RSAConference2015
Abu Dhabi | 4–5 November | Emirates Palace

SESSION ID: SSC-W10

Securing Smart City Platforms
IoT, M2M, Cloud and Big Data

Ibrahim Al Mallouhi
Vice President - Security Operations
Emirates Integrated Telecommunication Company (du)

Roshan Daluwakgoda
Senior Director - Managed Services Design
Emirates Integrated Telecommunication Company (du)

Agenda

- **UAE Smart City ambitions and progress**
- **Understanding and addressing Smart City platform security**
  - The new threat landscape
  - Secure IoT
  - Secure Big Data
  - Secure Cloud
- **Bringing this together - security governance**
- **Conclusion and action**

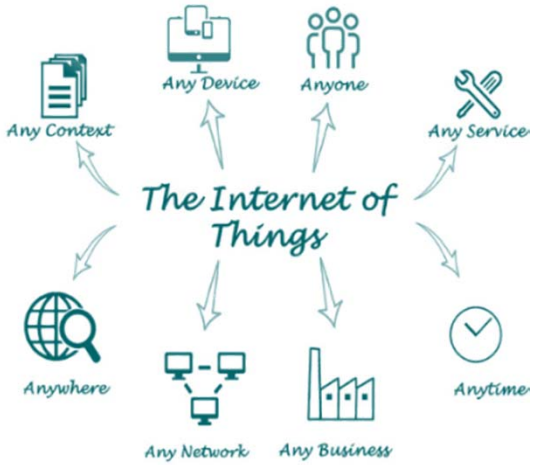
UAE Smart city ambitions

- **Dubai Smart City strategy confirmed** for 100 initiatives across 6 pillars
- **Technology adoption rate in the UAE is one of the fastest** if not the fastest in the world

دبي الذكية
SMART DUBAI
HAPPY LIVING لحياة أسعد

UAE progress - Internet of Things

- **Middle East's first successful Internet of Things network already deployed**
  8 Dubai locations with 5km radius each
- **Supports any kind of sensor**
  with minimal power consumption and can be installed for a variety of systems
- **Several smart initiatives in Dubai Silicon Oasis**
  have completed Proof of Concepts testing ahead of large scale implementation
  - E.g. Smart waste management
- **By 2020, hundreds of thousands of IoT sensors will be deployed**



UAE progress - Wi-Fi UAE

- **Free high bandwidth** for accessing government websites
- **Dubai coverage completed**, now extending across the country
- **By 2020, smartphones will be able to support up to 10Gbps 5G**

واي فاي الإمارات
WiFi UAE

RSA Conference 2015 Abu Dhabi

UAE progress - Big Data

- **Dubai data regulation recently approved** will open a host of opportunities for private and public companies
- **Dubai in 2020**
  - Significant government commitment to be the world's smartest city
  - Analytics afforded by IoT offers wide data benefit for consumers, businesses and government entities

Image courtesy of http://sfdata.startupweekend.org/

Security visibility today

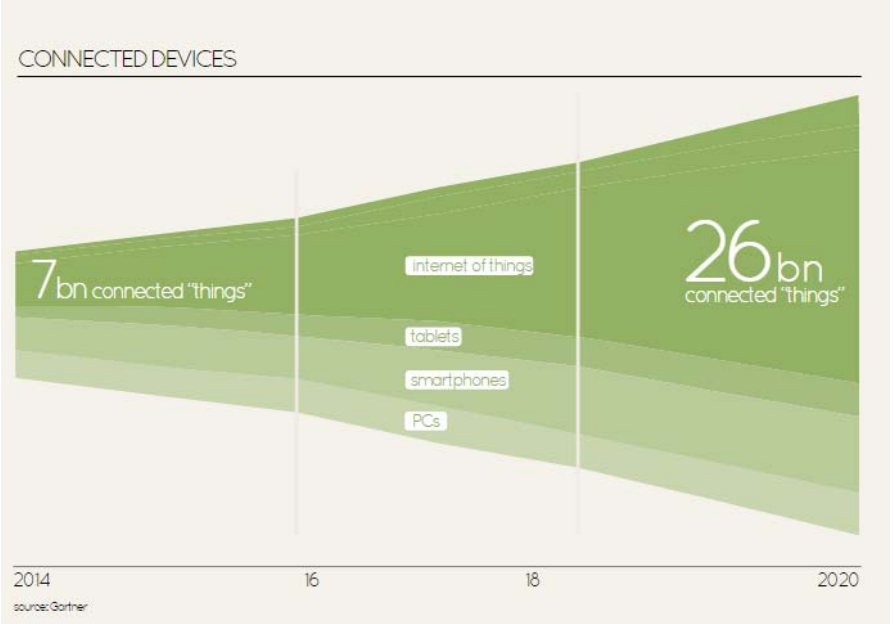
- **Annually we process**
  - 1.4Tb mobile & Voice services security events
  - 6.6Tb broadband services security events
  - 5.7Tb IP TV & streaming services events
- **Across**
  - 10,000+ network switches & routers
  - 3000+ server environment
  - 20+ data centres

- **2 billion events analysed daily**
  - 300 million security relevant events correlated per day
  - 25 unique security incidents investigated and mitigated daily
  - Supported by 540 intelligence use cases
  - Malicious code infection responsible for 49% of investigated incidence

    38% of which were not detected by standard anti-malware

Smart City context

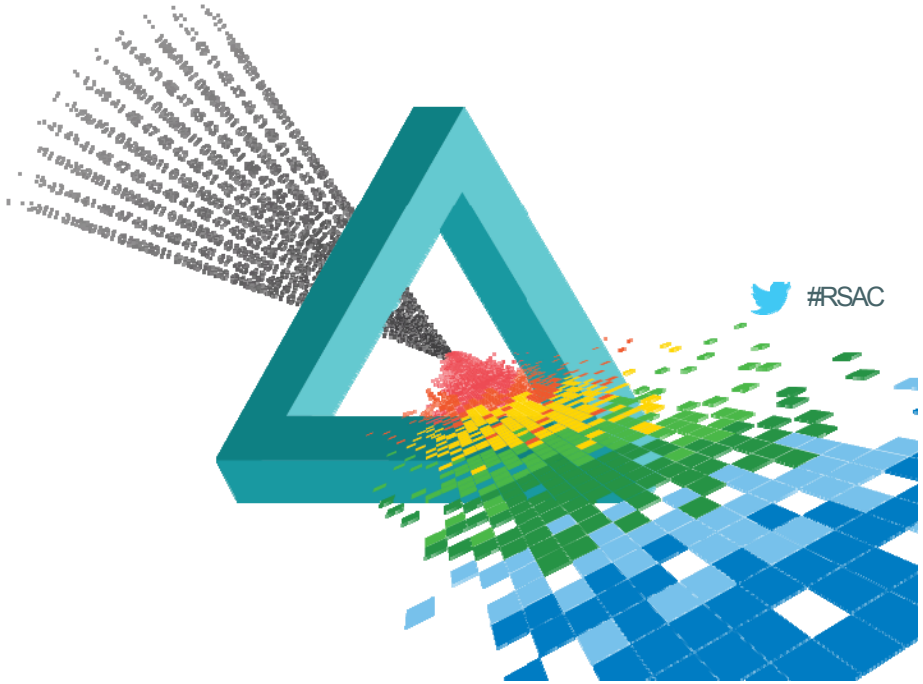
- **Significant change in landscape**
- Presents an x multiple in terms of data volume, devices and technologies
- **Traditional security approaches are no longer applicable** and must evolve
- **However, we must embrace the opportunities in open standards** in enabling diverse interfaces to work seamlessly in an integrated architecture



RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

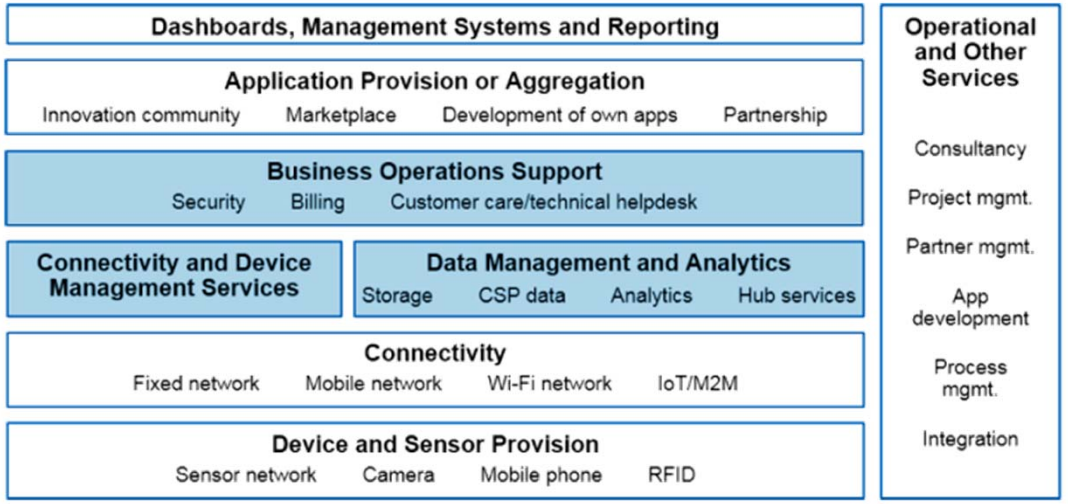
Understanding and addressing Smart City platform security



Smart City technology stack

Technology exposure

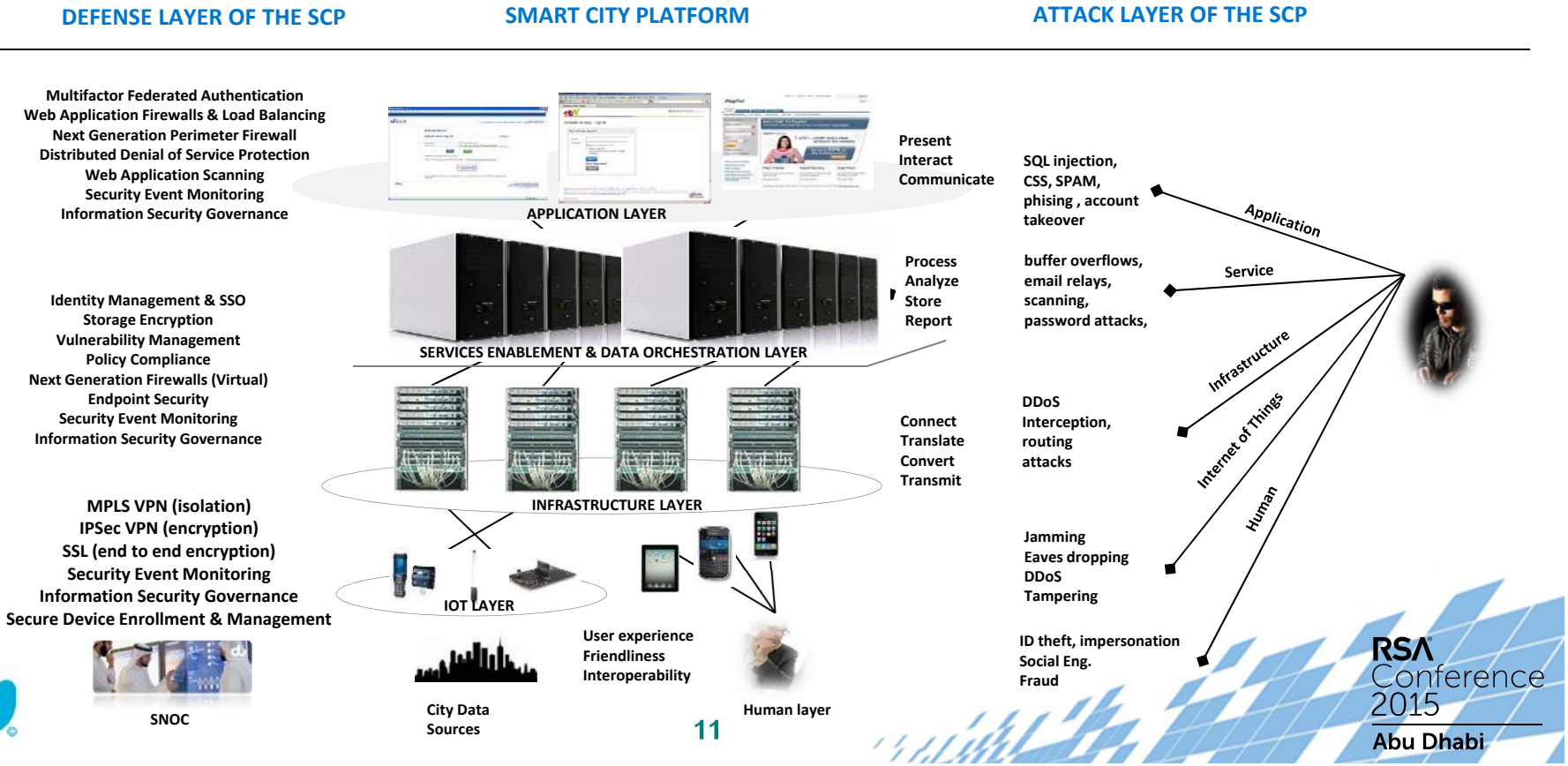
- **Devices and Sensors**
  IoT devices, sensor network, RFID, cameras
- **Connectivity** - M2M / IoT, WiFi , Fixed and Mobile
- **Data Orchestration**
  Structured/unstructured data, city semantics, Big Data
- **Infrastructure Cloud**
  IaaS, PaaS & SaaS



CSP = communications service provider; IoT = Internet of Things; M2M = machine to machine

Source: Gartner (January 2015)

Attack layer and defense layer



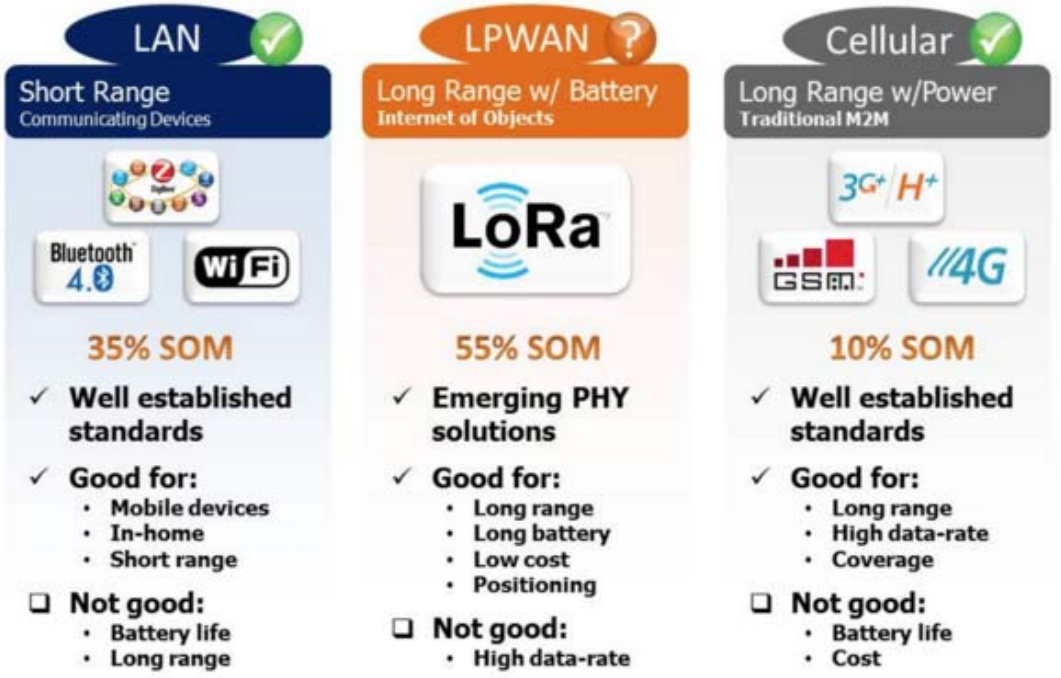
IoT – low power devices

- **Low power consumption** (to the range of nano amp) that enable devices to last for 10 years on a single charge
- **Optimized data transfer** (supports small, intermittent blocks of data)
- **Low device unit cost** (sub-$5 per module)
- **Simplified network topology and deployment** for example, via software upgrade
- **Optimized** for low throughput

IoT - market classifications

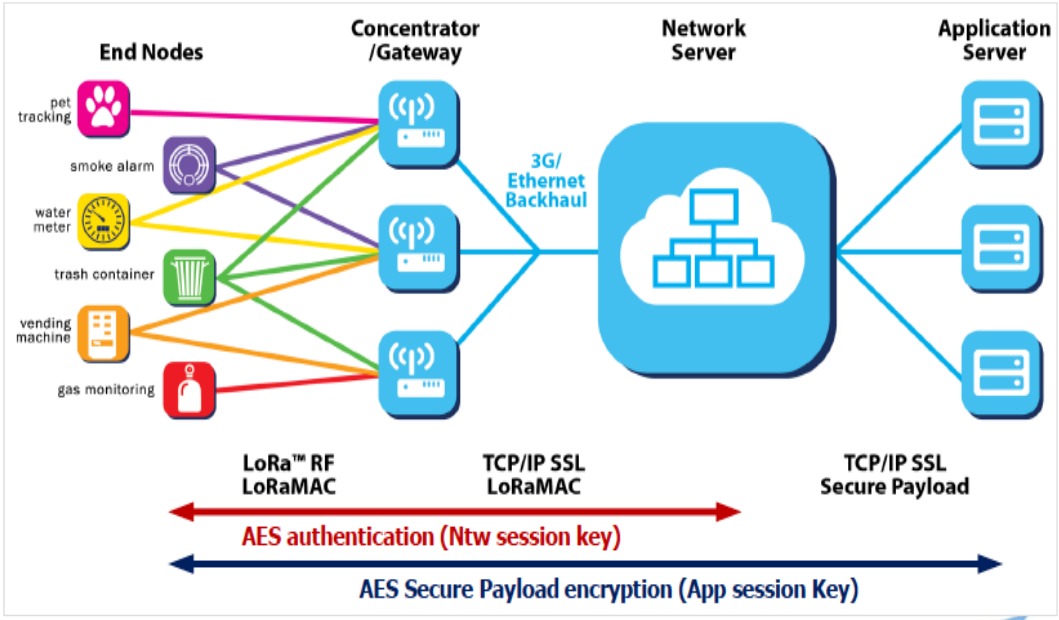
Two types of LPWAN network technologies to be considered

- **Unlicensed Networks**: such as LoRa, Sigfox, OnRamp wireless, Weightless, etc.
- **Licensed Networks** (3GPP/GSMA for Cellular IoT)



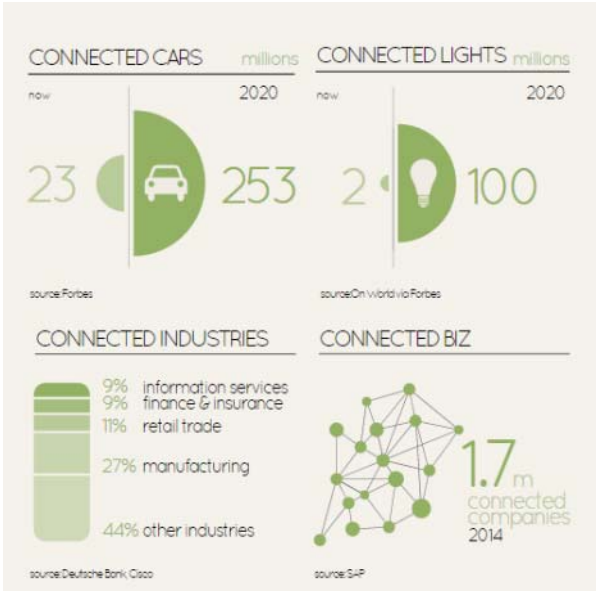
IoT - LoRa network security

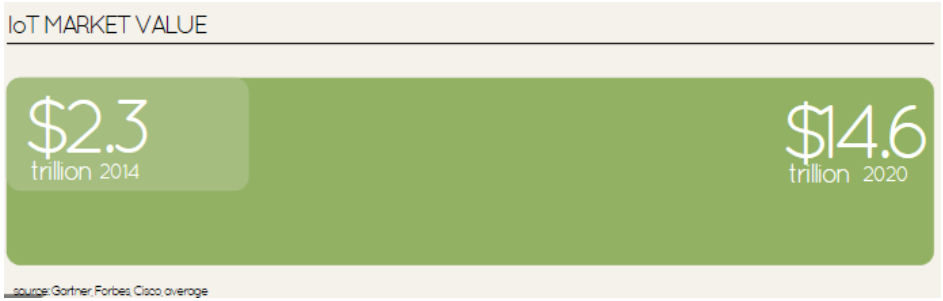
- **Security capabilities of LoRa network:**
  - Two levels of security deployed
- **Promoted by the LoRa Alliance**
  - An open standard for Low Power Wide Area Networks (LPWAN) to enable Internet of Things (IoT), machine-to-machine (M2M), smart city and industrial applications by utilizing the LoRa protocol (LoRaWAN).

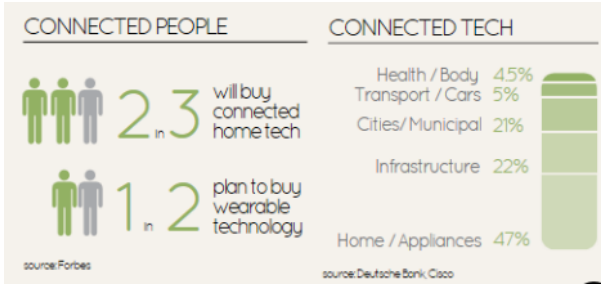


IoT - connected devices

- **26 billion connected devices in 2020 value $14.6 trillion**







IoT - vulnerabilities

Attack vectors

- IoT (sensors, devices, wifi, etc.)
  - Disable sensors and repeaters by changing configuration
  - Make sensors and repeaters unusable by changing firmware
  - Ability to flood access points with fake packets
  - Compromise single sensor or repeater with malicious firmware, replicate to other sensors

Impact

- Fake data generated by manipulation the packets
- Unauthorised connectivity, packet sniffing, DDoS attack

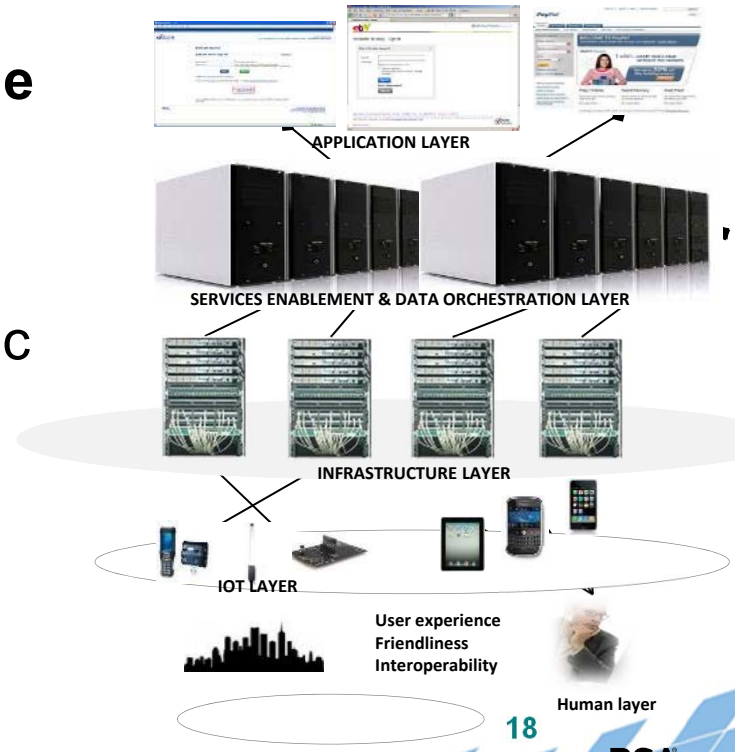
IoT - security

- Device Management
- Authentication and authorization
- Security logging sub-system
- Encrypted storage of all sensitive data
- Protection against common breach protocols
- Connectivity Security

Cloud - SCP architecture

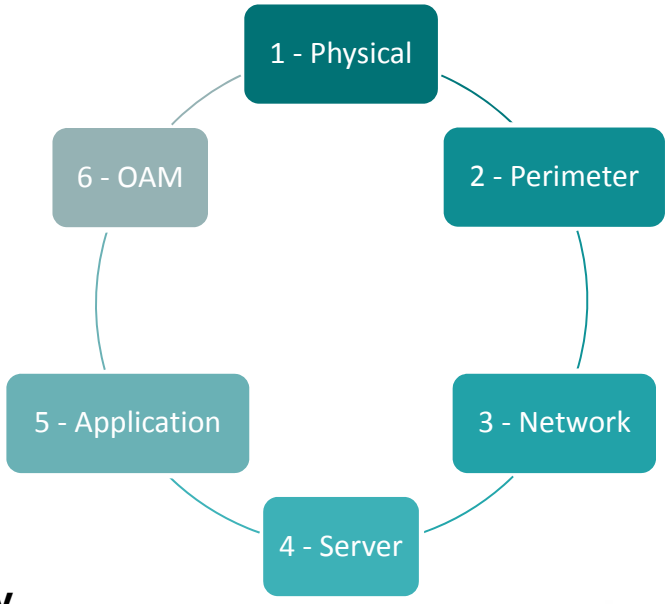
The architecture includes primarily the following functional layers:

- Cloud automation and assurance
- Software defined network (SDN) fabric
- Multi-layer security
- Integrated compute platform
- Multi-tier storage layer



Cloud - platform defence in depth security

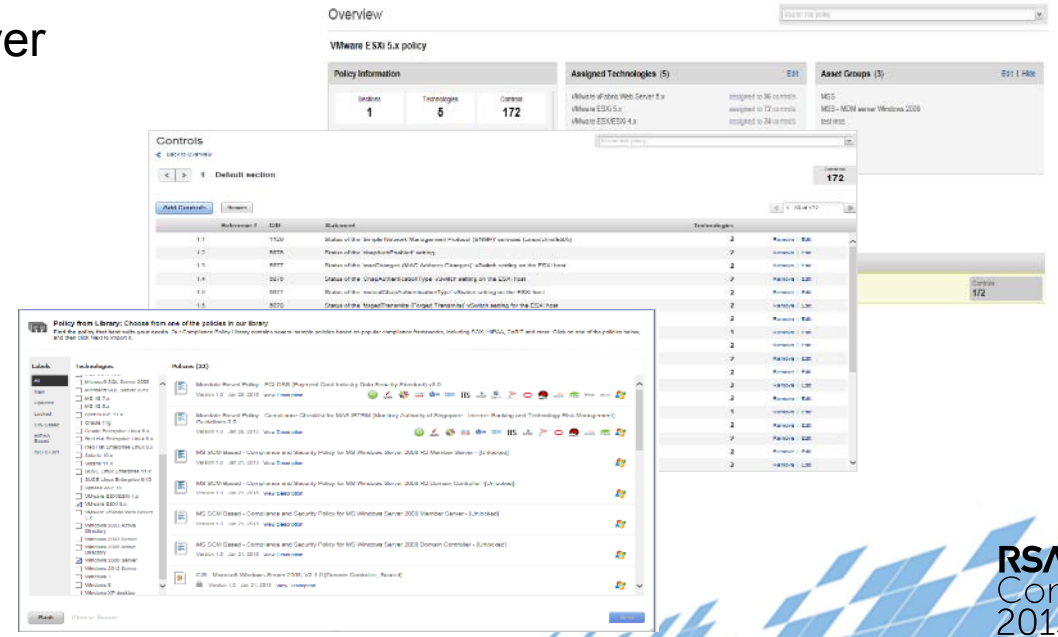
- **Physical security**
  access control, CCTV, security guard)
- **Perimeter Security**
  DDoS protection, Firewall, L7 Content security, etc.
- **Network Security**
  Virtual network security, tenet isolation, Network treat analysis etc.
- **Server Security**
  hypervisor & operating system security, server load balancing, etc.
- **Application Security**
  web app firewall, RBAC, etc.
- **Operations, administration and management security**
  monitoring, remote secure access, vulnerability scanning, policy compliance, etc.



Cloud - automated security policy compliance

continuously monitor security policy compliance in multiple layers

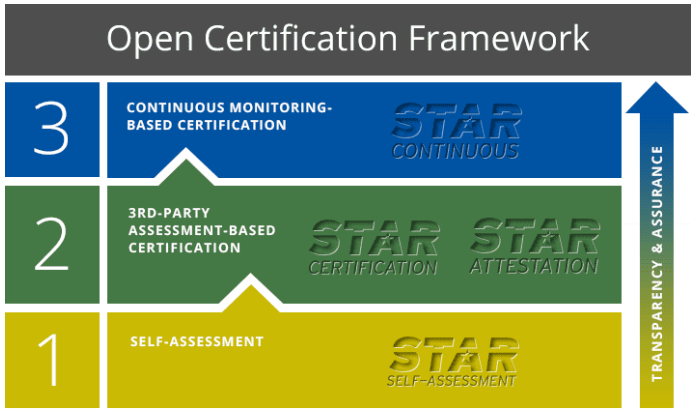
- Network Virtualization layer
- Hypervisor layer
- Operating system layer
- Application layer
- Database layer
- Security layer
- Orchestration layer



Cloud – security Trust and Assurance

CSA STAR continuous monitoring

- Providers publish their security practices according to CSA formatting and specifications.
- CSA STAR (security Trust and Assurance Registry) Continuous will be based on a continuous auditing/assessment of relevant security properties
  - Cloud Controls Matrix (CCM)
  - Cloud Trust Protocol (CTP)
  - CloudAudit (A6)

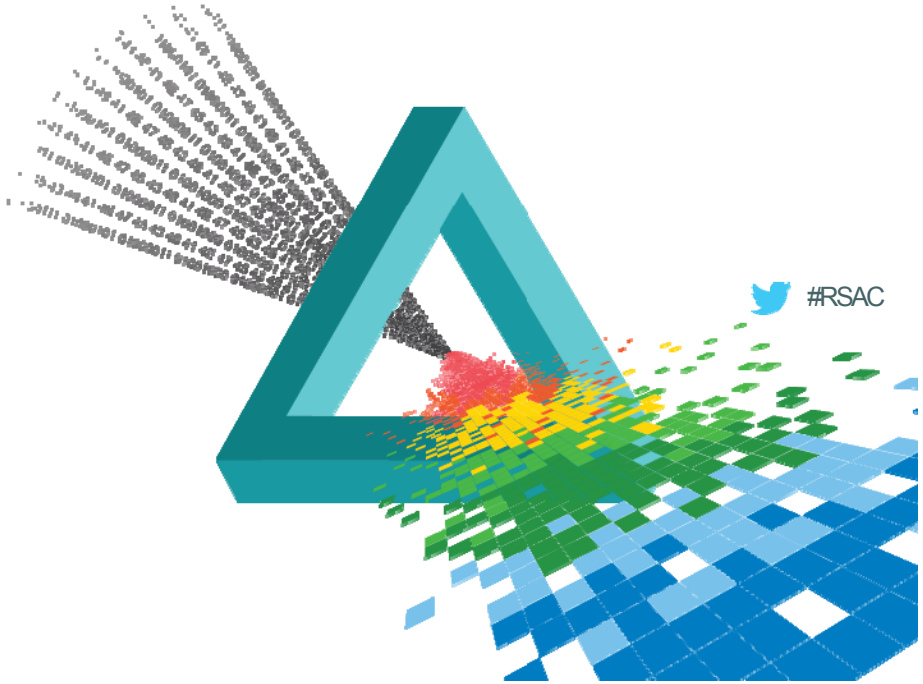


Source : Cloud Security Alliance

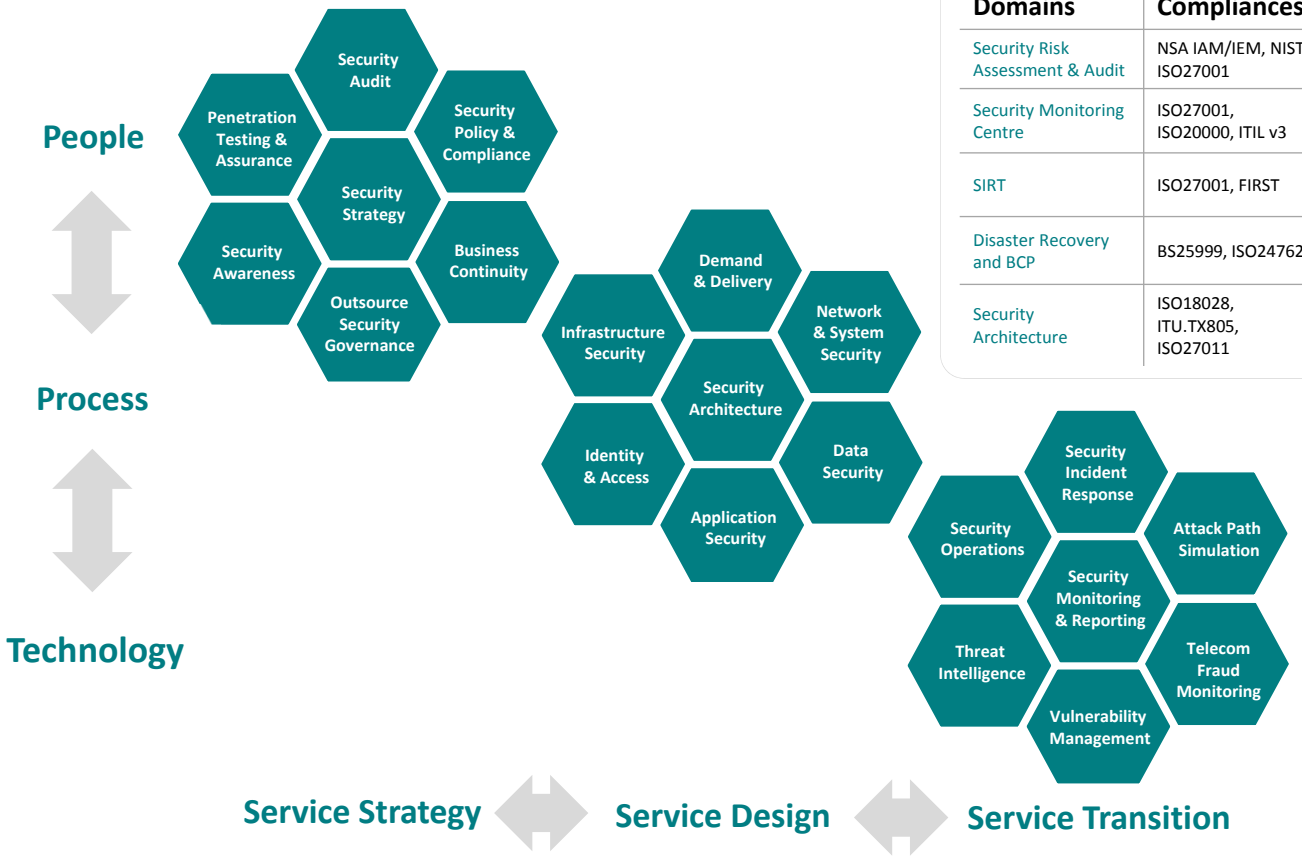
RSA Conference2015

Abu Dhabi | 4–5 November | Emirates Palace

Security Governance



Smart City - information security functional framework

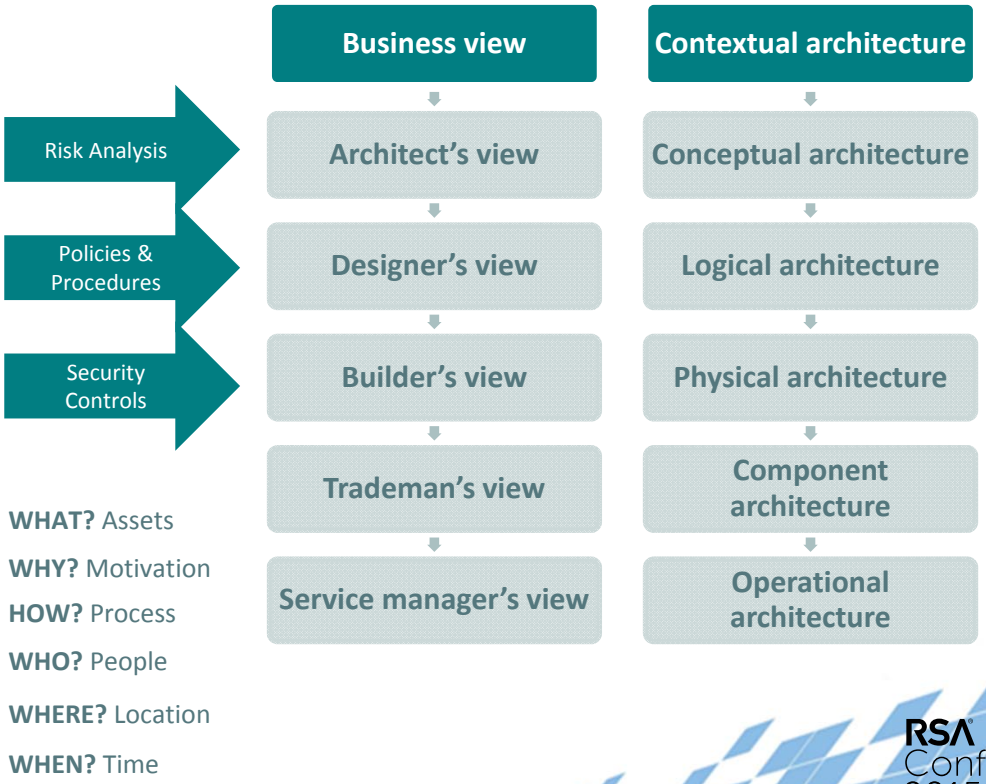


Security Domains	Applicable Compliances
Security Risk Assessment & Audit	NSA IAM/IEM, NIST, ISO27001
Security Monitoring Centre	ISO27001, ISO20000, ITIL v3
SIRT	ISO27001, FIRST
Disaster Recovery and BCP	BS25999, ISO24762
Security Architecture	ISO18028, ITU.TX805, ISO27011

The SCP's cornerstone architecture framework

SABSA®

"Security architecture, in terms of information technology, is best defined as the conceptualization, design and implementation of secure business information systems"



Smart City platform governance

security maturity

NG-ISMS

The Information Security Organization

The Information Security Principles

The Information Security Policy

The Information Security Procedures

DSA

Next Generation Firewall architecture
Systems Security architecture
Applications Security architecture
Management Security architecture
Web Application Security architecture
Database Security architecture
Cloud Security architecture
Big Data Security architecture
Intrusion Detection & Prevention Security architecture
Security Analytics architecture
VPN Gateways Security architecture

RA

Risk Identification

Threat Analysis

Vulnerability Analysis

Risk Estimation

Risk Evaluation

Risk Monitoring & Review

Risk Treatment

Control Implementation

Residual Risk Calculation

Ongoing security risk management

Maintenance and monitoring

Security Policy

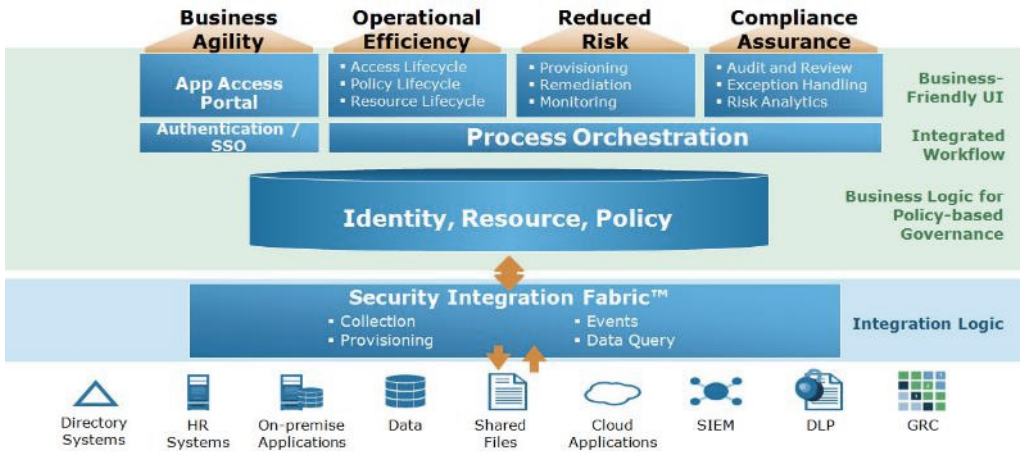
Maintenance & Improvement
Internal NG-ISMS Audit
Third Party Connectivity
Information Asset
Classification & Data
Protection
Equipment Security
Disposal & Re-use
System/Application
Acquisition, Development and Operation
Protection from malicious code
Internet & E-mail security
Remote Access
User Access
Communications and Network Security
Cloud Computing
Mobile Computing
Encryption
Incident Handling
Acceptable use
Personnel Security
Physical and Environmental Security
Security Monitoring
Security Testing
Backup & Restoration

Security Controls

Management Security Controls
Certified Security Operations
Security Incident Response
Security Monitoring
Disaster Recovery Planning
Information Asset Classification
Information Security Awareness
Technical Security Controls
Web Application Firewall & Load Balancing
Unified Threat Management
Protection from DDoS Attacks
Web Application Scanning
Identity Management & Trust Authentication
Storage Encryption
Vulnerability Management
Policy Compliance
Next Generation Firewall
Endpoint Security
Security Event Monitoring
Information Security Governance
Physical Security Controls

Governance, risk and compliance

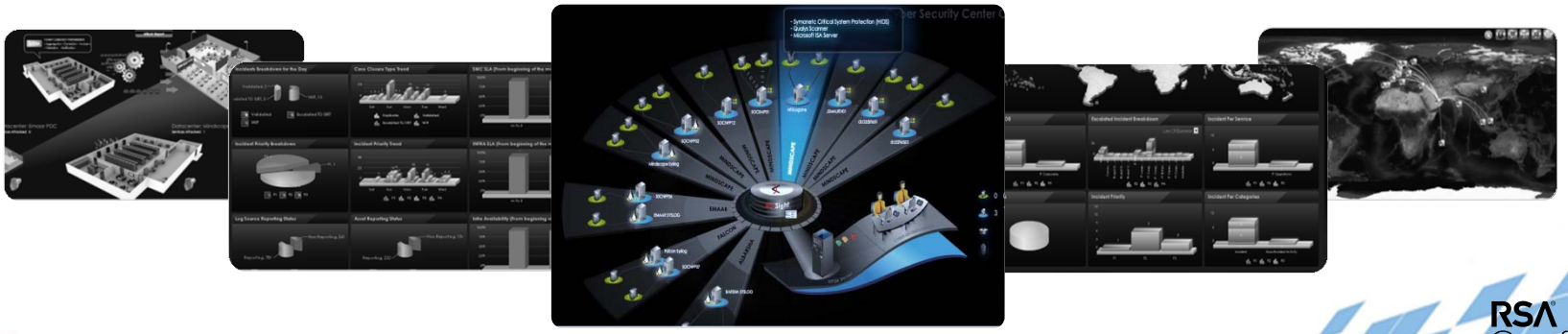
- Centralized SCP risk dashboard
- Continuous risk assessment and mitigation program



Advanced cyber security monitoring for smart city

Use case scenario

- Security Monitoring and Management - The cornerstone of the security monitoring of the SC²P is the security incident and event management (SIEM)



Next steps

- Smart city platforms are nations critical infrastructure, its country's pride, **it need to be protected**
- The impact of cyber attack cripple the nations ability to provide public services, **it threatens citizens safety and security**.
- Sheer number of IoT devices and volume of data exploded, security implications are multitude, **we got to evolve**
- If you embark on digital and IoT journey, understand your cyber threat exposure and **build security by design**.
- **Establish security governance** framework and continuous monitoring capabilities.
- Prepare for nation wide cyber attack and **build your response capabilities**

RSA Conference2015

Abu Dhabi | 4–5 November | Emirates Palace

Thank you