

# X-Force Red – OT Scary Stories

# Agenda

- About XFR
- Security challenges in OT/SCADA environment
- Our approach
- Stories:
  - Major energy company
  - Major airport
  - Utility provider

# About IBM X-Force Red

IBM elite team of hackers

Regular speakers at conferences

Dedicated to delivering offensive security testing

People with many years of global experience  
delivering projects for customers of all profiles

# Our delivery results are driven by the creativity and qualifications of our experts, combined with methodical approach & cutting edge tools

## CREATIVE METHODOLOGIES

### Creative approach to security assessment

- Thinking outside of the box
- Understanding the architecture and design of the solution first

### Rational method of automated testing

- Proper use of existing tools
- Creating own tools and scripts tailored to a particular scenario

### Choosing the right domain to focus on

- Source code and dynamic testing
- Device platform testing

### Collaborative team management

- Division of responsibilities, yet interchangeable skill-sets
- Dynamic testing and source review members collaborate to uncover and verify security issues



## TEAM SKILLS & QUALIFICATIONS

### PENTESTING

- **EC-Council** Certified Ethical Hacker
- **SANS** Advanced Penetration Testing - GXPN
- **SANS** Certified Web Application Penetration Tester (GWAPT)
- Offensive Security Certified Expert (OSCE)
- Offensive Security Certified Professional (OSCP)

### INCIDENT RESPONSE/FORENSICS

- **EC-Council** Certified Hacker Forensic Investigator
- **GREM** GIAC Reverse engineering malware

### SEMI-EMBEDDED SCADA-SPECIFIC

- **IACRB** Certified SCADA Security Architect

### INFORMATION SECURITY AND RISK MANAGEMENT

- **ISC2** Certified Information Systems Security Professionals (CISSP)
- **ISACA** Certified Information security manager (CISM)



# What IT Security is about?

- Today's security drivers



# OT Security Challenges

## Complex environment

Various integrated technologies operated by different vendors

Attack surface mostly unknown

## Lack of asset inventory

Which systems, applications and other assets do they have?

Which assets matter most?

## Fragile and critical systems

Many systems can become unstable if not tested properly

## Custom and specific systems

Often the technology is custom and not publicly known.

Requires a specific skillset and test strategy



# X-Force Red Penetration Testing Services

“Criminal-minded” testing to uncover vulnerabilities

Virtual and on-site manual testing

Ad-hoc testing or subscription services

Managed program prioritizes which assets need testing

“Red Labs” IoT, IIoT, OT testing during design and beyond

Testing covers various possibilities for intrusion

- External Threat
- Insider
- Malicious User or Customer
- Hacktivist

Report findings of what we tried and what we found



## Application

- Web
- Mobile
- Terminal
- Thick-client
- Mainframe
- Middleware



## Network

- Internal
- External
- Wireless
- Other radio frequencies
- SCADA



## Human

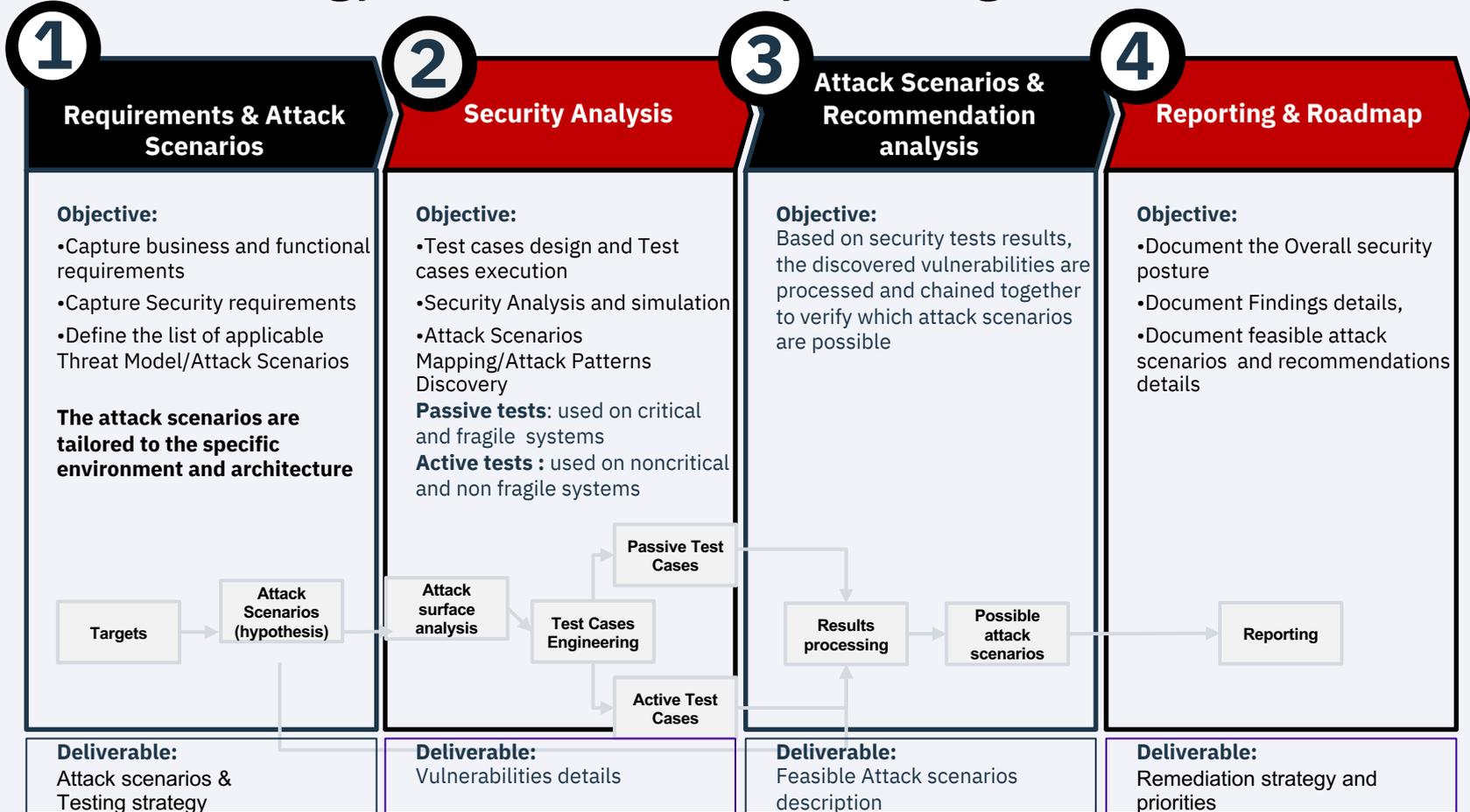
- Physical
- Social engineering
- Phishing



## Hardware and embedded devices

- Internet of Things
- Wearable technologies
- Point of Sale
- ATMs
- Self-checkout kiosks

# Methodology: OT/ICS Security Testing



# OT Assessment Story: A Major Power Company

## Business Challenge:

- The customer wanted IBM to test the security of their Smart Gateway devices prior to the roll out to customers to ensure that they were secure from attackers and customer tampering.

## What We Did:

- As this was an embedded device we used a different approach than for a typical penetration test. We used our embedded/mobile device test framework that we developed.
- Many critical vulnerabilities found which could lead to device, billing and backend system exploitation. This included root access to the device itself, passwords and customer data being sent over the Internet as clear text (un-encrypted), etc.

## Benefits:

- Customer was very pleased and extremely surprised by just how quickly and completely we had compromised the device and exposed serious flaws in it.
- We supplied the customer with a very detailed report and a set of recommendation to assist them in securing the device and data in transit.



**IBM tested the embedded device at the lowest possible level, using our embedded/mobile device test framework to identify security flaws in the OS, PCB and data transfer which could have led to the devices being compromised by an attacker or data modified by a customer.**

# OT Assessment Story: An International Airport

## Business Challenge:

- The airport wanted IBM to test the security of their baggage handling systems including SCADA and ICS.

## What We Did:

- Wireless networks connected to baggage infrastructure network were found in public areas of airport and used as an entry point.
- Exploiting multiple vulnerabilities discovered in systems it was possible to gain full control of Active Directory, all systems and applications, including direct access to PLC devices and manipulating registers on them
- It would give attacker possibility to even impact X-ray machines used to scan content of baggage, making possible to pass dangerous materials inside a plane!

## Benefits:

- The customer was given recommendations about how to implement remediation measures which would enhance security posture and protect this critical infrastructure from unauthorized access.



**IBM discovered wireless networks connected to critical baggage manipulation systems. These system having multiple vulnerabilities could give the ability for attacker to manipulate baggage controls leading to the possibility of loading dangerous materials and devices into a plane, which could have dire consequences!**

# OT Assessment Story: Utility Middle East

## Business Challenge:

- The company wanted IBM to test if it was possible to reach the internal SCADA networks from the internet, using a spear phishing attack via e-mail. The company wanted to target the technical staff specifically.

## What We Did:

- The client had a highly secure mail filtering system, efficiently preventing any e-mail attacks generated from any of the standard frameworks, freely available to, and in use by, hackers on the Internet.
- IBM instead designed the malicious mail-campaign, using a manual approach, tailored to circumvent the very restrictive filtering mechanism, that allowed the campaign to go through to the intended targets inside the organization.
- Once the campaign went through, a large percentage of the staff were tricked into giving up their intranet credentials (and full mailbox access through an insecure webmail) and several staff members were lured into installing a backdoor on their workstation, allowing IBM full access to the intranet from the outside, by pivoting off of the compromised workstations. This access included staff documents, sensitive fileshares and access to SCADA Web interfaces.

## Benefits:

- The customer learned, that while their mail filter was efficient, they should not rely on technology alone.
- Hackers often choose to go for the „human element“ and the customer was advised to work on security awareness campaigns and education, to strengthen the staff appreciation of the importance of Security.



**IBM showed, that using the human element as an attack vector, it was possible to circumvent system security. By not using common frameworks, but instead creating specific tools to generate the e-mail campaign and the backdoor payload, IBM demonstrated that a determined hacker can get around filters and antivirus deployed in an organization**

# Thank you

Follow us on:

[ibm.com/xforcered](https://ibm.com/xforcered)

[@xforcered](https://twitter.com/xforcered)

[securityintelligence.com](https://securityintelligence.com)

[ibm.com/security/community](https://ibm.com/security/community)

[xforce.ibmcloud.com](https://xforce.ibmcloud.com)

[youtube.com/ibmsecurity](https://youtube.com/ibmsecurity)

© Copyright IBM Corporation 2019. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.