RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: CRWD-W04

Attacks on Crown Jewels: SAP Vulnerabilities and Exploits

Mariano Nunez

Co-Founder and CEO
Onapsis, Inc.
@marianonunezdc

Agenda

- Key SAP Cyber-Security Trends
- What's the Probability? Killing some Myths
- So What?
- Common SAP Cyber-Attack Scenarios - Live Demos
- Monday Morning and Long Term Actions

RSAConference2015

San Francisco | April 20-24 | Moscone Center

SAP Cyber-Security Trends

Key SAP Cyber-Security Trends

SAP has released 3300+ security patches to date.

In 2014 alone, 391 were released - averaging 30+/month.

Over 46 percent of them were ranked as “high priority”.

– *Onapsis Research Labs*

Source: http://www.onapsis.com/blog/sap-security-advisories-a-preview-of-a-year-in-review-and-future-trends/

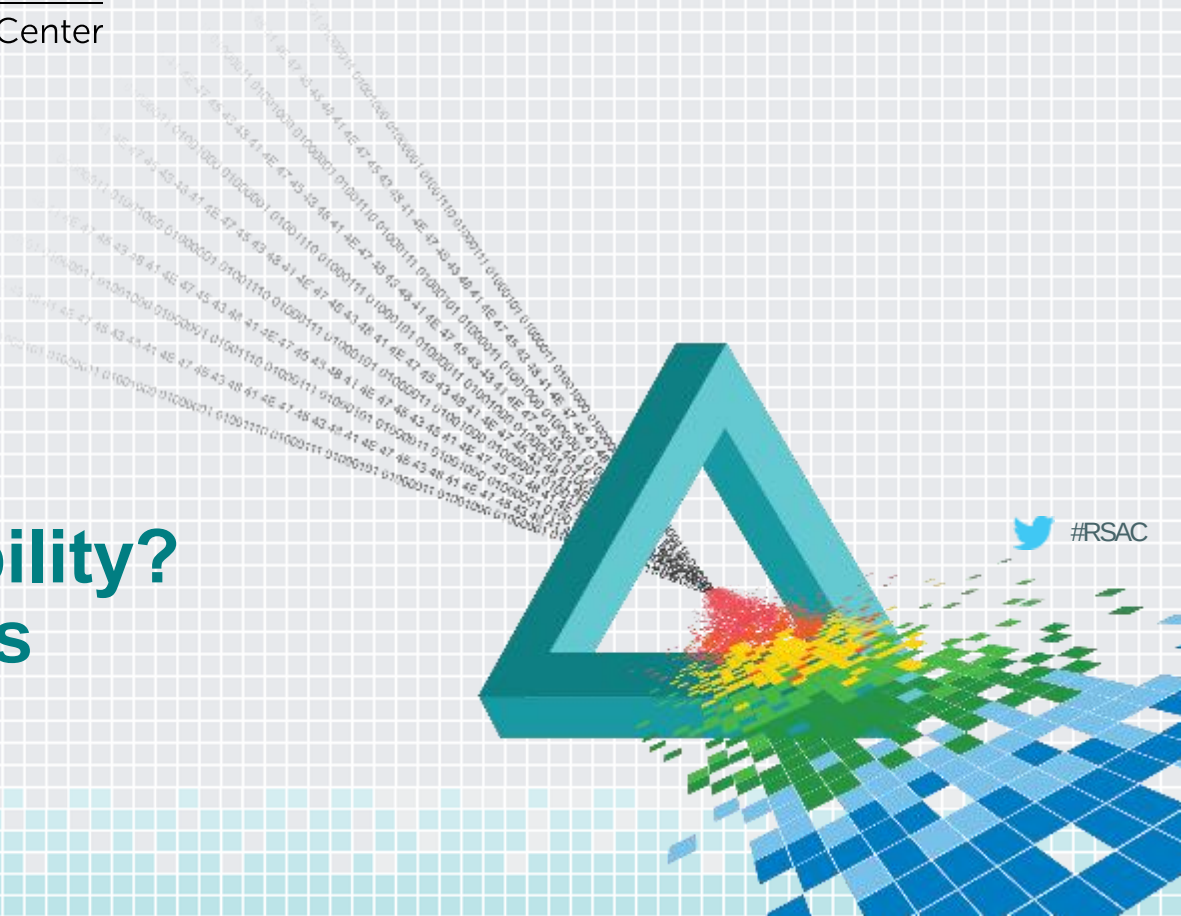
Key SAP Cyber-Security Trends

Over 95% of the SAP systems we have assessed were exposed to vulnerabilities that could lead to **full compromise** of the company's business processes and information. Most vulnerabilities could be exploited **anonymously and remotely.**

In most scenarios, **anyone that can "ping" an SAP server, can break into it.**

RSAConference2015

San Francisco | April 20-24 | Moscone Center



#RSAC

What's the Probability? Killing some Myths

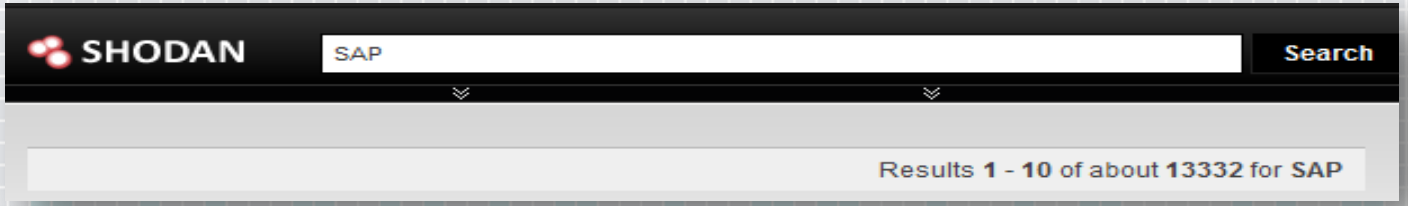
What Is the Probability? Killing Some Myths

- **"We have an SAP Security Team that looks after this"**
  - SAP Security Teams have been traditionally only focused in enforcing **Segregation of Duties controls (user roles and authorizations).**
    - Most do not have the right skills, focus or tools to deal with technical vulnerabilities and advanced threat vectors.
  - The IT Security Team is tasked with "cyber security _____ (fill in the blanks)", but does not have any visibility into the SAP platform….
  - Everyone's responsibility -> nobody's responsibility.
  - Leading organizations have in fact solved this Responsibility Gap.

What Is the Probability? Killing Some Myths

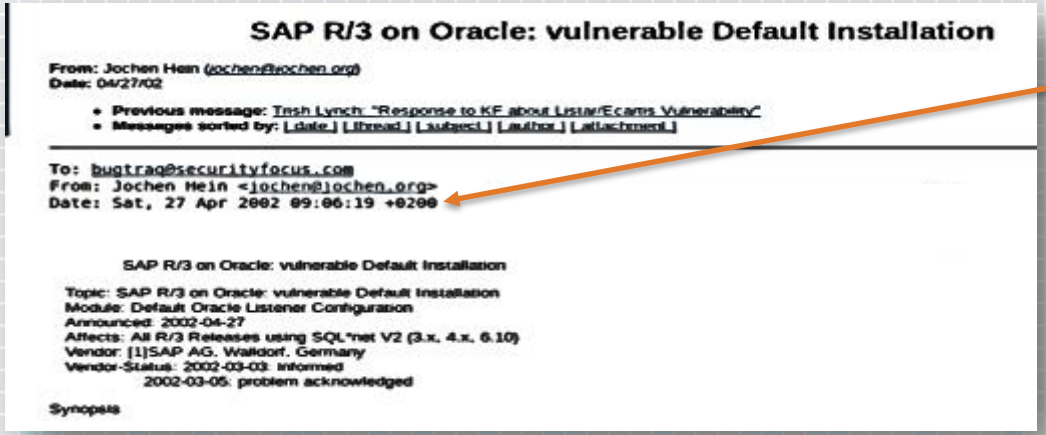
- **"Our SAP platform is only accessible through internal networks"**
  - There is no such thing as an "Internal" Network anymore
    - There are no more "perimeters" (spear-phishing, rough contractors, malicious employees)
    - Many SAP systems are connected to the Internet (Web apps, HANA, Mobile, Cloud deployments, etc.)

www.shodanhq.com/search?q=SAP



What Is the Probability? Killing Some Myths

- **"This can only be performed by highly-skilled attackers"**
  - Who is the Threat Actor? Most likely an unethical competitor, disgruntled employee, hacktivist or foreign state.
  - Even script kiddies – **the information is out there!**



SAP R/3 on Oracle: vulnerable Default Installation

From: Jochen Hein (jochen@jochen.org)
Date: 04/27/02

- Previous message: Trish Lynch: "Response to KF about Listar/Ecartis Vulnerability"
- Messages sorted by: [date] [thread] [subject] [author] [attachment]

To: bugtraq@securityfocus.com
From: Jochen Hein <jochen@jochen.org>
Date: Sat, 27 Apr 2002 09:06:19 +0200

SAP R/3 on Oracle: vulnerable Default Installation

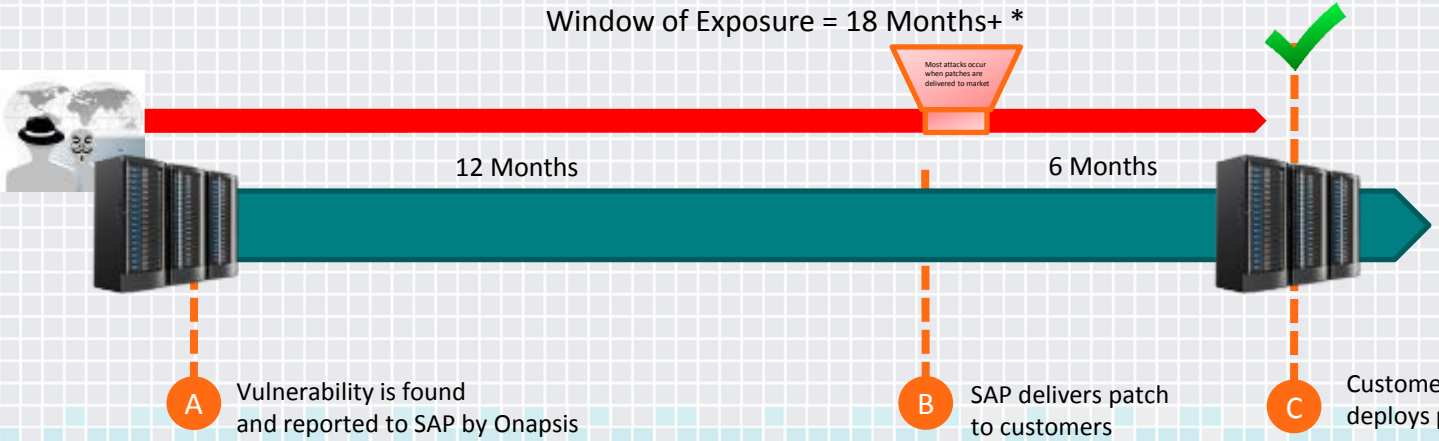
Topic: SAP R/3 on Oracle: vulnerable Default Installation
Module: Default Oracle Listener Configuration
Announced: 2002-04-27
Affects: All R/3 Releases using SQL*net V2 (3.x, 4.x, 6.10)
Vendor: [1]SAP AG, Walldorf, Germany
Vendor-Status: 2002-03-03: informed
2002-03-05: problem acknowledged

Synopsis

Date: Sat, 27 Apr **2002**

What Is the Probability? Killing Some Myths

- **"We are applying SAP patches regularly"**
  - Most patches that are applied are "functional", not security-related.
  - Applying security patches without the proper analysis introduces operational risk (more sensitive in business-critical platforms!).
  - Another risk: The Window of Vulnerability

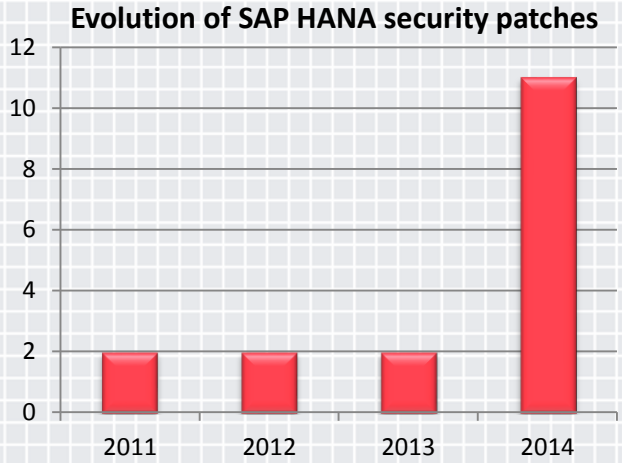


*Based on vulnerabilities reported to SAP by the Onapsis Research Labs

What Is the Probability? Killing Some Myths

- **"We are migrating to SAP HANA anyway, we are safe"**
  - SAP HANA is the new de-facto database/application server platform for new SAP solutions.
  - Thought to be "more secure"…
  - Results **(public)**:
    - 450% increase in new security patches.
    - In 2014: 82% "high priority" (!)

New critical issues waiting for patches…



What Is the Probability? Killing Some Myths

- **"Our SAP system has never been hacked"**
  - Most companies do not enable logging due to **the negative impact on performance.**
  - **Traditional SIEMs or log correlators won't help.** Even with the standard Security Audit features enabled, certain type of cyber security attacks can't be detected through log files.
  - Furthermore, several vulnerabilities have been discovered that could be used for anti-forensics purposes

So … the most honest answer is probably: "we don't know"

SAP Security Breaches and Threats Are Real: Companies and Government Targets

#RSAC

2012

Anonymous claimed breach and stated: *"A sweet 0day SAP exploit is in our hands and oh boy we're gonna sploit the hell out of it."*

2013

A malware targeting SAP systems discovered in the wild - A "Tsunami of SAP Attacks Coming?"

2014

A Chinese hacker exploited a vulnerability in a corporate SAP NetWeaver Portal.

onapsis

RSAConference2015

RSAConference2015

San Francisco | April 20-24 | Moscone Center

#RSAC

So What? SAP is Only Used For….

So What? SAP is Only Used For….

Oil & Gas

- Capital Spend Effectiveness & Procurement
- Digital Oilfield Operations
- Hydrocarbon Supply Chain
- Operational Integrity
- Human Resources
- Finance

Manufacturing

- Operations
- Production Planning and Execution
- Manufacturing Execution
- Process Visibility/Performance
- Lean Manufacturing
- Outsourced Manufacturing
- Business Suite Applications

Retail

- Customer Centric Marketing and Merchandising Solutions
- Sourcing, Buying and Private Label
- Supply Chain
- Omni commerce Customer Experience
- Finance
- Human Resources

What Could Be the Business Impact?

What Is the Impact? Killing Some Myths

- **"SAP Systems are Legacy anyway…"**

  Really??? According to SAP…

  - SAP serves > 282,000 customers in 190 countries
  - SAP customers include:
    - 87% of the Forbes Global 2000 companies
    - 98% of the 100 most valued brands
  - SAP customers produce …
    - 78% of the world's food
    - 82% of the world's medical devices
    - 69% of the world's toys and games
  - 74% of the world's transaction revenue touches an SAP system
  - SAP touches US$16 trillion of retail purchases around the world

RSAConference2015

San Francisco | April 20-24 | Moscone Center

#RSAC

SAP Cyber Attack Scenarios

Attack Scenarios

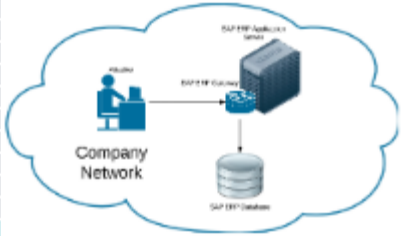
1

Pivoting between SAP systems:
Pivot from a system with lower security (Development or QA system) to a critical system (Production system), to execute SAP remote function modules in the destination system

2

Customer and Supplier Portal Attacks:
Create users in the SAP J2EE User Management Engine using the CTC servlet, by exploiting a vulnerability through HTTP verb tampering, and obtaining access to the SAP Portal business information (and internal systems).

3



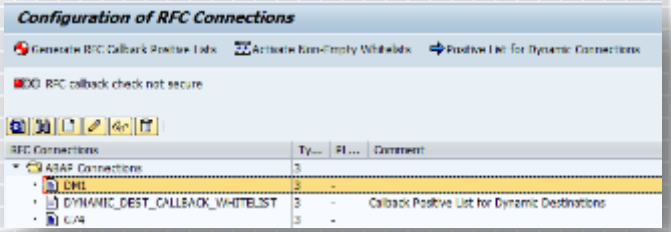
Attack on SAP services configuration:
Execute Operating System commands under the privileges of the user <sid>adm by exploiting vulnerabilities in the SAP RFC Gateway. Get and potentially modify credit card information stored in the SAP database.

onapsis

Attack Scenario 1

1. Attacker connecting to non-prod systems (Dev/QA)

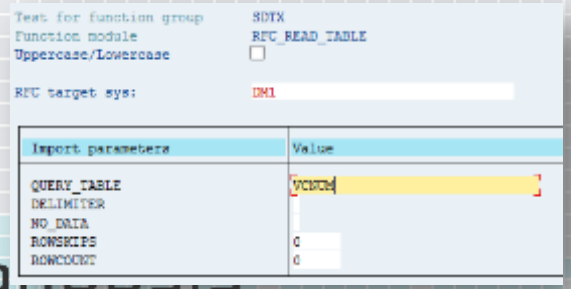
2. List of RFC destinations and its properties

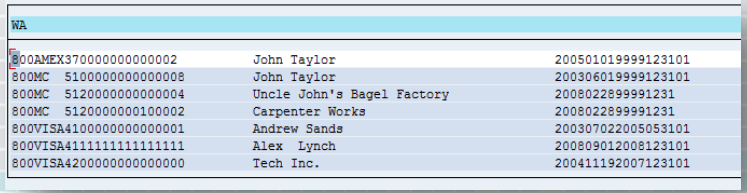


SM59

SE16 - RFCDES

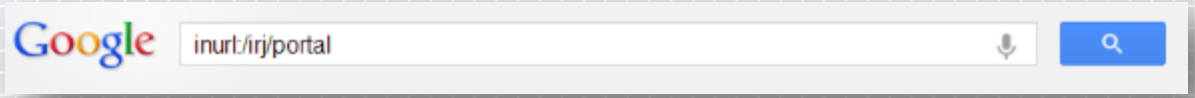
3. Attacker goes to transaction SE37 and leverages a destination and “data read” function module.



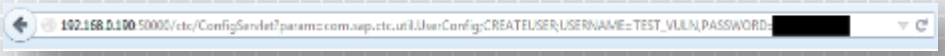


Attack Scenario 2

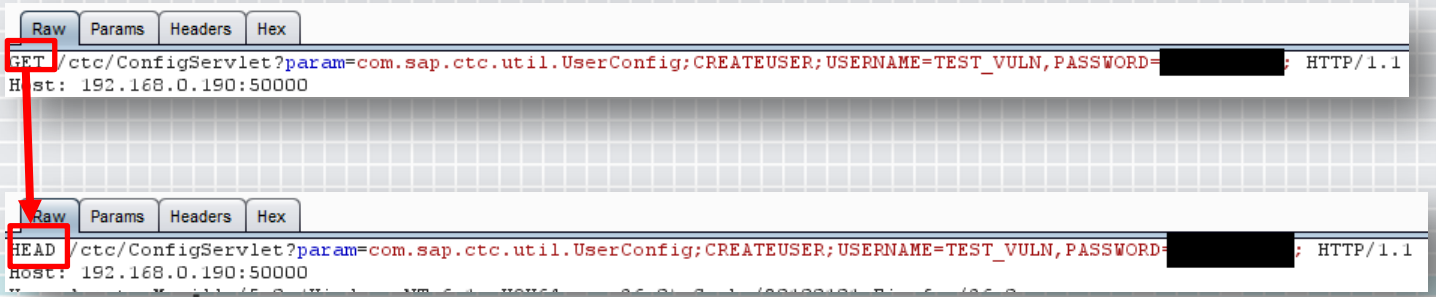
1. Vulnerable systems connected to Internet



2. Attacker sends HTTP request to the CTC servlet – Filtered.



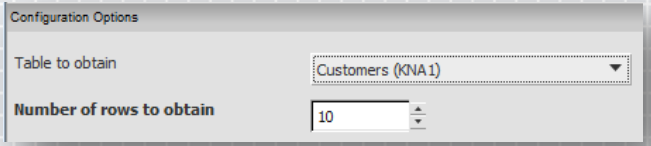
3. Using a local proxy tool, the attacker changes the HTTP verb from GET to HEAD and forwards it to the server. This command will send the user creation request to the CTC servlet



Attack Scenario 3

By abusing of insecure configurations in the SAP systems, there are different ways an attacker would use to get business data:

1. Exploits the SAP RFC Gateway -> OS control -> SAP DB schema control.



Request
Customers: table
KNA1

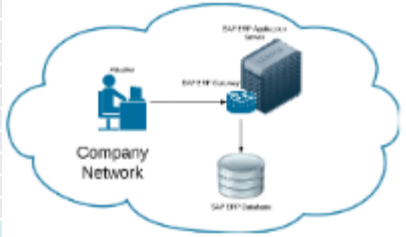
Customer table is displayed

Attack Scenarios

1

2

3



In these attack scenarios, any business information in SAP can be accessed and modified:

- **PA00*: group of tables with HR Information**
- **LFA1: Vendor Master Data**
- **KNA1: Customer Master Data**
- **VCNUM & MKNUM: Customer Credit Cards**
- **BKPF & BSEG: Financial Documents**
- **EKKO & EKPO: Purchase Orders**
- **AUFK: Production Orders**
- **KALC: Material quantity calculation formulas**
- **…**

onapsis

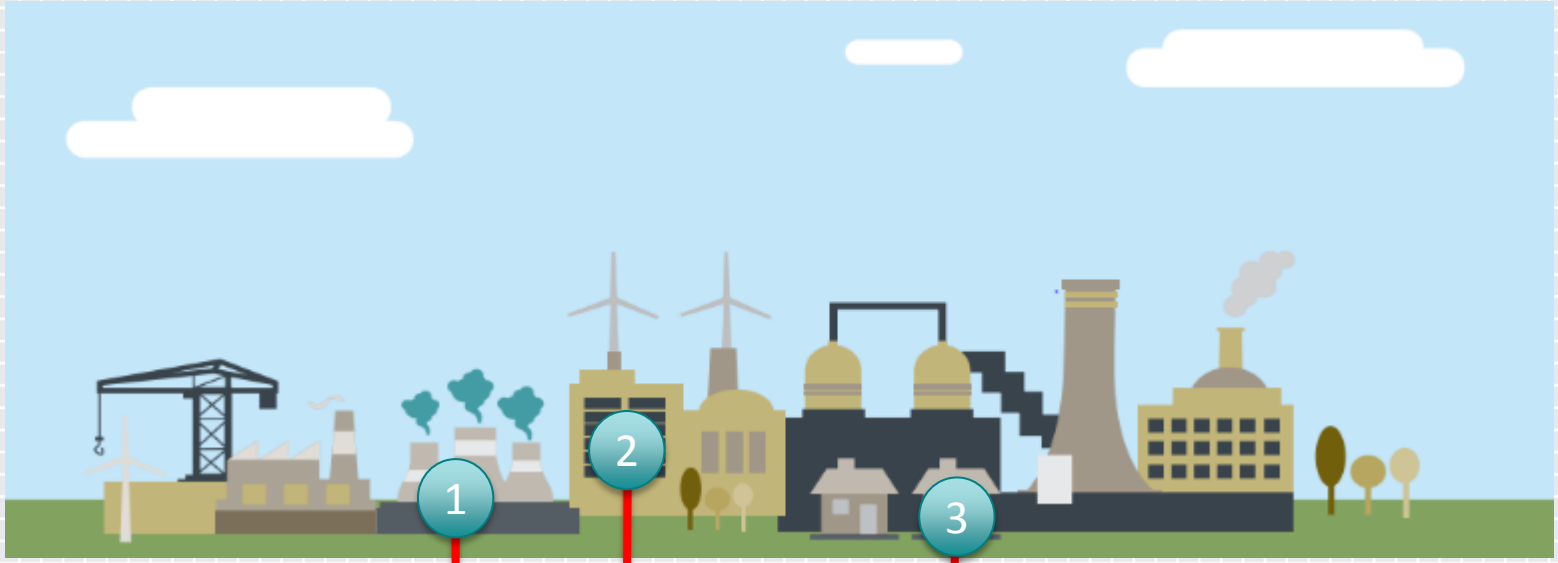
RSAConference2015

San Francisco | April 20-24 | Moscone Center

#RSAC

Monday Morning Actions

Map Your SAP Landscape and Terrain



1. Asset Discovery – find out if you have 1 or 100 SAP systems and their interfaces
2. Understand the business processes that each system supports
3. Understand the information that each system houses

Understand the Risks

Economic Impact

Understand the value chain that SAP systems and applications support. Also calculate the dollars that the SAP platform manages at your organization.

Compliance Impact

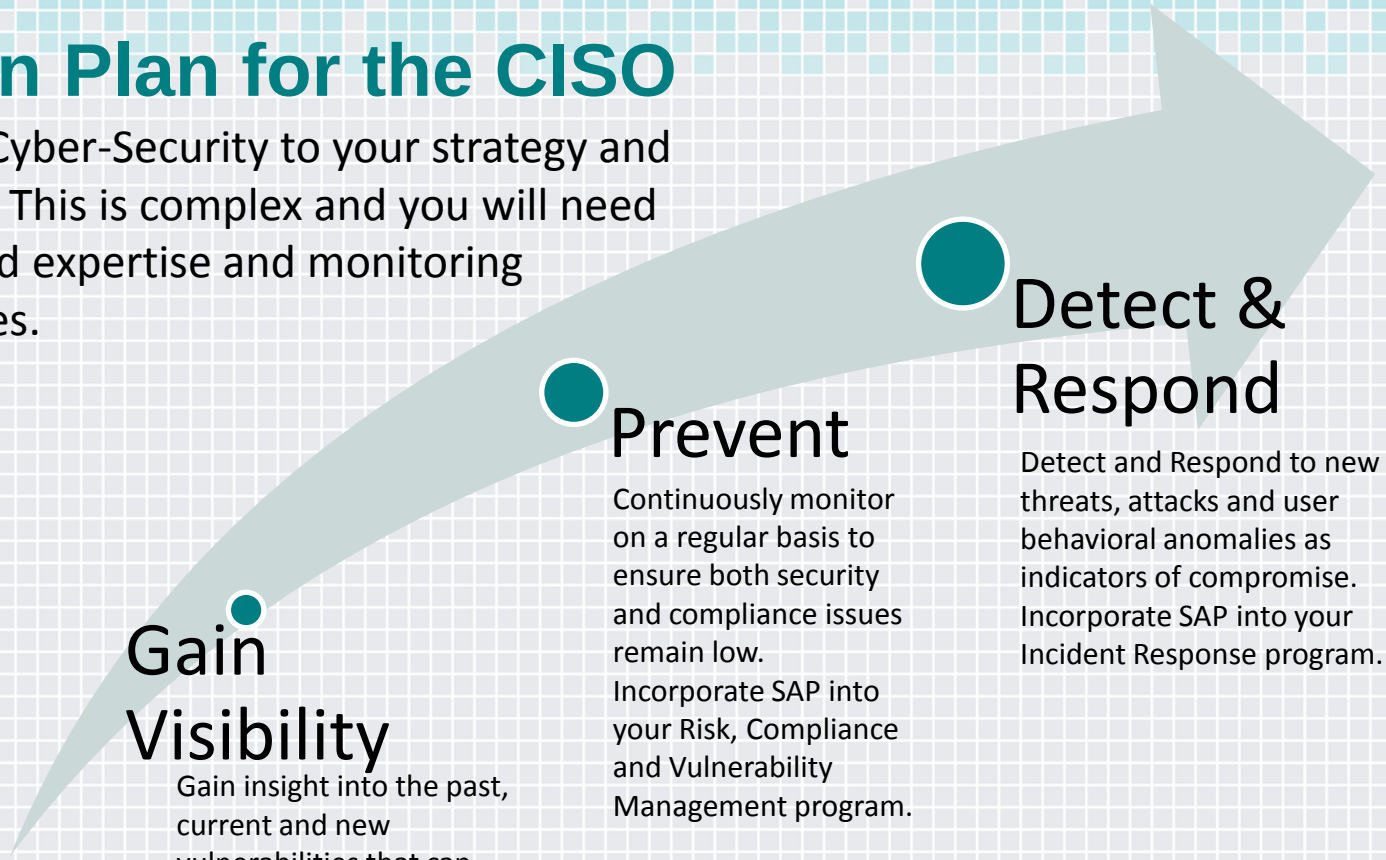
Map Policies with an SAP security lens (i.e. SAP Security Guidelines) as well as authoritative sources (SOX, PCI) and perform assessments to identify critical compliance gaps.

Context Impact

Prioritize risk by severity against assets (TOP-10, don't boil the ocean), likelihood and timing of the risks and the potential business impact.

Action Plan for the CISO

Add SAP Cyber-Security to your strategy and roadmap. This is complex and you will need specialized expertise and monitoring capabilities.



Gain Visibility

Gain insight into the past, current and new vulnerabilities that can impact the business. Understand the value of your SAP-based assets.

Prevent

Continuously monitor on a regular basis to ensure both security and compliance issues remain low. Incorporate SAP into your Risk, Compliance and Vulnerability Management program.

Detect & Respond

Detect and Respond to new threats, attacks and user behavioral anomalies as indicators of compromise. Incorporate SAP into your Incident Response program.

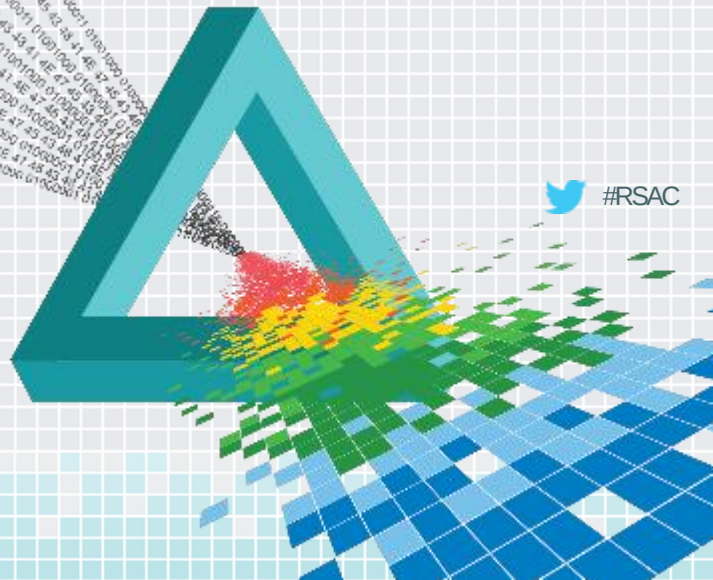
onapsis

Where to Find More Information & Solutions

- **Onapsis Research Labs Blog**
  - http://blog.onapsis.com
- **Relevant SAP Resources**
  - SAP Security Notes 1467771, 1445998
  - Secure Configuration of SAP NetWeaver Application Server Using ABAP™
  - SAP Security Guides

RSAConference2015

San Francisco | April 20-24 | Moscone Center



#RSAC

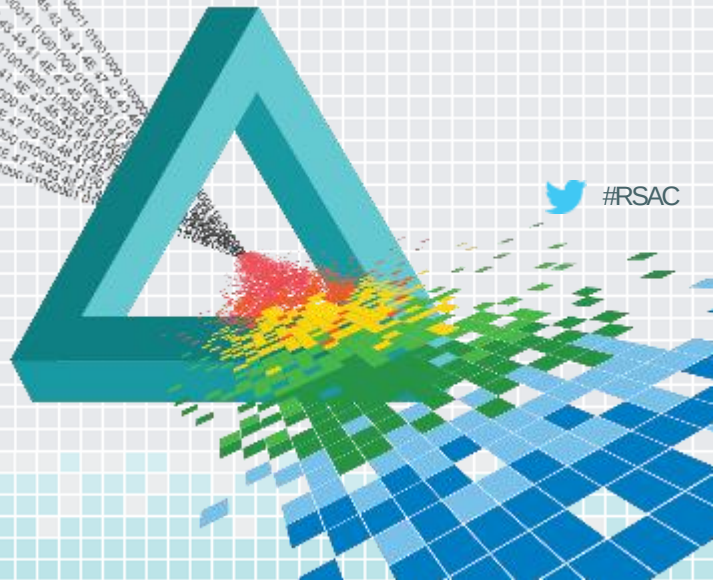
Questions?

Onapsis - Booth #1639
@marianonunezdc

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Thank You!



#RSAC