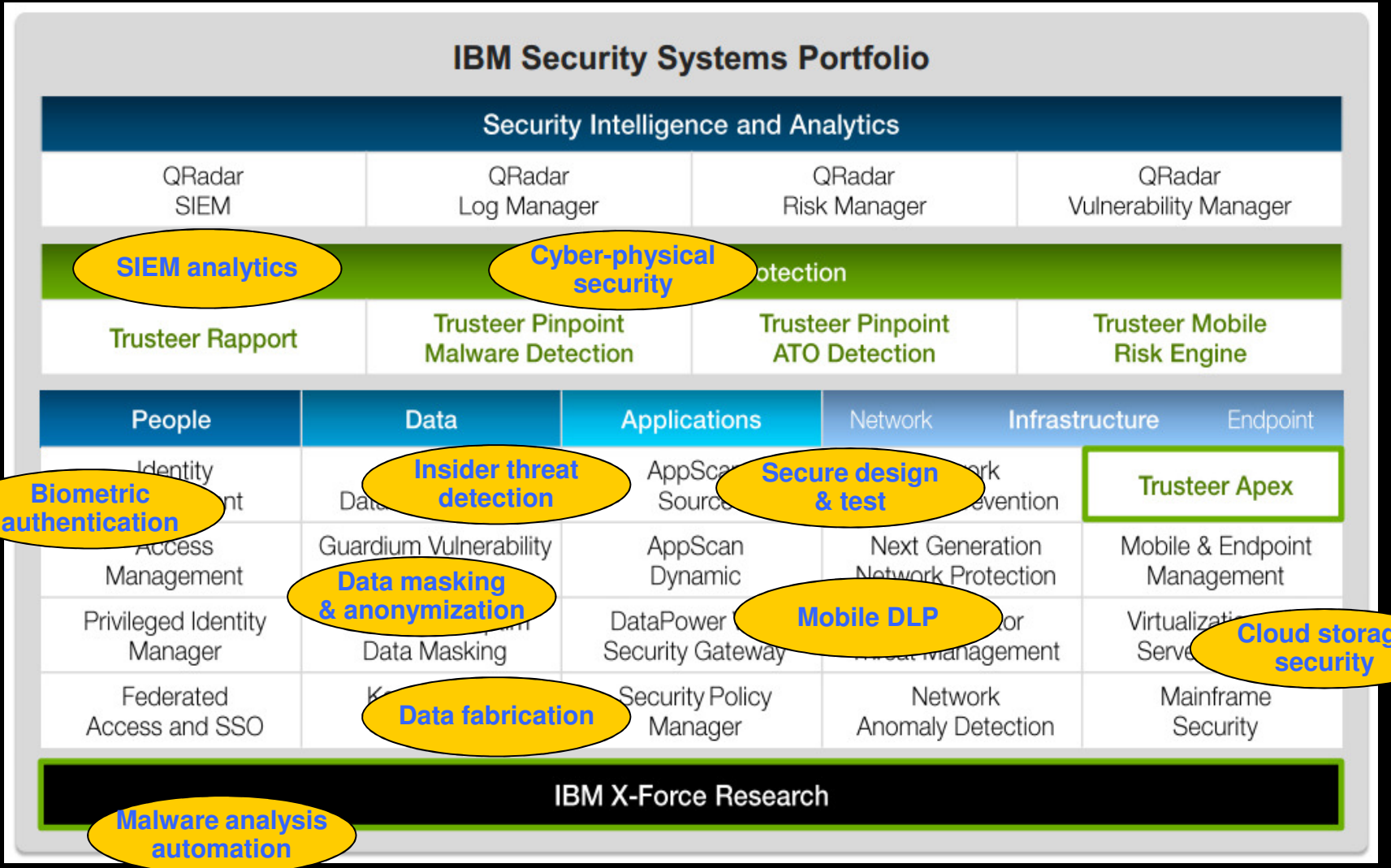
BusinessConnect
A New Era of Smart
June 12, 2014

Cyber-physical Security
Protecting IT, OT and IoT

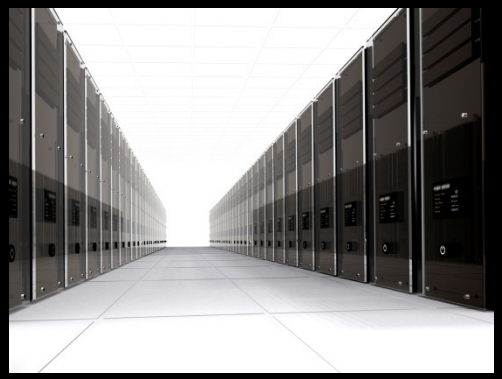
Itai Jaeger, IBM Research - Haifa
itaij@il.ibm.com

Cyber security research @ IBM Research - Haifa



Cyber-physical systems (CPS): IT, OT …. and IoT

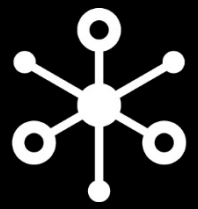
IoT



IT

OT

IoT goes to work…

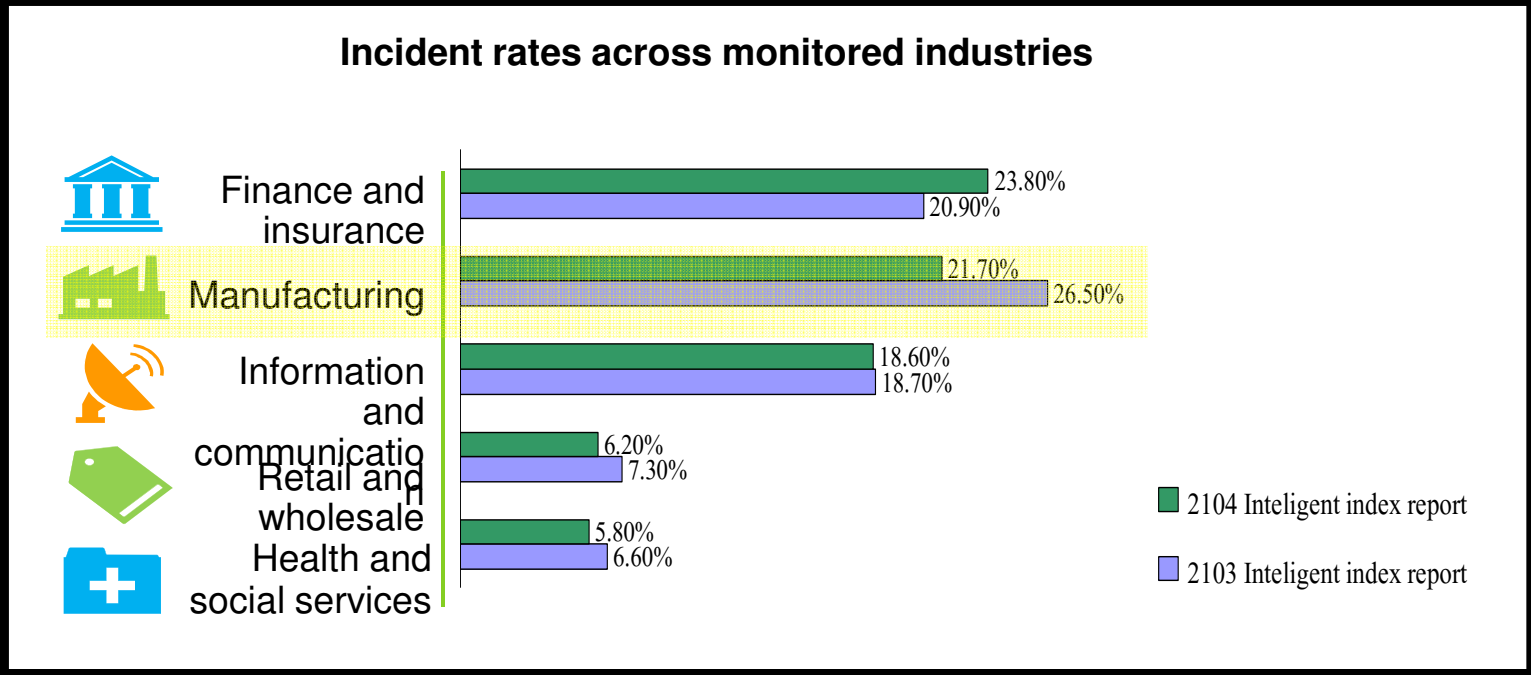


- **IoT** is a network of devices where all the devices:
  - Have local intelligence
  - Have a shared API so they can communicate in a meaningful way
  - Push and pull status and command information from the networked world

- **HIot** – Human IoT (or consumer IoT)
  - Revolving around and interacting with the human beings

- **IIot** - Industrial IoT (or enterprise IoT)
  - Must be autonomous, reliable and… secure
  - Facilitate peer-to-peer device communication -- without human intervention
  - Rely on and integrate many existing networks and communication protocols

CPS as an emerging security challenge



"We are seeing more cyber attacks focused on sabotage than espionage. These attacks are often aimed at causing physical damage, disruption, and safety issues — rather than accessing information. And they're raising new concerns about shifts across the threat landscape."

IBM Security Services Cyber Security Intelligence Index, June 2013

The CPS threat landscape

Attacks via the IT infrastructure
- Easy access – known vectors
- Increased risk compared to IT only attacks

- Device / identity takeover attacks
  - Extremely high risk
  - Hard to detect
- Offenses via the OT / IoT infrastructure and network
  - Emerging vectors – many times very simple to implement

- Risk is extremely high compared to regular IT attacks
  - Potential prolonged shutdown (weeks/months)
  - Human Life / health / safety
  - Disruption to society / region / nation

What makes OT cyber security unique?

- **Distributed systems**
  - Spread, connecting unmanned facilities
  - A hierarchy of control centers
    - With intricate Interdependencies
- **Protocol complexity**
  - Diversity in protocols and device types
    - Intermixed on the same domain
  - Multiple vendors
    - Using different proprietary protocols
- **Protocol obscurity**
  - Sensor reading and control commands are obscured
    - Same command may have different meanings based on context
- **Credentials and permissions**
  - OT systems assume users are trustworthy and meticulous
- **Old protocols and software**
  - Well known vulnerabilities
    - patches are rarely applied
  - Lateral movement of malware is greatly simplified
- **Intolerance of the physical domain**
  - Faults can have immediate consequences
    - With no easy remediation
  - Must not interfere with real-time actions
    - Prevention and healing is difficult

CPS security requires deep insight solutions

- Learning the unique characteristics of the CPS system
  - SCADA/DCS infrastructure
  - Control room network
  - Different components making up the system
- Adapting to the specifics of each system
  - Every SCADA/DCS has many unique features
  - Universal security mechanisms for the generic parts offer limited gain
- Understanding the problem domain
  - Model semantics of control commands and sensor signals
  - Adapt the security information extracted per industry / device type / vendor
  - Map signals and commands to the physical world
- **IT vendors offer their existing cyber security products**
  - A significant gap – no dedicated OT modeling
- **OT vendors shifting towards addressing cyber security concerns**
  - Some of the current solutions are basic / naive

CPS security research directions @ IBM Research – Haifa

- Leverage IBM QRadar to monitor OT and IoT events
  - Extending the QRadar model and feeds
- Design an OT/IoT network monitor
  - Apply analytics to network events
- Monitor the OT Historian
  - Look for anomalies…
- CPS security intelligence and risk management
  - Discover vulnerabilities
  - Detect ongoing attacks
  - Protect & heal compromised systems
- **Tell us about your pain points…**