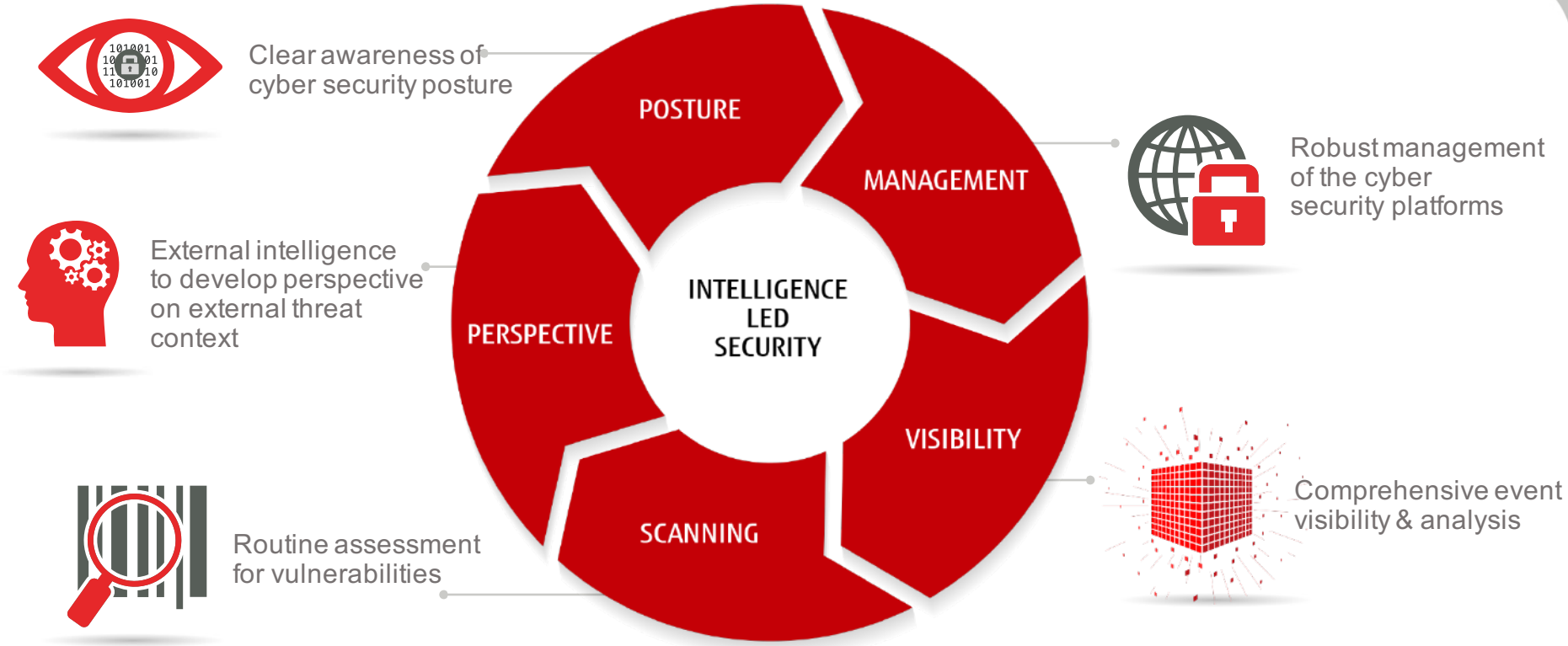# Agenda

- Security Challenge

- Comparing IoT and HPC

- Lessons Learnt

Security Challenge

- Security Architecture: Defence in Depth

  - End-point, Network, System architecture

- Stakeholder's View

- Risk Management Framework

- Security Policy

Intelligence Led Security Lifecycle

Clear awareness of cyber security posture

External intelligence to develop perspective on external threat context

Routine assessment for vulnerabilities

POSTURE

MANAGEMENT

PERSPECTIVE

INTELLIGENCE LED SECURITY

VISIBILITY

SCANNING

Robust management of the cyber security platforms

Comprehensive event visibility & analysis

Internet of Things

Millions and Billions of Devices
Generating Data every second, every year
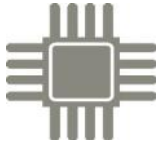
Key Elements in IoT System

Analytics and Applications

IoT Platform (Cloud)

Core and Edge Networks

Devices & Sensors, Sensor Network

Potential IoT Application Scenarios

Potential Themes

- Operational Optimization
- Workers Safety
- Worker Productivity
- Inventory Management
- Equipment Preventive Maintenance
- Physical Security
- Energy Management
- Many More...

IoT Platform Analytics

Security Threats in IoT
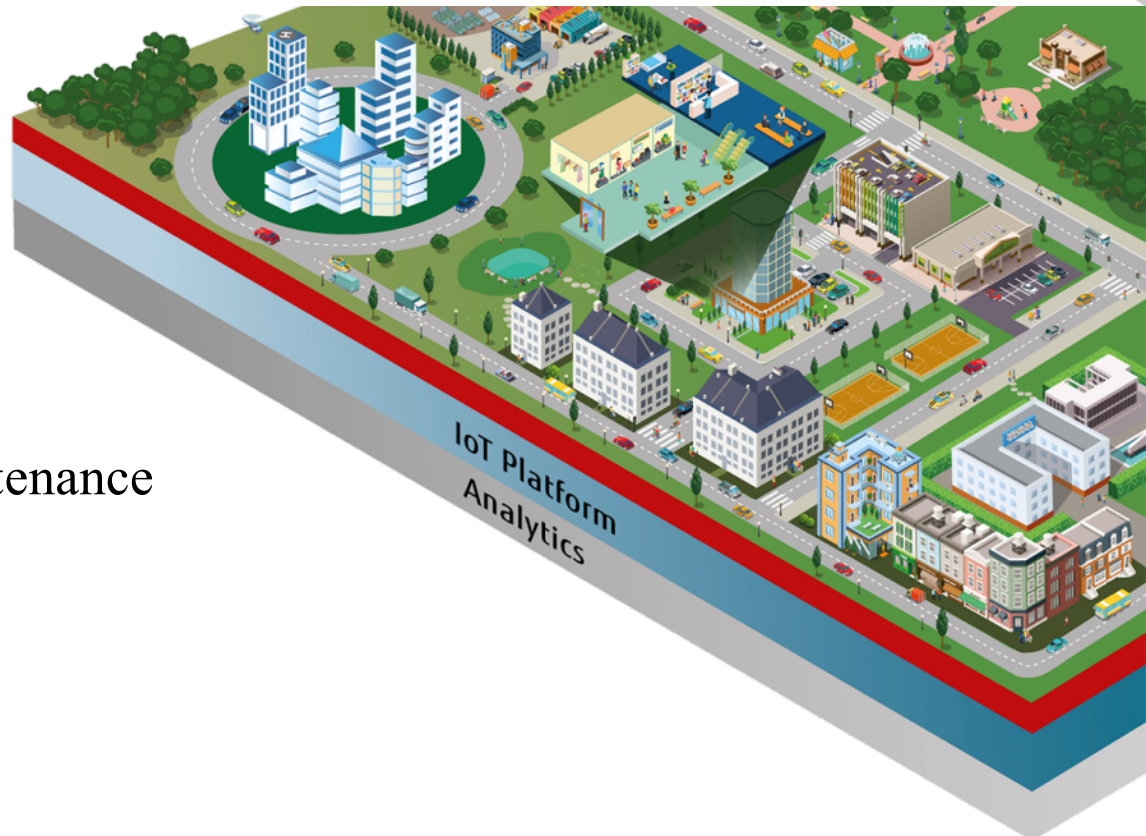
■ **Famous attacks**

- Mirai Botnet – DDOS attack
  - Initiate DDOS

- Hackable Cardiac Devices from St Jude
  - Change pacing

- Owlet Wifi Baby Heart Monitor
  - Unsecured Wifi Router

- TRENDnet Webcam Hack

- The Jeep Hack

Source: https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/

Threat Analysis

- **Public access to IoT Device, Gateway**
  - Potential rootkit attack
- **Simple but many Device**
- **Sensor Data Privacy**
- **Authentication and Confidentiality**
  - Password Management and Data Encryption
- **Firmware Update/Configuration Management**

Lessons Learnt

- Security often come last
  - Password Management
- Cost Benefit Analysis (against potential threats)
- Trade-off between User Experience vs Ideal State

Comparing Key Elements HPC:IoT

Simulation and Modelling Workloads
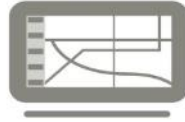
Analytics and Applications
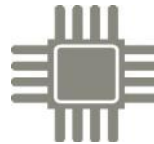
HPC Cluster, Scheduler, File System

IoT Platform

Core and Edge Networks

Core and Edge Networks

Servers and Interconnect

Devices & Sensors, Sensor Network

Why HPC on Cloud?

■ Quick Scaling

■ Focus on Software to increase productivity

■ Flexible Architecture

■ Utility Costing Model

■ Easy integration with other Cloud services

Recommendations to secure HPC on Cloud

FUJITSU

- **Don't open to public**
  - Use 2-factor based VPN if public
  - Limit outgoing access
- **Simplicity is Safety**
  - Don't overly complicate your stack
- **Automate your stack (build whole stack everytime)**
  - Don't rely on configuration management
- **Make data not valuable (eg. use Data Masking)**