INDUSTRIAL CONTROL SECURITY MANAGEMENT AND OT SECURITY ANALYSIS

Aleksandar Andric IoT Solutions Architect - Cisco

ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China

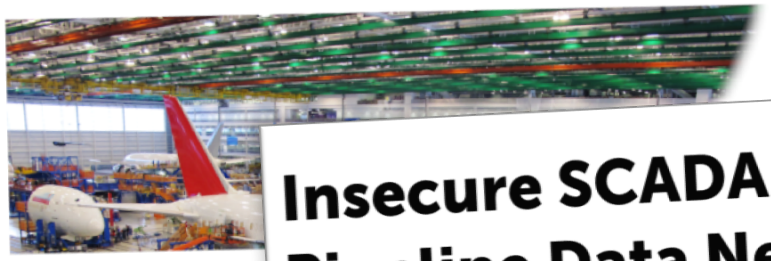
Contents

INTRODUCTION

Boeing & Aerospace | Business | Technology

Boeing hit by WannaCry virus, but says attack caused little damage

Originally published March 28, 2018 at 3:16 pm | *Updated March 28, 2018 at 9:16 pm*



Technology

Energy Transfer Says 'Cyber Attack' Shut Pipeline Data System

By Meenal Vamburkar, Naureen S Malik, and Ryan Collins
3 April 2018, 01:21 GMT+8 *Updated on 3 April 2018, 12:12 GMT+8*

Insecure SCADA Systems Blamed in Rash of Pipeline Data Network Attacks

Technology

Cyberattack Pings Data System Least Four Gas Networks

By Naureen S Malik, Ryan Collins, and Meenal Vamburkar
4 April 2018, 02:29 GMT+8 *Updated on 4 April 2018, 21:39 GMT+8*

- Oneok system joins Energy Transfer, Boardwalk, Eastern Shore
- Websites for a broad community of companies also affected

ANDY GREENBERG SECURITY 12.14.17 10:00 AM

UNPRECEDENTED MALWARE TARGETS INDUSTRIAL SAFETY SYSTEMS IN THE MIDDLE EAST

ANDY GREENBERG SECURITY 06.12.17 08:00 AM

'CRASH OVERRIDE': THE MALWARE THAT TOOK DOWN A POWER GRID

ZERO TRUST SECURITY

CISCO

WEB INTERNET
TECHNOLOGY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION

ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China

Security is the main concern for industrial IoT adoption

"Security managers should analyse their current and planned security architectures to determine how well they are positioned to deal with the security issues of the current, and coming, Internet of Things."

SANS

"Security is clearly a top concern, with 84% of those implementing IoT already having experienced a security breach."

Aruba

"Security and risk concerns will continue to be the greatest impediment to IoT adoption."

Gartner

"Security Is Of Paramount Concern When Implementing Internet-Of Things Solutions."

Cisco

ZERO TRUST SECURITY

ICS TAILORED MALWARE

Stuxnet

Crashoverride

Havex

TRITON/TRISIS

BlackEnergy

- Discovered in 2010
- Iran
- Targets SCADA systems
- Infects Microsoft Windows machines, and then seeks for Siemens Step 7 software
- Estimated to have ruined 20% of Iran's nuclear centrifuges

ICS TAILORED MALWARE

Stuxnet

Crashoverride

Havex

TRITON/TRISIS

BlackEnergy

- Discovered in 2016
- Ukraine
- Attacks electrical grids
- Modular malware, establishes a backdoor, and targets particular industrial communication protocols
- The attack cut 20% of Kiev off power for one hour

CISCO

ZERO TRUST SECURITY

ICS TAILORED MALWARE

Stuxnet

Crashoverride

Havex

TRITON/TRISIS

BlackEnergy

- Discovered in 2013
- USA & Europe
- Targeting SCADA systems abusing OPC protocol
- Used for espionage campaign targeting energy, aviation, pharmaceutical, defence, and petrochemical sectors

CISCO

ZERO TRUST SECURITY

ICS TAILORED MALWARE

Stuxnet

Crashoverride

Havex

TRITON/TRISIS

BlackEnergy

- Discovered in 2017
- Middle East
- Safety Systems
- Targets Schneider Electric's Triconex safety instrumented system (SIS) enabling the replacement of logic in final control elements

ICS TAILORED MALWARE

Stuxnet

Crashoverride

Havex

TRITON/TRISIS

BlackEnergy

- Discovered in 2007
- Ukraine
- Attacks ICS/SCADA and energy companies
- The attack starts with spear-phishing, installs trojan and lunches DDoS
- The attack from 2015 left 50% of homes in the Ivano-Frankivsk region in Ukraine with no electricity for a few hours.

$1.5+ Billion

The cost to a set of six industrial companies due to incidental infections in industrial spaces last year, as per their government mandated financial statement

Source:
Government mandated financial statements across industrial companies

COMMON OT SECURITY CHALLENGES

- No asset inventory
- Legacy systems
- External vendors
- Limited security skills

ZERO TRUST SECURITY

CYBER ATTACKS STATISTICS

66%
of breaches took months or even years to discover

60%
of breaches have data exfiltrated in first 24 hours

60,000
Number of alerts hackers set off at Global Retailer

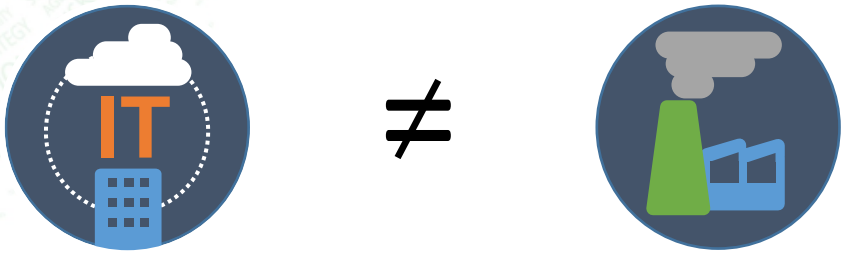
184
Median number of days advanced attackers present before detection

33%
Of organizations discover breaches through their own monitoring

CISCO

ZERO TRUST SECURITY

SECURITY IN OT IS DIFFERENT FROM IT



Security Control	Information Technology	Operations Technology
Vulnerability management	Active scanning	Passive scanning
Concept of least privilege	Layered RBAC	Limited access segmentation
Authenticator	Complex password, 2FA, unique	Code, pin, key sequence, common
Change Management	Regular Scheduled	Highly managed and complex
Time Critical Content	Generally delays accepted	Delays are unacceptable
Availability	Generally delays accepted	24x365 (continuous)
Patching/Malware	Regular Scheduled	Rare, Unscheduled; Vendor specific
Traffic flows	Ability to block in-line	No inhibitors for flow
Logical Access	People ~= Devices	Few people; Many, many devices
Event logging	Standardized corelation	Proprietary protocols
Failover capability	critical component has a redundant counterpart	Parts replacement and repairs
Physical Security	Secure (server rooms, etc.)	Remote / Unmanned Secure

ZERO TRUST SECURITY

ICS SECURITY SOLUTION USE CASES

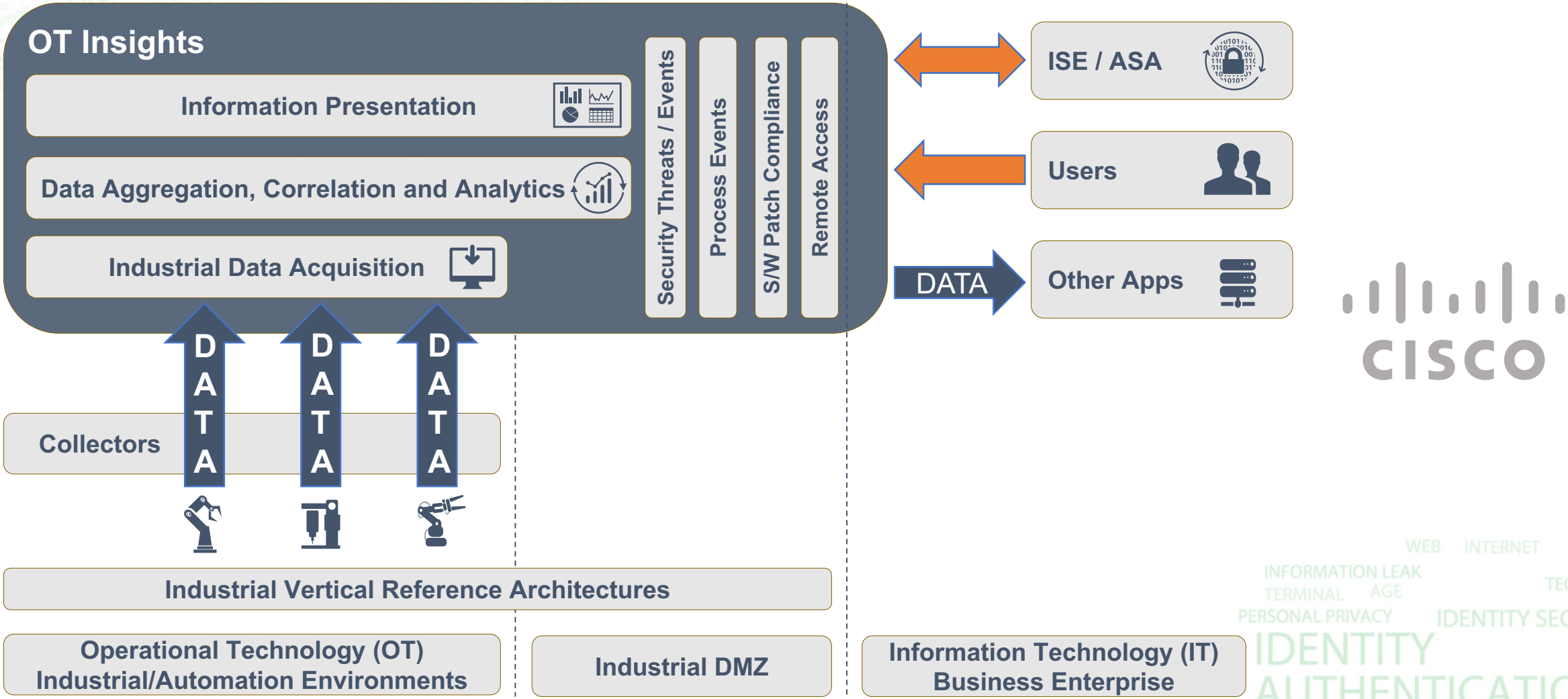
Visibility

Segmentation (zoning)

Network traffic-based anomaly detection

OT influenced remote user access

ICS SECURITY SOLUTION ARCHITECTURE



ZERO TRUST SECURITY

OT INSIGHTS – OPTIMIZING INDUSTRIAL CONTROL ENVIRONMENT

Asset Visibility

- Real-time 360° view of devices
- Passive & active asset discovery
- Inventory all critical operational assets
- Rapid discovery of ICS configuration anomalies

Malware Detection

- Quickly detect anomalous communication patterns
- Leverage large industrial threat knowledge base
- Prioritize protections and respond proactively

Secure Remote Access

- Unify remote access solution access for all systems and networks, regardless of vendor
- Maintain complete, centralized control and visibility of remote access activities

Compliance

- Determine compliance of all assets, including endpoint status for antivirus software, installed programs, services running, and installed patches

CISCO

ZERO TRUST SECURITY

CALL TO ACTION

Understand your challenges

- Evaluate your environment
- Identify risks
- Secure your assets

Learn more

https://www.cisco.com/c/en/us/solutions/internet-of-things/iot-security.html

Connect

aandric@cisco.com
www.linkedin.com/in/aleksandarandric

扫描二维码，

获取更多会议资料！

ZERO TRUST SECURITY


ISC
2018
ISC互联网安全大会
360互联网安全中心
THANKS
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China