RSAC Sandbox

RSAConference2020

HUMAN ELEMENT

SESSION ID: **SBX1-R6**

Evolution of AIOps to Watch Over Smart City IoT

Tom Caldwell

CTO
Techniche-Statseeker-Urgent
@cybersdtom

Darren Bennett

Deputy Director – CISO
City of San Diego
@DarrenLBennett

Smart City IoT

- Light Industry IoT adds to the Threat Landscape
- The City as a Platform
- A CISO view of best practices and strategic planning
- A technologist view of the next decade of AI solutions

The need for
SMARTER
CITIES
DRIVEN BY:
Sensors
+ Networks
+ Engagement
RESULTING IN:
REAL-TIME
URBAN INFORMATICS
With the combination of low power sensors, wireless networks, and web and mobile-based applications, Smart Cities have arrived.
DEVELOPED CITIES
MEASUREMENT: Your city as a platform

Source: World Economic Forum

Light Industry IoT is a Risk

- Attached to Facilities network
- Revenue-generating and critical assets
- AC, smart lighting, sensors, AI optic sensors (cameras), sound…
- Example: CCTV cameras are a major risk in the threat landscape
- What does "cyber hygiene" mean?

> “Every opportunity can be a threat, and every threat an opportunity.”

The IoT market grew to 15.4 billion devices in 2015 and will increase to 30.7 billion devices in 2020 and as many as 75.4 billion in 2025.

Source: IHS.com - IoT platforms: enabling the Internet of Things, March 2016

Smart Cities need to take advantage of the opportunities that come from this boom in technology while planning for and managing the threats that can come with it.

Smart Cities and IoT - Threats and Opportunities

- Opportunities:
  - Increased engagement with citizens (mobile apps, self service portals, kiosks)
  - Ability to use data analytics to make decisions (traffic management, electric and water distribution, parking trends, garbage collection, street improvements)
  - Safer Communities (police body cameras, security sensors, access control devices, security lighting)
  - Greener Cities (saving resources: using temperature sensors for HVAC, light sensors, water monitoring sensors for parks and plants)
- Concerns:
  - Managing, securing and monitoring IoT in the organization
  - Keeping up with the radical growth
  - Service disruption due to failure of systems/devices be it hackers or not
  - Legal liability or damage to organizational image - compromised IoT devices being misused or used to attack other entities

Protection and defense:

- Understand IoT components and the risks associated with each: Device → Transport → Cloud → Interface
- For SAAS and vendor provided tech, having technical expertise to evaluate solutions is key
- Governance - knowing and controlling IoT use, especially with vendor provided solutions such as HVAC, alarm systems, etc
- Combination of old school security "best practices" and new technology AI/Orchestration

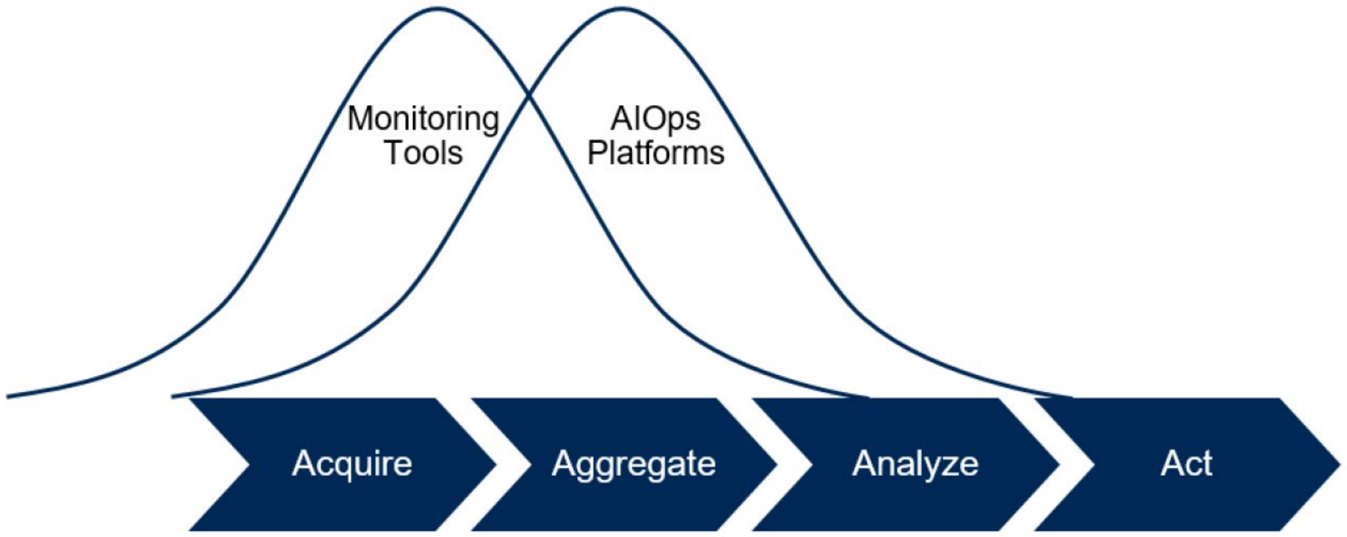
AIOps: What does it mean?

- Gartner: "AIOps helps ITOps and DevOps teams detect and resolve IT problems quickly by analyzing and contextualizing massive amounts of operational data"
- Noted AIOps vendors: Moogsoft, IBM, Splunk, BigPanda…
- Artificial intelligence for IT operations = Automation
- Big Data Analytics, Machine Learning (ML) and other artificial intelligence (AI) technologies to automate the Detection and Response of IT issues
- Three types of algorithms: 1) Predictive 2) Correlation 3) Remediation
- Situation Rooms/War Rooms bringing IT Ops, SecOps, Facilities together
- "Alert Babysitters" - Let's solve the alert fatigue in the NOC and SOC!!!

AIOps: Gartner Four Stages of Monitoring

- Basic and advanced statistical analysis
- Automated pattern discovery and prediction
- Anomaly detection
- Root cause determination
- Prescriptive advice
- Topology

Four Stages of Monitoring



ID: 340492

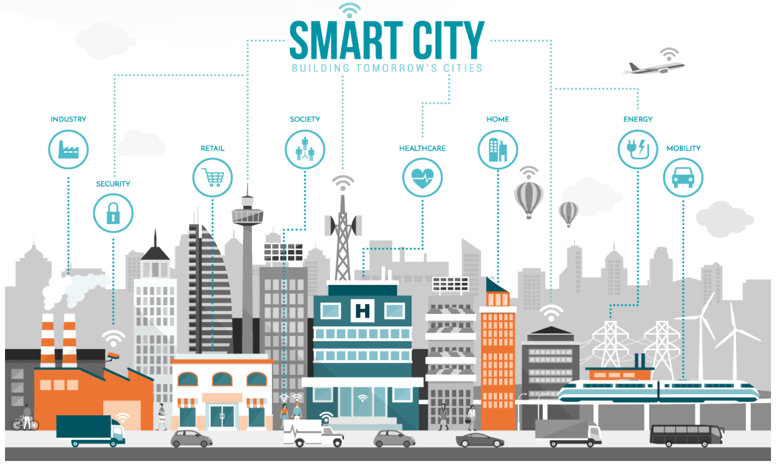
© 2018 Gartner, Inc.

Does IoT mean an integration of Clouds?

- Each IoT device sends data back to a vendor cloud
- Look for APIs to push alerts to AIOps system (e.g. Webhooks)
- Enrich alerts with Metadata, e.g. lat/lon geolocation, time-of-day shifts, meaningful context
- AIOps will centralize, normalize, aggregate and prioritize alerts into tickets = actionable intelligence
- Automated "Alert Babysitters" become machines

Light Industry IoT: Bringing it Together

- The Future: Smart Cities, Petrol Retail, Enterprise
- Growth of Smart Assets attached to Facilities (IoT)
- Still need the basic cyber hygiene and best practices: e.g. NIST framework
- AIOps: Digital Transformation technology for Automation and to transform “Alert Babysitters” to new smart “Operational Analysts
- Facility, IT, NetOps, SecOps, Devops as a Unified Team around an AIOps common tool



Smart City IoT – Build the Plan

- Next week you should:
  - Identify your facility-related IoT devices across your threat landscape
  - Outline your current security strategy relating to these devices
  - Share the investigative results with your peers in facilities, IT and senior management
  - Work the feeedback into your Governance and Vendor strategies
- Within 6-9 months you should:
  - Educate yourself on AIOps solution and what they could mean to you
  - Develop a plan to trial AIOps solutions towards focused IoT/IT areas

RSAConference2020

RSAC Sandbox

Evolution of AIOps to Watch over Smart City IoT

Questions?

Tom Caldwell Tech:niche.

CTO
Techniche
@cybersdtom
Tom.Caldwell@technichegroup.com

Darren Bennett The City of SAN DIEGO

Deputy Director – CISSP
City of San Diego
@DarrenLBennett
Dbennett@sandiego.gov