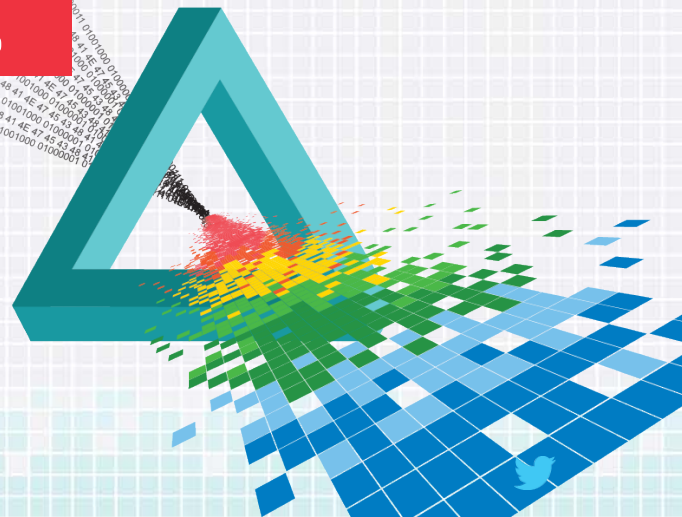
RSA Conference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

WHEN IT THREATS MEET OT INNOCENCE



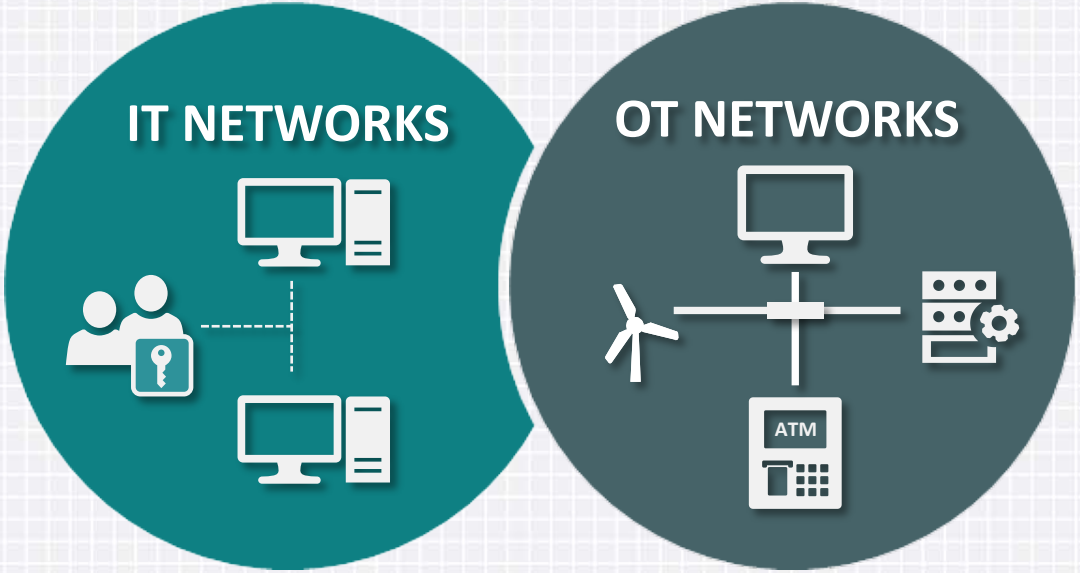
SESSION ID: STU-T8

Udi Solomon

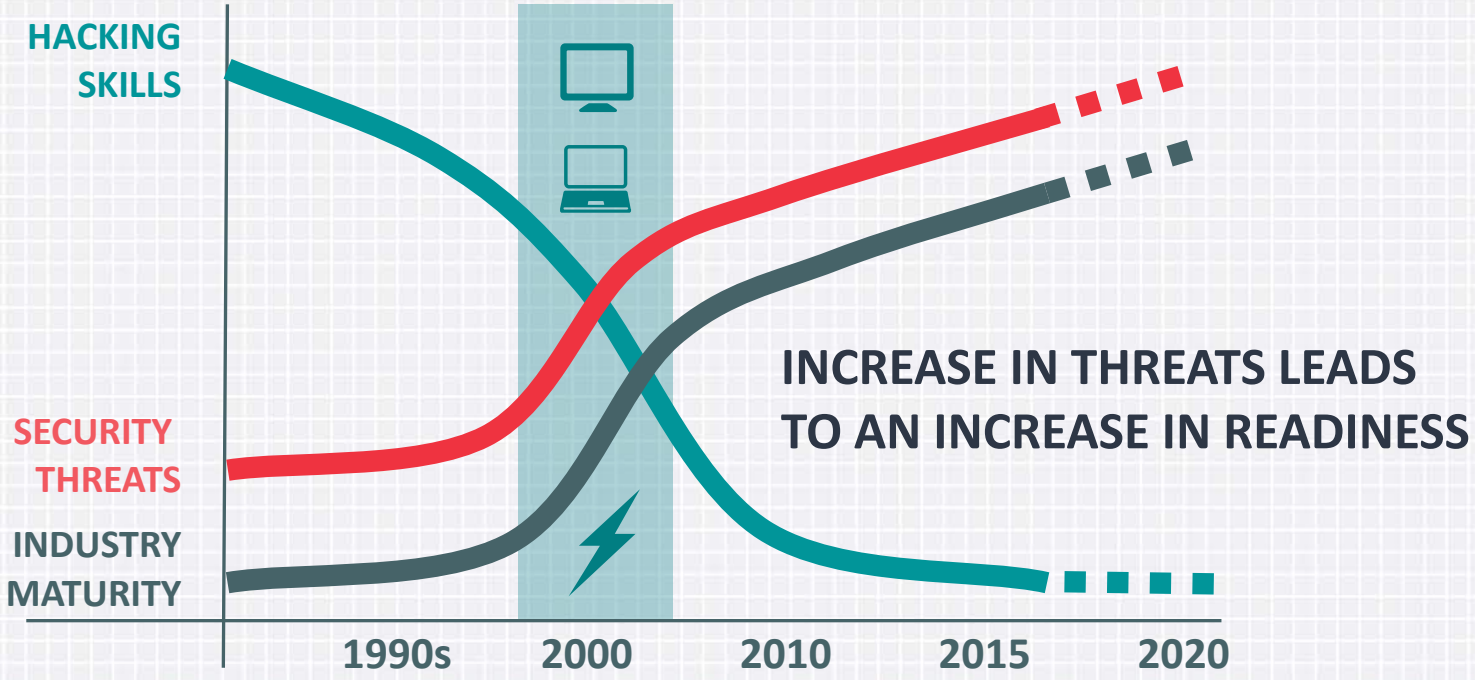
VP Product

ThetaRay

People vs. Machines



IT TECHNOLOGY EVOLUTION



IT TOOK TWO DECADES

TO REACH IT MATURITY

OT SECURITY NEEDS TO CATCH UP

LIMITED OT SECURITY MATURITY

SECURITY UPDATES

48% Systems are NOT patched on a regular basis

EXPERT PERSONNEL

50% Incidents are NOT handled by IT security teams

ORGANIZATIONAL AWARENESS

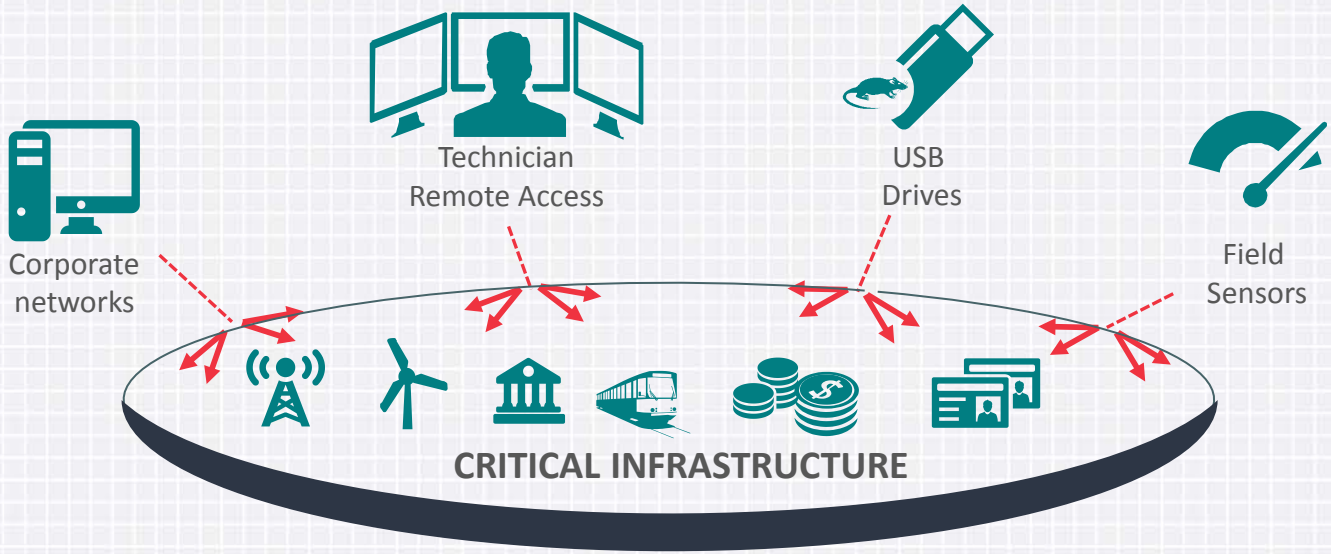
70% CI Organizations view cyber risk to be high or critical

NEARLY 7000 IT VULNERABILITIES

LESS THAN 200 OT VULNERABILITIES

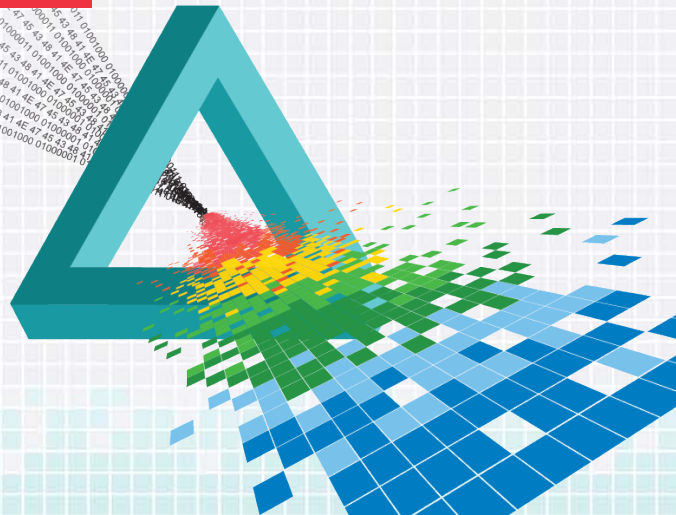
1. SANS Institute, SCADA and Process Control Security Survey, 2013
2. ICS-CERT Industrial Control Systems Cyber Emergency Response Team, 2013
3. NSS Labs, 2014

THE NETWORK ISOLATION DREAM

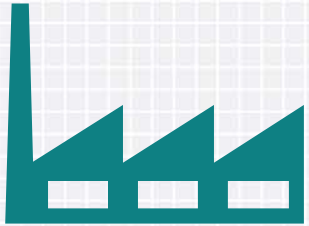


THE FUTURE OF OT THREATS

APTs ARE ALREADY HERE



THE THREAT IS REAL



Dec 2014

ATTACK ON GERMAN STEEL MILL

Spear Phishing	Malware Installation	Recon & Spread	Operational Impact

54%

THIS IS NOT AN ISOLATED EVENT

SURVEYED CI ORGANIZATIONS HAVE IDENTIFIED “ATTEMPTS TO MANIPULATE” EQUIPMENT VIA CONTROL SYSTEM.

1. www.securityweek.com/cyberattack-german-steel-plant-causes-significant-damage-report
2. SANS Institute, ICS Defense Use Case (DUC), Dec 30 2014
3. TrendMicro, Destructive hacking attempts target critical infrastructure in Americas – survey, April 2015

THE THREAT IS REAL

Feb 2015

GLOBAL ATTACK ON ATMs

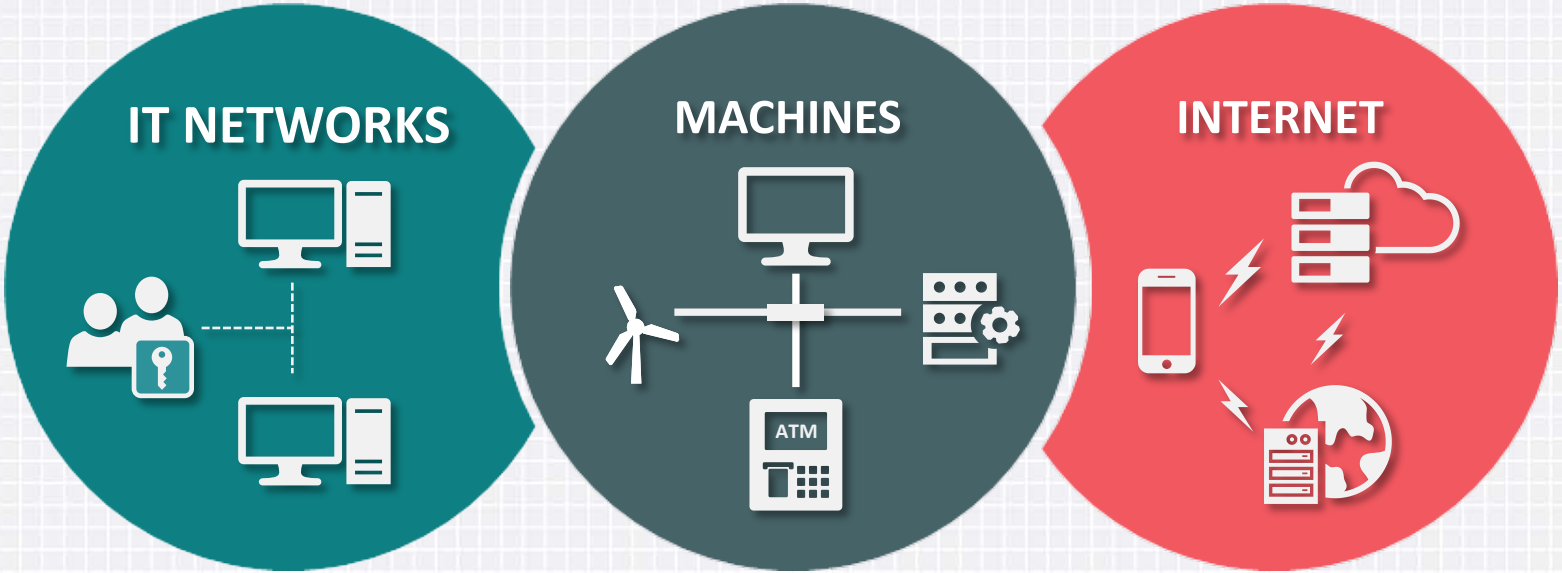
Spear Phishing	Malware Installation	Recon & Spread	Operational Impact

1 BILLION STOLEN FROM 100 BANKS IN 25 COUNTRIES

OT THREATS: IMPACT ALL CRITICAL INFRASTRUCTURE SEGMENTS INLUDING FINANCIAL, UTILITIES, TRANSPORTATION, AND TELCOS

1.www.securityweek.com/hackers-hit-100-banks-unprecedented-1-billion-cyber-attack-kaspersky-lab
2. CARBANAK APT – The Great Bank Robbery, Feb 2015

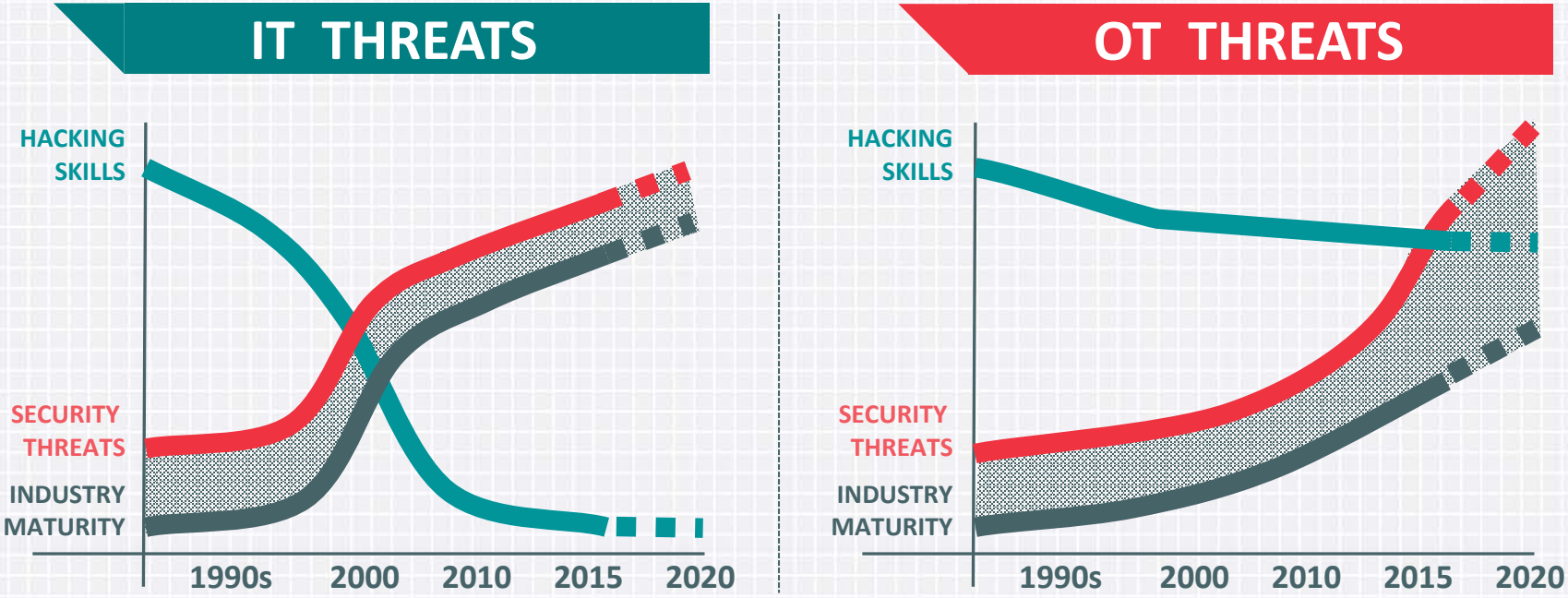
THE WEAKEST LINK



IT THREATS INFILTRATE OT INFRASTRUCTURE

CONNECTED MACHINES ARE EXPOSED

OT TECHNOLOGY EVOLUTION



IT TOOK TWO DECADES

TO REACH IT MATURITY

WE CANNOT WAIT

ANOTHER 20 YEARS

IT SECURITY LESSONS

SECURITY FOCUS

- OT Security Team
- IoT Expertise
- OT Budget

INTERNAL AWARENESS

- Policies
- Procedures
- Education

OT DEFENSE IN-DEPTH

- Internal Networks
- Machine Monitoring
- Industrial Protocols

OT SECURITY SOLUTIONS

ANALYZE MACHINE DATA

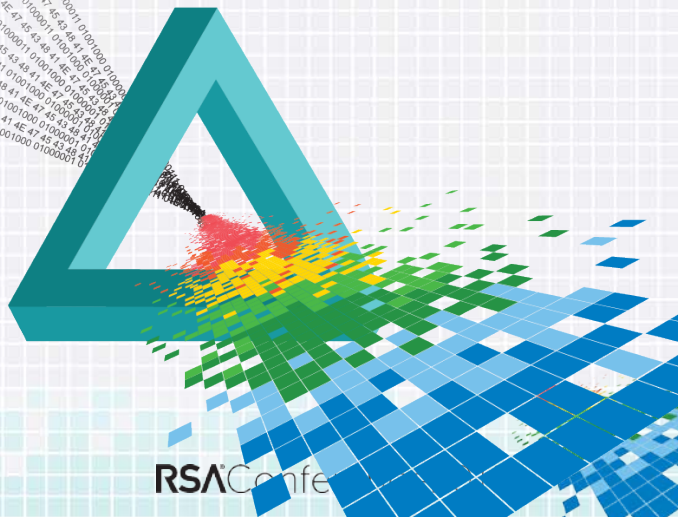
RULE FREE DETECTION

ACCURACY & RELIABILITY

EARLY DETECTION

IT'S NOT ABOUT IDEAS.

IT'S ABOUT MAKING IDEAS HAPPEN.



THANK YOU !

THIS PRESENTATION BROUGHT TO YOU BY ThetaRay

COME VISIT US AT: **BOOTH #N3036**