IBM Security

Stay Ahead of Cyber Threats with X-Force Threat Management for OT

Rafal Czerniewicz
IBM Security
Managed Security Leader EMEA

IBM Security / © 2019 IBM Corporation

IBM

IBM Security

Agenda

- X-Force Threat Management - Introduction
- XFTM Architecture
- OT Team
- Use case example
- Key take away

IBM

X-Force Threat Management

- Our clients want **visibility**
- **Speed** to notification, investigation, and response
- **Consistency** in identification and investigation
- **Quality** investigation
- Our clients want a team **member/partner**
- **Governance** and continuous improvement

Enhanced to deliver same level of protection for OT, IoT, IoMT domains

IBM Security / © 2019 IBM Corporation

X-Force Threat Management for OT / IoT / IoMT

Insight → *Protection* → *Detection* → *Response* → *Recovery*

IBM **X-Force Threat Management Services**

Identify and protect critical assets, detect advanced threats, respond and recover faster from disruptions

Governance and Continuous Process Improvement

A smarter platform that can accelerate investigation and response

Watson AI | X-Force Exchange | Analytics Engines | Use Case Library | Portal & Mobile App

XFTM Integrated Global Service

Co-located Monitoring of Corporate IT Systems and Operations Systems

QRadar / X-Force

Resilient an IBM Company

Managed IDS for Infrastructure Monitoring & Ecosystem Integration

NOZOMI NETWORKS

Zingbox A PALO ALTO NETWORKS® COMPANY

ARMIS™

CYBERX

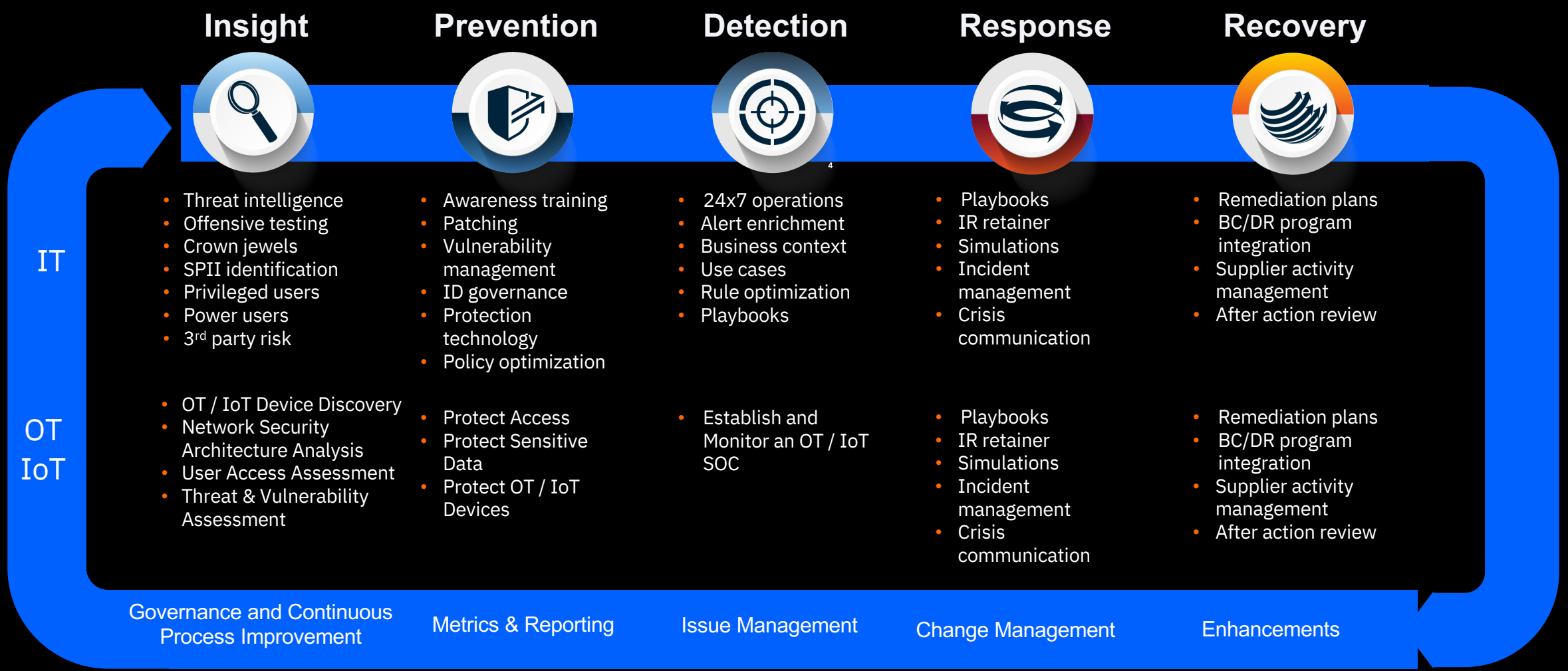
CLAROTY Clarity for OT Networks

Dedicated Delivery Process with Specialized Environment Expertise

IBM Security / © 2019 IBM Corporation

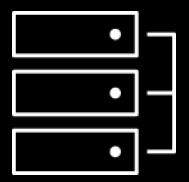
How should we think about creating an OT / IoT Security Program?

Strategically focused and balanced security program based on risk



NIST CSF

Solution coverage

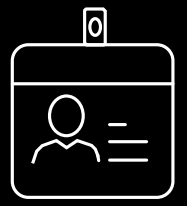


LEVELS 5 & 4
Enterprise / Site Network

Corporate Users | Business Apps | Servers | Network Devices | Security Devices

LEVEL 3.5
DMZ

DMZ Firewalls | DMZ Switches | Application Servers



LEVELS 3 & 2
Area Operations & Supervisory Control

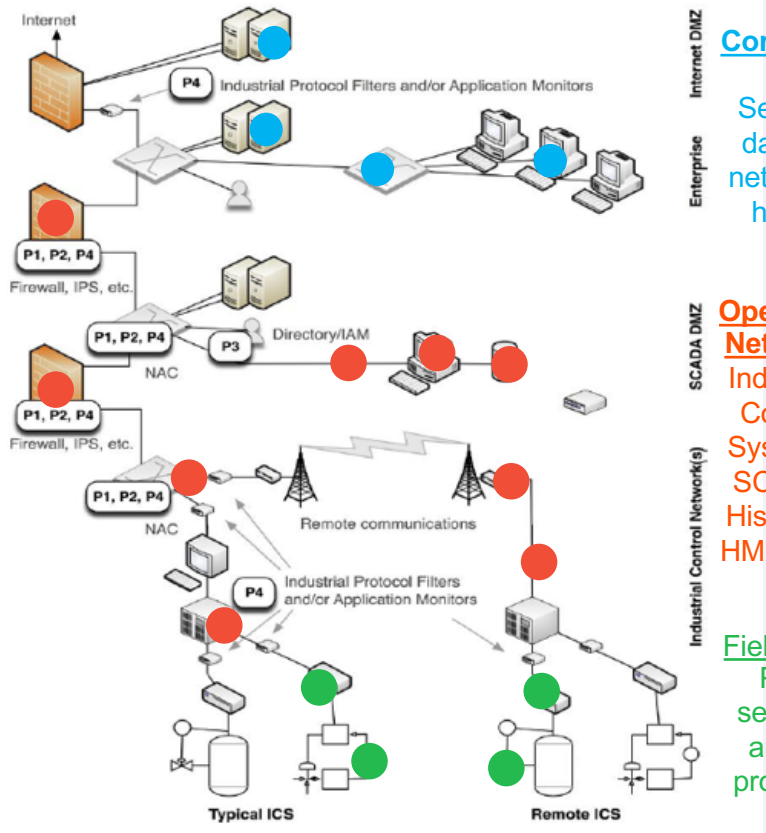
Engineer Workstations | L2/L3 Firewalls | Data Historians | Operator Interface | SCADA / DCS | OPC Servers

LEVELS 1 & 0
Basic Control & Instrumentation

PLCs | RTUs | Sensors | Actuators | Physical Equipment

IBM | ABB | CYBERX | NOZOMI NETWORKS | FORTINET | CISCO | tdi technologies

Solution approach by network level (low detail)



Internet DMZ

Enterprise

SCADA DMZ

Industrial Control Network(s)

Corporate IT: Security data on networks, hosts.

Operation Network: Industrial Control Systems/ SCADA, Historian, HMI, PLC.

Field level: PLC, sensors, analog protocols

DATA SOURCES including INDUSTRIAL PROTOCOLS

IBM QRadar

IBM Resilient

DETECT

- Asset and risk discovery
- Operation network threat picture
- SCADA & ICS monitoring
- Remote vendor service access
- Security breach detection and forensics down to field level
- Alerts on sensor anomalies

Prioritized incidents

RESPOND

- Operational & Security Response Procedures
- Attack path & time analysis
- Identify to running and even advanced attacks

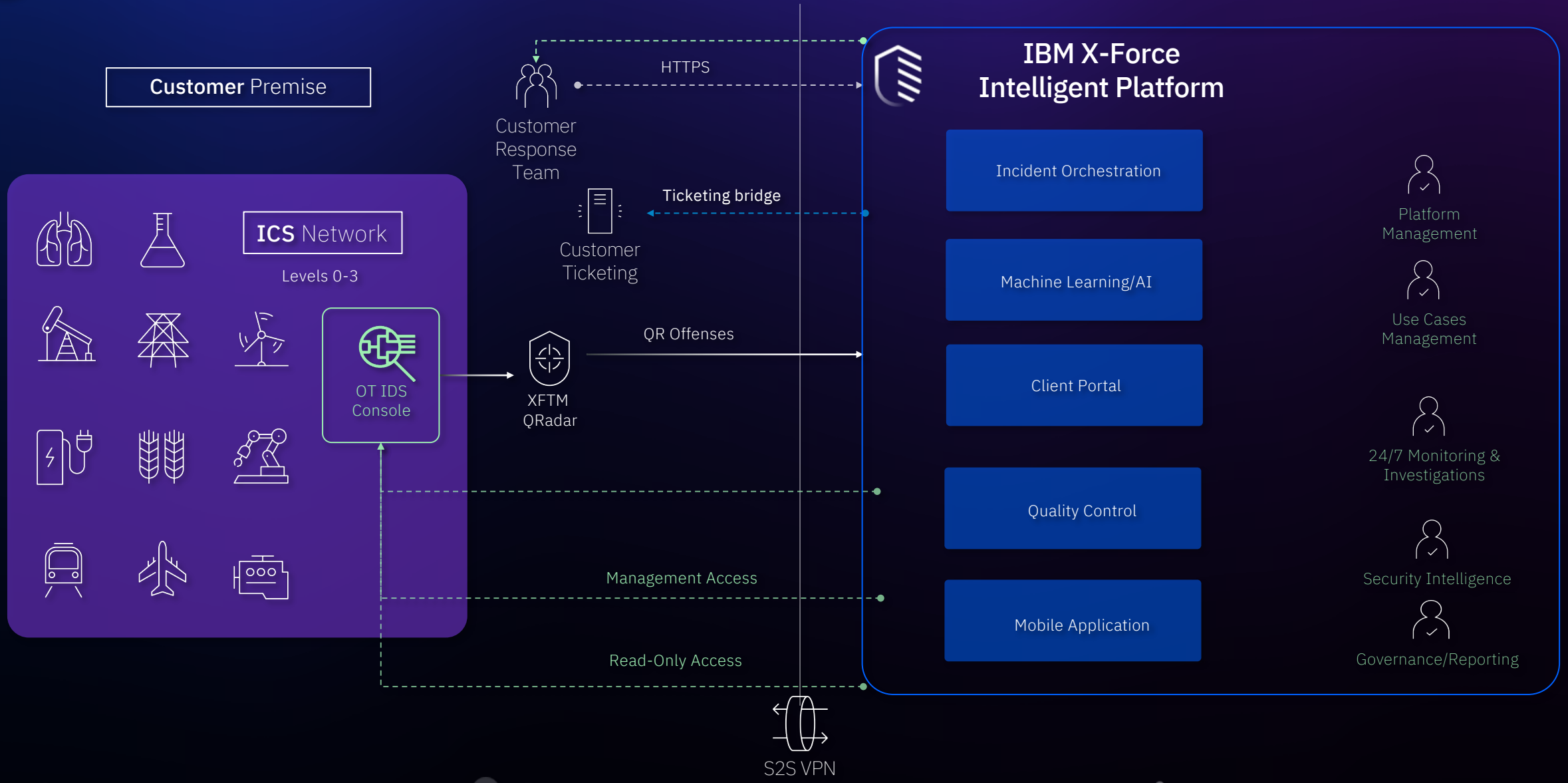
Security Intelligence

Embedded Response

* SIEM = Security Incident and Event Management with 3rd party integrations

IBM Security / © 2020 IBM Corporation

IBM XFTM for OT

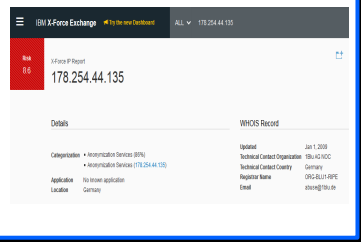


Consuming Tools and Threat Intelligence via your Security Partner

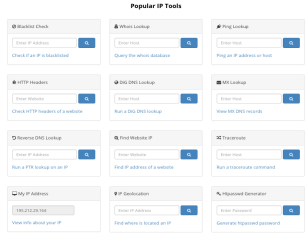
IBM X-FORCE Threat Management Services

PUBLIC TOOLS

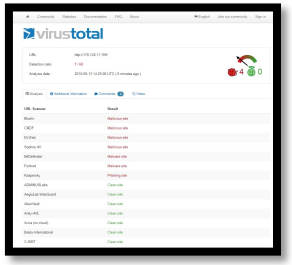
X-Force Exchange



IP VOID



Virus Total



IBM COMMERCIAL TOOLS

Use Case Library

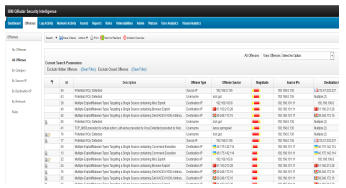
Resilient

resilient

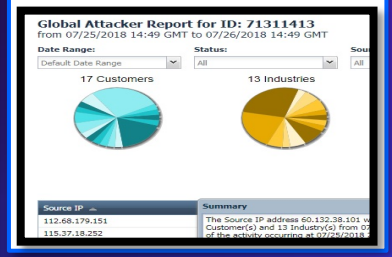
Watson for Cybersecurity

IBM PROPRIETARY TOOLS

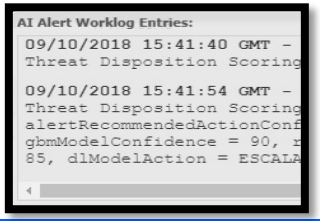
Master Console



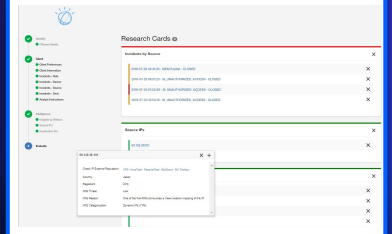
Threat Intelligence



False Positive Reduction



Second Screen

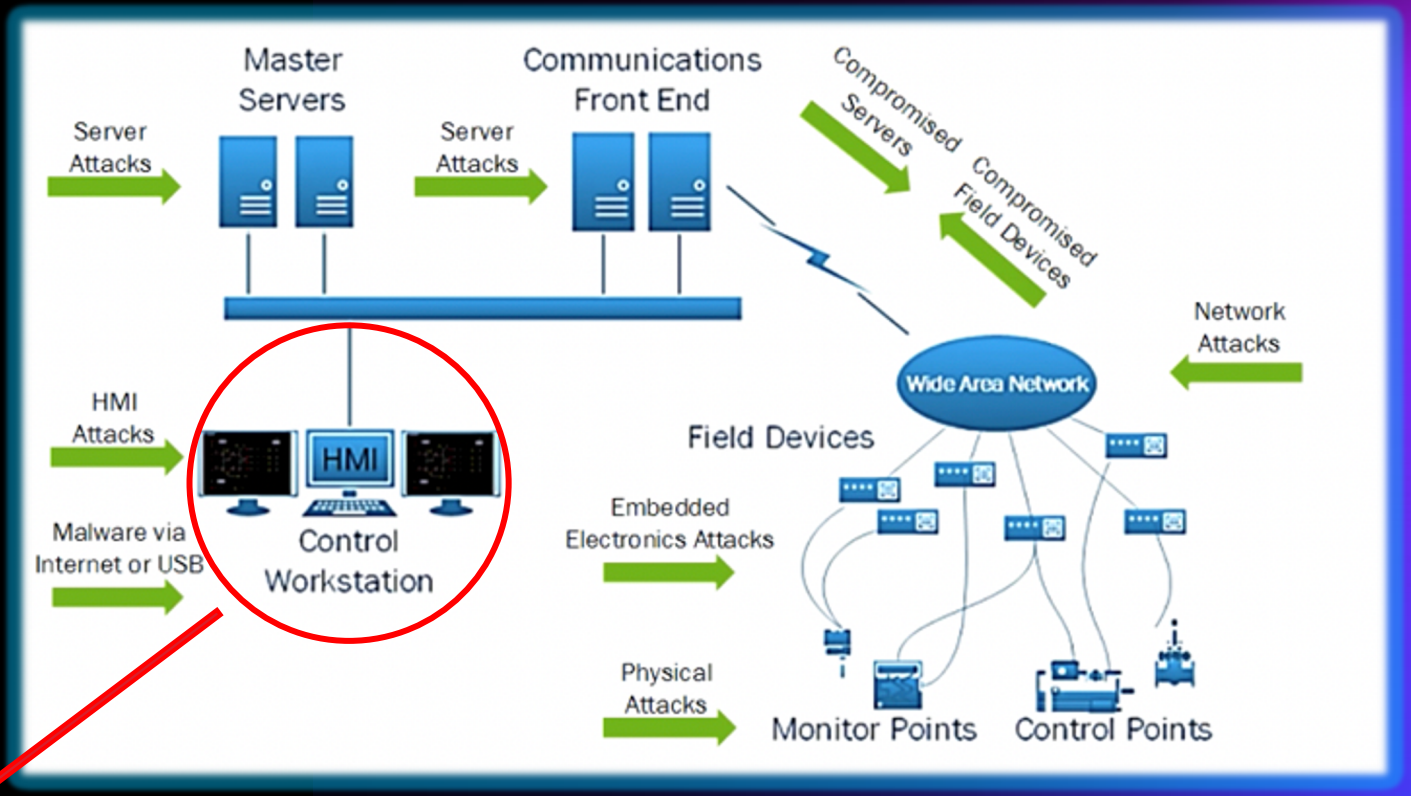


MSS Education

Use Case – Threat Scenario

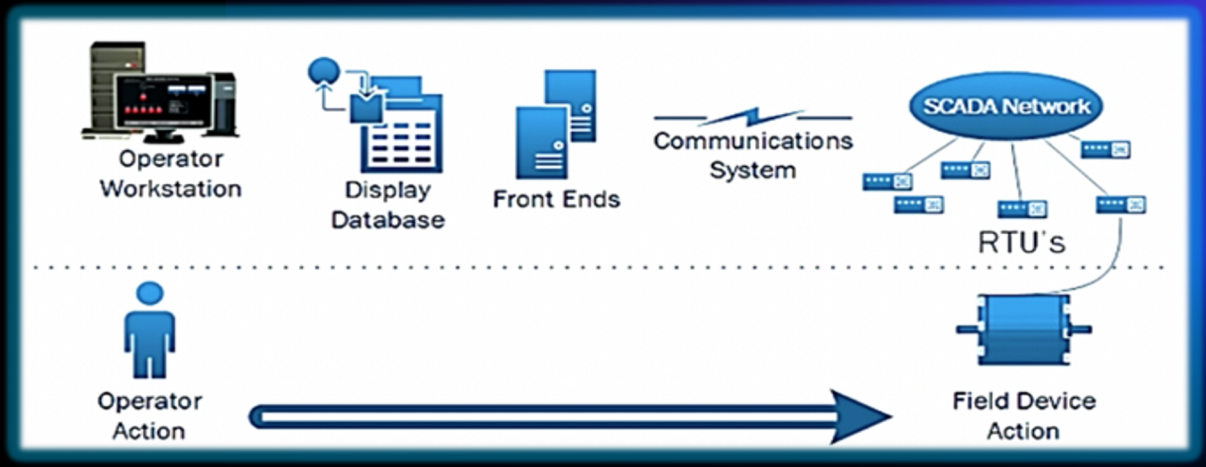
BASIC ATTACK TREE

- Malicious Insider → Authentication Bypass on HMI →
- Remote Access Compromised → Compromised Engineer Credentials →
- Malicious USB Key → Compromised Engineer Credentials →



HUMAN MACHINE INTERFACES (HMIS)

Access to the HMI usually means access to the process



IBM Security / © 2020 IBM Corporation

Use Case - Detection

ATTACK MODEL

- Password Guessing - HMI
- Access to HMI
- Configuration Change

QRADAR DETECTION

Event Name	SIGN:PASSWORD:WEAK
Low Level Category	Security Event
Event Description	
Magnitude	

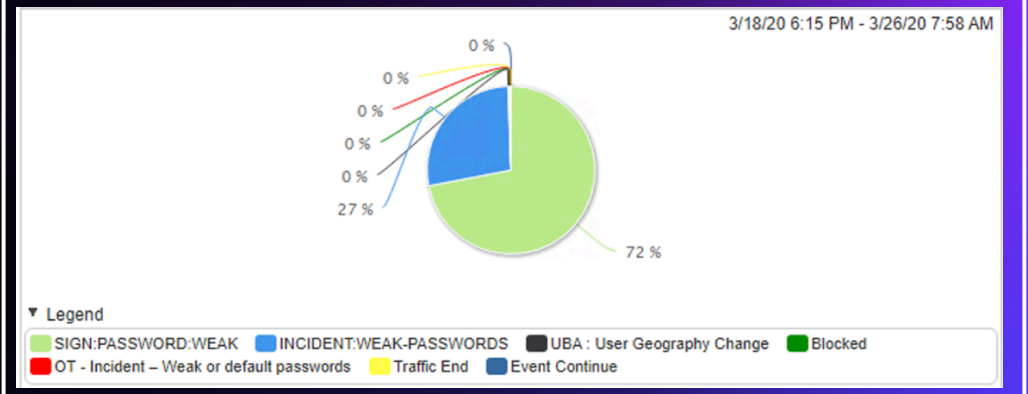
Event Name	VI:NEW-PROTOCOL
Low Level Category	Security Event
Event Description	
Magnitude	

Event Name	VI:NEW-PROTOCOL:CONFIRMED
Low Level Category	Security Event
Event Description	
Magnitude	

Event Name	SIGN:PROGRAM:DOWNLOAD
Low Level Category	Security Event
Event Description	
Magnitude	

Event Name	VI:PROC:NEW-VAR
Low Level Category	Security Event
Event Description	
Magnitude	
EventName (custom)	New SCADA variable appeared

QRADAR CORRELATION WITH OTHER LOG SOURCES



Event Name	Log Source (Unique Count)	Event Count (Sum)
SIGN:PASSWORD:WEAK	Nozomi @ 172.27.149.4	27,539
INCIDENT:WEAK-PASSWORDS	Nozomi @ 172.27.149.4	4,526
UBA : User Geography Change	Custom Rule Engine-8 :: qradar	28
Blocked	Endpointprotection @ SEPDC1P01	27
OT - Incident – Weak or default passwords	Custom Rule Engine-8 :: qradar	27
Traffic End	PaSeries @ IPSFWP01.gerdau.net	14

Offense

IBM Security / © 2020 IBM Corporation

X-Force Threat Management across OT – Standard Package

Scalable Platform

IBM has invested in a scalable platform for easier and more efficient service delivery
XFTM for OT will utilize the MSPP in the same manner as traditional XFTM

Consulting Services

IBM Security offers consulting and systems integration services for your environment

- SOC integration
- Custom SOC builds

Partner Ecosystem

Nozomi Networks, the industry leader in OT technology, is the IBM strategic partner. IBM deploys and tunes the Nozomi devices to provide customers with more than just asset monitoring

Integrated Global Service

Co-located global monitoring

Visibility and monitoring of OT devices

Dedicated delivery with specialized OT Security expertise

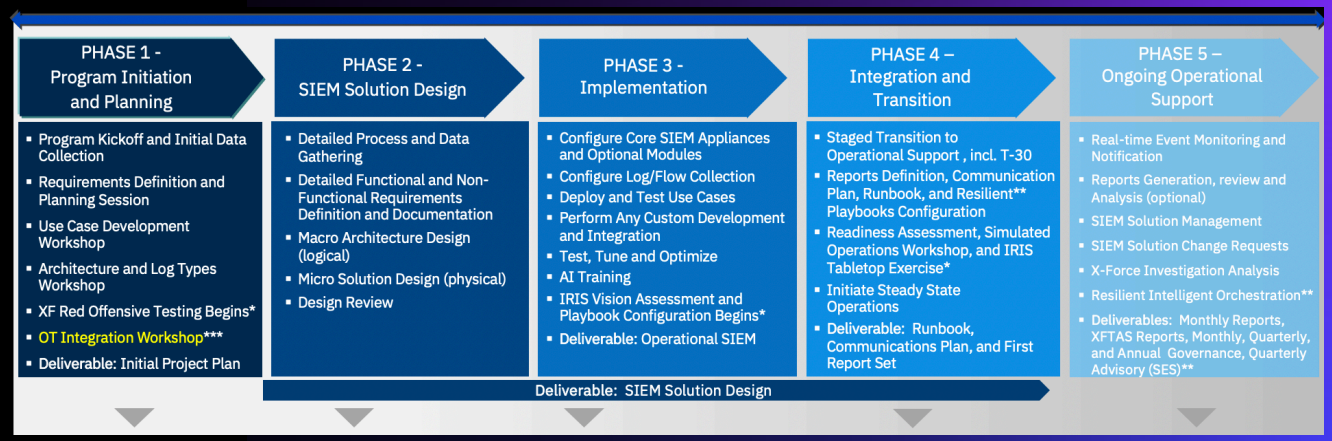
IBM QRadar / Resilient

IBM Security

IBM Security / © 2020 IBM Corporation

Take away

Difficult to do it alone



IBM Security / © 2020 IBM Corporation

Take away

- Difficult to do it alone
- Requires investment
-

IBM Security / © 2020 IBM Corporation

Take away

- Difficult to do it alone
- Requires investment
- Closer than you think

Hacker Tried to Poison Florida City's Water Supply, Police Say

The hacker tried to drastically increase sodium hydroxide levels in the water, Pinellas County, Florida, officials said on Monday.

vice.com

11:44 PM · Feb 8, 2021

851 779 Copy link to Tweet

IBM Security / © 2020 IBM Corporation