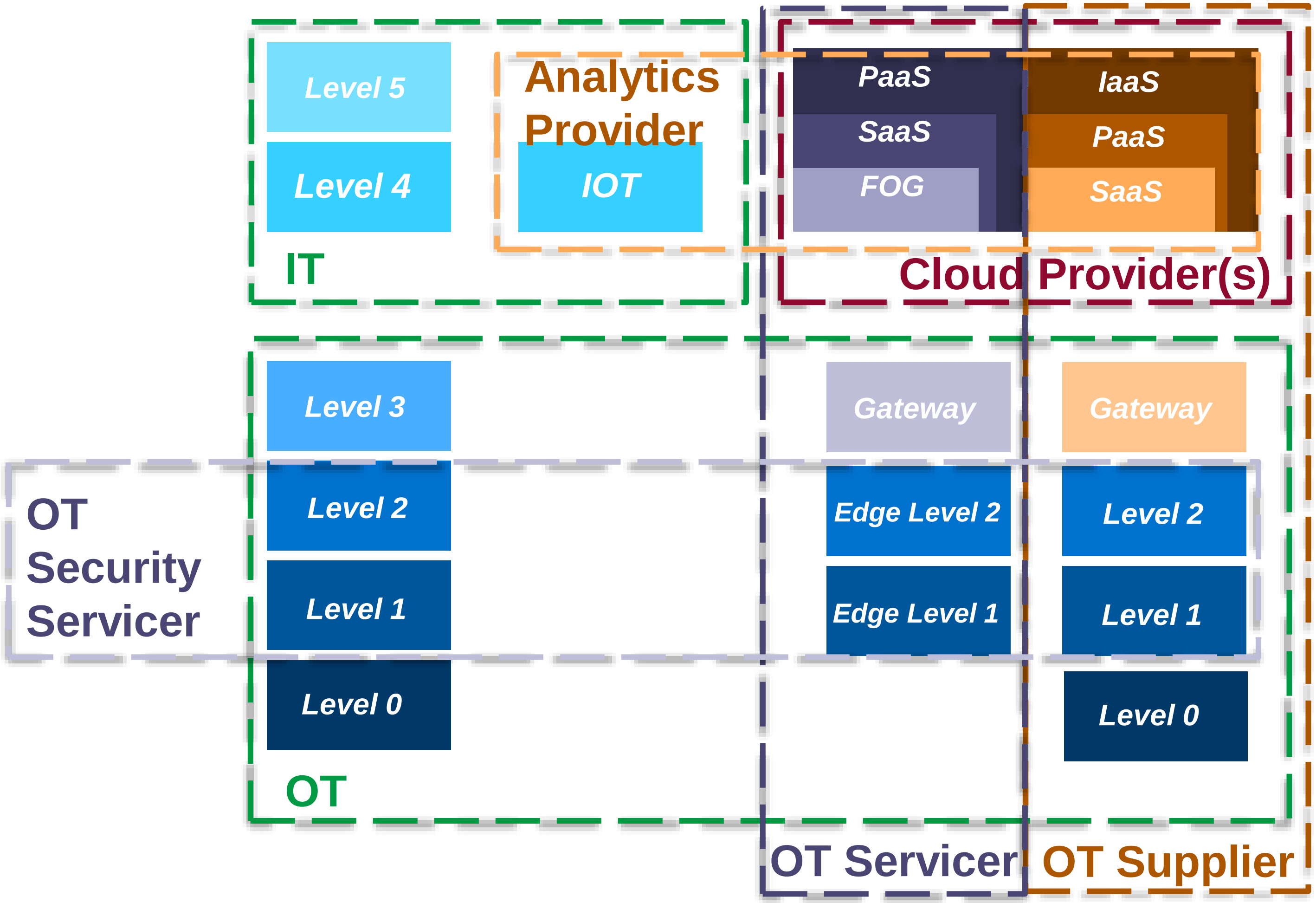
= Trust Boundary

Historical OT
(Procure, Own, Operate)



Level 5	Enterprise Network
Level 4	Business Logistics Systems: inventory, shipping, billing, email
	IT
Level 3	Manufacturing Operations Systems: maintenance, plant performance
Level 2	Supervisory Control Systems: SCADA / HMI / real-time control
Level 1	Intelligent Devices: controllers / PLCS
Level 0	Physical Process: sensors / actuators / valves
	OT
	Owner

Modern OT
(Complex Integrations and Partnerships)



Level 5

Level 4

IT

Analytics Provider

IOT

PaaS

SaaS

FOG

IaaS

PaaS

SaaS

Cloud Provider(s)

Level 3

Gateway

Gateway

OT Security Servicer

Level 2

Edge Level 2

Level 2

Level 1

Edge Level 1

Level 1

Level 0

Level 0

OT

OT Servicer

OT Supplier

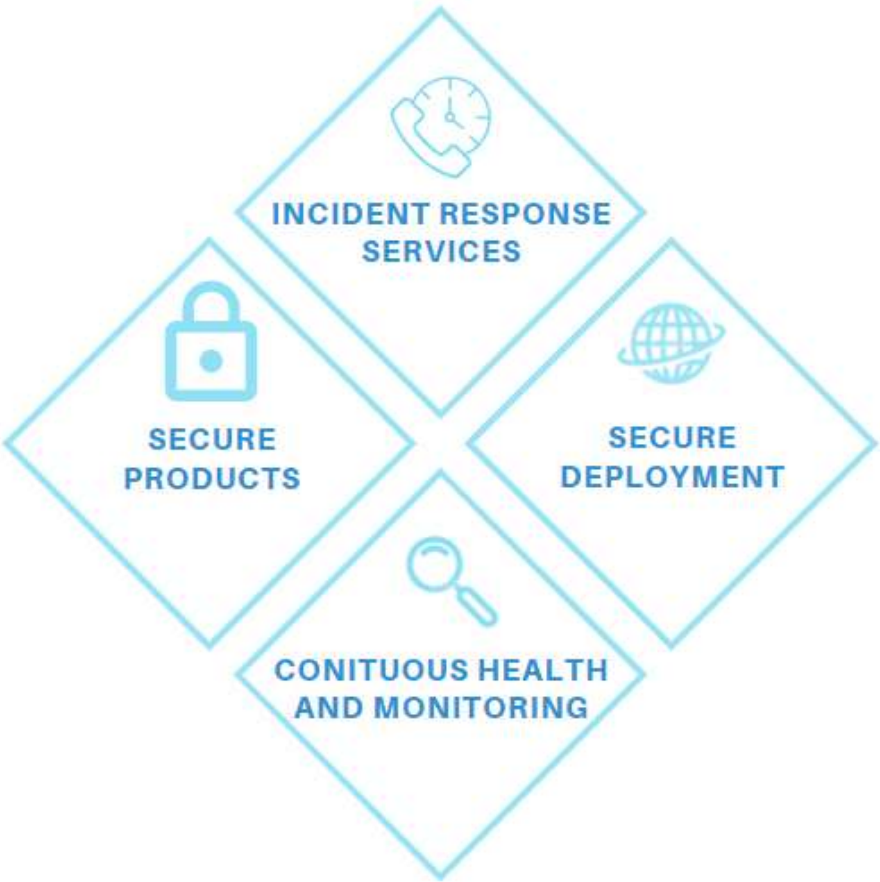
Increased integrations creates new risks.

xylem
Let's Solve Water

Cybersecurity requires a partnership across the supply chain

3

Cybersecurity Multi-Barrier Approach



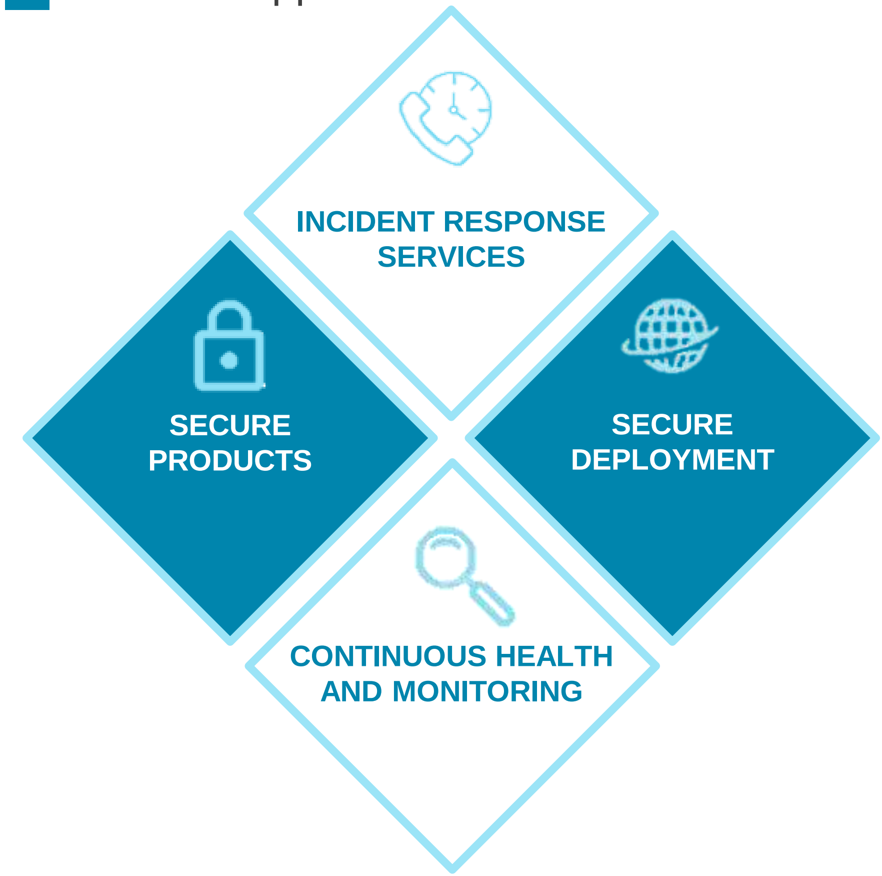
- **Secure products** by finding and fixing weaknesses while engineering
- **Secure deployments** with defense-in-depth that manages risks to the operations of systems and products
- **Continuous health and monitoring** ensures continuous improvement against emerging vulnerabilities and threats
- **Incident response services** assures optimal forensics and response for safe and continuous operations

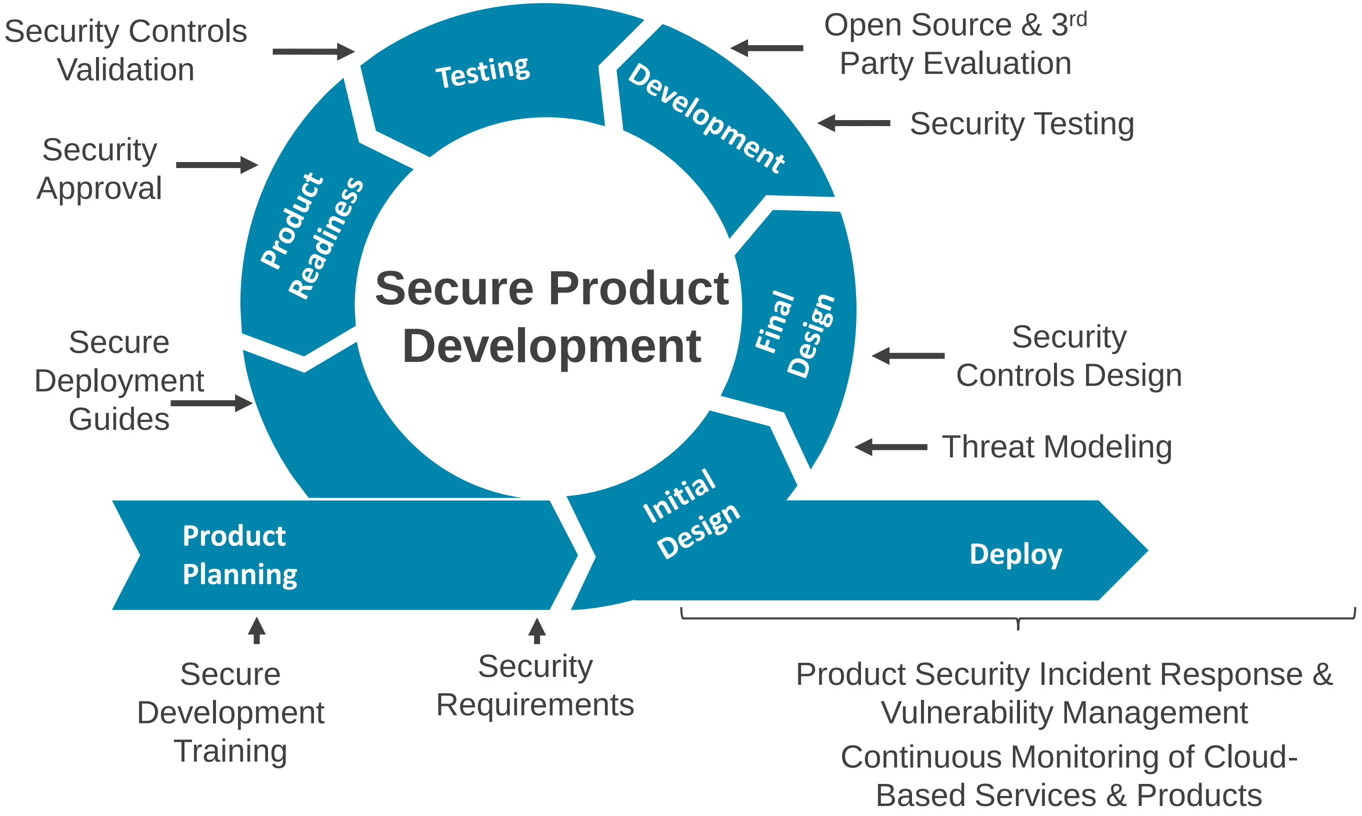
The operator of the utility is the end owner of security risk, but responsibility for security protection falls on the product vendor, integrator, and operator.

Product Supplier Responsibilities

- Secure product strategies: *Threat Modeling, Testing, Functional Roles, Encryption, Code Signing, Responsible Disclosure*
- Secure deployment guidelines: *Network Segmentation, Patch Management, Security Architecture, Access Controls*

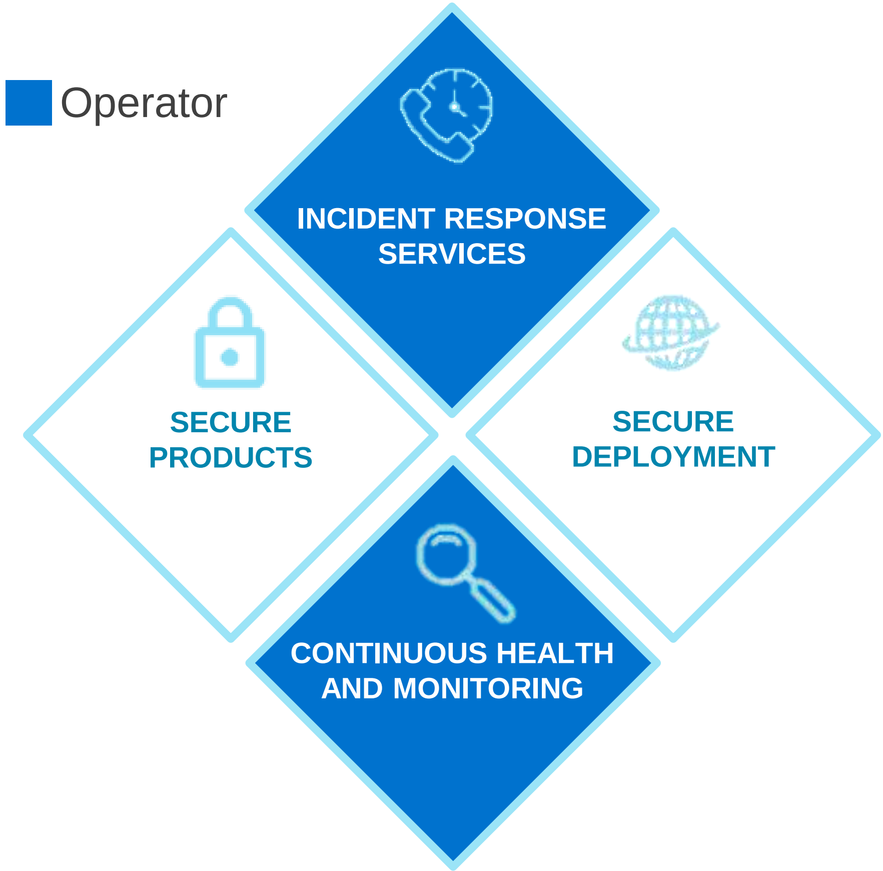
■ Product Supplier




Secure Product Development
Product Planning
Initial Design
Final Design
Development
Testing
Product Readiness
Deploy
Security Controls Validation
Security Approval
Secure Deployment Guides
Open Source & 3rd Party Evaluation
Security Testing
Security Controls Design
Threat Modeling
Secure Development Training
Security Requirements
Product Security Incident Response & Vulnerability Management
Continuous Monitoring of Cloud-Based Services & Products

Operator Responsibilities

- Continuous health and monitoring strategies: *Log Monitoring, Event Monitoring, Backups, Patch Management, Anti-malware, Firewalls, Produce Reviews, Secure DMZ, External Reviews, Threat hunting*
- Incident response: *Log Management, Cyber Intel, Incident Reporting, Escalation Management, Security Exercises, Response and Recovery, Digital Forensics*



■ Operator

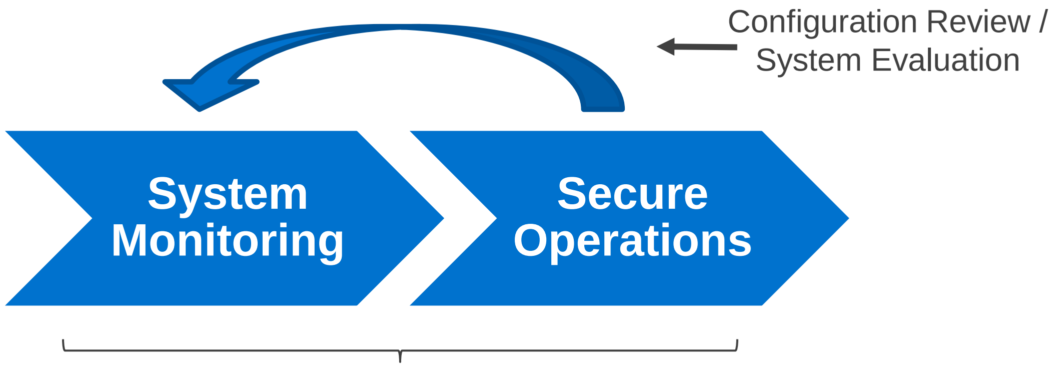
INCIDENT RESPONSE SERVICES

SECURE PRODUCTS

SECURE DEPLOYMENT

CONTINUOUS HEALTH AND MONITORING

Secure Product Operation



Configuration Review / System Evaluation

System Monitoring

Secure Operations

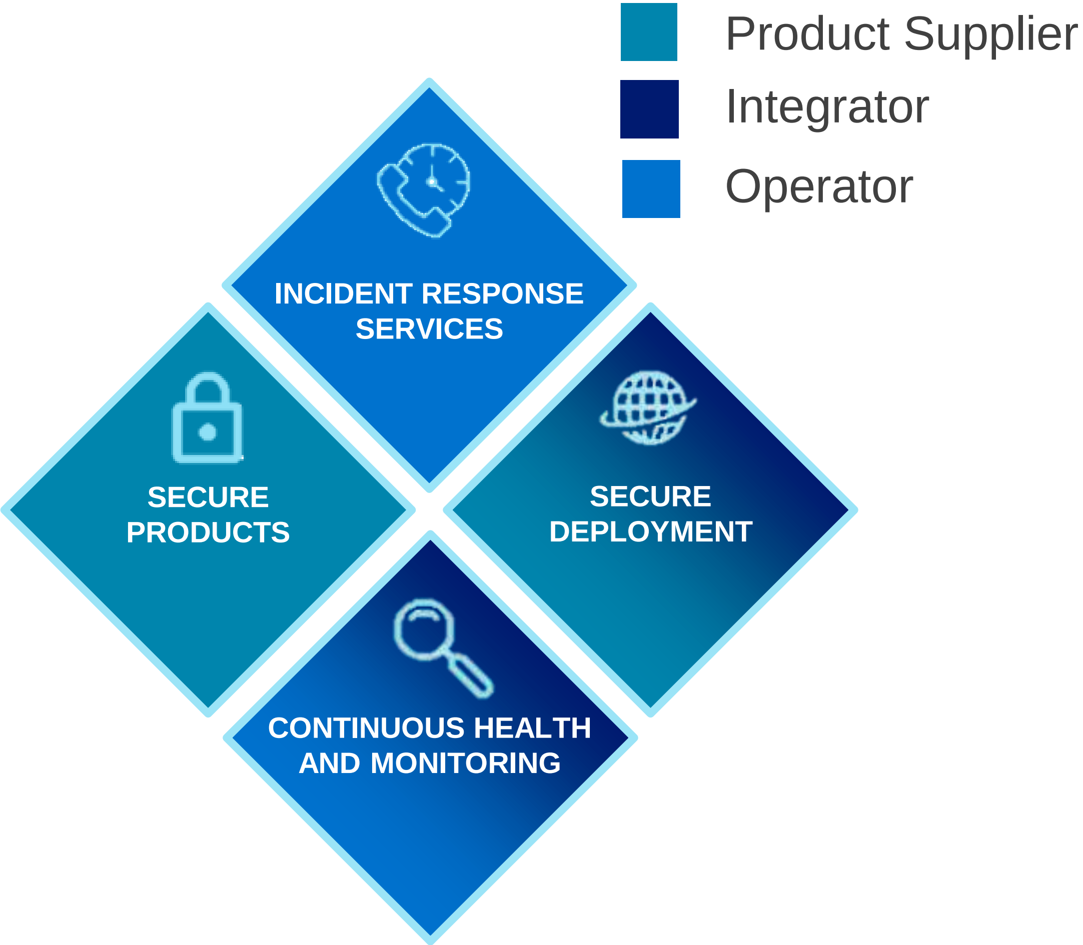
Security Training and Testing
Asset Management
Access Management
Events and Alerts Management
Traffic Monitoring
Application Monitoring
Log Monitoring
Information Sharing with Cloud Services
Incident Response

Strong Cybersecurity Requires Partnership

1. **Digital transformation is necessary** to enable environmental and financial benefits in the water industry

2. Strong security will be built out through a **multi-barrier approach** involving **collaboration and engagement** across multiple parties

3. Industry focus should be on building **strong access control,** organizing **collection management and response,** and creating **strong IIOT-based reference architecture for evaluation**



🟦 Product Supplier

🟦 Integrator

🟦 Operator

INCIDENT RESPONSE SERVICES

SECURE PRODUCTS

SECURE DEPLOYMENT

CONTINUOUS HEALTH AND MONITORING

Strong cyber security requires clearly defined roles for security management and partnerships across certain responsibilities.

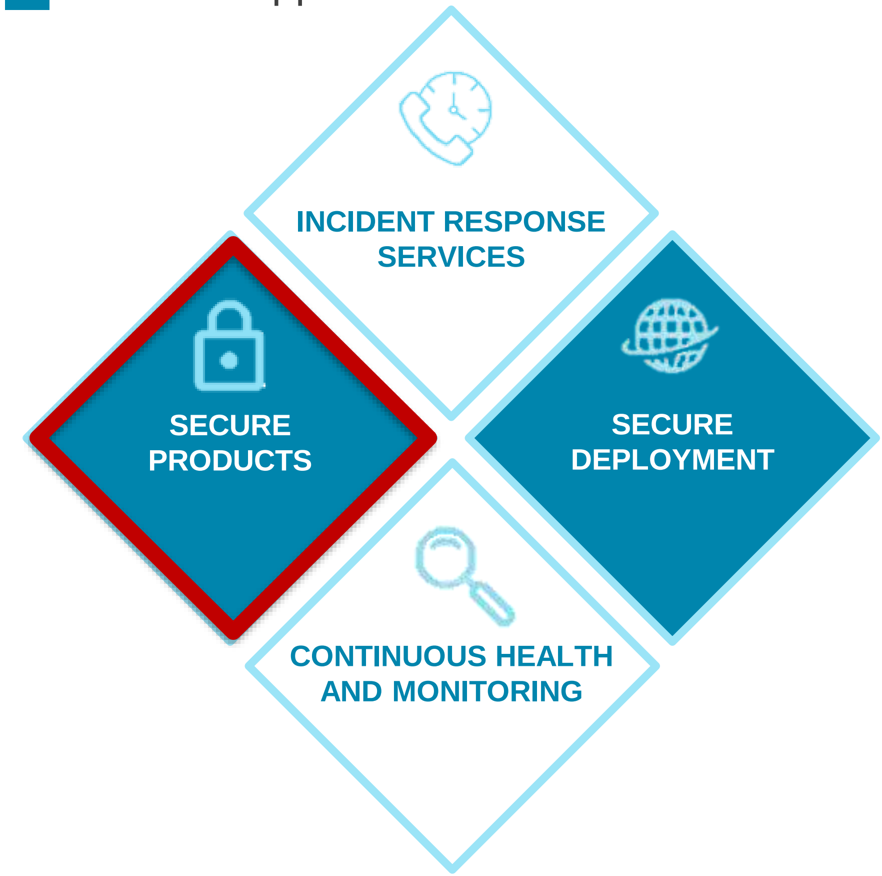
Xylem is building cybersecurity into products and solutions

4

Product Supplier Responsibilities

- Secure product strategies: *Threat Modeling, Testing, Functional Roles, Encryption, Code Signing, Responsible Disclosure*
- Secure deployment guidelines: *Network Segmentation, Patch Management, Security Architecture, Access Controls*

■ Product Supplier

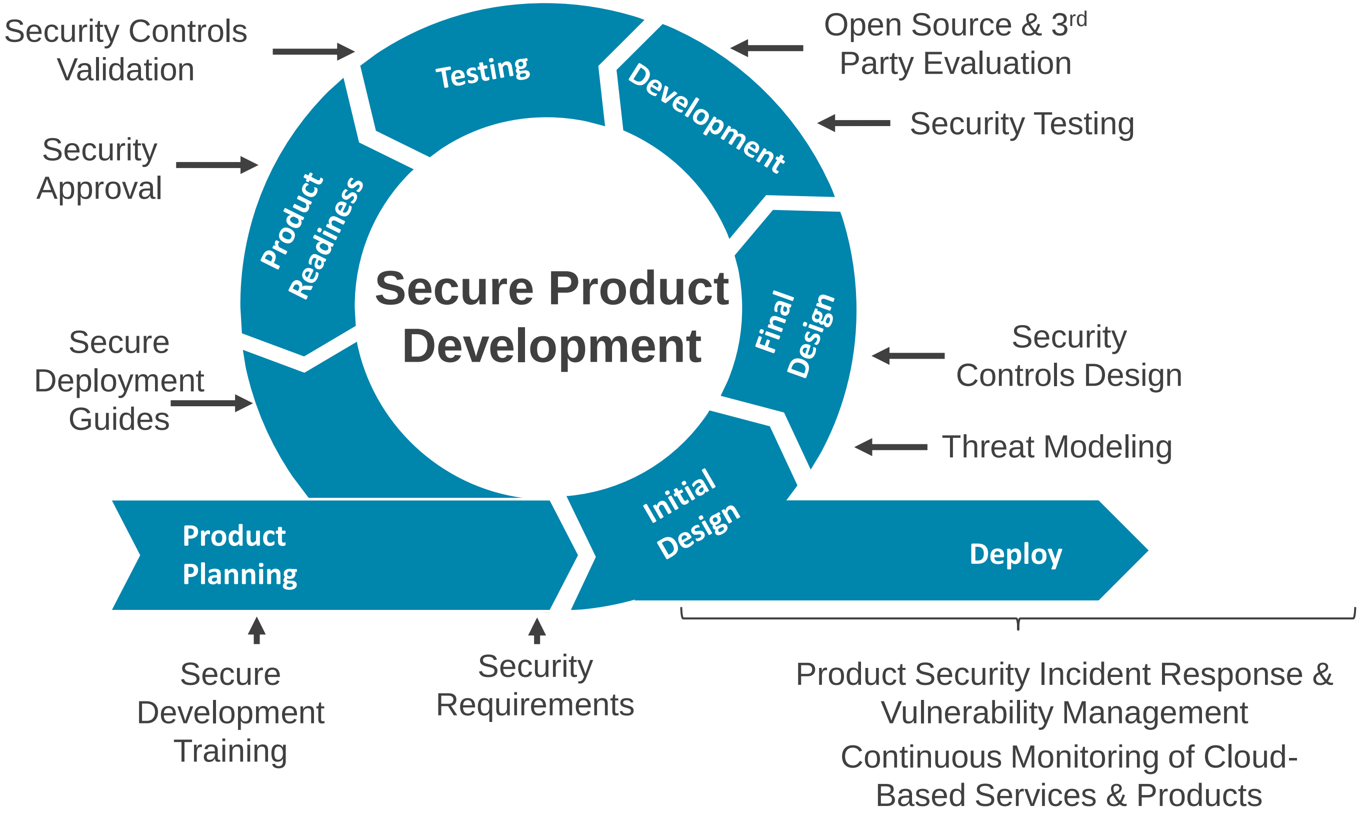


INCIDENT RESPONSE SERVICES

SECURE PRODUCTS

SECURE DEPLOYMENT

CONTINUOUS HEALTH AND MONITORING



Secure Product Development

Product Planning

Initial Design

Final Design

Development

Testing

Product Readiness

Deploy

Security Controls Validation

Security Approval

Secure Deployment Guides

Open Source & 3rd Party Evaluation

Security Testing

Security Controls Design

Threat Modeling

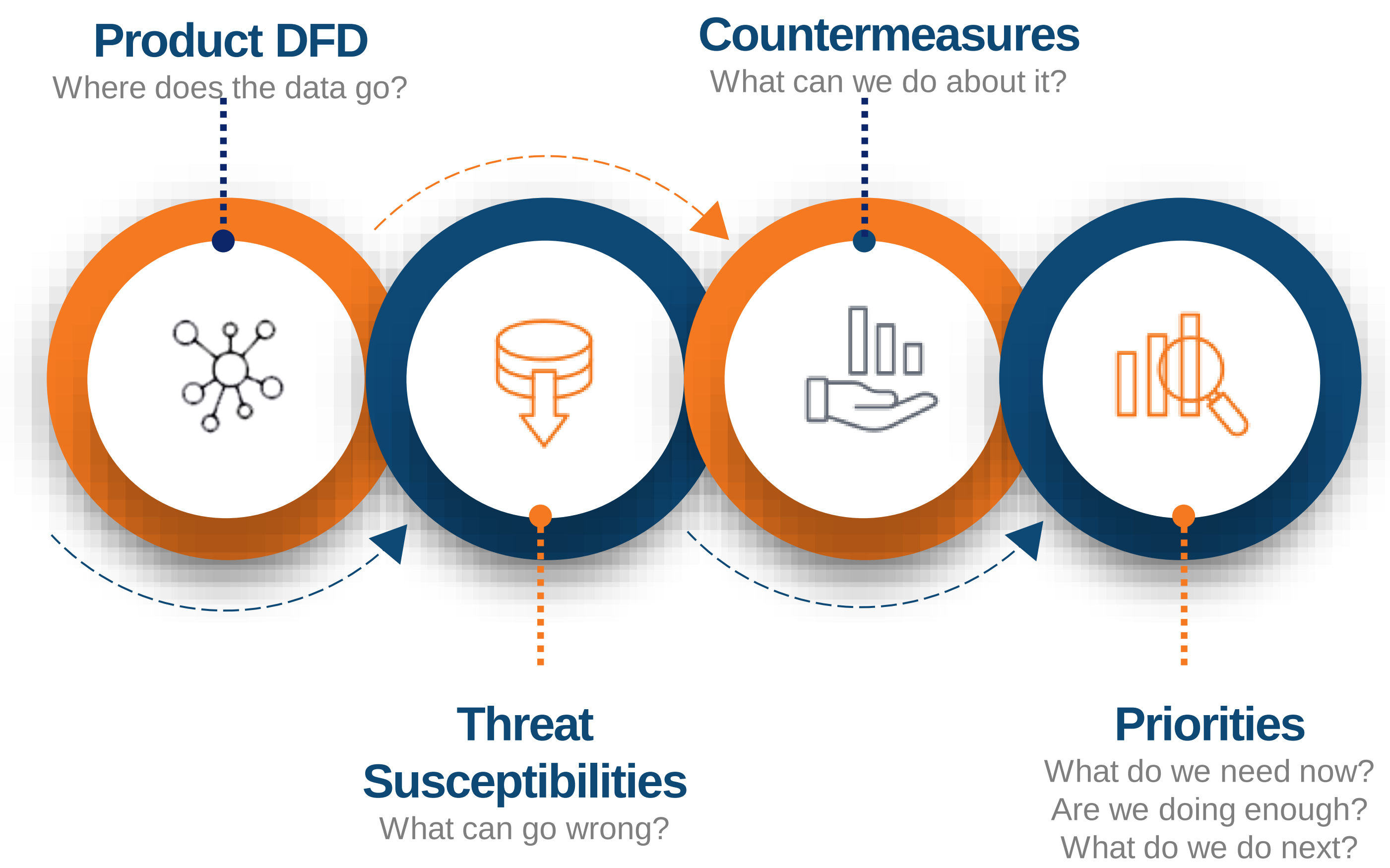
Secure Development Training

Security Requirements

Product Security Incident Response & Vulnerability Management

Continuous Monitoring of Cloud-Based Services & Products

Product Threat Model (focus on data flow, storage, processes)

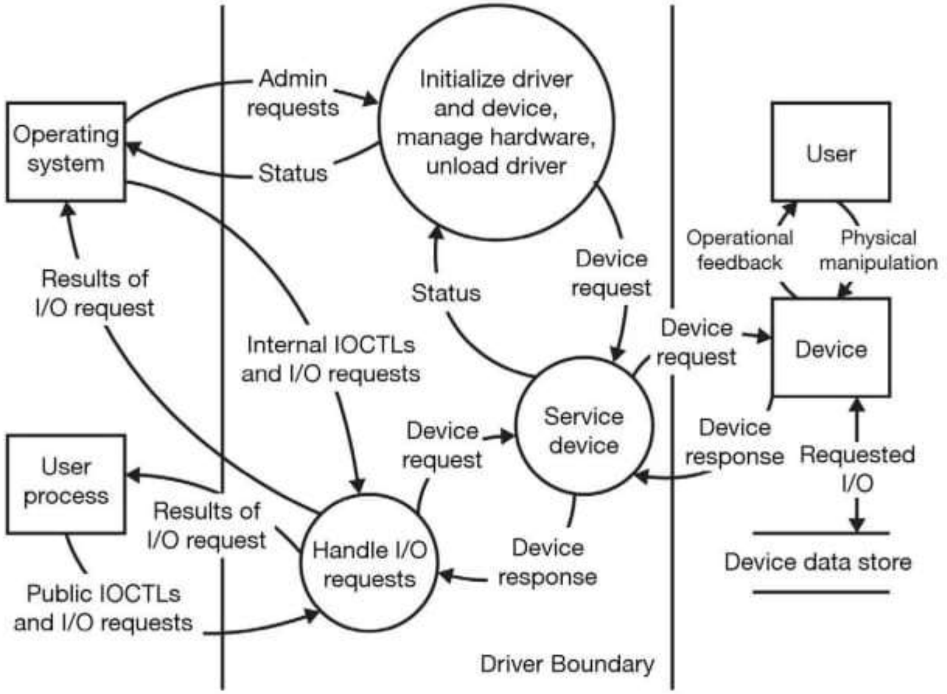


Product DFD
Where does the data go?

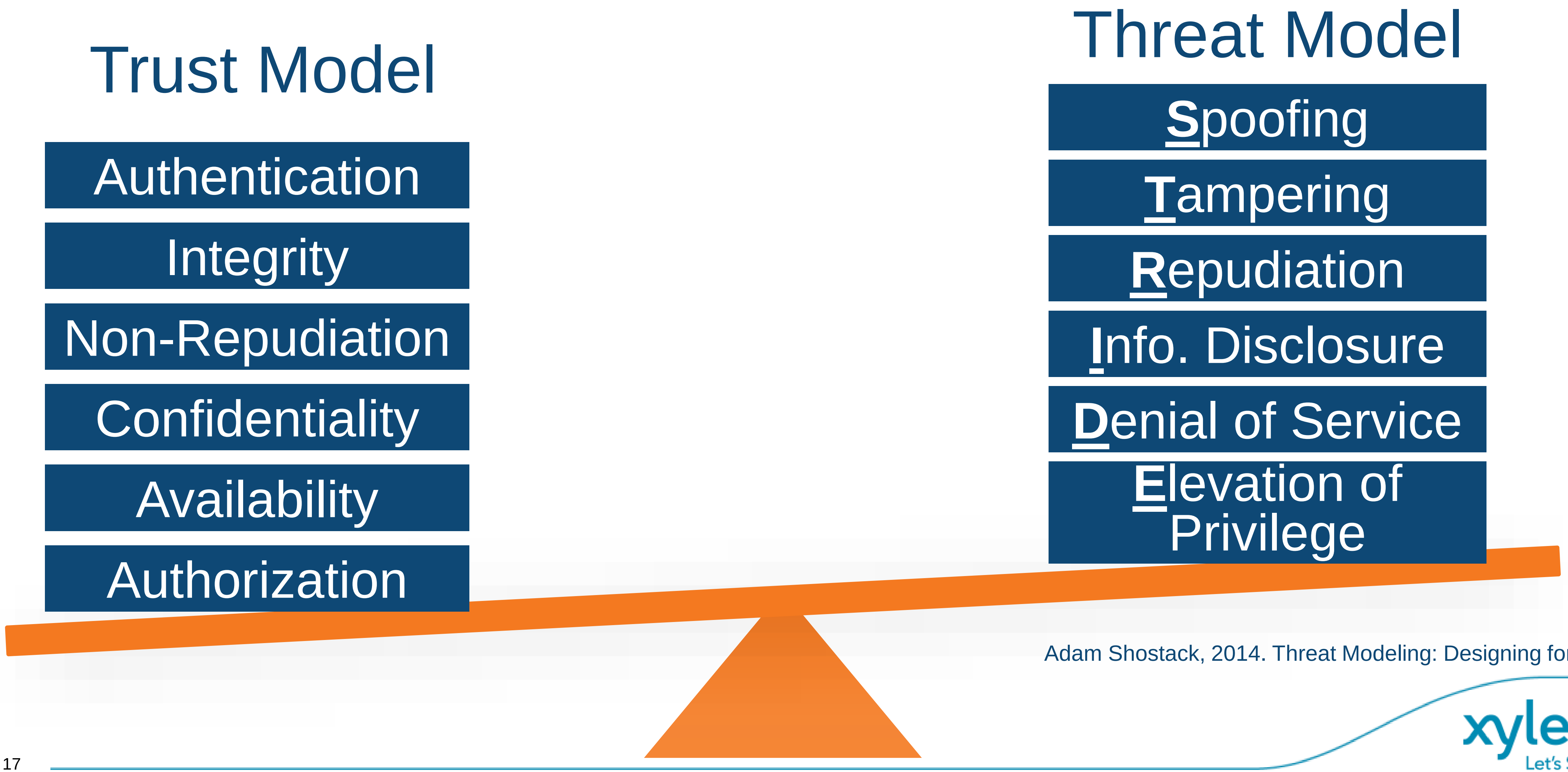
Countermeasures
What can we do about it?

Threat Susceptibilities
What can go wrong?

Priorities
What do we need now?
Are we doing enough?
What do we do next?



Threat Model – Xylem uses **STRIDE** for identifying/classifying threats.



Trust Model

- Authentication
- Integrity
- Non-Repudiation
- Confidentiality
- Availability
- Authorization

Threat Model

- **S**poofing
- **T**ampering
- **R**epudiation
- **I**nfo. Disclosure
- **D**enial of Service
- **E**levation of Privilege

Adam Shostack, 2014. Threat Modeling: Designing for Security

Threat Model – Xylem uses DREAD to help scoring/prioritization.

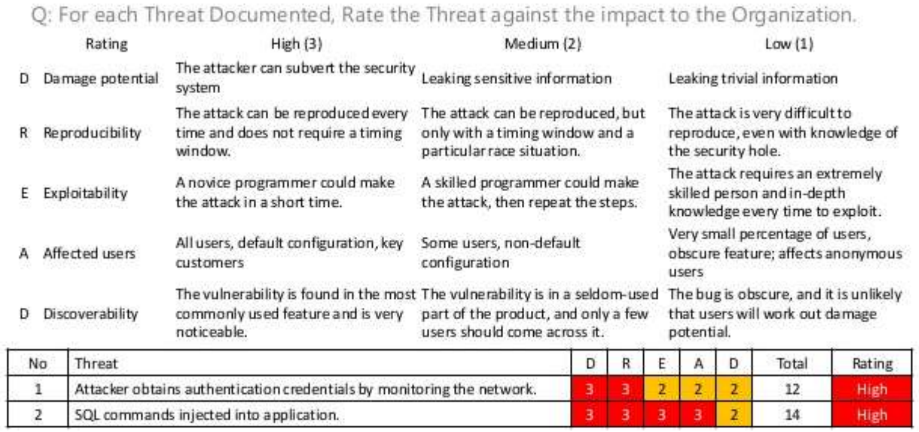
Damage – how bad would an attack be?

Reproducibility – how easy is it to reproduce the attack?

Exploitability – how much work is it to launch the attack?

Affected users – how many people/customers will be impacted?

Discoverability – how easy is it to discover the threat susceptibility?



Q: For each Threat Documented, Rate the Threat against the impact to the Organization.

	Rating	High (3)	Medium (2)	Low (1)
D	Damage potential	The attacker can subvert the security system	Leaking sensitive information	Leaking trivial information
R	Reproducibility	The attack can be reproduced every time and does not require a timing window.	The attack can be reproduced, but only with a timing window and a particular race situation.	The attack is very difficult to reproduce, even with knowledge of the security hole.
E	Exploitability	A novice programmer could make the attack in a short time.	A skilled programmer could make the attack, then repeat the steps.	The attack requires an extremely skilled person and in-depth knowledge every time to exploit.
A	Affected users	All users, default configuration, key customers	Some users, non-default configuration	Very small percentage of users, obscure feature; affects anonymous users
D	Discoverability	The vulnerability is found in the most commonly used feature and is very noticeable.	The vulnerability is in a seldom-used part of the product, and only a few users should come across it.	The bug is obscure, and it is unlikely that users will work out damage potential.

No	Threat	D	R	E	A	D	Total	Rating
1	Attacker obtains authentication credentials by monitoring the network.	3	3	2	2	2	12	High
2	SQL commands injected into application.	3	3	3	3	2	14	High

Testing (a variety of testing methods help track flaw remediation)

SCA – Software Composition Analysis (easy way to find known libraries, licenses, vulnerabilities)

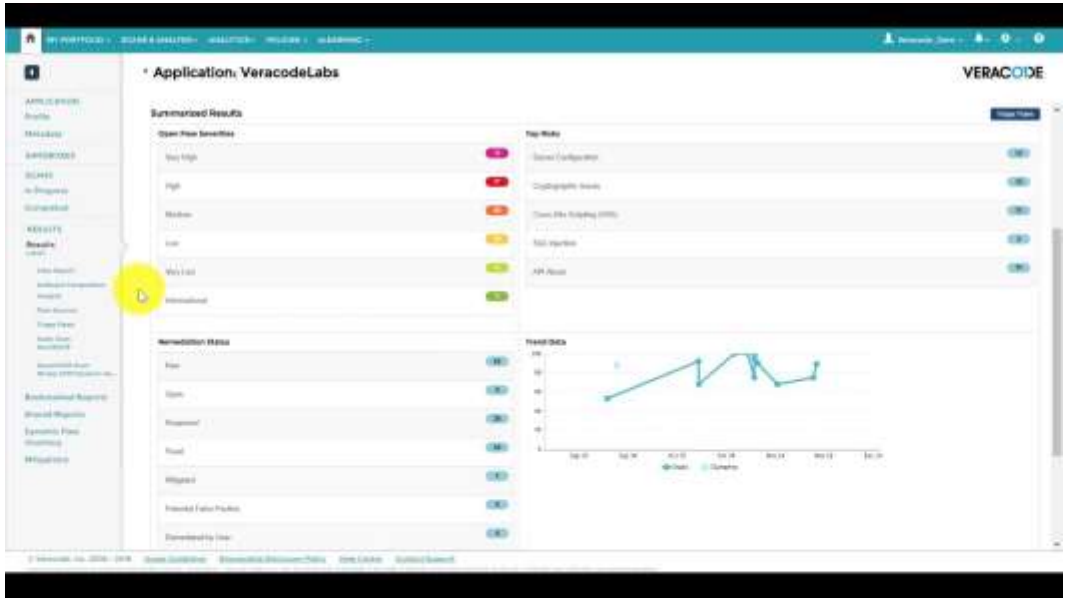
SAST – Static Application Security Testing (looks at code design to find common security flaws) Example: Veracode works for:

- Java, Javascript, C++, Go, etc…
- iOS apps, Android apps (when built in certain way)
- C (when built w GCC-compiler for ARM-based chipset)

Hardware and Firmware Security Testing (manually looks at peripheral connectivity and code design for security flaws)

Protocol / Fuzz Testing (sends malformed information to look for coding errors and security flaws)

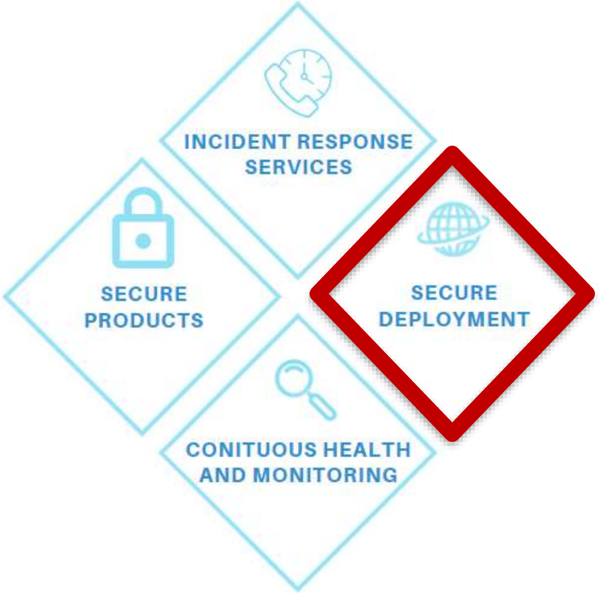
Penetration Testing (schedule for high-risk products)

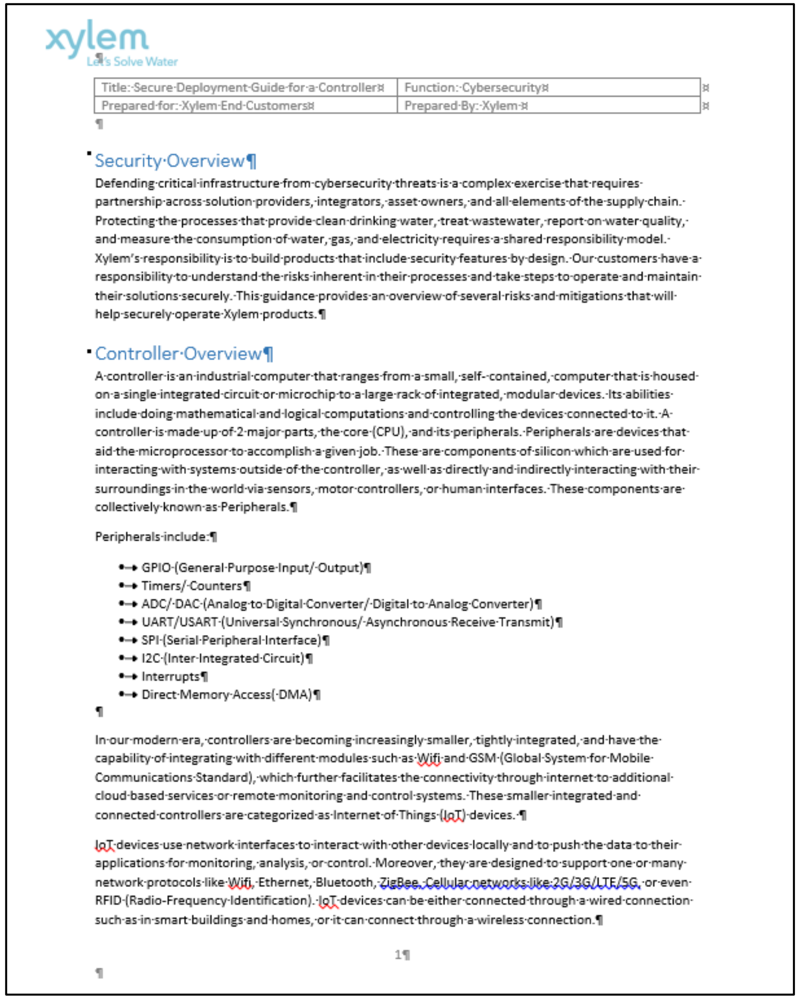


Secure Deployment Guides help integrators and customers

Supplement Installation and Operations Manuals.

- Overview of product security
- Description of product cybersecurity features
- Customer guidance for secure deployment





Title: Secure Deployment Guide for a Controller	Function: Cybersecurity
Prepared for: Xylem End Customers	Prepared By: Xylem

Security Overview

Defending critical infrastructure from cybersecurity threats is a complex exercise that requires partnership across solution providers, integrators, asset owners, and all elements of the supply chain. Protecting the processes that provide clean drinking water, treat wastewater, report on water quality, and measure the consumption of water, gas, and electricity requires a shared responsibility model. Xylem's responsibility is to build products that include security features by design. Our customers have a responsibility to understand the risks inherent in their processes and take steps to operate and maintain their solutions securely. This guidance provides an overview of several risks and mitigations that will help securely operate Xylem products.

Controller Overview

A controller is an industrial computer that ranges from a small, self- contained, computer that is housed on a single integrated circuit or microchip to a large rack of integrated, modular devices. Its abilities include doing mathematical and logical computations and controlling the devices connected to it. A controller is made up of 2 major parts, the core (CPU), and its peripherals. Peripherals are devices that aid the microprocessor to accomplish a given job. These are components of silicon which are used for interacting with systems outside of the controller, as well as directly and indirectly interacting with their surroundings in the world via sensors, motor controllers, or human interfaces. These components are collectively known as Peripherals.

Peripherals include:

- GPIO (General Purpose Input/ Output)
- Timers/ Counters
- ADC/ DAC (Analog to Digital Converter/ Digital to Analog Converter)
- UART/USART (Universal Synchronous/ Asynchronous Receive Transmit)
- SPI (Serial Peripheral Interface)
- I2C (Inter Integrated Circuit)
- Interrupts
- Direct Memory Access(DMA)

In our modern era, controllers are becoming increasingly smaller, tightly integrated, and have the capability of integrating with different modules such as Wifi and GSM (Global System for Mobile Communications Standard), which further facilitates the connectivity through internet to additional cloud based services or remote monitoring and control systems. These smaller integrated and connected controllers are categorized as Internet of Things (IoT) devices.

IoT devices use network interfaces to interact with other devices locally and to push the data to their applications for monitoring, analysis, or control. Moreover, they are designed to support one or many network protocols like Wifi, Ethernet, Bluetooth, ZigBee, Cellular networks like 2G/3G/LTE/5G, or even RFID (Radio-Frequency Identification). IoT devices can be either connected through a wired connection such as in smart buildings and homes, or it can connect through a wireless connection.

1

Product Security Operations Center (PSOC) & Product Security Incident Response Team (PSIRT)

PSOC

- continuously collect logs (firewall, IOT connections, certificate usage, product changes)

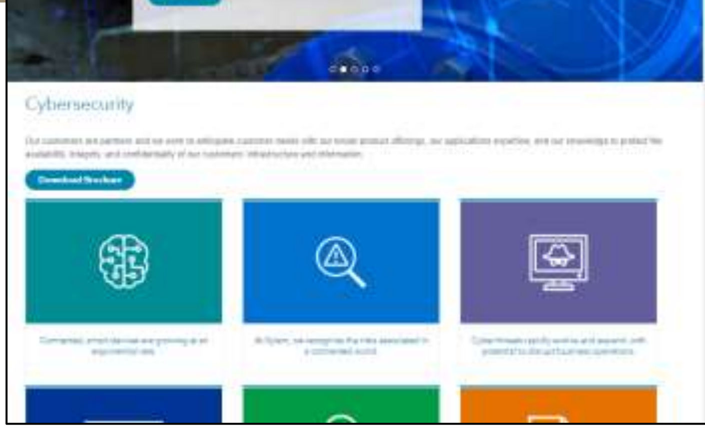
- continuously deploy updates and monitor infrastructure

- continuous collect threats and do threat hunting for "indicators of possible compromise"

PSIRT

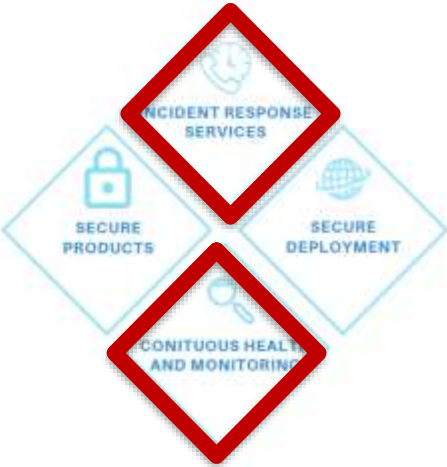
- continuous monitor threat researcher community

- quickly coordinate across product teams for updates and communication to customers



Cybersecurity

Download Brochure


NCIDENT RESPONSE SERVICES

SECURE PRODUCTS

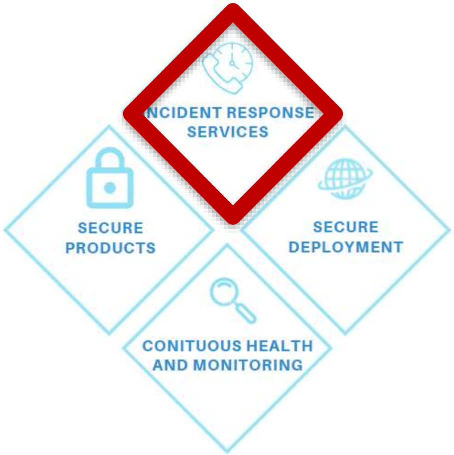
SECURE DEPLOYMENT

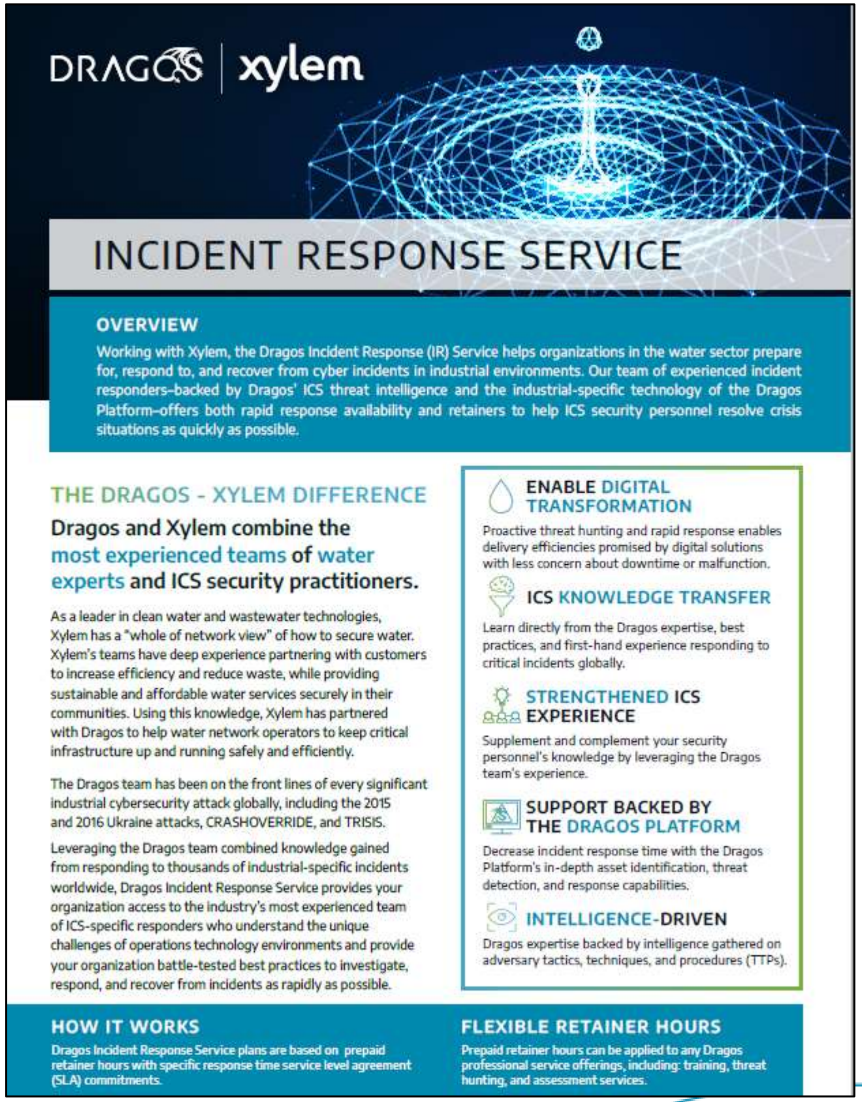
CONITUOUS HEALT AND MONITORIN

xylem.com/security

Partnership with Dragos (for security evaluations and IR services

- Enables rapid response to active industrial intrusion
- Reduces mean time to recover from industrial incidents
- Prepares customers for industrial incidents across all business units
- Prevents future industrial accidents




DRAGOS | xylem

INCIDENT RESPONSE SERVICE

OVERVIEW

Working with Xylem, the Dragos Incident Response (IR) Service helps organizations in the water sector prepare for, respond to, and recover from cyber incidents in industrial environments. Our team of experienced incident responders–backed by Dragos' ICS threat intelligence and the industrial-specific technology of the Dragos Platform–offers both rapid response availability and retainers to help ICS security personnel resolve crisis situations as quickly as possible.

THE DRAGOS - XYLEM DIFFERENCE

Dragos and Xylem combine the most experienced teams of water experts and ICS security practitioners.

As a leader in clean water and wastewater technologies, Xylem has a "whole of network view" of how to secure water. Xylem's teams have deep experience partnering with customers to increase efficiency and reduce waste, while providing sustainable and affordable water services securely in their communities. Using this knowledge, Xylem has partnered with Dragos to help water network operators to keep critical infrastructure up and running safely and efficiently.

The Dragos team has been on the front lines of every significant industrial cybersecurity attack globally, including the 2015 and 2016 Ukraine attacks, CRASHOVERRIDE, and TRISIS.

Leveraging the Dragos team combined knowledge gained from responding to thousands of industrial-specific incidents worldwide, Dragos Incident Response Service provides your organization access to the industry's most experienced team of ICS-specific responders who understand the unique challenges of operations technology environments and provide your organization battle-tested best practices to investigate, respond, and recover from incidents as rapidly as possible.

ENABLE DIGITAL TRANSFORMATION

Proactive threat hunting and rapid response enables delivery efficiencies promised by digital solutions with less concern about downtime or malfunction.

ICS KNOWLEDGE TRANSFER

Learn directly from the Dragos expertise, best practices, and first-hand experience responding to critical incidents globally.

STRENGTHENED ICS EXPERIENCE

Supplement and complement your security personnel's knowledge by leveraging the Dragos team's experience.

SUPPORT BACKED BY THE DRAGOS PLATFORM

Decrease incident response time with the Dragos Platform's in-depth asset identification, threat detection, and response capabilities.

INTELLIGENCE-DRIVEN

Dragos expertise backed by intelligence gathered on adversary tactics, techniques, and procedures (TTPs).

HOW IT WORKS

Dragos Incident Response Service plans are based on prepaid retainer hours with specific response time service level agreement (SLA) commitments.

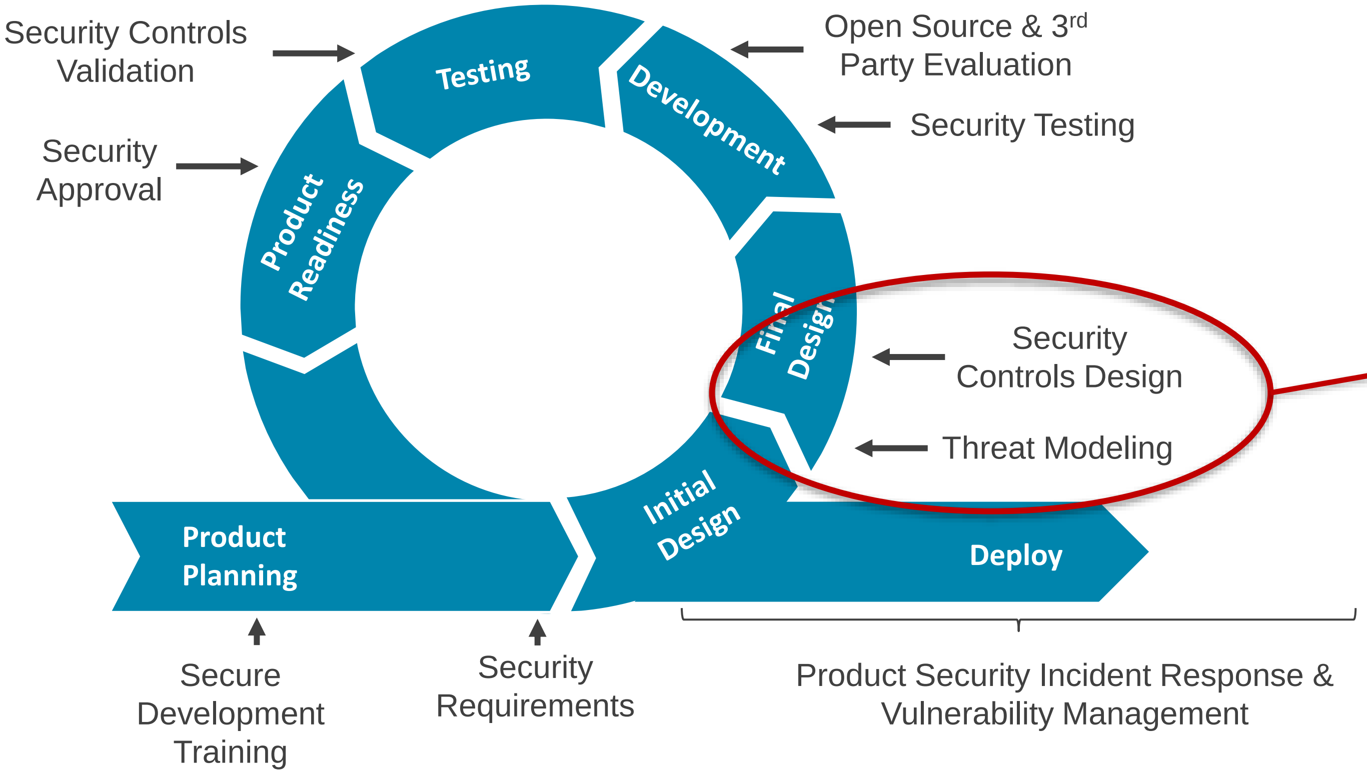
FLEXIBLE RETAINER HOURS

Prepaid retainer hours can be applied to any Dragos professional service offerings, including: training, threat hunting, and assessment services.

xylem
Let's Solve Water

Protecting Over-the-air firmware updates (FOTA) for Industrial Internet of Things (IIOT) - Threat Model

5



Product Planning

Initial Design

Final Design

Development

Testing

Product Readiness

Deploy

Security Controls Validation

Security Approval

Open Source & 3rd Party Evaluation

Security Testing

Security Controls Design

Threat Modeling

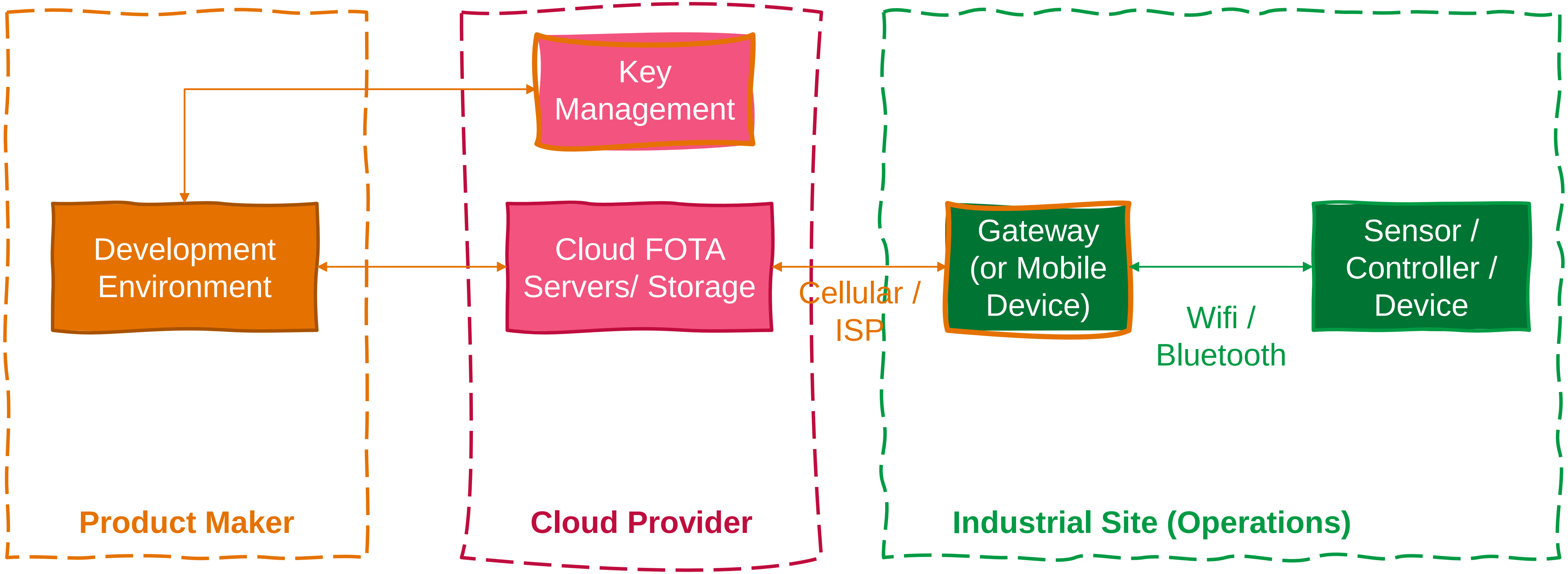
Secure Development Training

Security Requirements

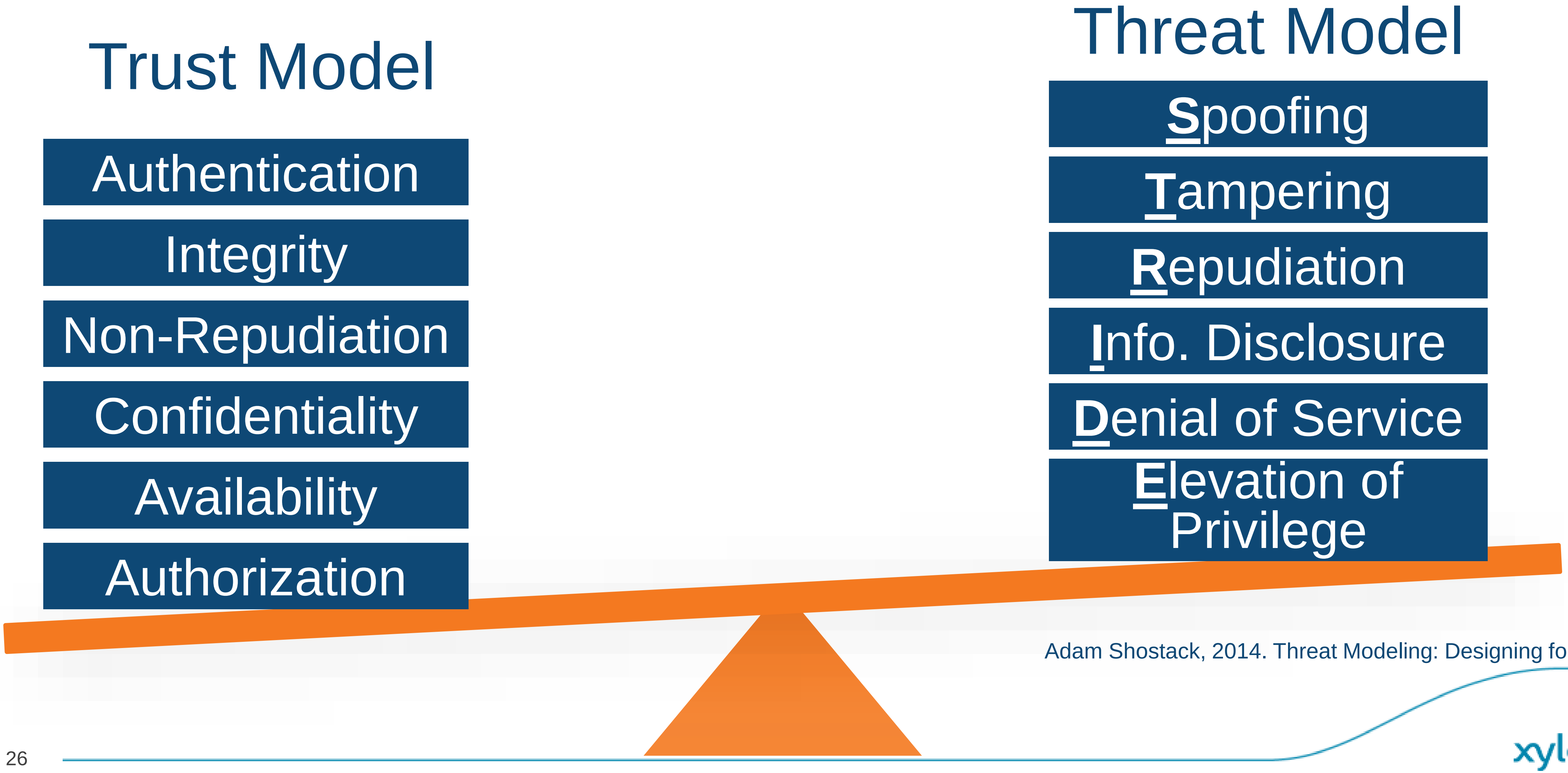
Product Security Incident Response & Vulnerability Management

Inherent risk is high for FOTA;
No security requirements/specs;
Focus is on threat modeling for strong security controls

Over-the-air firmware updates (FOTA) – rough sketch


Key Management
Development Environment
Cloud FOTA Servers/ Storage
Cellular / ISP
Gateway (or Mobile Device)
Wifi / Bluetooth
Sensor / Controller / Device
Product Maker
Cloud Provider
Industrial Site (Operations)

Threat Model – Xylem uses STRIDE for identifying/classifying threats.



Trust Model

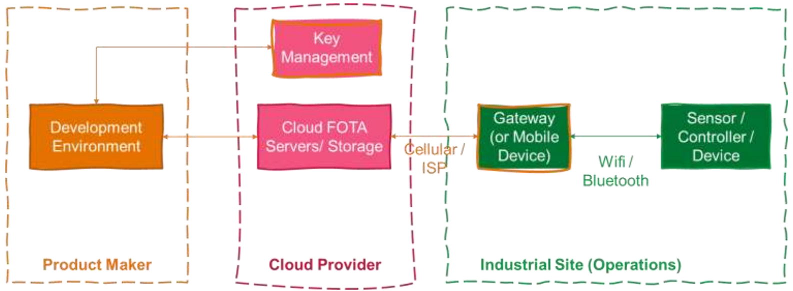
- Authentication
- Integrity
- Non-Repudiation
- Confidentiality
- Availability
- Authorization

Threat Model

- **S**poofing
- **T**ampering
- **R**epudiation
- **I**nfo. Disclosure
- **D**enial of Service
- **E**levation of Privilege

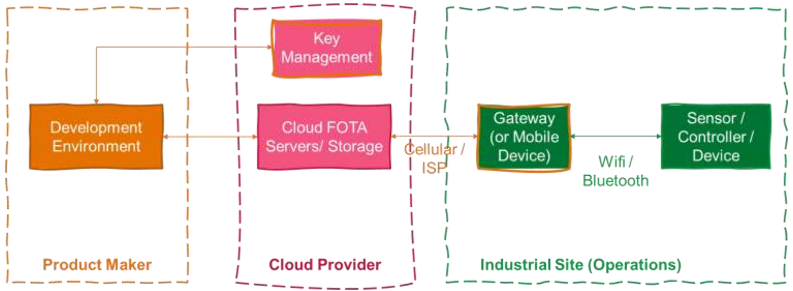
Adam Shostack, 2014. Threat Modeling: Designing for Security

FOTA attack surface (examples)


Key Management
Development Environment
Cloud FOTA Servers/ Storage
Cellular / ISP
Gateway (or Mobile Device)
Wifi / Bluetooth
Sensor / Controller / Device
Product Maker
Cloud Provider
Industrial Site (Operations)

	Product Maker	Pipeline/Cloud	Operations
S	Spoof developers' identity	Masquerade as the FOTA server endpoint	Installed signed firmware with stolen private key
T	Change firmware in dev environment	Rogue firmware available for update	Tamper firmware in transit over Bluetooth
R		Untracked changes to config file for controlling updates	Untracked changes by adversary
I	Stolen copy of firmware from repository for counterfeit		Steal copy of firmware while in transit over Bluetooth to make counterfeit
D		Pretend to be a gateway and flood the update channel	Download “really large” update (unsigned) to use-up battery
E	DevOps admin changes firmware	Internal user gets higher level access (e.g., to other’s data)	

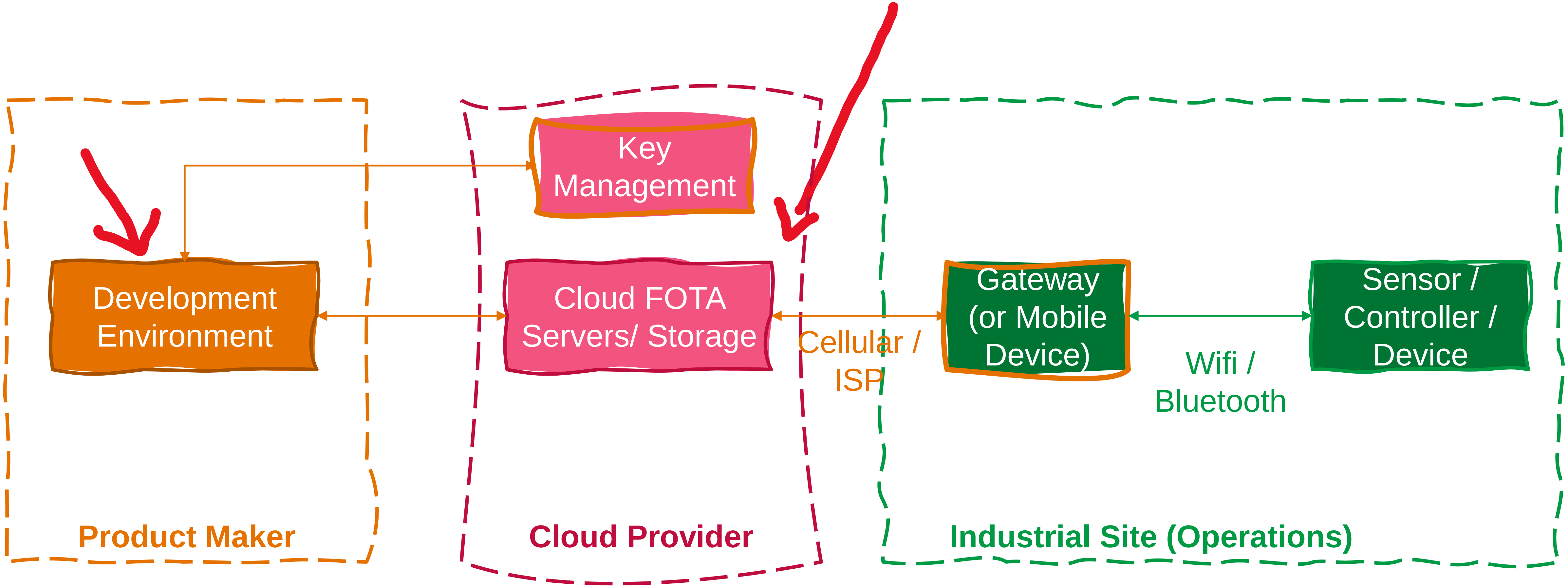
FOTA attack surface - Example 1


Key Management
Development Environment
Cloud FOTA Servers/ Storage
Cellular / ISP
Gateway (or Mobile Device)
Sensor / Controller / Device
Wifi / Bluetooth
Product Maker
Cloud Provider
Industrial Site (Operations)

	Product Maker	Pipeline/Cloud	Operations
S	Spoof developers' identity	Masquerade as the FOTA server endpoint	Installed signed firmware with stolen private key
T	Change firmware in dev environment	Rogue firmware available for update	Tamper firmware in transit over Bluetooth
R		Untracked changes to config file for controlling updates	Untracked changes by adversary
I	Stolen copy of firmware from repository for counterfeit		Steal copy of firmware while in transit over Bluetooth to make counterfeit
D		Pretend to be a gateway and flood the update channel	Download “really large” update (unsigned) to use-up battery
E	DevOps admin changes firmware	Internal user gets higher level access (e.g., to other’s data)	

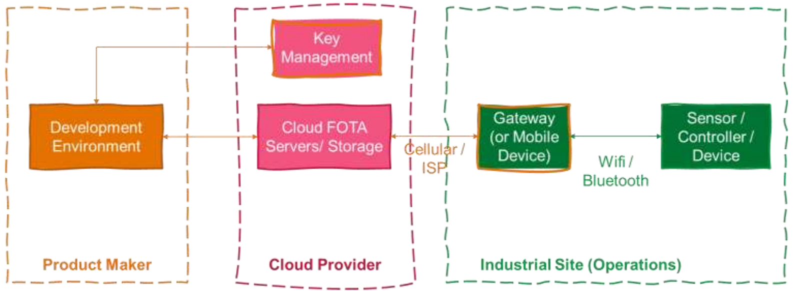
FOTA Threats – Example 1

Threats: Internal users getting elevation of privileges; spoof developer's identity


Key Management
Development Environment
Cloud FOTA Servers/ Storage
Cellular / ISP
Gateway (or Mobile Device)
Wifi / Bluetooth
Sensor / Controller / Device
Product Maker
Cloud Provider
Industrial Site (Operations)

Controls: authorization checks, multifactor authentication, two-party approval process, logging, network segmentation

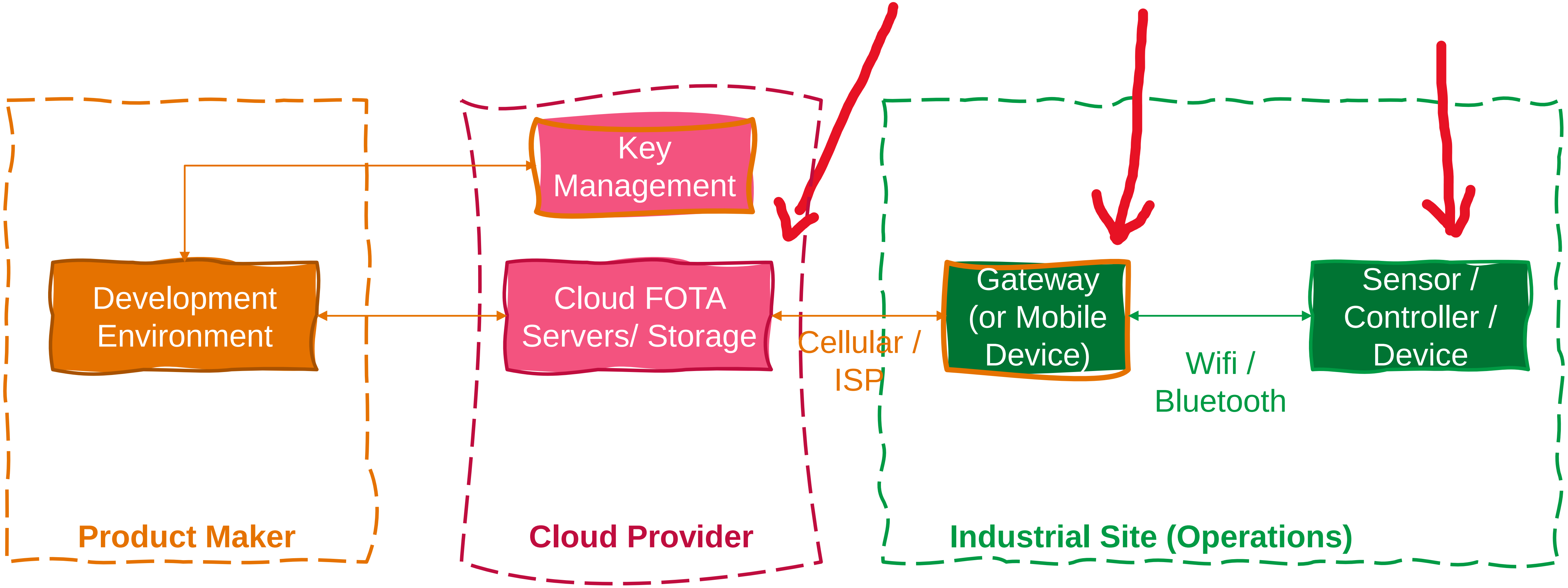
FOTA attack surface - Example 2


Key Management
Development Environment
Cloud FOTA Servers/ Storage
Cellular / ISP
Gateway (or Mobile Device)
Wifi / Bluetooth
Sensor / Controller / Device
Product Maker
Cloud Provider
Industrial Site (Operations)

	Product Maker	Pipeline/Cloud	Operations
S	Spoof developers' identity	Masquerade as the FOTA server endpoint	Installed signed firmware with stolen private key
T	Change firmware in dev environment	Rogue firmware available for update	Tamper firmware in transit over Bluetooth
R		Untracked changes to config file for controlling updates	Untracked changes by adversary
I	Stolen copy of firmware from repository for counterfeit		Steal copy of firmware while in transit over Bluetooth to make counterfeit
D		Pretend to be a gateway and flood the update channel	Download “really large” update (unsigned) to use-up battery
E	DevOps admin changes firmware	Internal user gets higher level access (e.g., to other’s data)	

FOTA Threats – Example 2

Threats: rogue firmware updates; really large update files


Key Management
Development Environment
Cloud FOTA Servers/ Storage
Cellular / ISP
Gateway (or Mobile Device)
Wifi / Bluetooth
Sensor / Controller / Device
Product Maker
Cloud Provider
Industrial Site (Operations)

Controls: signing, logging, version tracking and verification, validation checks on the update size and battery

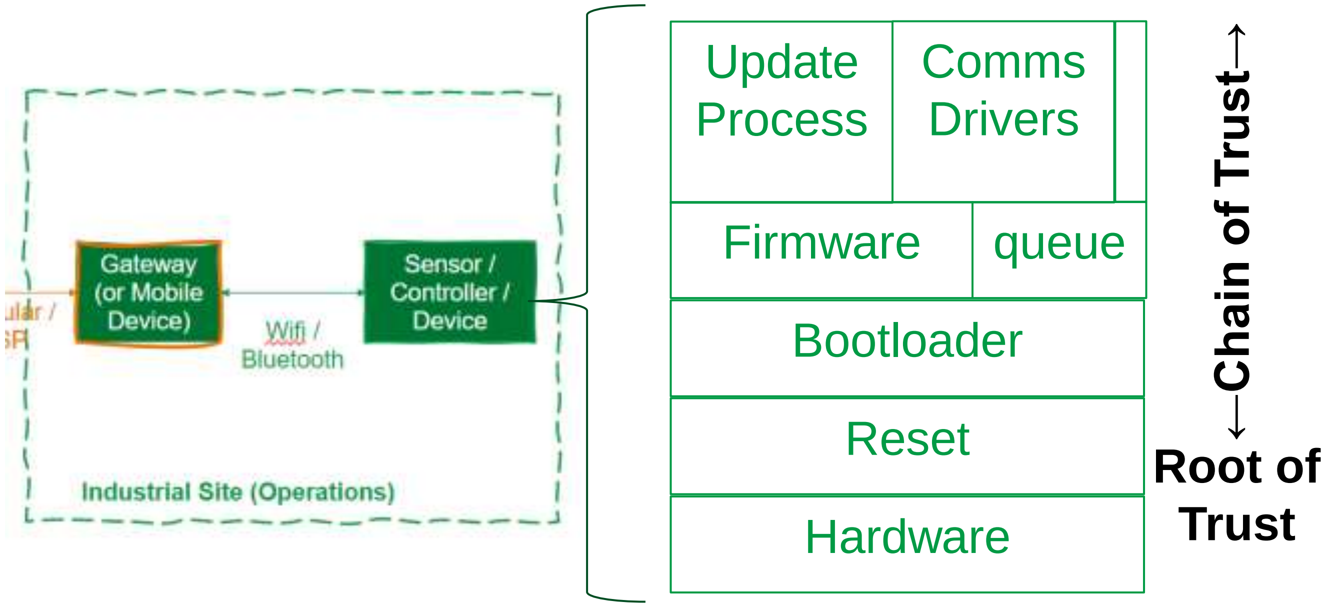
xylem
Let's Solve Water

Protecting Over-the-air firmware updates (FOTA) for Industrial Internet of Things (IIOT) - Security Controls

6

1. Ensure that the device can verify the authenticity and integrity of any FW, and that it can continue to securely operate if the FW update process is interrupted.

- Firmware signing
- Private key protection
- Secure boot / boot integrity
- Secure update process
- Device resilience and rollback


ular /
SP
Gateway (or Mobile Device)
Wifi / Bluetooth
Sensor / Controller / Device
Industrial Site (Operations)

Update Process | Comms Drivers

Firmware | queue

Bootloader

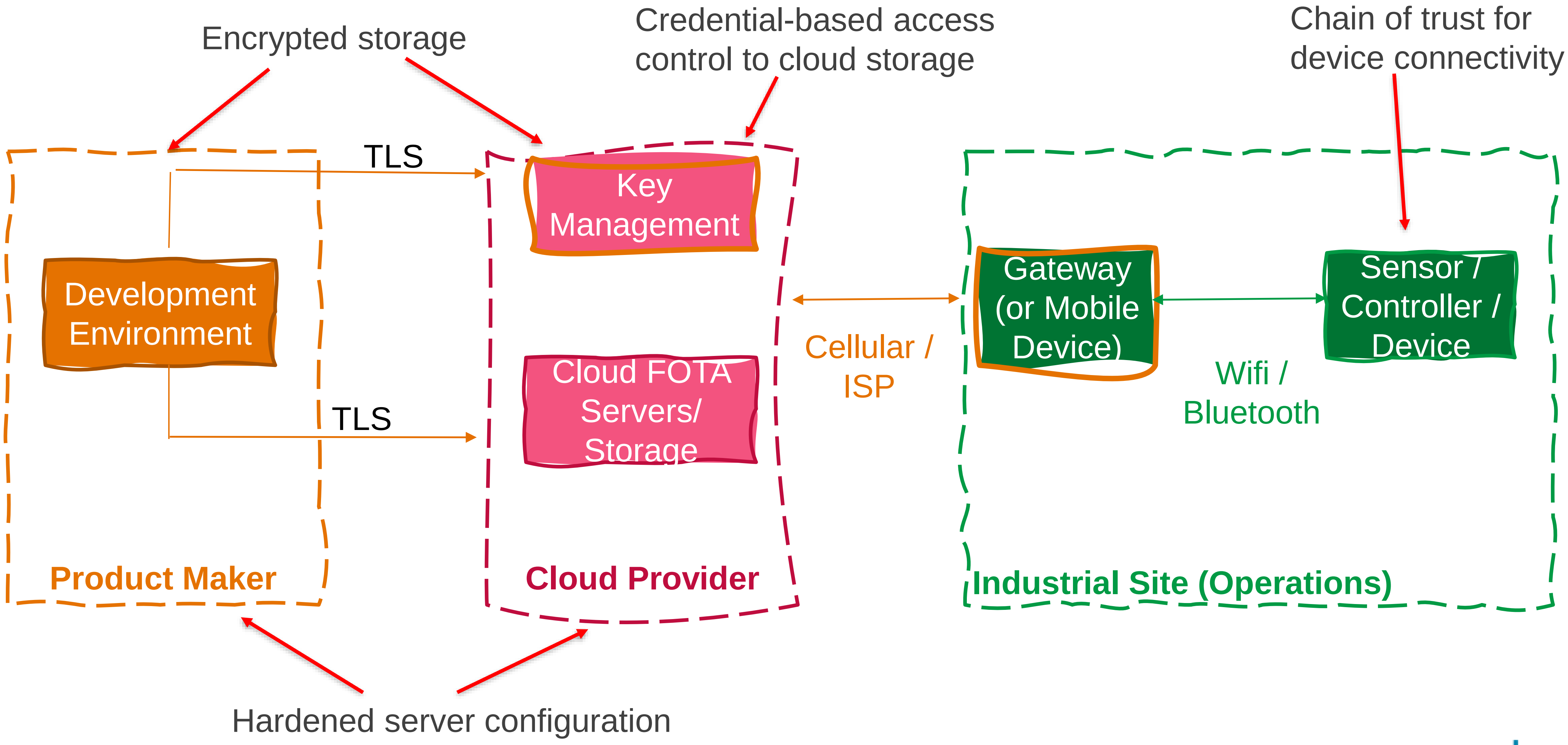
Reset

Hardware

←Chain of Trust→

Root of Trust

2. Ensure that the FW is protected from time of compilation/signing, at rest on cloud servers, and in transit.

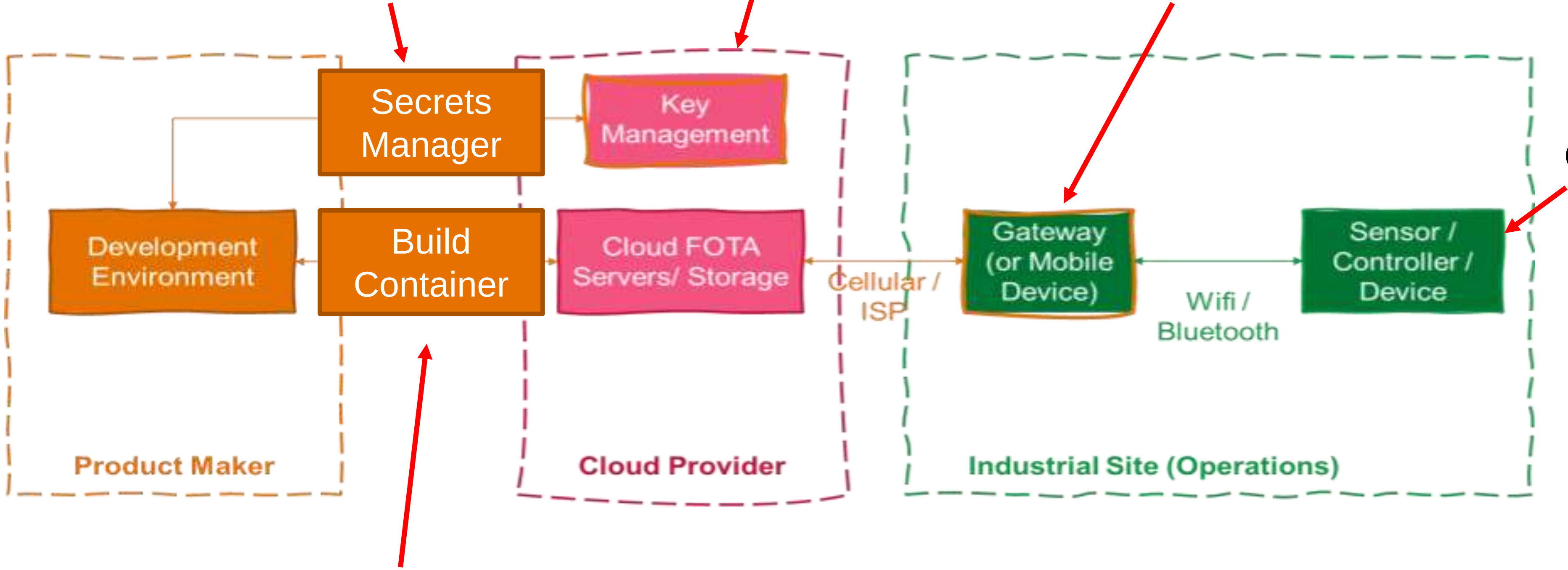

Encrypted storage
Credential-based access control to cloud storage
Chain of trust for device connectivity
TLS
Key Management
Development Environment
TLS
Cloud FOTA Servers/ Storage
Cellular / ISP
Gateway (or Mobile Device)
Wifi / Bluetooth
Sensor / Controller / Device
Product Maker
Cloud Provider
Industrial Site (Operations)
Hardened server configuration

3. Automate the build pipeline for FOTA.

Separate credentials from
the build container

Use cloud KMS
with unshared
private key

Gateway pre-verification

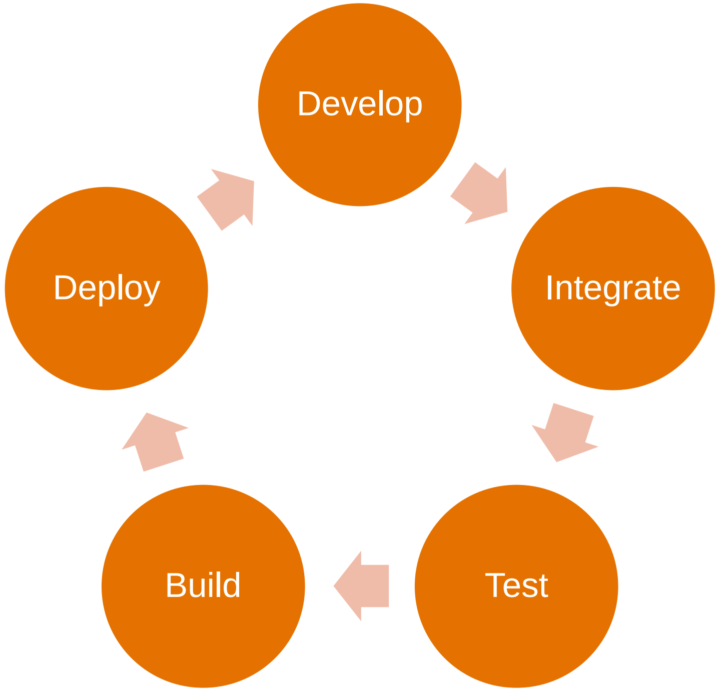


Crypto agility –
know whether
how to rotate
keys or
algorithms

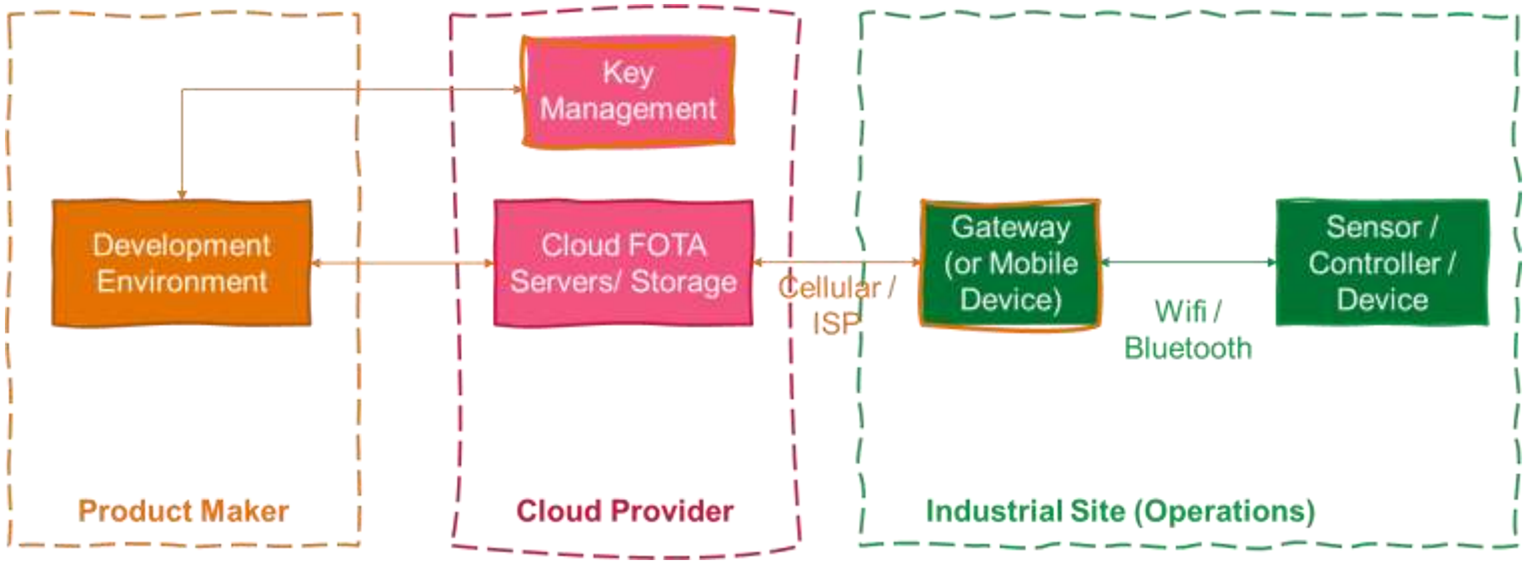
Automated firmware build & sign
might require special tools.
(Use logs and log-suppression
appropriately.)

4. Ensure that the FW build process minimizes the possibility of tampering, repudiation, etc. and that the FW builds are verified and logged prior to distribution.

- Role-based access control
- Firmware testing and verification
- Two+ person “merge to master” approval process
- Multi-factor authentication for privileged roles
- Full logging and log comparison
- Version verification
- Pipelines automation



Over-the-air firmware updates (FOTA) – Summary


Key Management
Development Environment
Cloud FOTA Servers/ Storage
Cellular / ISP
Gateway (or Mobile Device)
Wifi / Bluetooth
Sensor / Controller / Device
Product Maker
Cloud Provider
Industrial Site (Operations)

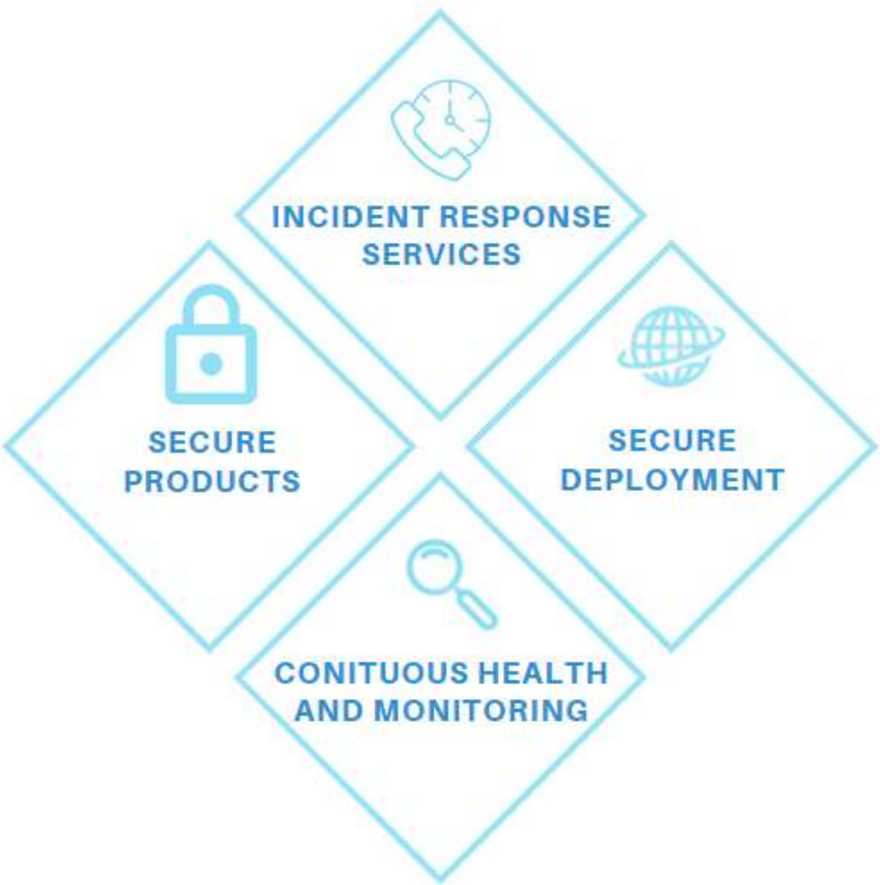
1. Ensure that the ***device can verify the authenticity and integrity*** *of any FW, and that it can continue to securely operate if the FW update process is interrupted.*

2. Ensure that the ***FW is protected from source to destination*** *from time of compilation/signing, at rest on cloud servers, and in transit.*

3. ***Automate*** *the build pipeline for FOTA.*

4. Ensure that the ***FW processes are hardened*** *minimizing the possibility of tampering, repudiation, etc. and that the FW builds* ***are verified and logged*** *prior to distribution.*

Cybersecurity Multi-Barrier Approach is a Partnership



Secure products by finding and fixing weaknesses while engineering

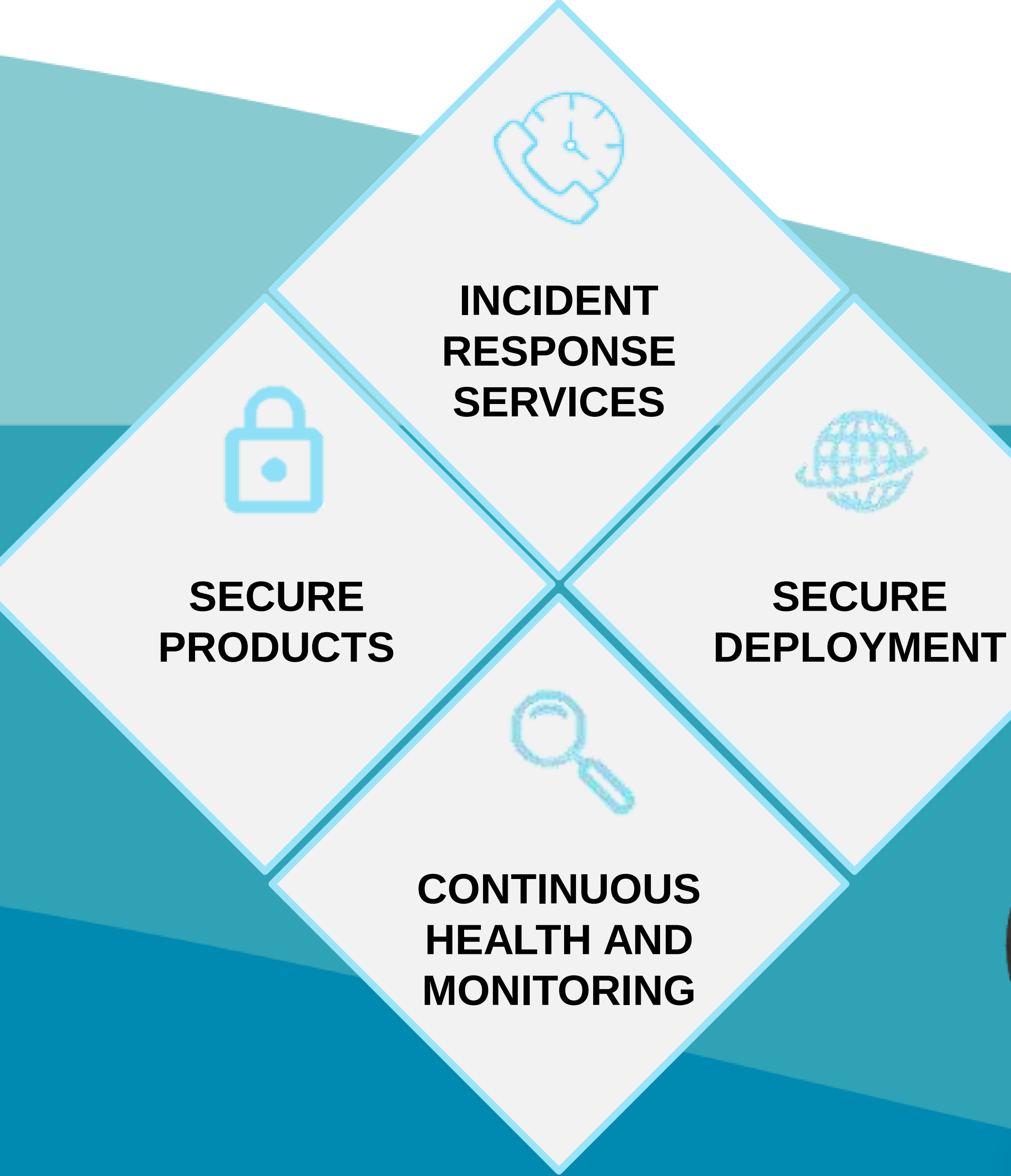
Secure deployments with defense-in-depth that manages risks to the operations of systems and products

Continuous health and monitoring ensures continuous improvement against emerging vulnerabilities and threats

Incident response services assures optimal forensics and response for safe and continuous operations

The operator of the utility is the end owner of security risk, but responsibility for security protection falls on the product vendor, integrator, and operator.

xylem



INCIDENT RESPONSE SERVICES

SECURE PRODUCTS

SECURE DEPLOYMENT

CONTINUOUS HEALTH AND MONITORING

Questions?

Dr. Kenneth G. Crowther
Product Cybersecurity Leader
Americas Commercial Teams, Xylem Inc.
Kenneth.Crowther@xylem.com