“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.
SAP houses a multitude of organizational assets which span industries and motivate cyber security attacks

- Intellectual property
  - High value industry data
- Sensitive customer information
  - High volume customer data
- Business process trade secrets
  - Competitive insights
- Treasury and cash
  - Corporate bank accounts
- Financial reporting insights
  - Inside financial information
- Sensitive employee information
  - High volume employee data
- Network front door
  - Access point to the corporate network
- Life blood of the business
  - Single point of operational failure
TYPICAL SAP ENVIRONMENT

SAP Systems Run the Business

Mapping SAP Systems and Connections is Complex
SAP Security Breaches in the Press

The Escalation of SAP Security Breaches

2012
Anonymous claimed breach to Greek Ministry of Finance using SAP zero-day exploit

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.

May 2015
Report: Chinese Breach of USIS targeted SAP. Went unnoticed for over six months and compromised over 48,000 employee records of DHS and OPM.
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.
“We are applying SAP patches regularly”

Window of Exposure = 18 Months +

A: Vulnerability is found and reported to SAP.
B: SAP delivers a patch to the market
C: Organization deploys patch.

Most attacks occur when patches are delivered to market.
What Is the Probability? Killing Some Myths

**MYTH**

“Our SAP platform is only accessible through internal networks”

**TRUTH**

Inurl:/irj/portal

www.shodanhq.com/search?q=SAP
What Is the Probability? Killing Some Myths

**MYTH**

“We have an SAP Security Team that looks after this”

**TRUTH**

Enforcing Segregation of Duties controls (user roles and authorizations) will not stop advanced threat vectors on SAP.
“We are migrating to SAP HANA anyway, we are safe”

Results (public):
450% increase in new security patches.
In 2014: 82% “high priority”
November 2015 Onapsis discovered and helped mitigate 21 vulnerabilities:

- Critical risks could allow cyber attackers to steal, delete or modify corporate business information.
- Over 10,000 companies potentially affected.
- Both a TREXNET configuration issue which is “unpatchable” and non-deployed SAP patches.
- Through cutting edge research major large-scale attacks potentially avoided.
- Customer using Onapsis Advanced Threat Detection get zero-day coverage and a virtual patch capability.
SAP Attacks Evade Traditional Security Approaches

Attackers are going after the crown jewels and traditional security solutions won’t stop them.

Using advanced malware to get into an SAP system - once in the attacker has full access to the business’s “Crown Jewels” - information and processes – All residing within SAP.
TOP 3 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.
ATTACK SCENARIO 1

1. Attacker compromising an initial system, typically a non-prod system (Dev/QA)
2. List of RFC destinations and its properties

   ![Configuration of RFC Connections](image1)

   ![Data Browser: Table RFCDES Select Entries](image2)

   SM59

3. Attacker goes to transaction SE37 and abuses pre-established interfaces

   ![Test for function group RFC_READ_TABLE](image3)

   ![List of RFC Descriptions](image4)
ATTACK SCENARIO 2

1. Vulnerable systems are also connected to Internet!

2. Attacker sending HTTP request to the CTC servlet and creating a user

3. Using the web browser, the attacker will send the user creation request to the CTC using the invoker servlet

4. Attacker repeats the process to add roles to the created user:

   http://192.168.0.190:50000/ctc/servlet/com.sap.ctc.util.ConfigServlet?param=com.sap.ctc.util.UserConfig;ASSIGN_ROLE_TO_USER;ROLE=\<ROLE\>,USERNAME=\<user\>:
ATTACK SCENARIO 3

By abusing of insecure configurations in the SAP systems, there are different techniques an attacker would leverage to access business data:

1. Using exploiting the SAP Gateway (“Get Business table”)

![Request Customers: table KNA1](image)

![Customer table is displayed](image)
GENERAL ACTION PLAN

**Respond**
Respond to new threats, attacks, or user behavioral anomalies as indicators of compromise. Incorporate SAP into your Incident Response program. Deploy zero day signatures to systems vulnerabilities.

**Gain Visibility**
Gain insight into your SAP infrastructure, the connections between systems and the past, current and new vulnerabilities that can impact the business.

**Detect**
Leveraging vulnerability and compliance gap analysis to determine likelihood and impact of threats, Notifications of attacks with prioritization based on business-context.

**Prevent**
Continuously monitor systems for exploits. Patch systems with security notes and incorporate SAP into your risk, compliance and vulnerability management processes.
**Onapsis Security Platform Solutions**

**Vulnerability and Compliance**
- Identify all SAP infrastructure and generate graphical topology maps along with the connections between systems and applications.
- Assess risks based on vulnerabilities and tie business context into remediation planning processes.
- Performs audits to identify compliance gaps and report when systems don’t meet requirements based on policies and industry regulations.

**Detection and Response**
- Continuous monitoring of advanced threats and anomalous user behavior on SAP infrastructure.
- Provides visibility into attacks, with context, to determine if the attack is likely to be successful.
- Leverages real-time reporting on the likelihood and impact of threats from SAP exploits.
- Delivers attack signatures to identify anomalous user behaviors.
- Detects system changes that make organizations more vulnerable to attack.

**Advanced Threat Protection**
- Provides protection against SAP security issues for which no SAP note has been released for Onapsis customers to eliminate the risks.
- Eliminates the window of exploitability and protects customers against known but unpublished vulnerabilities.
- Customers who subscribe to Advanced Threat Protection receive signatures for exploitation attempts against zero day vulnerabilities.

**Onapsis Security Platform**
Provides organizations a holistically adaptive approach to focus on the factors that matter most to their business – critical applications running on SAP that house vital data and run mission-critical business processes. Delivers three solutions