

RSA[®]Conference2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID: **SBX1-W1**

Internet of Food: How IoT Threatens Fields, Farms and Factories

Ryan Flores

Senior Manager
Forward Looking Threat Research,
Trend Micro Inc

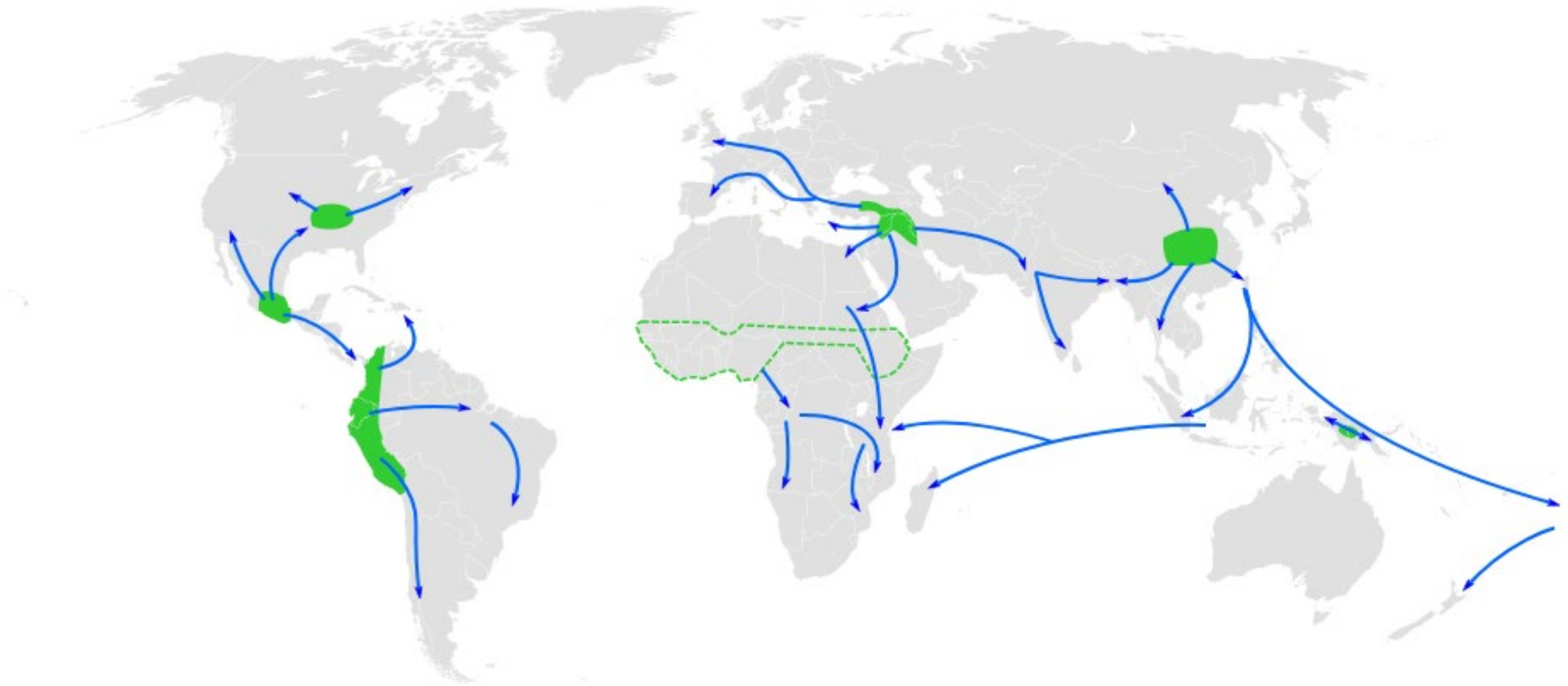
Akira Urano

Senior Threat Researcher
Forward Looking Threat Research,
Trend Micro Inc

#RSAC

Where will we
find enough food
for 9 billion?

Cradles of Agriculture



Humans Controlling the Environment



Humans Controlling the Environment



Humans Controlling the Environment



Industrialization of Food Production

- The need to feed...
 - 7.7 billion people as of 2018
 - Projected to reach 9.7 billion by 2050
- Less farmers
 - 2 out of 3 persons would be living in urban environments
- No additional farmland please
 - Agriculture and ranching are the biggest reasons for forest loss

68 - 75 Fahrenheit





Trends in Smart Agriculture

Category	Description
Precision Farming	Sensor Network, GNSS, 1km-mesh weather data, Smart Drip Irrigation
Remote Access	VNC access, Mobile Apps, Remote Support
Remote Sensing	Temperature, Humidity, Dissolved Oxygen
AI	Crop Profile, Soil Profile, Climate Profile, AI-based decision support
Automation	Automated Steering, Irrigation, Feeding, Temperature Control



Wiser spending, More yield,
Less workload/damage

RSAConference2019

Cyber-security risks in Food Production IoT and Automation

An abstract graphic in the bottom right corner of the slide. It consists of numerous thin, light blue lines that form overlapping circles and arcs. Small blue dots are scattered along these lines, creating a sense of motion or a network. The overall effect is a complex, organic pattern that suggests connectivity or data flow.

Online Farm Management

RTK Base Stations

Exposed Systems

Physical Security

Patching and
Secure Configurations

1. Exposed Systems

- Exposed VNC server to the Internet (without password)
- ***Exposed System Explorer*** - internal system with data enrichments on top of Shodan

OCR Text	Text, Language, (x,y)Location on the image.
Image Hash *	To find similar images.
Image Info	sha256, file size.
Web Detection	URL to Same / similar image.
Label Detection	Name of things in the image. (e.g. cat, dog)
Logo Detection	Name of logos in the image.

* Source: <https://github.com/JohannesBuchner/imagehash>

“Exposed System Explorer” - Brewery

Exposed System Explorer

google_vision.labelAnnotations.description:"beer"

Search

Showing 1-6 of 6

First

Previous

1

Next

Last



38.98



Current Water Level

74 inches

18958 Echo

Color

Y Prime:3940

Pump Speed: 50 %

Wtr. Bug: Tray

Wtr. Bug: Floor

Wtr. Bug: Pan

"Exposed System Explorer" - Brewery

Exposed System Explorer

google_vision.labelAnnotations.description

on:"beer"

Search

Showing 1-6 of 6

First

Previous

1

Next

Last

Image recognition

38.98



Current Water Level

74 inches

18958 Echo

Color

Y Prime:3940

Pump Speed: 50 %

Wtr. Bug: Tray

Wtr. Bug: Floor

Wtr. Bug: Pan

“Exposed System Explorer” - HVAC for poultry barn

Exposed System Explorer

google_vision.fullTextAnnotation.text:"poultry barn"

Search

Showing 1-1 of 1

First

Previous

1

Next

Last

Poultry Barn -- 2018/11/03 - 00:53:05

HEAT MINIMUM VENT COOL INLETS

Set Temperature **0.0 °C**

STATIC PRESSURE PRESSURE TEST

Stage #	Start Temp	Stop Temp	Bandwidth	Static Pressure			
Stage 1	20.0 °C	19.0 °C	1.0 °C	0.08 "	V/S FAN	INLET	STAGING
Stage 2	0.0 °C	0.0 °C	0.0 °C	0.00 "	V/S FAN	INLET	STAGING
Stage 3	0.0 °C	0.0 °C	0.0 °C	0.00 "	V/S FAN	INLET	STAGING
Stage 4	0.0 °C	0.0 °C	0.0 °C	0.00 "	V/S FAN	INLET	STAGING
Stage 5	0.0 °C	0.0 °C	0.0 °C	0.00 "	V/S FAN	INLET	STAGING
Stage 6	0.0 °C	0.0 °C	0.0 °C	0.00 "	V/S FAN	INLET	STAGING
Stage 7	0.0 °C	0.0 °C	0.0 °C	0.00 "	V/S FAN	INLET	STAGING
Stage 8	0.0 °C	0.0 °C	0.0 °C	0.00 "	V/S FAN	INLET	STAGING
Stage 9	0.0 °C	0.0 °C	0.0 °C	0.00 "	V/S FAN	INLET	STAGING

50.67.

“Exposed System Explorer” - HVAC for poultry barn

Exposed System Explorer

google_vision.fullTextAnnotation:

.text:"poultry barn"

Search

Showing 1-1 of 1

First

Previous

1

Next

Last

OCR

Poultry Barn

2018/11/03 - 00:53:05

HEAT



MINIMUM
VENT

COOL



INLETS



Set Temperature

0.0 °C

STATIC
PRESSURE



PRESSURE
TEST



Stage #	Start Temp	Stop Temp	Bandwidth	Static Pressure			
Stage 1	20.0 °C	19.0 °C	1.0 °C	0.08 "	V/S FAN	INLET	STAGING
Stage 2	0.0 °C	0.0 °C	0.0 °C	0.00 "	V/S FAN	INLET	STAGING
Stage 3	0.0 °C	0.0 °C	0.0 °C	0.00 "	V/S FAN	INLET	STAGING
Stage 4	0.0 °C	0.0 °C	0.0 °C	0.00 "	V/S FAN	INLET	STAGING
Stage 5	0.0 °C	0.0 °C	0.0 °C	0.00 "	V/S FAN	INLET	STAGING
Stage 6	0.0 °C	0.0 °C	0.0 °C	0.00 "	V/S FAN	INLET	STAGING
Stage 7	0.0 °C	0.0 °C	0.0 °C	0.00 "	V/S FAN	INLET	STAGING
Stage 8	0.0 °C	0.0 °C	0.0 °C	0.00 "	V/S FAN	INLET	STAGING
Stage 9	0.0 °C	0.0 °C	0.0 °C	0.00 "	V/S FAN	INLET	STAGING

50.67.

"Exposed System Explorer" - Aquaculture

Exposed System Explorer

google_vision.logoAnnotations.description:"Pentair"

Search

Showing 1-10 of 156

First

Previous

1

2

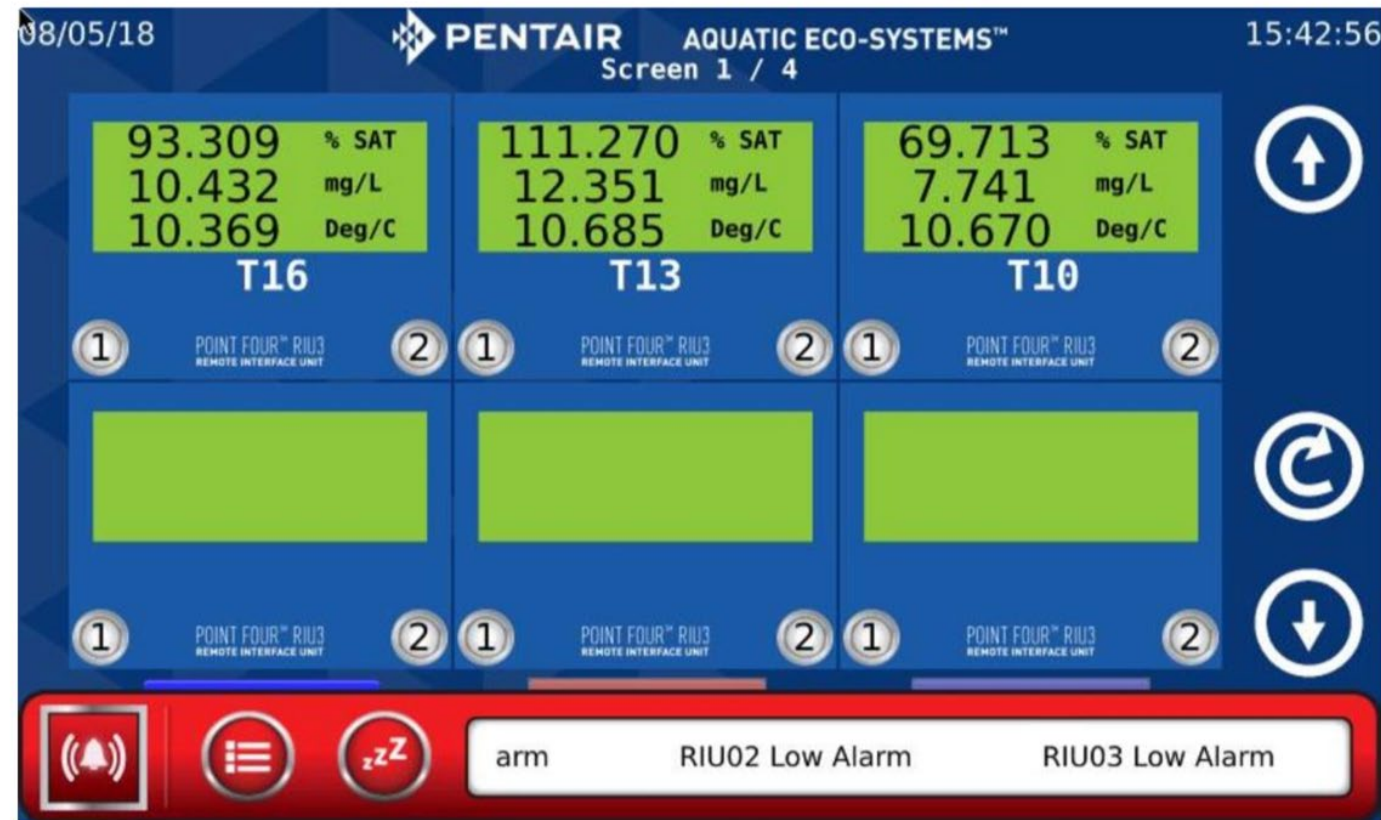
3

4

5

Next

Last



182.54.

"Exposed System Explorer" - Aquaculture

Exposed System Explorer

google_vision.logoAnnotations.descrip

"Pentair"

Search

Showing 1-10 of 156

First

Previous

1

2

3

4

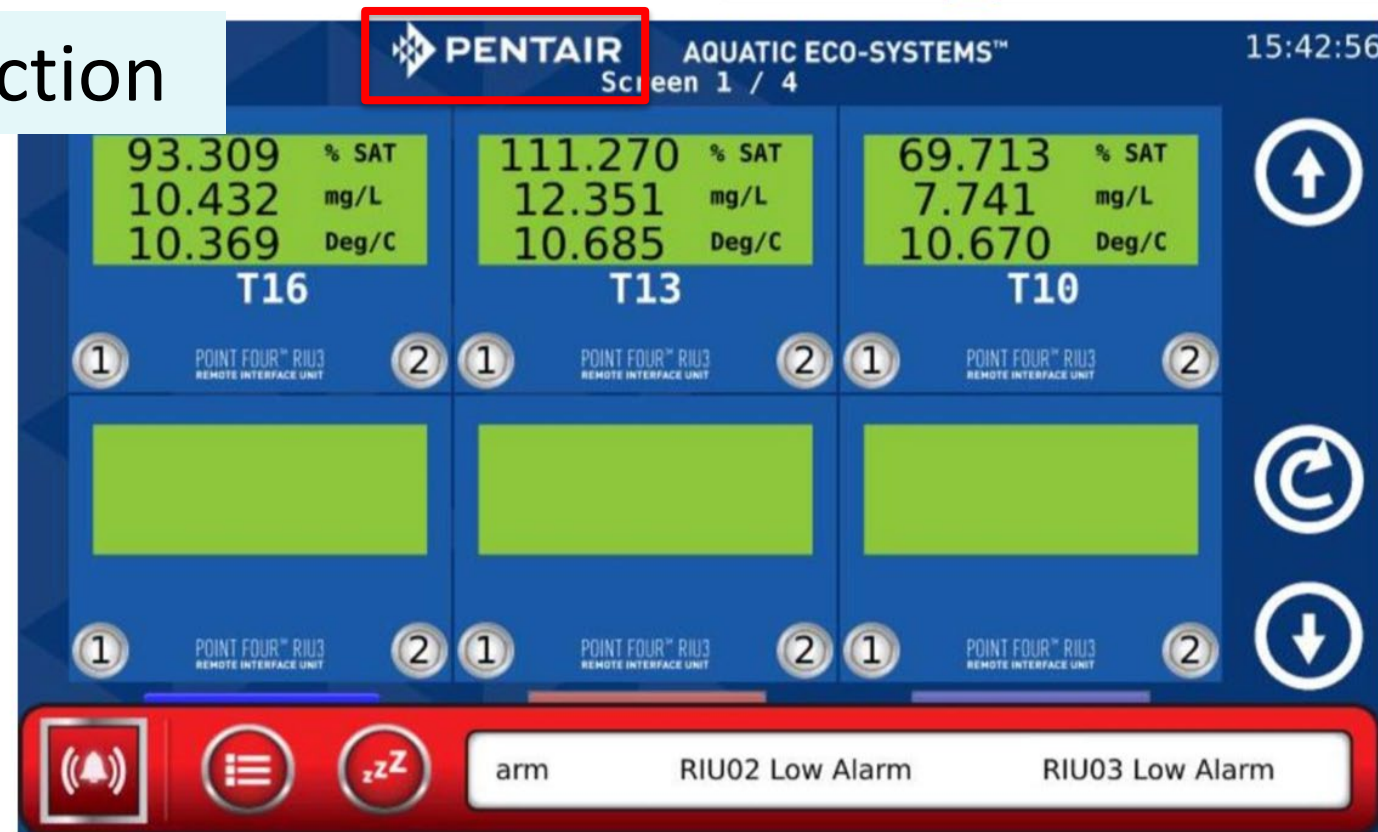
5

Next

Last

Logo detection

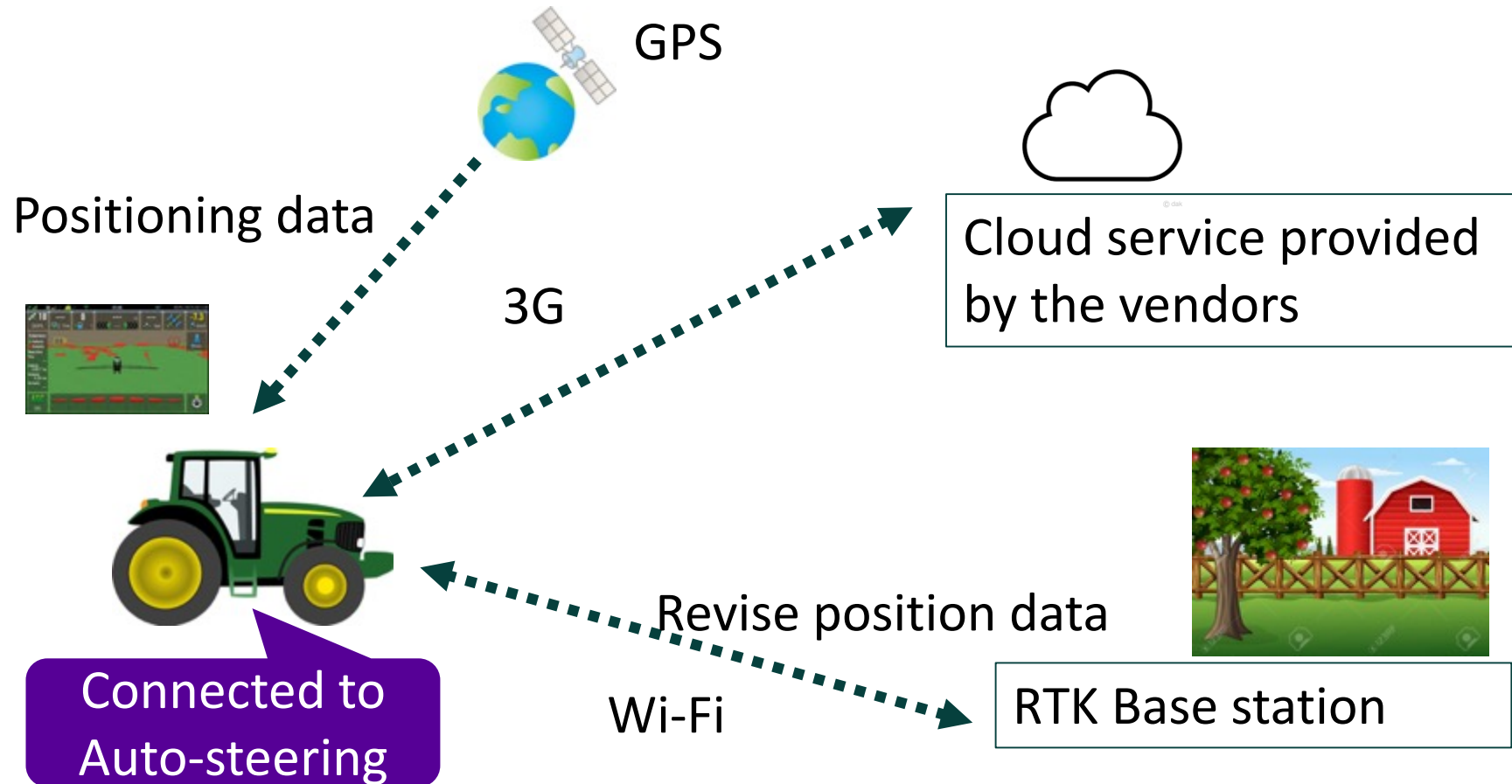
182.54.



1. Exposed Systems

Category	Type of System, Device
Farming	Tractor, GPS Base station for tractor, Irrigation Management, Storage, Silo Management, Weather Monitoring, Farm Management,
Stock breeding	Feeding, Waste Treatment, Ventilation Control for Poultry,
Aquaculture	Water Management, Oxygen Generator
Food processing	Sausage Maker, Refrigeration System, Brewery
Others	Biogas Plant, Biomass Plant

2. RTK Base Stations



RTK: Real Time Kinematic


2. RTK Base Stations

SHODAN

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS
70

TOP COUNTRIES



Country	Count
United States	21
Poland	14
Canada	12
China	7
Netherlands	4

TOP SERVICES

Service	Count
HTTP (8181)	19
8080	16
Synology	15
8081	12
Webmin	4

TOP ORGANIZATIONS

Organization	Count
Verizon Wireless	12
Orange Polska	7
Bell Mobility	7
B2B Groningen	3
Entel PCS Telecomunicaciones S.A.	2

TOP OPERATING SYSTEMS

Operating System	Count
Linux 3.x	1

91.228.136.208
91-228-136-208.mponet.pl
MPC Pawel Oleksiewicz
Added on 2019-01-10 22:09:10 GMT
Poland, Kutno

HTTP/1.1 200 OK
Server: /1.2
Date: Thu, 10 Jan 2019 22:09:05 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Expires: Fri, 30 Oct 1998 14:19:41 GMT
Connection: close
Content-Type: text/html

<html xmlns="http://www.w3.org/1999/xhtml" lang="en-US"> <head> <meta http-equ...

166.154.57.23
23.sub-166-154-57.myvzw.com
Verizon Wireless
Added on 2019-01-10 16:18:28 GMT
United States

HTTP/1.1 200 OK
Server: /1.2
Date: Thu, 10 Jan 2019 16:18:46 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Expires: Fri, 30 Oct 1998 14:19:41 GMT
Connection: close
Content-Type: text/html

<html xmlns="http://www.w3.org/1999/xhtml" lang="en-US"> <head> <meta http-equ...

81.26.139.162
host-162.ugtel.ru
Yuzhniy TELECOM ltd.
Added on 2019-01-10 13:39:10 GMT
Russian Federation, Krasnodar

HTTP/1.1 200 OK
Server: /1.2
Date: Thu, 10 Jan 2019 13:39:28 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Expires: Fri, 30 Oct 1998 14:19:41 GMT
Connection: close
Content-Type: text/html

<html xmlns="http://www.w3.org/1999/xhtml" lang="en-US"> <head> <link rel="sho...

3. Online Farm Management



MyJohnDeere

Sign in to MyJohnDeere

Username

▶ [Forgot username?](#)

Password

▶ [Forgot password?](#)

SIGN IN ☐ Remember Me

Not registered? [Create New Account](#)

▶ [Help Signing In ?](#) ▶ [Notifications \(0\)](#)
Your use of this site is governed by our [Terms of Use](#)

Your gateway to better business decisions

MyJohnDeere makes it simple to access secure John Deere web applications:

- Manage your John Deere Financial accounts, including online payments.
- Collect and analyze machine and agronomic information.
- Manage all your John Deere tech subscriptions.
- Search for parts solutions—including pricing—then place orders.
- Reduce the number of user IDs and needed to access your application

CREATE ACCOUNT

LEARN MORE

slingshot.

Username *

Username cannot be blank.

Password *

Request Account **Forgot Password?** **Login**

Trimble

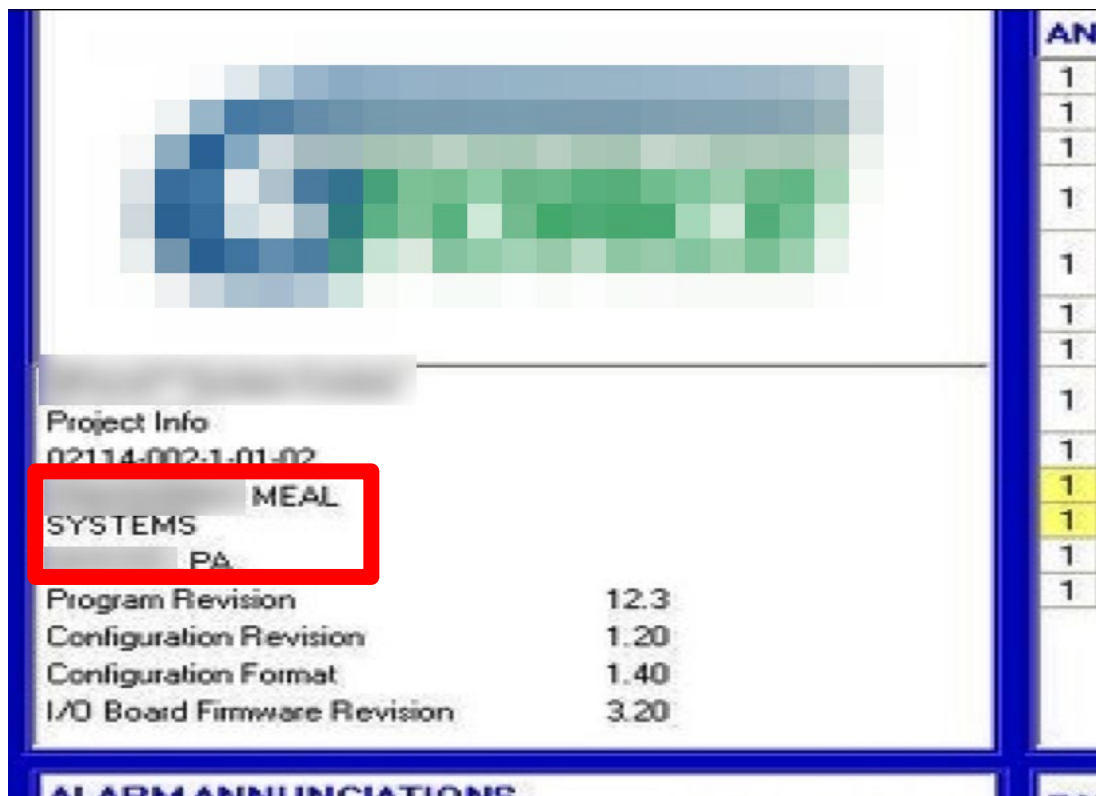
Email address

Password

Sign in

☐ Stay signed in [Forgot password?](#)

4. Physical Security



Search by the name of company and address

5. Patching and Secure Configurations

Sierra Wireless Technical Bulletin: Mirai Malware

Products: Sierra Wireless LS300, GX400, GX/ES440, GX/ES450 and RV50

Date of issue: 4 October 2016

Sierra Wireless FAQ: Malware Threat

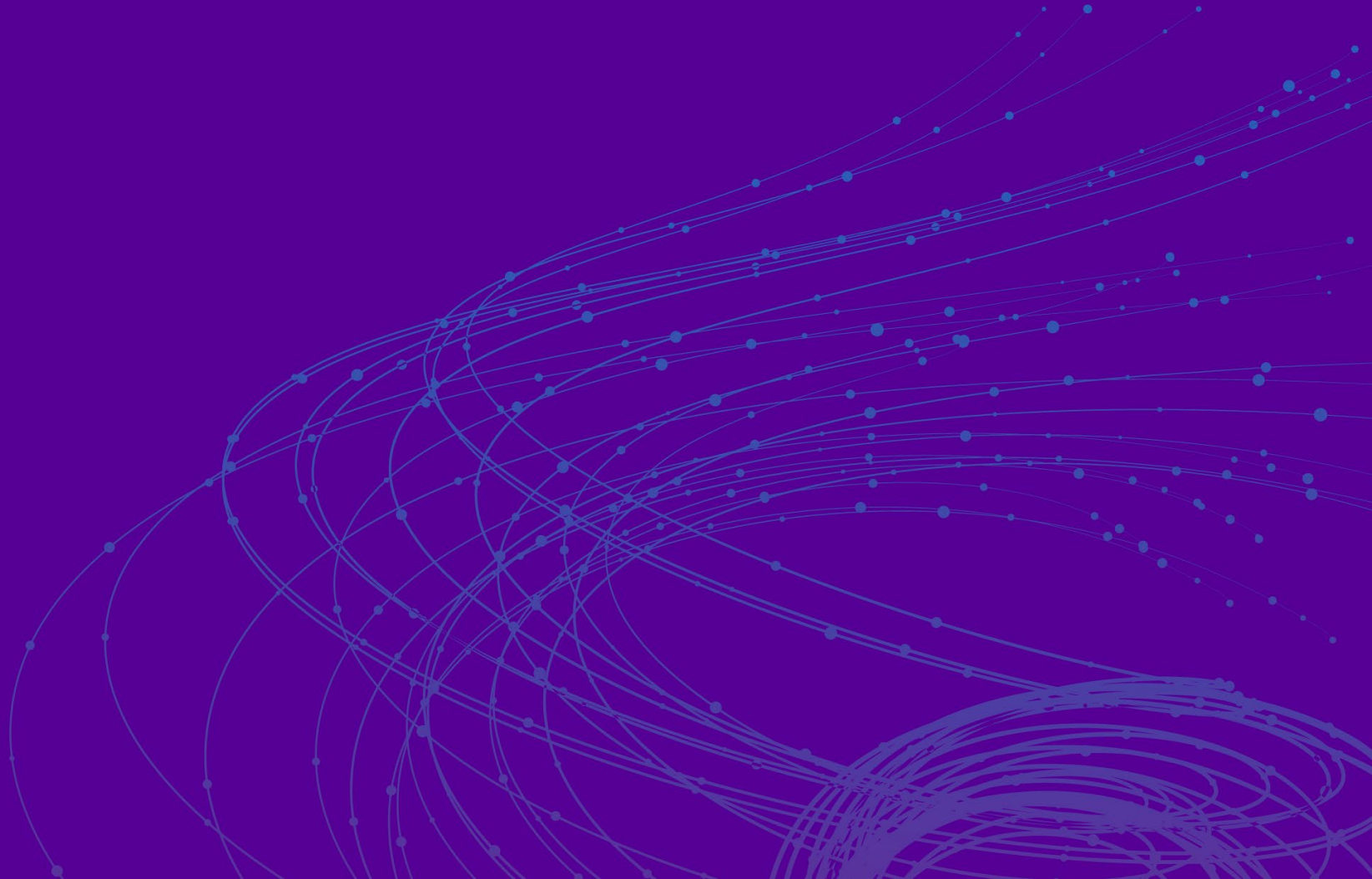
Products: AirLink® Gateways running ALEOS 4.5.2 or older using default user or viewer password

Date of issue: 11 September 2017



RSA®Conference2019

Impact



Impact: Food Safety Traceability and Recall

GAP: Good Agricultural Practices

HACCP: Hazard Analysis Critical Control Point

Goal: to make food processing safer
through records of critical control points



Data integrity issues on compromise or
ransomware situation

Impact: Growing and Harvesting Cycle

- Spinach: 30 days
- Chicken: 39 days
- Corn: 2 months
- Rice: 3 months
- Tilapia: 6 months
- Hog: 6 months
- Cattle: 18 months

Nobody knows why 320,000 chickens were killed in looks like an

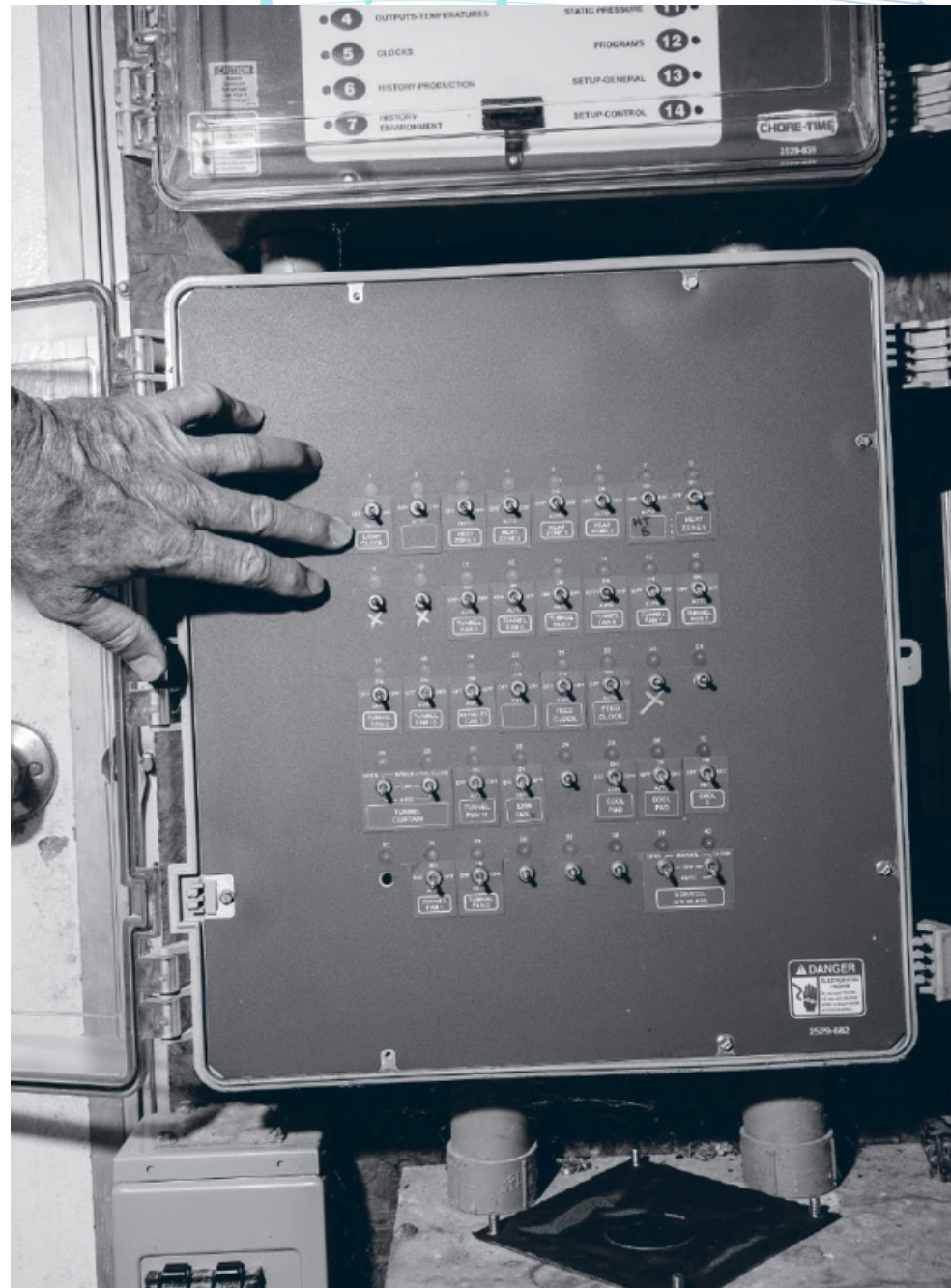
Bloomberg Businessweek

Janaki Jitchotvisut, First We Fea

Who's Murdering Thousands of Chickens in South Carolina? 10,000 ed in South 1 Attacks After Plant Closing

By BEN MATHIS-LILLEY

MARCH 05, 2015 • 1:58 PM





What to do?

- Audit IoT devices and identify underlying OS, applications, services and opened ports. Look for common vulnerabilities and poor security configurations.
- User Education: we are asking farmers to operate technologies they may not be familiar with, or understand the risk implications.
- IT best practices apply:
 - Secure configurations
 - Threat of phishing
 - Patching and device management

Conclusion

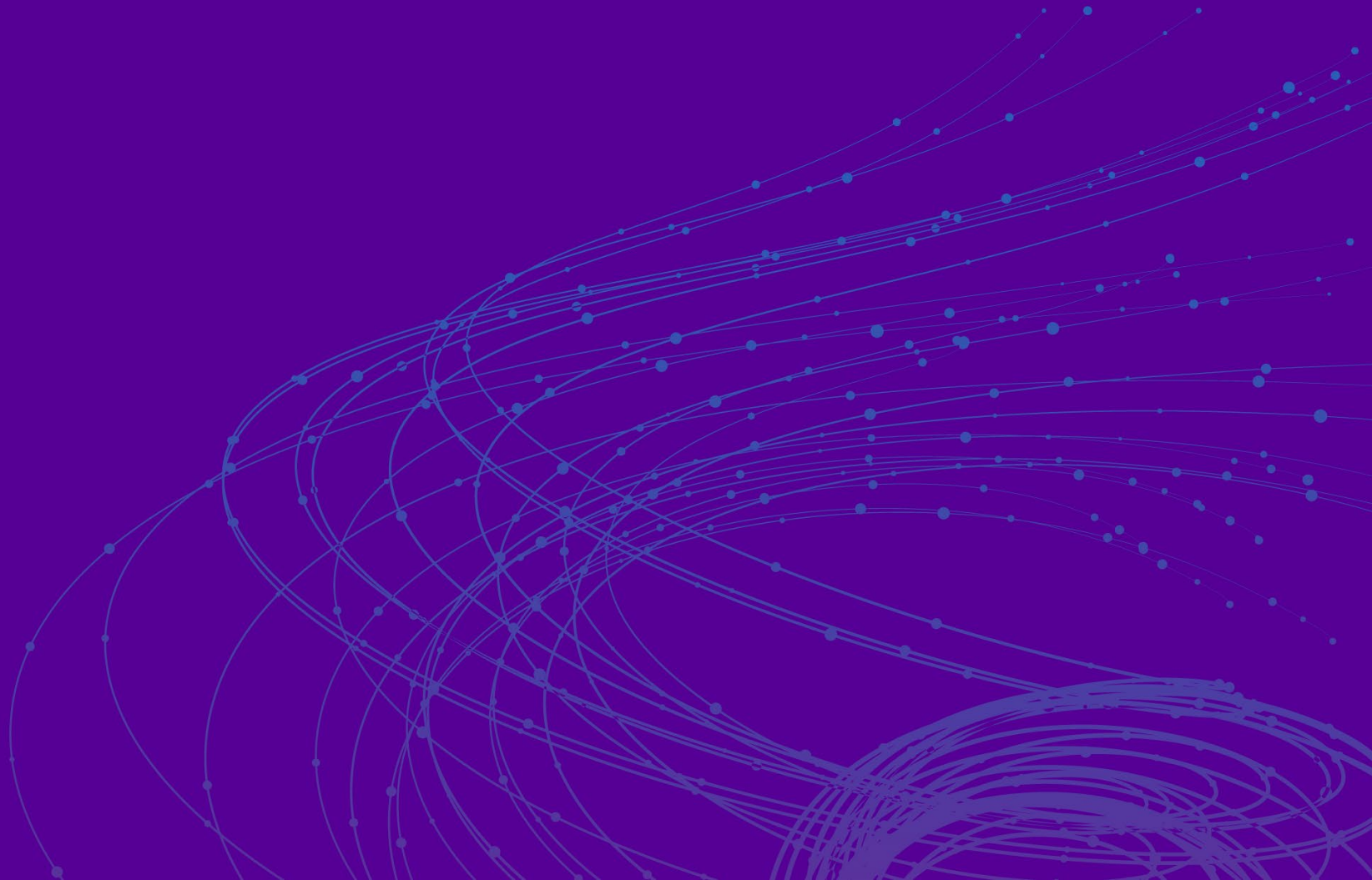
- IoT in farming and food production is a national and global concern.
- A successful attack results in tangible losses – lost growing cycle, financial loss, environmental concerns.
 - Exposed Internet Connected Systems
 - Internet Connected Positioning Receivers and Base Stations
 - Online Farm and Data Management
 - Pinpointing the Position of Farms and Facilities for Physical Access
 - Unpatched Common Operation Systems and Applications
- Treat IoT systems as if they are IT systems

RSA[®]Conference2019

Thank you!

Questions?

RSA[®]Conference2019



RSA[®]Conference2019



RSA[®]Conference2019

