ICS Cybersecurity trends and challenges

WHAT’S HAPPENING IN ICS WORLD

WTF ??
ICS & SCADA ARE ON THE OPEN INTERNET.

- Shodan.io
  - Let’s hack a windturbine ☺
- Business needs are more important
- Exposed core systems
- Open doors for fun :D

Information Technology (IT) versus Operational Technology (OT)

Information Technology

1. Confidentiality
2. Integrity
3. Availability

of information

Operational Technology

0. Safety
1. Availability
2. Integrity
3. Confidentiality

Reliability

Triton exploited zero-day flaw to target industrial systems

Schneider Electric h

Recommended Content:

Tools & Templates:

Far too many enterprises are consequences if they don't. T

businesses

stability issues

SCADA security: Bad app design could give hackers access to industrial control systems

'Shocking' flaws show apps for industrial control systems are being built without enough thought for security, according to researchers.

Recommended Content:

Research: IT security and privacy: Concerns, initiatives, and predictions (TechRepublic Premium)

This archived TechRepublic Premium report, originally published in February 2015, is available for free to registered TechRepublic members. For all the latest research reports, 100+ ready-made policies, IT job descriptions, and more, check out...

Download Now

By Danny Palmer | January 11, 2018 -- 16:23 GMT (16:23 GMT) | Topic: Security

RECOMMENDED FOR YOU

Remote access policy

urity

lprit

This 'm probing

Hackers that tried

Recommended Content:

Research: More companies turn

Desktop virtualization (VDI) use has more than d computing. BYOD and employee flexibility are a

procedure to ensure that equipment is safe to reassign. This checklist will help ensure that no steps are missed...

d Now

By Charlie Osborne for Zero Day | April 30, 2018 -- 11:08 GMT (12:08 BST) | Topic: Security

RECOMMENDED FOR YOU

What businesses need to know about the California Consumer

Real World Attacks?

Total Results 137,867

Top Services	
Tridium Fox	29,114
Modbus	21,794
S7	17,833
BACnet	15,075
HMI	4,858

Top Countries	
US	93,325
IT	7,814
DE	7,576
CA	7,058
ES	6,741

Top Organizations	
Verizon Wireless	9,640
Comcast Business	6,942
Deutsche Telekom AG	4,620
AT&T Internet Services	2,997
Orange	2,565

Search
United States
Mexico
Cuba
SHODAN

Internet Scanning

GeoStalking

SELECTOR
CONSIGNAS
GRAFICAS
416 cm/s
266 l/min
6.05 Bar
15.60 l/min
Oil & Gas
Tank/Pit
Wells
Well Summary
Shutdown Detail
Last SD Events
ECD
SD Reset
Last Events
HOME

Shutdown	Manual Shutdown	Reset Shutdown	Status	Last Shutdown Event
	Shutdown	Reset	Shutdown	High O2 Levels / SHUT/DI[40]
	Shutdown	Reset	Shutdown	W02 Top Vessel PSI / SHUT/LO AI[126]
	Shutdown	Reset	Shutdown	High O2 Levels / SHUT/DI[40]
	Shutdown	Reset	Shutdown	High O2 Levels / SHUT/DI[40]
	Shutdown	Reset	Shutdown	W05 Top Vessel PSI / SHUT/LO AI[129]
	Shutdown	Reset	Shutdown	W06 Top Vessel PSI / SHUT/LO AI[130]
Full Site SD	Shutdown	Reset	Running	

Tank Pressure SD [illegible]   Seperator SD Pressure [illegible]

[illegible]   SD Reopen Pressure [illegible]

HOW THIS AFFECTS YOU

Smart Ports

Components

Smart Cities

- Components
- Architecture
- Vulnerabilities

Ukraine 2015 vs. 2016

Attack Operations

- 2015: Manual interaction with control systems
- 2016: Interactions encoded in malware*

Attack Impact

- 2015: Disrupt electricity distribution, inhibit recovery
- 2016: Disrupt electricity transmission, inhibit recovery, attempt to impact protection systems

Attack Success

- 2015:
  - 3 distribution companies
  - 225k customers
  - Several hours
- 2016:
  - Single transmission/distribution site
  - <225k customers
  - Approx. 1-2 hours

FORA DA

BREAKING NEWS

25 DEAD IN RAIL CYBER ATTACK

11:16 MINISTERS ASKING WHY CYBER SECURITY WAS NOT ADDRESSED | RAILWAY SHUTDOW

WHAT TO DO?

Securing the OT environment requires a **Security Program**

People

Right access to
right people

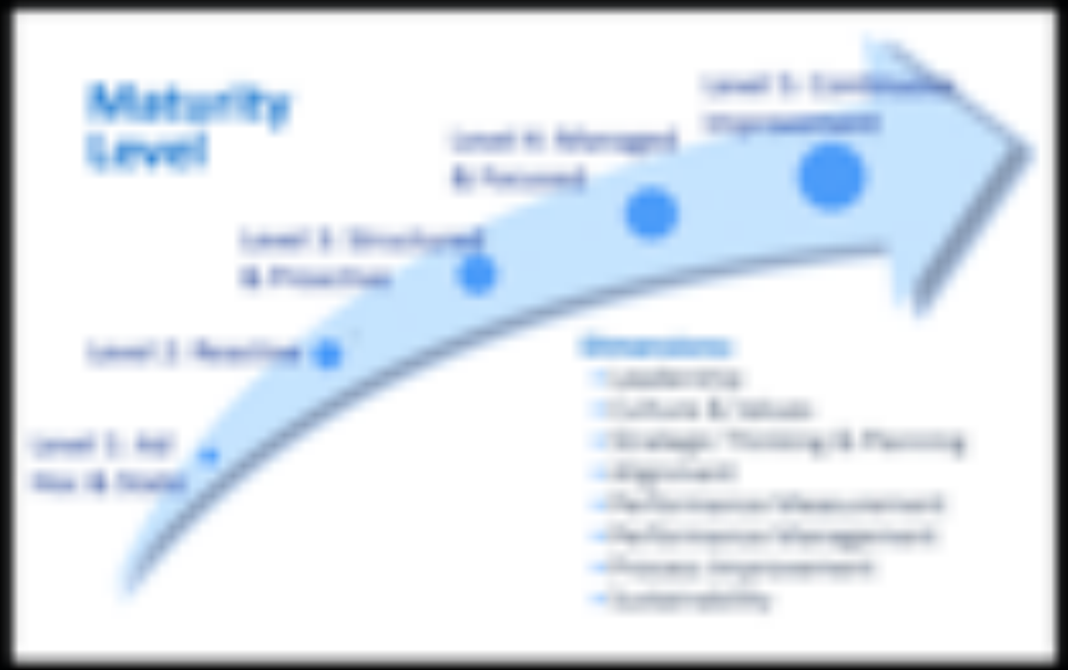
Process

Security processes aligned
to OT environment

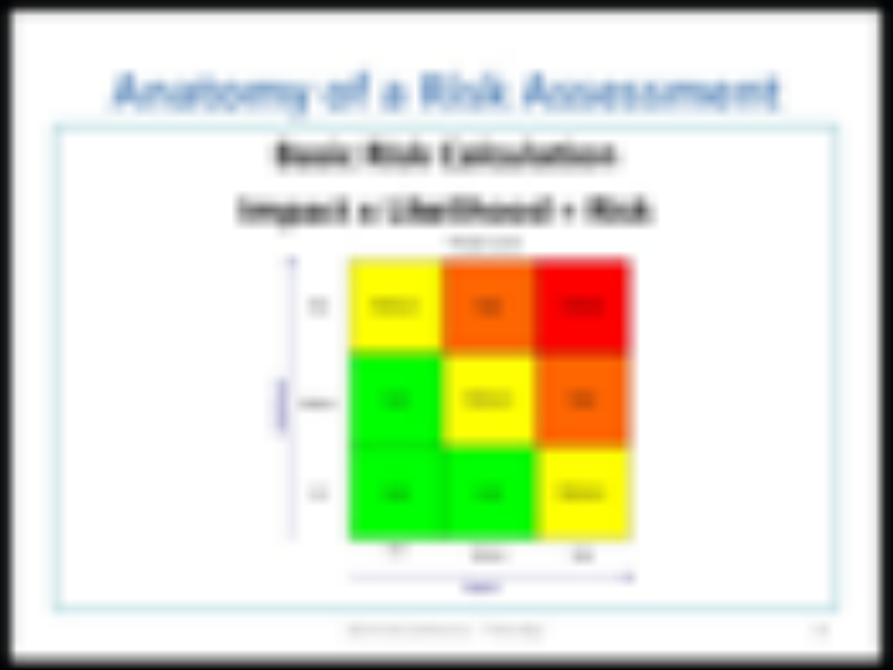
Technology

Right technology
to support

OT Security Program, aligned to business objectives and regulatory requirements



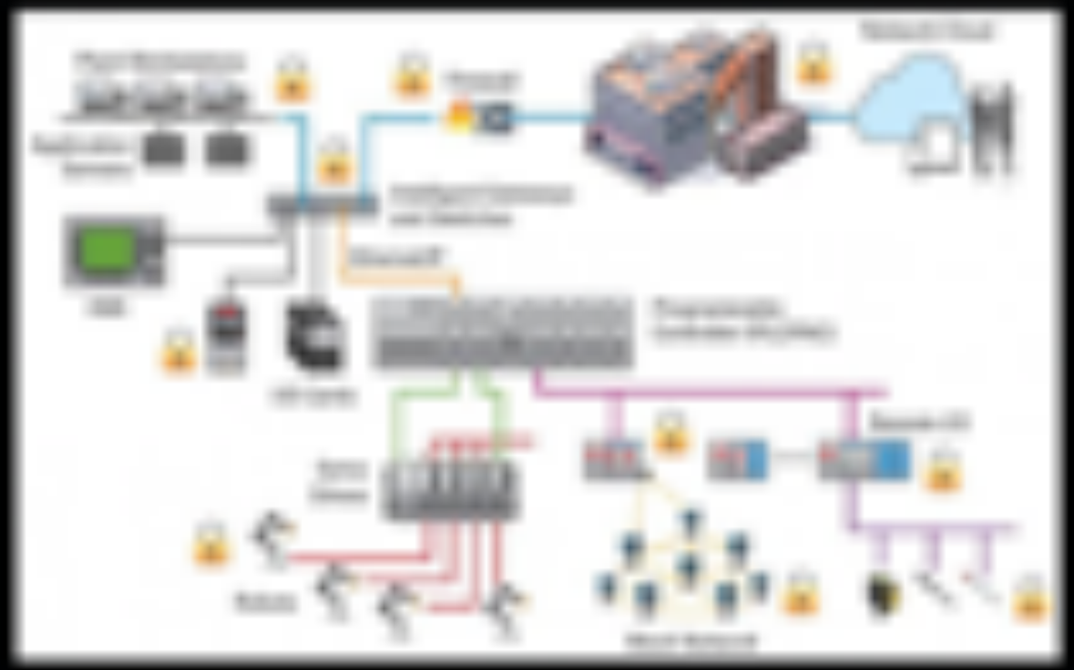
OT Security Strategy & Plan



Security Risk Assessment & Management

Governance / Compliance (RACI)

Device Discovery and Management



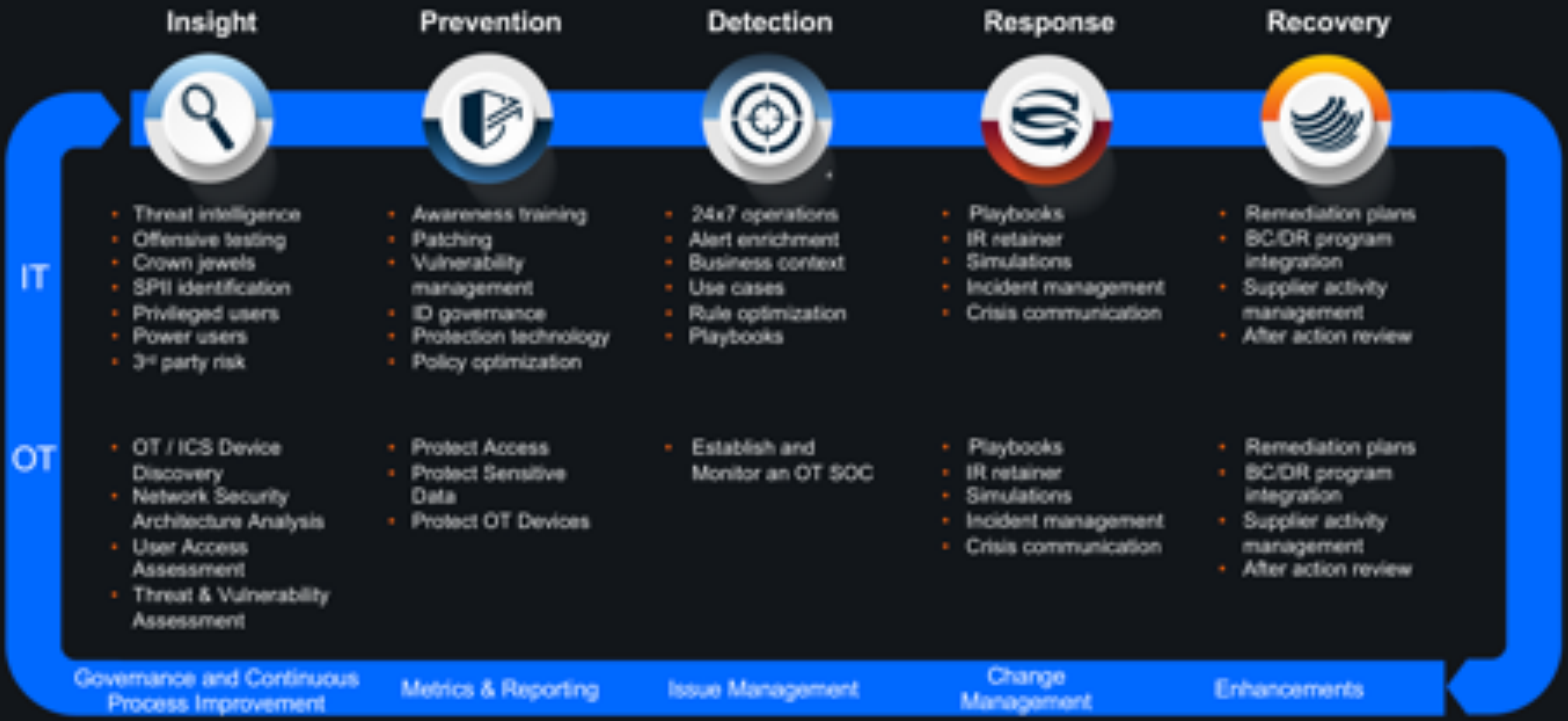
Network Discovery & Security Architecture

Role Based Access Controls (3rd Party Security)

Data Discovery, Classification & Protection

Security Event & Incident Monitoring

Security Incident Response



	Insight	Prevention	Detection	Response	Recovery
IT	- Threat intelligence - Offensive testing - Crown jewels - SPII identification - Privileged users - Power users - 3rd party risk	- Awareness training - Patching - Vulnerability management - ID governance - Protection technology - Policy optimization	- 24x7 operations - Alert enrichment - Business context - Use cases - Rule optimization - Playbooks	- Playbooks - IR retainer - Simulations - Incident management - Crisis communication	- Remediation plans - BC/DR program integration - Supplier activity management - After action review
OT	- OT / ICS Device Discovery - Network Security Architecture Analysis - User Access Assessment - Threat & Vulnerability Assessment	- Protect Access - Protect Sensitive Data - Protect OT Devices	- Establish and Monitor an OT SOC	- Playbooks - IR retainer - Simulations - Incident management - Crisis communication	- Remediation plans - BC/DR program integration - Supplier activity management - After action review

Governance and Continuous Process Improvement

Metrics & Reporting

Issue Management

Change Management

Enhancements

THANK YOU!