Enterprise Defense

and why you're most likely doing it all wrong

onapsis

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/

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.**

BlackHat EU 2012 – "Cyber Attacks & SAP Systems" by Mariano Nunez

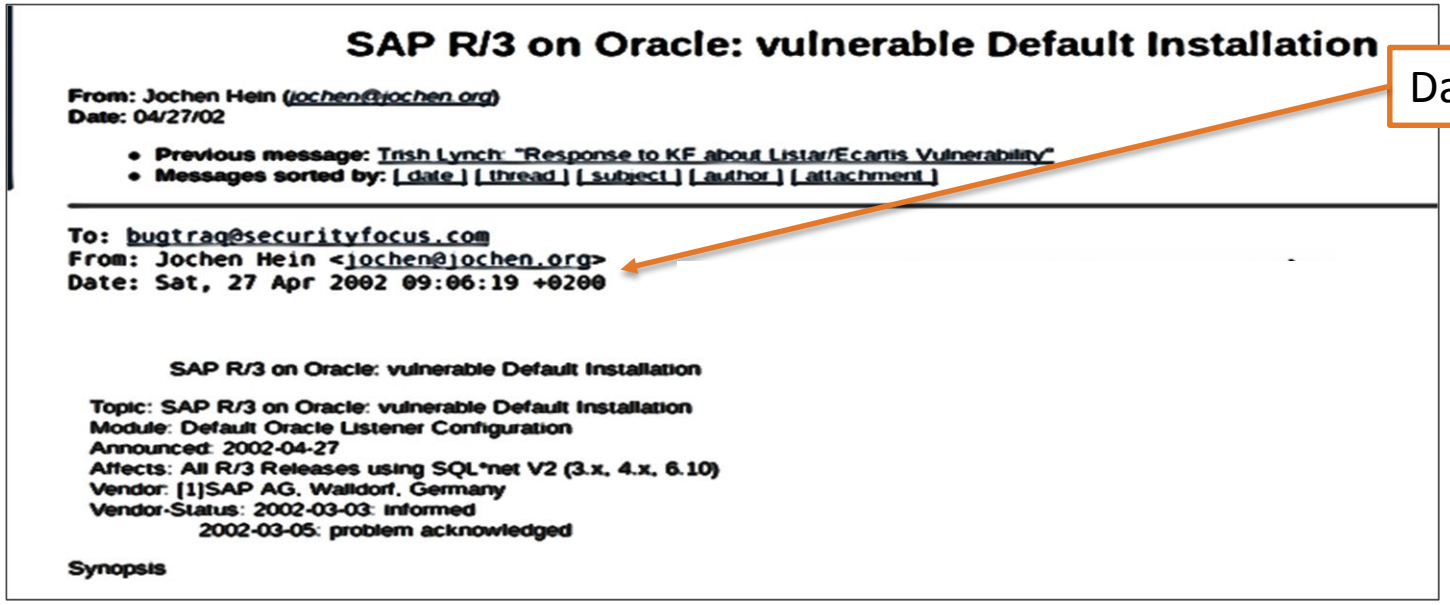
What Is the Probability? Killing Some Myths

- "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 directly connected to the Internet (Web apps, 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

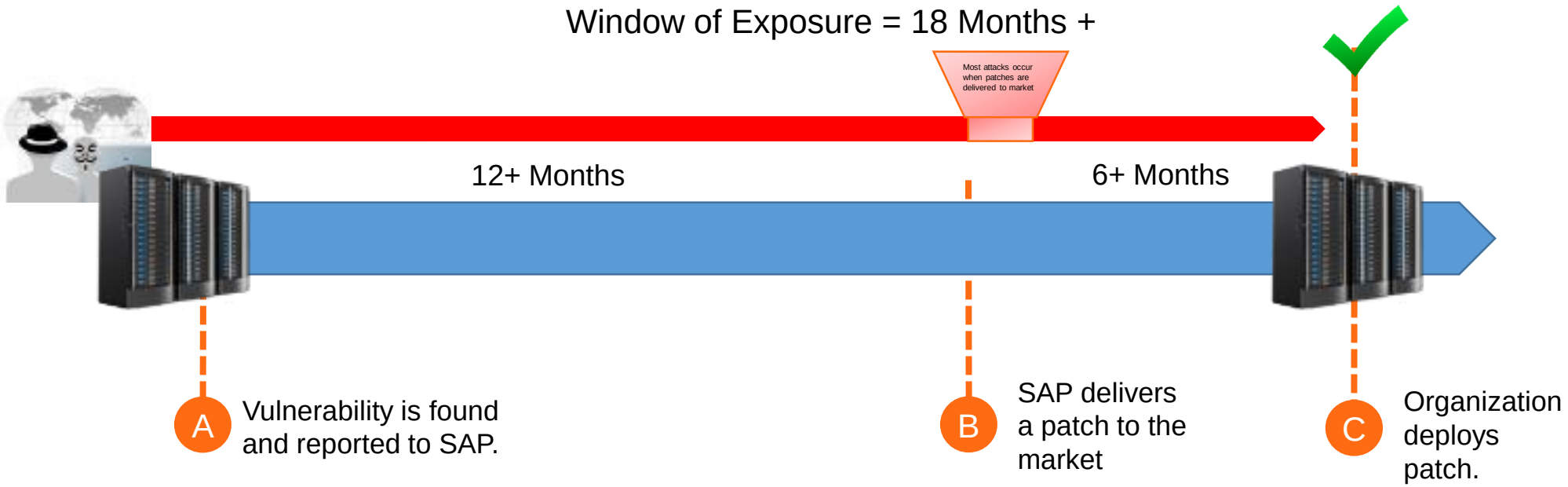
What Is the Probability? Killing Some Myths

- "Our SAP system has never been hacked"
  - Most companies do not enable (security) 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"

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



What Is the Probability? Killing Some Myths

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

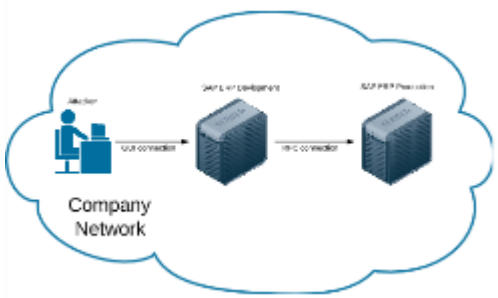
A Chinese hacker exploited a vulnerability in a corporate SAP NetWeaver Portal.

What Could Be the Impact?

Attack Scenarios

Attack Scenarios

1

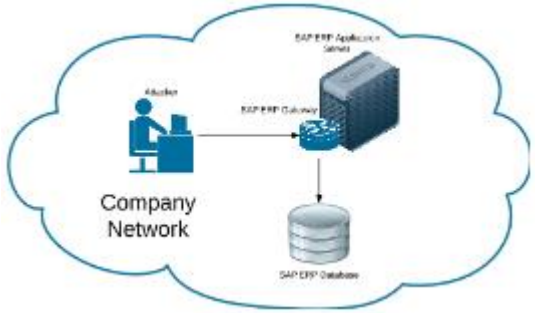


Pivoting between SAP systems:
Pivot from a system with lower security (Development or QA system) to a critical system (Production system), to execute SAP remote function modules in the destination system

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

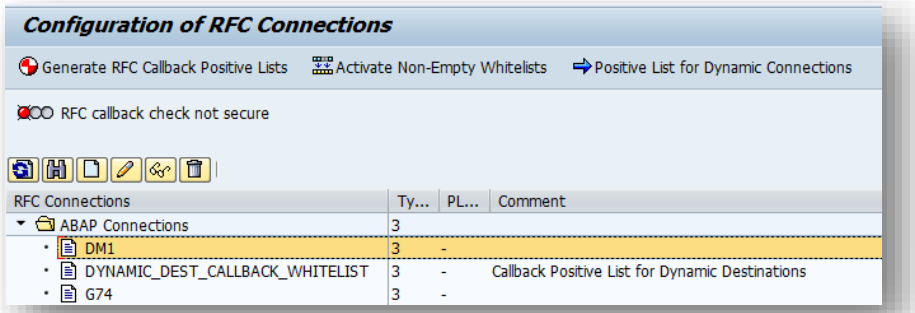


Attack on SAP services configuration:
Execute Operating System commands under the privileges of the user <sid>adm by exploiting vulnerabilities in the SAP Gateway. Get and potentially modify credit card information stored in the SAP database.

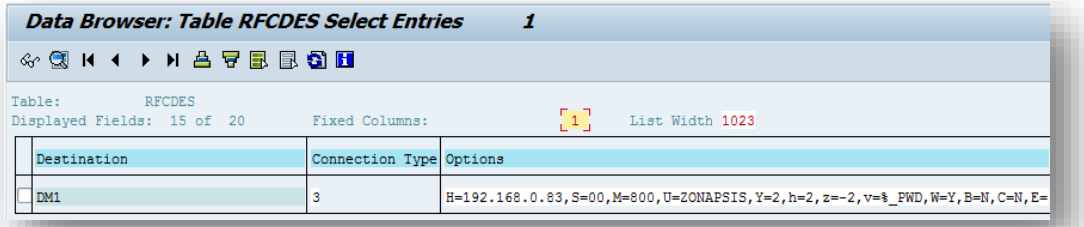
Attack Scenario 1

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

2. List of RFC destinations and its properties

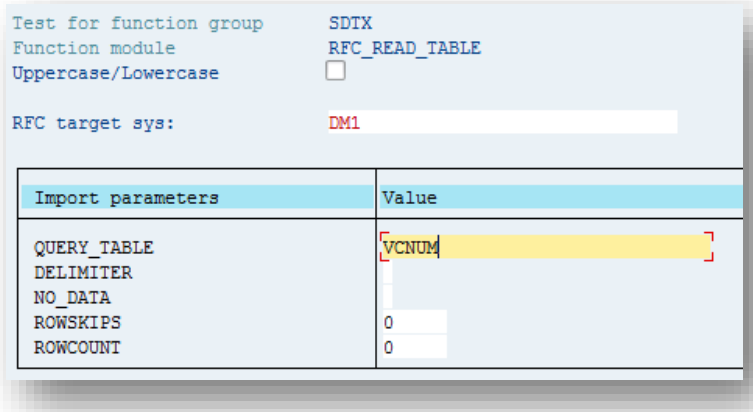


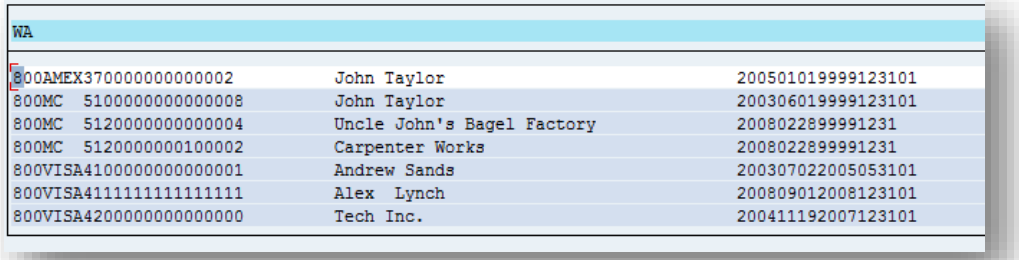
SM59



SE16 - RFCDES

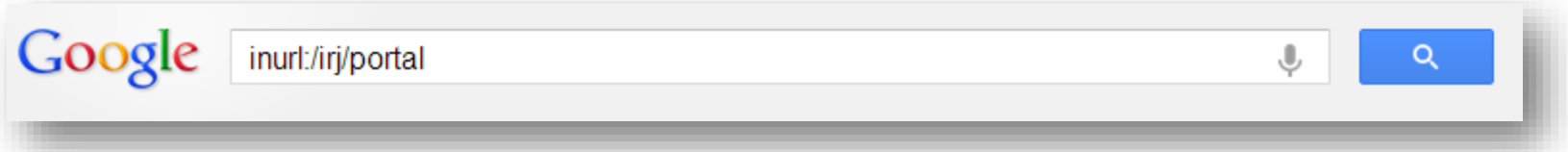
3. Attacker goes to transaction SE37 and leverages a destination and “data read” function module.



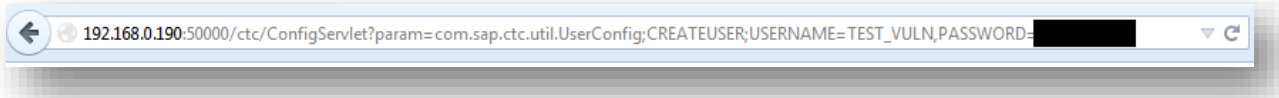


Attack Scenario 2

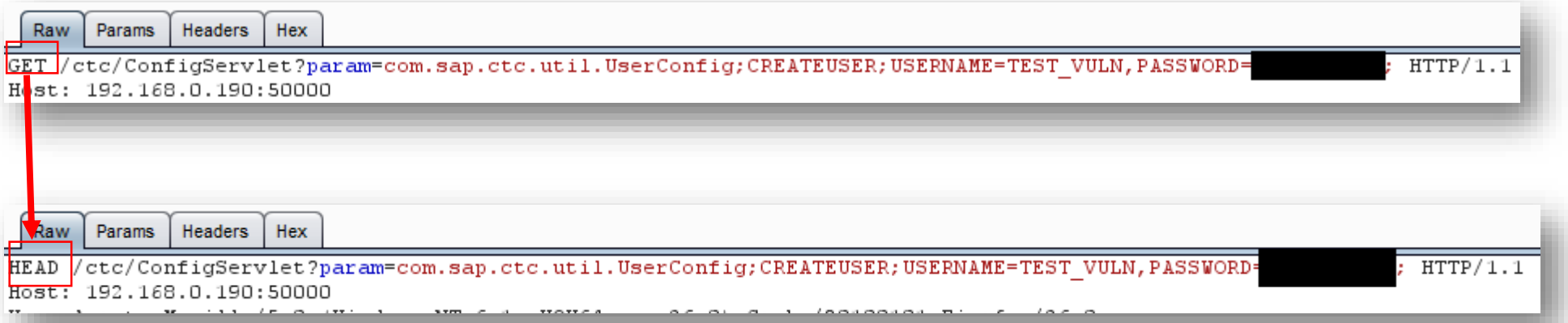
1. Vulnerable systems are also connected to Internet!



2. Attacker sending HTTP request to the CTC servlet and creating a user – **Filtered…**



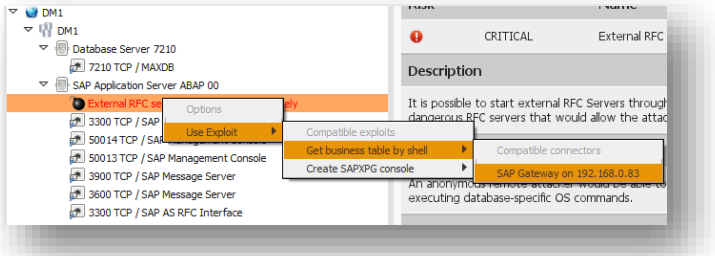
3. Using a local proxy, the attacker changes the HTTP verb from GET to HEAD and forwards it to the server. This command will send the user creation request to the CTC servlet

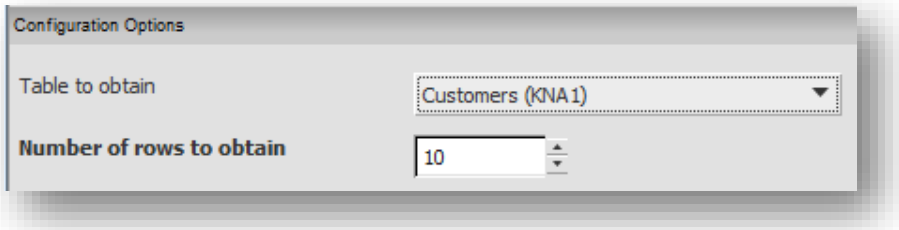


Attack Scenario 3

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

Get business table by shell

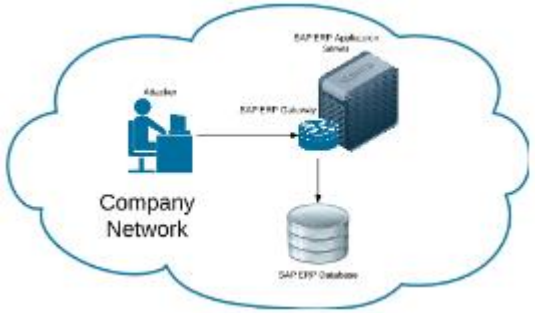
KUNNR	LAND1	NAME1	NAME2	BEGRY	BRSCH	ERDAT
0000000001	US	Nelson Tax & Associates			19990520	
0000000002	DE	Welt			19950323	
0000000049	CN	Ku Ping Enterprise Co. Ltd			20100618	
0000000099	DE	Einmalkunde			19990712	
0000000110	DE	Auto Klement	Exclusive Automobile		19950809	

Attack Scenarios

1

2

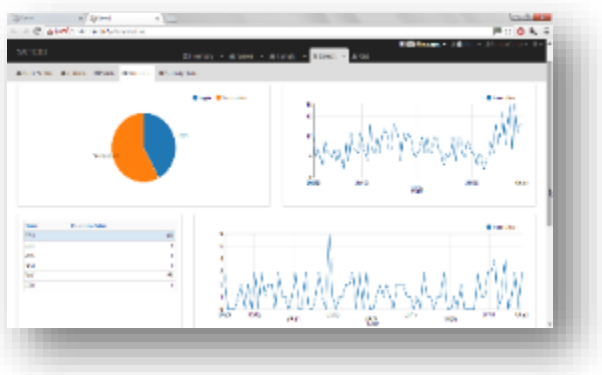
3



In these attack scenarios, <u>any</u> business information in SAP can be displayed:

- 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 Security Platform



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.

SAP® Certified
Integration with SAP NetWeaver®

Vulnerability and Compliance

- Identify all SAP infrastructure and generate graphical topology maps along with the interfaces 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

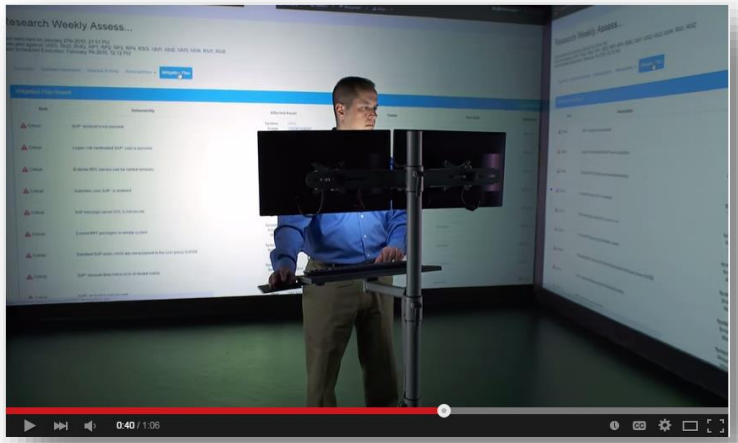
- Continuous monitoring of advanced threats and anomalous user behavior on SAP infrastructure.
- Provides visibility into attacks, with context, to determine if the attack is likely to be successful.
- Leverages real-time reporting on the likelihood and impact of threats from SAP exploits.
- Delivers 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.
- 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.

Engage with Onapsis

Video



1 minute Onapsis Security Platform Demo on SAP Cybersecurity

https://youtu.be/38T-_yvTroc

Blog

Visit our Blog – The source For SAP Cybersecurity Expertise

Onapsis.com/blog

Training

BlackHat USA 2015 ERP Security Training – Aug. 3-4

http://ubm.io/1MbaYe3

Thank You
@marianonunezdc

onapsis