

# **RSA**Conference2016

San Francisco | February 29 – March 4 | Moscone Center

SESSION ID: HT-F02

## **Cybersecurity for Oil and Gas Industries: How Hackers Can Steal Oil**



Connect **to**  
Protect

**Alexander Polyakov**

CTO  
ERPScan  
@sh2kerr



#RSAC

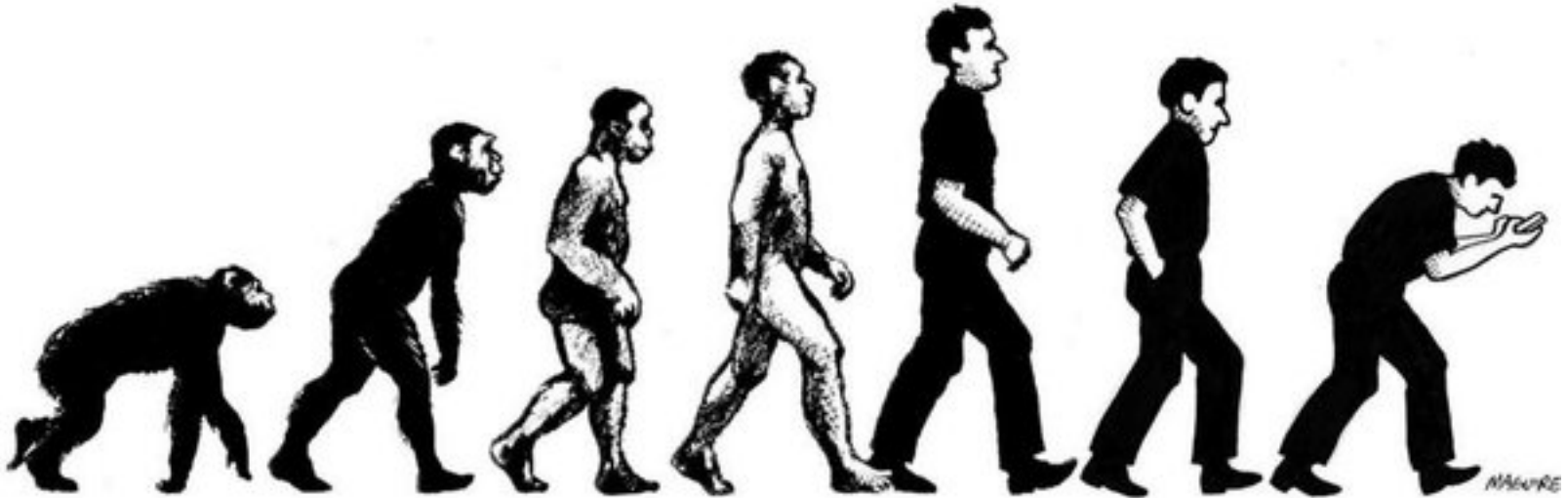


- The only 360-degree SAP Security solution - ERPScan Security Monitoring Suite for SAP and Oracle
- Leader by the number of acknowledgements from SAP ( 250+ ) and Oracle (40+)
- 80+ presentations key security conferences worldwide
- 30+ Awards and nominations
- Research team – 20+ experts with experience in different areas of security from ERP to ICS and Mobile
- Offices in Palo Alto, Amsterdam, Copenhagen, Sidney

# Evolution?



#RSAC



**ERPScan**

Security Solutions for SAP

# How does traditional VAPT works



- A company hire experts for VAPT service or Product
- Those specialists run some pentesting tools
- They (may) manually test vulnerabilities, escalate privileges and as a result write report about vulnerabilities
- Report looks like

**“we found vulnerability X on the server Y**

**look at the black screenshot with command line”.**

# Common VAPT report



#RSAC

```
root@kali:/opt/icmpsh# sysctl -w net.ipv4.icmp_echo_ignore_all=1 >/dev/null
root@kali:/opt/icmpsh# chmod 777 icmpsh_m.py
root@kali:/opt/icmpsh# ./icmpsh_m.py 10.0.0.8 10.0.0.11
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 10.0.0.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.0.1

C:\>systeminfo
systeminfo

Host Name:                 TESTER-PC
OS Name:                   Microsoft Windows XP Professional
OS Version:                5.1.2600 Service Pack 2 Build 2600
OS Manufacturer:          Microsoft Corporation
```



**ERPScan**

Security Solutions for SAP

# Why?



#RSAC

- Everybody know that there are vulnerabilities in almost every system
- The question now
  - how dangerous are they
  - how easy is to exploit them
  - what can happen after the exploitation?
  - and what kind of **REAL** risks to **YOUR** organization it provides.



# Risks are different



#RSAC



## Espionage:

Pharmacy  
Retail  
Manufacturing  
Private Sector



## Sabotage:

Manufacturing  
Oil and Gas  
Utilities  
Energy



## Fraud:

Retail  
Financials  
Transportation  
All others....



ERPScan

Security Solutions for SAP

# Why Oil and Gas?



#RSAC

- Critical
- Industry-Specific
- And I know it )

## Oil & Gas Industry



What my parents  
think I do



What my friends  
think I do



What I  
think I do



What my boss  
thinks I do



What I tell my  
wife could happen



What I  
actually do



**ERPScan**

Security Solutions for SAP



# Why Oil and Gas?



#RSAC

- PS: And something strange is happening here )

Current market price in USD per barrel



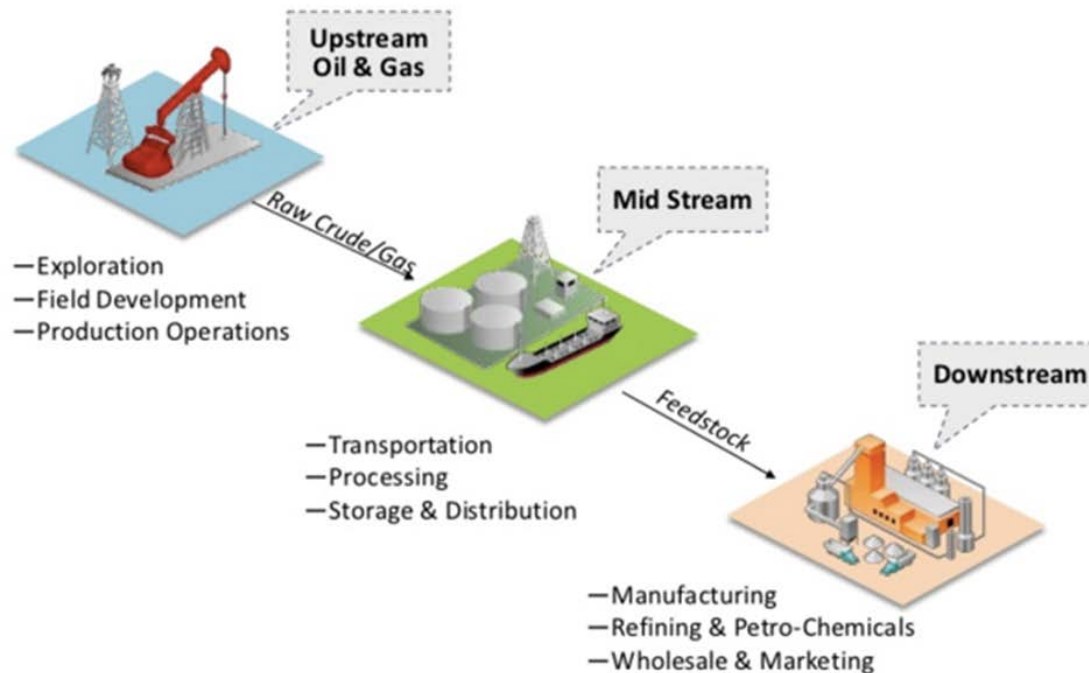
ERPScan

Security Solutions for SAP

# Oil and Gas 101



#RSAC



# Upstream: Critical processes and systems



- Extraction (Drilling)
- Gathering (From earth to separators)
- **Separation (Separate oil, gas and water)**
- Gas compression (Prepare for storage and transport)
- Temporary Oil Storage (Temporarily store before loading)
- Waste disposal (Water disposal)
- **Metering (Calculate quantity before loading)**

# Midstream: Critical processes and systems



#RSAC

- Terminal management (Obtain oil from upstream)
- Gas Processing (Separate natural gas and NGL)
- Gas Transportation (Transfer gas to storage via pipelines)
- Oil transportation (Transfer oil to storage via pipeline/Truck/Barge/Rail)
- Base load Gas storage (Temporary and long-term)
- Peak load Gas Storage
- LNG Storage
- **Oil Storage (Long-term oil storage)**

- Refining (Processing of Crude Oil)
- Oil Petrochemicals (Fabrication of base chemicals and plastics)
- Gas Distribution (Deliver gas to utilities)
- Oil Wholesale (Deliver petrol to 3rd parties)
- Oil Retail (Deliver petrol to end users)

# What can happen?



#RSAC

World | Tue Dec 30, 2014 12:19pm EST

Related: WORLD, LIBYA

## Fire at Libyan oil port destroys up to 1.8 million barrels of crude

BENGHAZI, LIBYA/CAIRO | BY AYMAN AL-WARFALLI AND ULF LAESSING



# Why should we care

#RSAC



## Caribbean Petroleum Refining Tank Explosion and Fire

**FINAL REPORT: Final Investigation Report - Caribbean Petroleum**

Location: Bayamón, PR

Accident Occurred On: 10/23/2009

Final Report Released On: 10/21/2010

Accident Type: Chemical Distribution

Company Name: Caribbean Petroleum

### Oil refinery catches fire in western Turkey

12/19/10

1 Like 0 Comments 0 Shares on Facebook

TUPRAŞ authorities said in a written statement that a fire erupted at 10:50 a.m. at TUPRAŞ's Izmir refinery because of "illegal" or improper electrical wiring. They also said the security personnel of the refinery immediately stepped in, extinguishing the fire within a short time and adding that the fire posed no danger to the environment and public health.

July 17/2015

## INVESTIGATION INFORMATION



ars technica

MAIN MENU

MY STORIES: 25

FORUMS

SUBSCRIBE

JOBS

Ars Technica has arrived in Europe. Check it out!

## RISK ASSESSMENT / SECURITY & HACKTIVISM

### Internet attack could shut down US gas stations

More than 5,000 service stations use a monitoring unit vulnerable to attack.

by Robert Lemnos - Jan 23, 2015 2:15pm MBK

1 Share 0 Tweets 0 Likes 70

A device used to monitor the gasoline levels at refueling stations across the United States—known as an automated tank gauge or ATG—could be remotely accessed by online attackers, manipulated to cause alerts, and even set to shut down the flow of fuel, according to research to be published on Thursday.



DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS HARDWARE

## Science

### Major cyber attack hits Norwegian oil industry

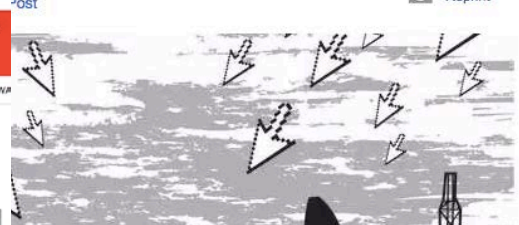
Statoil, the gas giant behind the Scandic social miracle, targeted



## Cyberattack threat in Canada's oil patch raises risk of disruptions, stolen data

STEPHEN STARR, SPECIAL TO FINANCIAL POST | January 3, 2013 4:37 PM ET

Republish Reprint



The Washington Post

+ More



CONTENDERS, REVEALED: The Washington Post's inaugural look at the 2016 contenders. Enhanced for iPad/tablet.

## Investigations

### Hackers break into energy technology company

A Save for Later Reading List

By Robert O'Harrow Jr. September 27, 2012 Follow @robertoharrow

A major technology company that enables energy suppliers and others to remotely control their operations has been penetrated by hackers from China, according to security researchers and company officials.



ERPScan

Security Solutions for SAP

# What can happen?



Plant Sabotage/Shutdown

Equipment damage

Utilities Interruption

Production Disruption (Stop or pause production)

Product Quality (bad oil and gas quality)

Undetected Spills

Illegal pipeline tapping

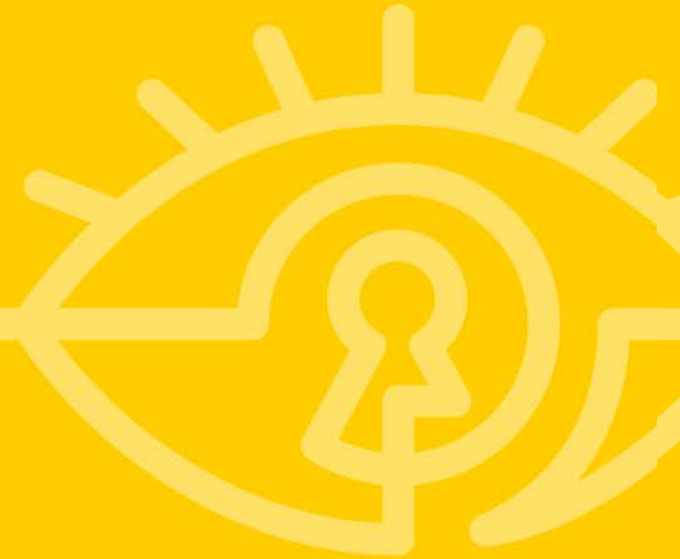
Compliance violation (Pollution)

Safety violation (Death or injury)





## What about Security



# Three aspects of Oil and Gas Cyber Security



#RSAC



**ERPScan**

Security Solutions for SAP

# Three aspects of Oil and Gas Cyber Security



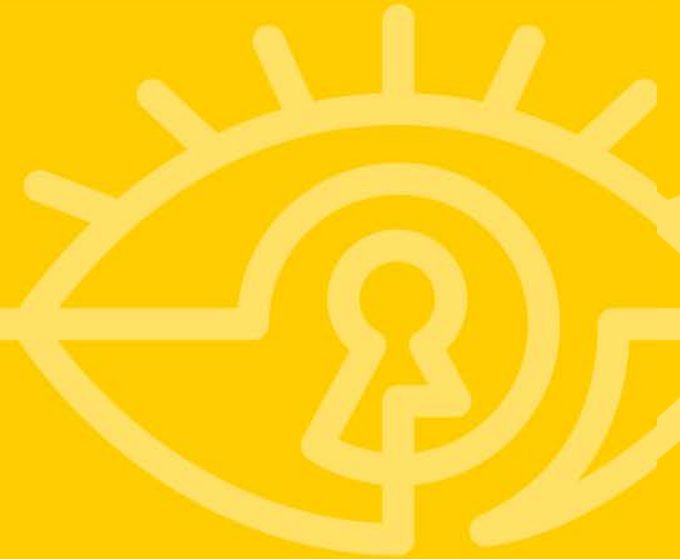
#RSAC

When we speak about securing oil and gas companies we should cover

- Operational Technology security
- Enterprise Application security
- Connections security



## **ICS Security in Oil and Gas**



# Oil and Gas Cyber-Security (OT part)



#RSAC



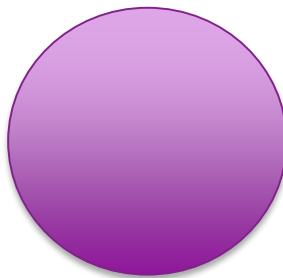
**3 Areas:**

Upstream  
Midstream  
Downstream



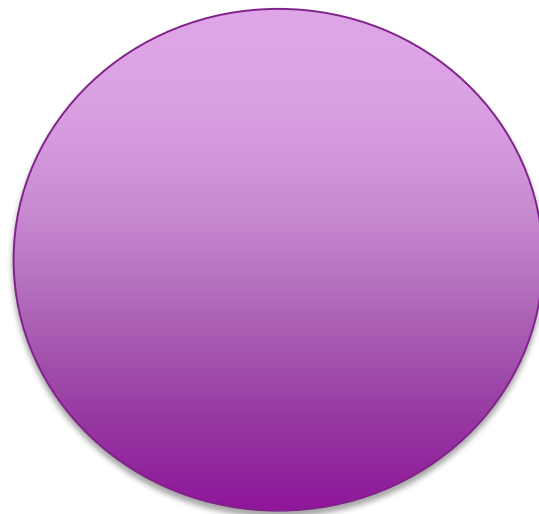
**20+ processes:**

Separation  
Drilling  
.....



**100+ System Types:**

Burner Management  
Fiscal Metering  
....



**1000+ Solutions  
from hundreds of vendors:**

Emerson  
Rockwell  
Siemens  
....

# Lets look at those systems



- Burner Management System (Gas Oil Separation)
- Metering (Fiscal Metering System (Metering)
- Tank Inventory System (Oil Storage )

- Risks:
  - Product Quality, Equipment damage, Plant Sabotage, Production Disruption, Compliance violation
- Details
  - Separate Oil, Gas and Water using multiple stages
- Systems
  - **Burner Management Systems (BMS)**
  - Compressor Control System (CCS)
  - Vibration Monitoring System (VMS)

# SEPARATION: Burner Management System (BMS)



- Description
  - Used in a variety of applications: Separators, tanks, heaters, Incinerators, flare stacks, etc.
- Systems:
  - Management: Emerson's DeltaV SIS, Invensys BMS, Honeywell's BMS, Combustex BMS-2000, Allen-Bradley, Siemens SIMATIC BMS400F
  - PLC vendors: GE, Modicon, Allen-Bradley, Koyo, Siemens
  - Flame sensors: Fireye, PPC, Honeywell, IRIS, Coen

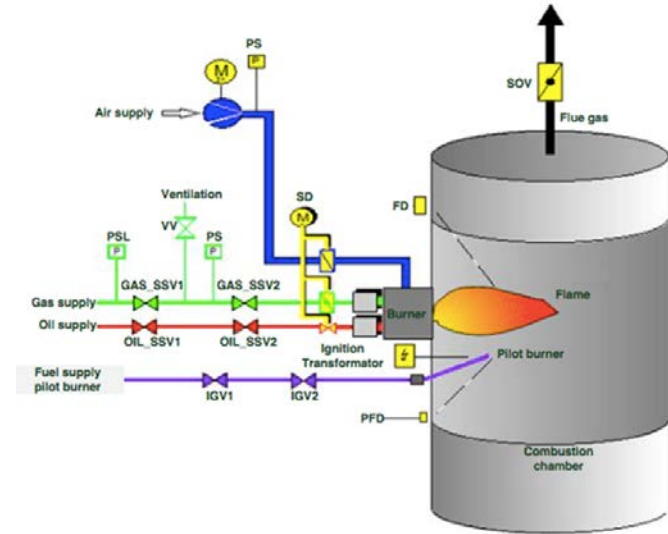


# SEPARATION: Burner Management System (BMS)



## Simple Burner Management System

Designations	Definition
IGV1	Pilot gas valve 1
IGV2	Pilot gas valve 2
OIL_SSV1	Oil safety shut-off valve 1
OIL_SSV2	Oil safety shut-off valve 2
GAS_SSV1	Gas safety shut-off valve 1
GAS_SSV2	Gas safety shut-off valve 2
PSL	Gas pressure sensor lower limit
VV	Vent valve
FD	Flame detector
SD	Servo drive
PS	Pressure sensor
SOV	Shut-off valve
PFD	Pilot flame detector



[https://cache.industry.siemens.com/dl/files/036/109477036/att\\_856487/v2/109477036\\_Burner\\_Application\\_Example\\_TIAP\\_DOC\\_v102\\_en.pdf](https://cache.industry.siemens.com/dl/files/036/109477036/att_856487/v2/109477036_Burner_Application_Example_TIAP_DOC_v102_en.pdf)

# SEPARATION: Burner Management System (BMS)



OK, what if somebody will have access to BMS?

What he can do?

Any physical attacks?

# SEPARATION: Burner Management System (BMS)



- ***If an attacker wants to commit sabotage and stop operations by destructing burning process, he needs to control any of the sources of flammable mixtures***

# Flammable mixture sources:



- Oil or gas leaking into the combustion chamber through the burner as a result of **leaking fuel shut off valves**.
- **insufficient combustion air** resulting unburnt fuel in the dust collector.
- **oil is not properly purged**
- **Quenching of the flame by cold dust entering the furnace**
- Fuel entering the furnace as a result of **repeated unsuccessful ignition attempts**. This is the significant risk with oil firing, A typical cause is a cold oil remaining in pipes during a shutdown

# SEPARATION: Burner Management System (BMS)



- The main function of the BMS is to allow and ensure the safe start-up, operation, and shutdown of the Fired Heater.
- Unauthorized access to BMS can lead to multiple risks including Explosion.
- The simplest attack on BMS System is to **turn off the purge**.
- Cold oil left in pipes during previous shutdowns can burn and damage the equipment.

- Risks:
  - Product Quality, Monetary loss
- Details
  - Analyzes density, viscosity of content, temperature, and pressure
  - Divided into several runs
- Systems
  - **Fiscal Metering System**
  - Liquid Flow Metering
  - Gas Flow Metering System
  - Wet Gas Metering System



## ■ Description

- Custody transfer, or fiscal metering, occurs when fluids or gases are exchanged between parties.
- Payment is a function of the amount of fluid or gas transferred.
- A small error in measurement leading to financial exposure
- Over a year, the 0.1% error would amount to a difference of \$50m.
- The engine of a custody transfer or fiscal metering installation is the flow computer.

- Production Accounting System
  - FlawCall – FlawCall Enterprise (**connected with IT**)
  - KROHNE SynEnergy (**connected with IT**)
  - Honeywell's Experion® Process Knowledge System (PKS), MeterSuite™
  - Schneider Electric InFusion
  - Schneider Electric SCADAPack
- Flow computing
  - KROHNE Summit 8800, ABB TolatFlow, Emerson FloBoss S600 (previously known as Daniel DanPac S600), Schneider Electric RealFlo





- Risks
  - Plant Sabotage/Shutdown, Equipment damage, Production Disruption, Compliance violation, Safety violation
- Description
  - Consist of 10-100+ tanks with 1-50m barrels
  - Tank Inventory Systems (TIA) collects data from special **tank gauging systems**
  - Accurate records of volumes and history are kept for **Forecasting for stock control**
  - Tank level deviations can result in hazardous events such as a tank overfilling, liquefied gas flashing, etc.
- Systems
  - Terminal Management Systems, Tank Inventory Systems, Tank Management Systems







## Enterprise Applications Security in Oil and Gas

85% of Fortune 2000 Oil and Gas companies use SAP



***70 million barrels per day of oil are produced by companies using SAP solutions***

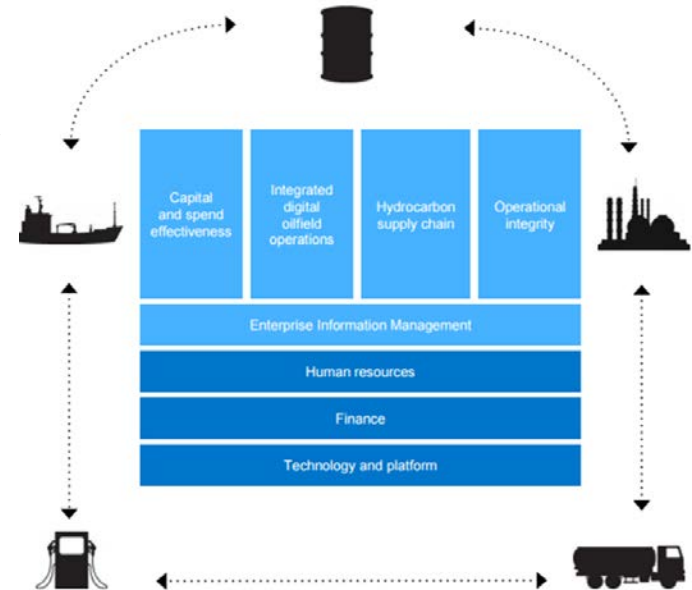
***(75% of total Oil production)***





According to SAP:

*..platform for operations and maintenance, to enable you to **gather, analyze, decide, and execute** across the many elements that drive performance of assets....*



# Enterprise applications VS Oil And Gas processes



- PPM (Project portfolio management)
- ALM (Asset Lifecycle Management)
- LIMS (Laboratory Information Management System)
- PAS (Production Accounting System)
- ERP (Enterprise Resource Planning)
- + HR, CRM, PLM, SRM, BI/BW, SCM

# Enterprise applications



- PPM <-> Exploration
- ALM <-> Refinery, Separation, etc.
- LIMS <-> Refinery, Separation
- PAS <-> Tank Inventory, Metering
- ERP <-> Tank Inventory, Metering
- + HR, CRM, PLM, SRM, BI/BW, SCM



# Project Portfolio Management (PPM)



## Risks:

- Espionage – information about new explorations
- Fraud – improper management decisions, lost profits

## Advantages:

- Enhancing visibility and transparency

## Examples:

- SAP PPM, Oracle Primavera, MS Project, MS SharePoint



- Risks:
  - Fraud – fake data about asset conditions
  - Sabotage - Physical damage to production and engineering devices
  - Compliance Violation – Data manipulation to give an illusion of Compliance
- Advantages:
  - Maintain integrity of your physical assets
  - Manage emissions, hazardous substances, and product and regulatory compliances
- Applications:
  - SAP PM (Plant Maintenance), SAP EAM, AssetWise APM, Oracle EAM, Avantis, IBM Maximo, Aspentech PIMS

# LIMS (Laboratory Information Management)



- Risks
  - Fraud – modifying sample data results
  - Espionage – stealing secret information
  - Sabotage – publication of non-compliant results, denial of service attacks
- Advantages:
  - quality control of the samples, utilized equipment and inventory
  - the storage, inspection, assignment, approval, and compilation of the sample data for reporting and/or further analysis
- Examples:



ERPScan  
Security Solutions for SAP

LabWare, thermoscientific, AspenPIMS and In-house developments on Oracle DB

- Risks
  - Supply chain Availability – direct impact on cost effectiveness
  - Fraud – Manipulations with quantities
- Advantages:
  - Production accounting
  - Automated data collection and validation
  - Forward looking production planning
- Examples
  - SAP IS-OIL PRA, SAP ERP MM-IM, Honeywell PAR



- Risks
  - Supply chain Availability – direct impact on cost effectiveness
  - Fraud – Manipulations with quantities
- Advantages:
  - Forward looking production planning
  - Automated data collection and validation
  - Analyze production deferments
  - Production accounting
- Systems
  - SAP ECC IS-OIL, SAP IS-OIL PRA, Honeywell PAR, Oracle JDE Manufacturing Accounting



# Enterprise apps security



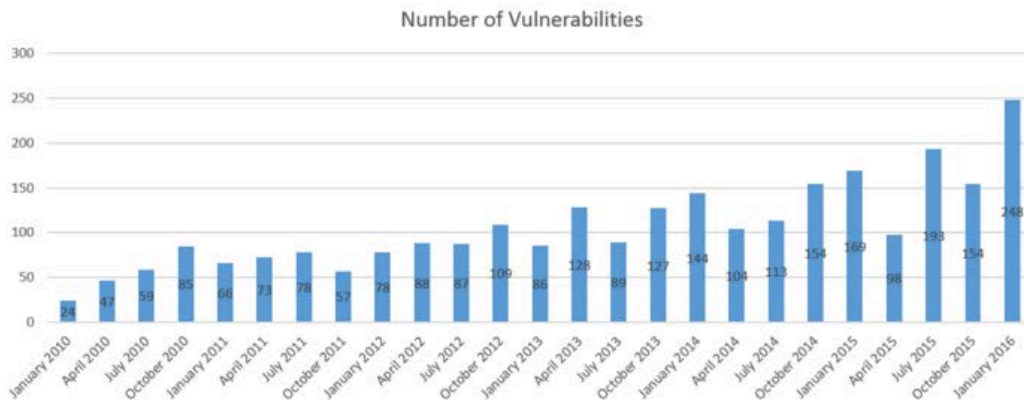
Ways to compromise SAP ERP:

- Vulnerabilities
- Misconfigurations
- Unnecessary privileges
- Custom code issues

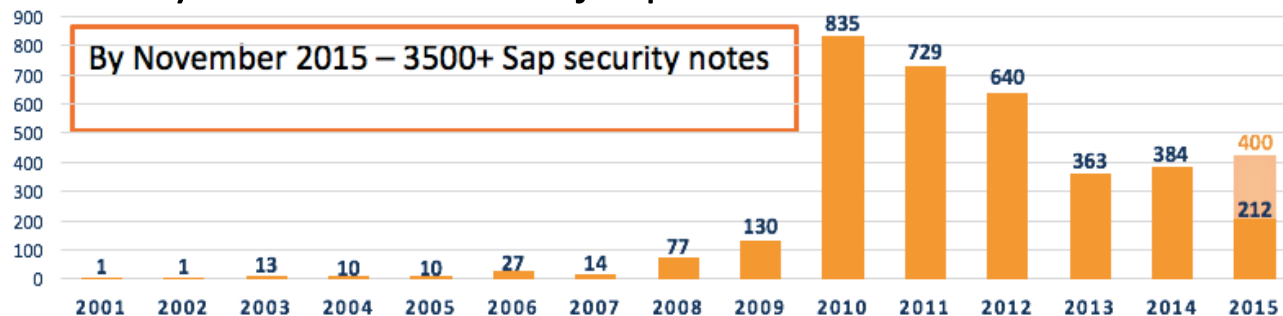
# Vulnerabilities in SAP and Oracle



#RSAC



Only one vulnerability would suffice to jeopardize ALL business-critical data



ERPScan

Security Solutions for SAP

# Misconfigurations in SAP



- ~1500 General profile parameters
- ~1200 Web applications to configure
- ~700 web services to secure
- ~100 specific management commands to filter
- ~100 specific parameters for each of the 50 modules (FI, HR, Portal, MM, CRM, SRM, PLM, Industry solutions...)

<http://erpscan.com/wp-content/uploads/publications/EASSEC-PVAG-ABAP.pdf>



# Custom code issues in SAP, Oracle and MS



#RSAC

SAP's - ABAP, XSJS, JAVA, JavaScript

Oracle's - PeopleCode, PL/SQL

Microsoft's - X++

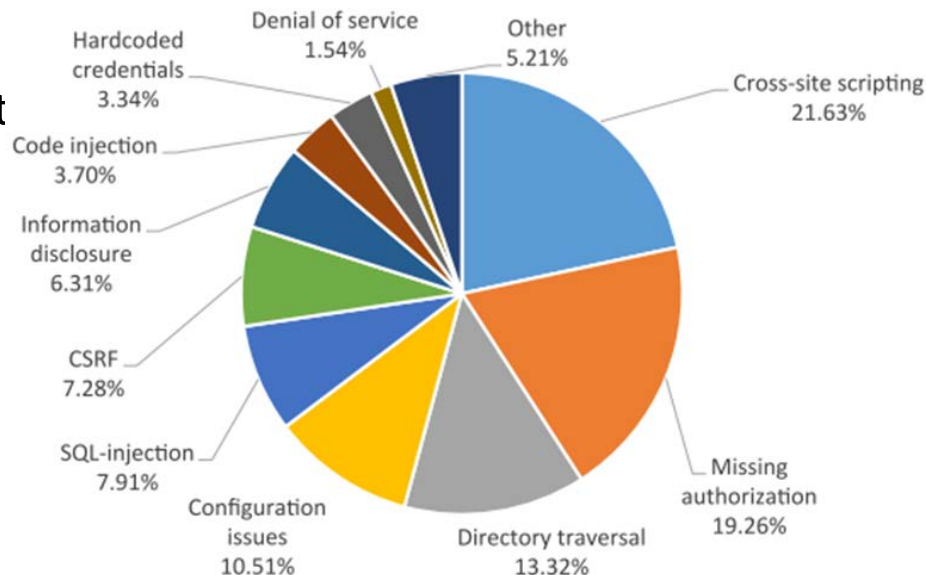


Figure 3.4-1 TOP-10 SAP Security Vulnerabilities, sorted by type

<http://erpscan.com/wp-content/uploads/publications/3000-SAP-notes-Analysis-by-ERPScan.pdf>



**ERPScan**

Security Solutions for SAP

# Unnecessary privileges in ERP



## Critical privileges and SoD issues

- For example: Create vendor + Approve payment order
- 200-500 Rules for typical application
- 500k conflicts in typical company after first audit

More on ERP Security:

<https://erpscan.com/research/white-papers/>

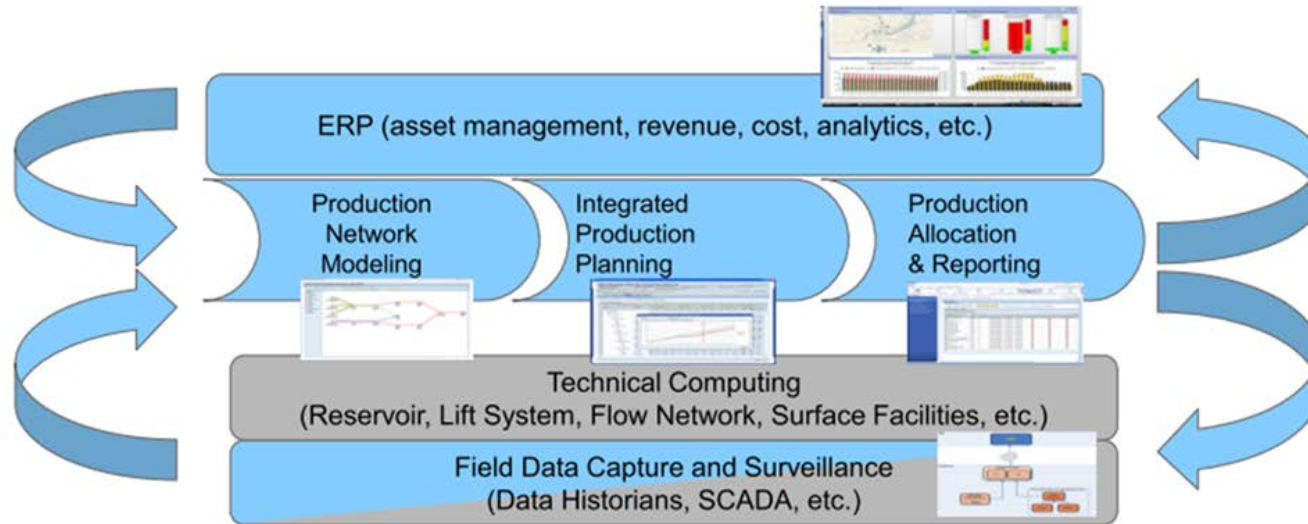


## **Security of Connections between IT and OT**

# IT/OT connection looks like this



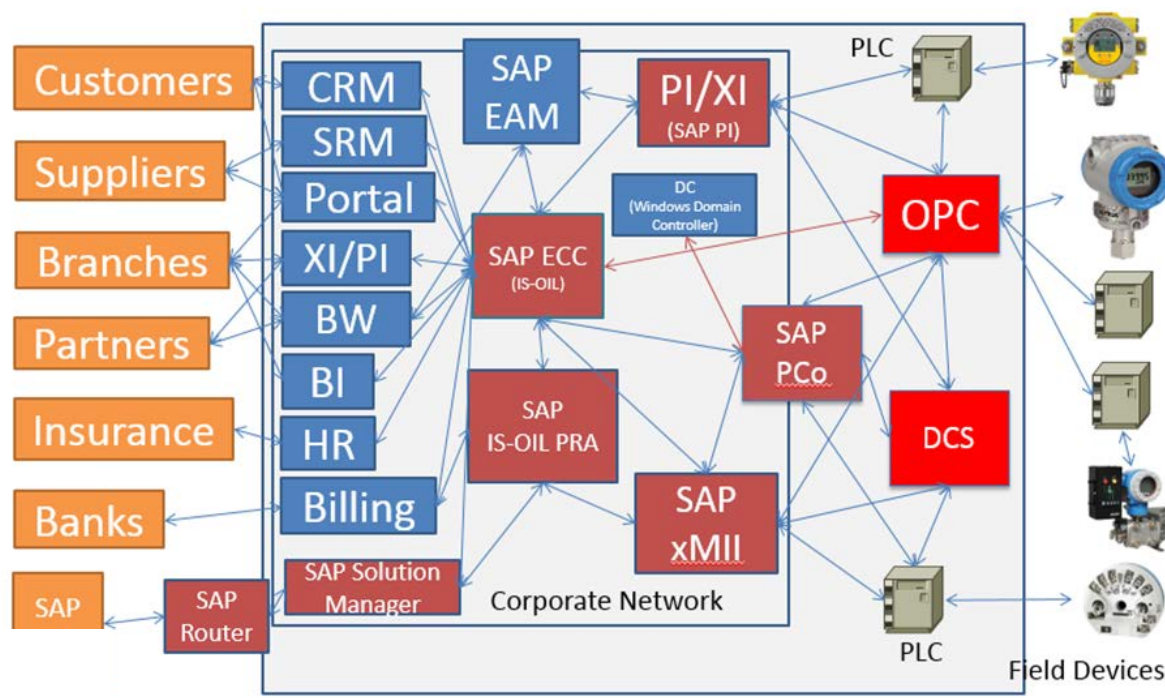
#RSAC



# Or like this



#RSAC



# From IT to OT. How they connected

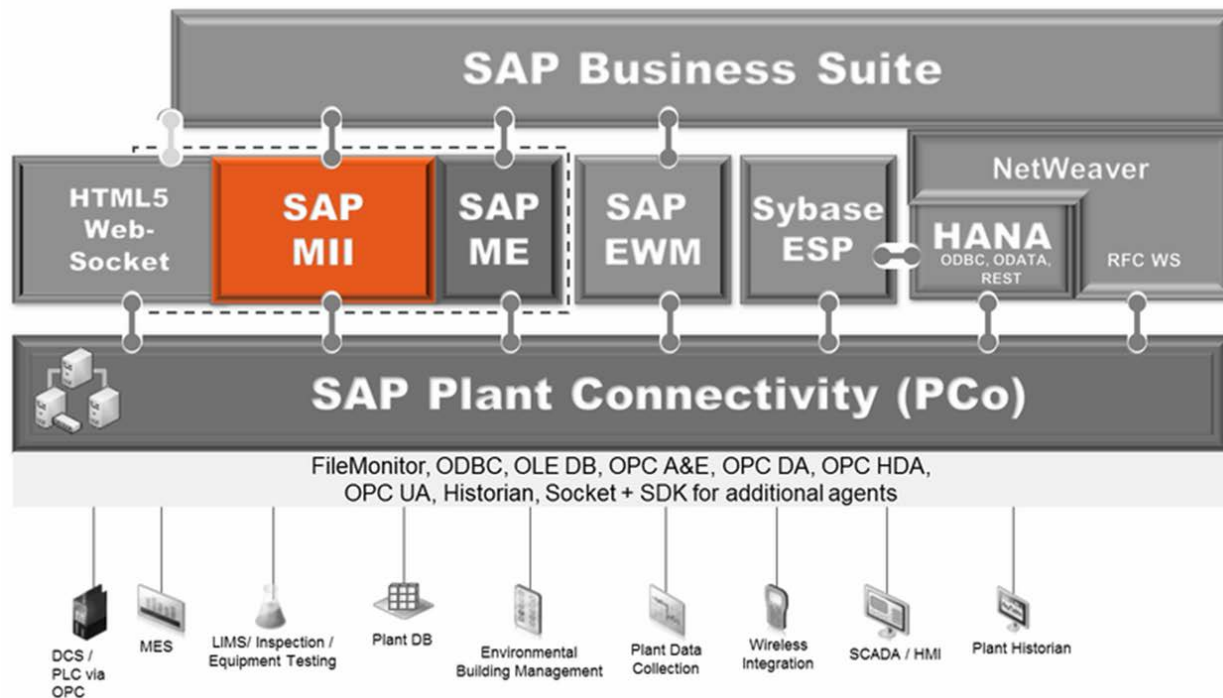


- Historian Process Integration (OT to OT/ OT to IT)
  - OSIsoft PI, Aspen Info Plus 21, Honeywell PHD, Rolta Oneview
- Enterprise Service Bus (IT to IT/ IT to OT)
  - SAP PI
  - IBM Websphere ESB
  - Microsoft BizTalk
  - Oracle ESB
- Other (IT to OT/ OT to IT)
  - SAP xMII

# IT and OT, SAP example



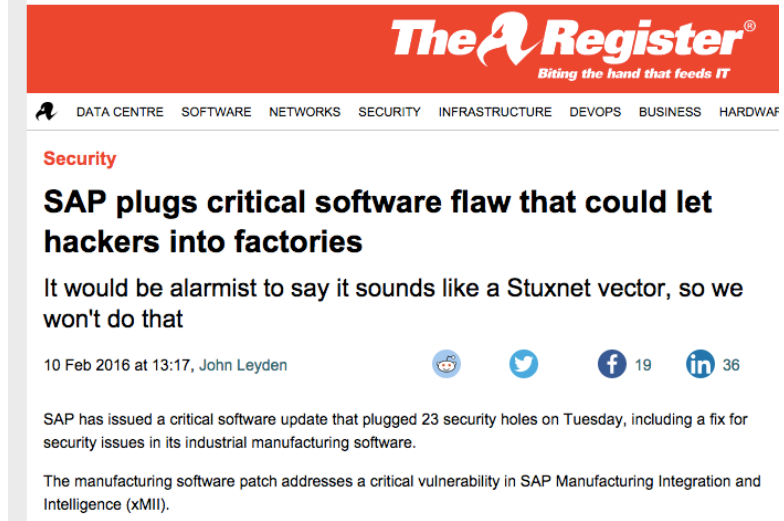
#RSAC



# SAP xMII overview



- Connects manufacturing with enterprise business processes, provides information to improve production performance
- On top of SAP Netweaver J2EE (with its vulnerabilities)
- Located on the corporate network
- Has some vulnerabilities



**The Register®**  
*Biting the hand that feeds IT*

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS HARDWARE

**Security**

**SAP plugs critical software flaw that could let hackers into factories**

It would be alarmist to say it sounds like a Stuxnet vector, so we won't do that

10 Feb 2016 at 13:17, John Leyden

SAP has issued a critical software update that plugged 23 security holes on Tuesday, including a fix for security issues in its industrial manufacturing software.

The manufacturing software patch addresses a critical vulnerability in SAP Manufacturing Integration and Intelligence (xMII).



# Attack Surface (SAP xMII Security):



#RSAC

- Database links to xMII from systems such as LIMS
- SAP J2EE Platform vulnerabilities (core of xMII)
- SAP xMII vulnerabilities
- SAP RFC links from ERP to xMII
- Shared SSH keys
- Similar passwords
- Others

Home / Security

## SAP slaps patch on leaky factory software

A flaw in SAP Manufacturing Integration and Intelligence (xMII) allows attackers to extract information without authorization

**The Register**  
Biting the hand that feeds IT



DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS HARDWARE

### Security

## Mixing ERP and production systems: Oil industry at risk, say infosec bods

There will be owndage

Malware & Threats Cybercrime Mobile & Wireless Risk & Compliance Security Architecture

Risk Management Security Architecture Disaster Recovery Training & Certification Incident R

Home > Security Infrastructure



## SAP Patches Flaws in xMII, Other Products

SAP fixed a flaw in xMII that could open the door to nation-state hackers

February 10, 2016 By Pierluigi Paganini



**ERPScan**

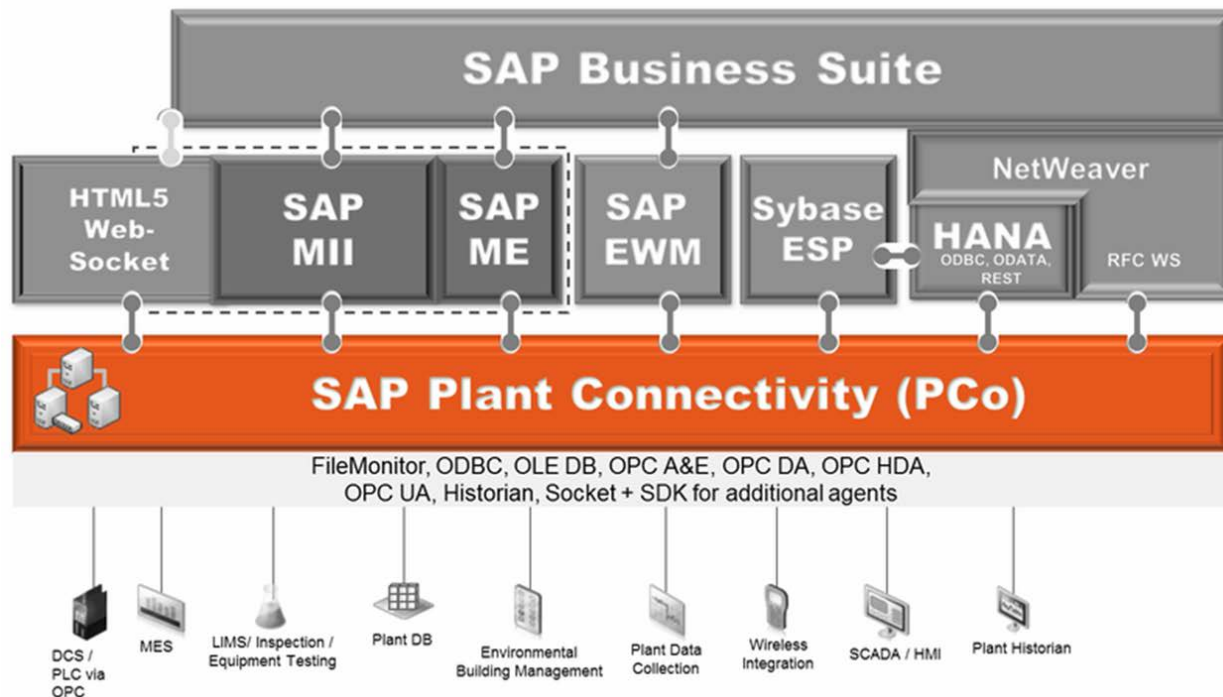
Security Solutions for SAP

**RSA**Conference2016

# SAP Plant Connectivity



#RSAC



**ERPScan**

Security Solutions for SAP

- Bridge between the industrial world and SAP Manufacturing modules
- .NET application for Windows
- Usual pipeline Source → Processing → Destination
- Source:
  - OPC server (MatrikonOPC, KEPServerEX) or DCS
- Destination:
  - SAP HANA, SAP XI, SAP xMII, LIMS, DB...
- Agent: Windows service that does the polling



# Hacking SAP Plant Connectivity



- Connections with IT systems (MES, LIMS, PI, Custom)
- **Domain credentials (if improperly secured)**
- **SAP xMII connections (password decryption)**
- **SAP PCo vulnerabilities**
- SAP PCo extensions
- Similar passwords



Traffic modification: attacks based on the fact that the MII-PCo connection is not authenticated by default:

- Fake Pco (Fraud)
  - Kill the actual PCo and show that everything is OK in MII
  - MITM + selective modification
  - Steal your oil, but tank level doesn't change
- Protocol attack (Sabotage)
  - XML Protocol parsing on the PCo side
  - Vulnerabilities found (Kill agent + mem leak) (**SAP Note 2238619**)



# Now they are inside your OT network and can do whatever they want.

**ATTACKERS CAN USE SAP TO BRIDGE CORPORATE,  
OPERATIONAL ICS NETWORKS**

by **Michael Mimoso** [Follow @mike\\_mimoso](#)

November 16, 2015 , 2:34 pm

Much in the same way the **Target hackers used a HVAC management system to catapult onto the corporate network**, attackers focused on oil and gas and other critical industries may be finding similar openings via enterprise applications such as SAP.



- SAP Plant Connectivity interacts with DCS/OPC/PLC
  - On the same workstation
    - Required when configuring some DCS/SCADA systems
  - On the same network
    - Example: OPC vulnerabilities
      - KEPServerEX Resource exhaustion <https://ics-cert.us-cert.gov/advisories/ICSA-15-055-02>
      - KEPServerEX Input Validation <https://ics-cert.us-cert.gov/advisories/ICSA-13-226-01>
      - MatrikonOPC Gateway DoS <https://ics-cert.us-cert.gov/advisories/ICSA-13-106-01>
      - MatricanOPC DoS (0-day)

# DEMO



#RSAC







## Oil market fraud attack:

- Imagine what would happen if a cyber criminal uploads a malware that dynamically changes oil stock figures for all Oil and Gas companies where SAP is implemented. Attackers will be able to deliberately understate data about Oil in stocks.

## Plant equipment sabotage attack

- Hackers can spoof a report about equipment status in a remote facility. Companies will spend a lot of time and money to investigate the incident

## Plant Destruction attack

- With access to BMS systems, via SAP Pco and SAP xMII hackers can perform physical attacks.





**How does one go about securing it?**



- Step 1 Next Month
  - Protect your ERPs and other business applications (Automatic: Scanning and Monitoring tools)
- Step 2 Next Quarter
  - Review all connections (Semi-Automatic/Manual)
- Step 3 This Year
  - Secure connections where possible (Manual)

# How to apply ERP Security



#RSAC

## Business security (SoD)

*Prevents attacks or mistakes made by insiders*

## Code security

*Prevents attacks or mistakes made by developers*

## Application platform security

*Prevents unauthorized access both within corporate network  
and from remote attackers*



**ERPScan**

Security Solutions for SAP

# About



[a.polyakov@erpscan.com](mailto:a.polyakov@erpscan.com)

228 Hamilton Avenue, Fl. 3,  
Palo Alto, CA. 94301

**USA HQ**

Luna ArenA 238 Herikerbergweg,  
1101 CM Amsterdam

**EU HQ**

[www.erpscan.com](http://www.erpscan.com)

[info@erpscan.com](mailto:info@erpscan.com)