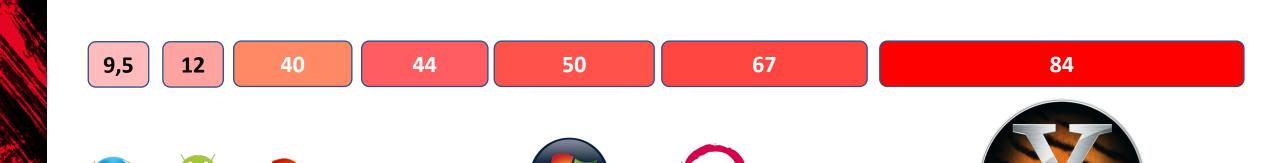


#### IT complexity vs. SAP complexity - is SAP really just another App?





Windows Vista 2007 - 2008







# Some SAP Whoopsies



First widely known SAP-Malware, targeting SAP Logon Client



21.5 Millionen PII records have been stolen (OPM-Hack) via an SAP exploit



Security Warning Because of recognised attacks to SAP Installation by Homeland Security



7 Days Production Outage Because of unplanned downtime of the SAP systems at Porsche - said to be caused by hardware



**Empty Retail Stocks** Due to ransomeware attack which encrypted SAP system databases



**Data Leakage** Attackers claim to have stolen all SAP data and still be in the network and asking for a 8-digit ransom (unconfirmed)

01/2022

05/2015

2/2016

10/2019

05/2021

05/2023





100 Mio. \$ loss of the Bank of Bangladesh after a breach in via SAP Multi-Bank Connectivity



5/2019

**Security Warning** because of the the RCE Exploit 10KBLAZE targeting the SAP Message Server component



10/2019

**Public Excuse** by SAP after security incident at the weapon buy back program in New Zealand



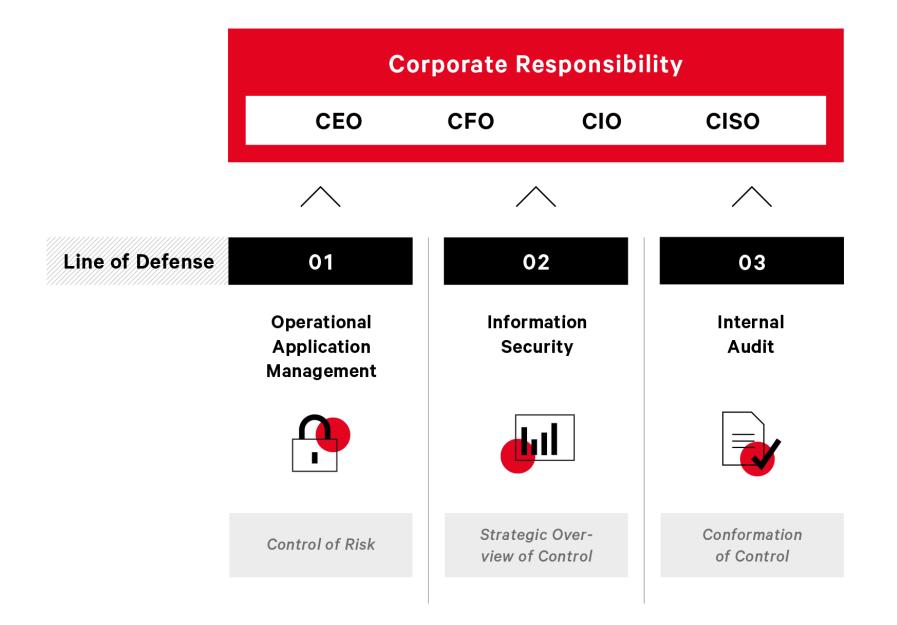
**Multi Million Finance** Fraud Campaign by threat group Elephant Beetle utilising exploits for known ERP software vulnerabilities including SAP Java Stack.

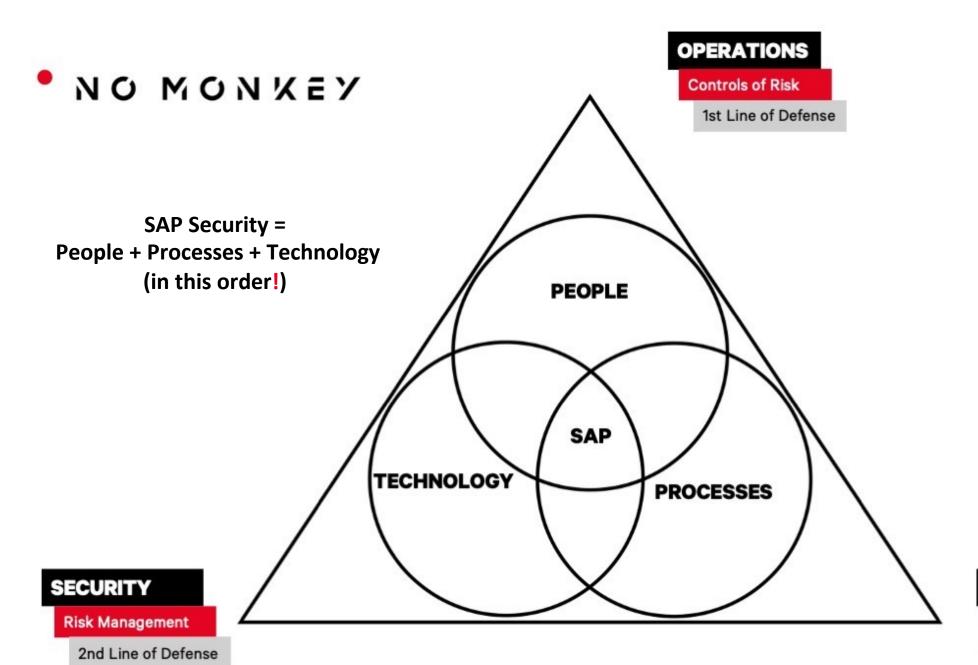
Anonymous declares successful attack with SAP 0-day of the greek ministry of finance (unconfirmed)

**Leaked Customer Accounts** after the SAP customer der SWIFT Network, accessed web portal got hacked

#### Who is responsible to run SAP secure and compliant?







**AUDIT** 

**Verification of Control** 

3rd Line of Defense



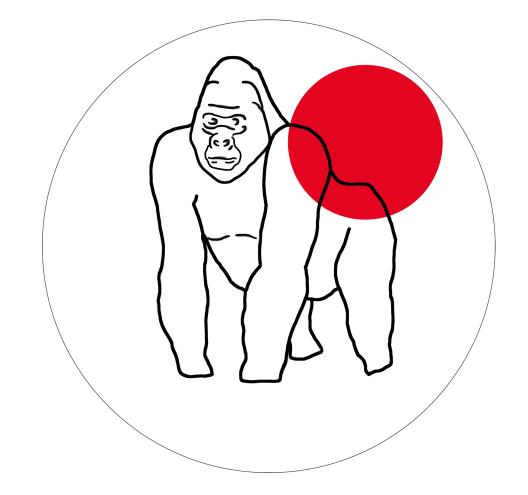
## SAP security is culture – and culture starts with people

### Main challenges when dealing with SAP security

- Lack of skills
  - > People don't understand SAP in CONTEXT of Cybersecurity
- No security governance
  - Who is responsible to run SAP secure and compliant? SAP, IT-Security, Audit?
- Silo thinking
  - > People don't see the big picture just their point of view
- ➤ No mandate or C-Level backup
  - > C-Level is in charge in latest consequence, but not aware of the risk in SAP
- Blind trust
  - > Too much trust in SAP, 3rd Partys and even the own organization in terms of SAP security
- Missing responsibility of individuals
  - > Security is everyones responsibility at any time
- > Lazyness and comfort zones
  - > Simplicity first. People to like extra work, which is outside of their comfort zone







# **OWASP - Core Business Application Security**

- Help organizations to protect themselves and the society
- Security methodology with a people first approach
- Help to liberate organizations from biased advice

https://owasp.org/www-projectcore-business-application-security/



#### **NIST CSF**

IPAC Model		Identify	Protect	Detect	Respond	Recover
		[0]			<b>3</b>	
Integration	<b>*</b>					
Platform						
Access	Ŷ					
Customization	<b>AHP</b>					

#### Within the NO MONKEY Security Matrix we aligned 2 important perspectives

- The Cyber Security Framework of the National Institute for Standards and Technology (NIST)
- The SAP world split up into the areas Integration, Platform, Access and Customization (short IPAC)



### **Create Your Course List**

All courses are based off our Security Matrix. It combines the genius of the NIST framework, which points out classic security challenges that need to be addressed, and the IPAC challenges that showcase the challenges SAP presents. We combined the two "worlds" to show what component each course focuses on.

#### **NIST CSF** Identify **Protect** Respond Recover Detect **IPAC Model** [0] • • • • Integration • • • Platform **P** • • **•** Access • • **•** Customization 1111

Click the target to get more information

# 3 important questions that every C-Level should be able to answer in 2023:

- How much is SAP in your yearly IT-Budget ?
- How much is Security in your yearly SAP-Budget ?
- How much does a complete loss of SAP cost your company per week?

HOPE IS NOT A STRATEGY!



☐ Inbox - NO MONKEY 30. May 2023 at 11:52

Details

Re: SAP Sicherheit // CIO Roundtable // NO MONKEY

To: Jochen Fischer CEO, Cc: Marco Hammel Keine Angabe

Guten Tag Herr Fischer,

Danke für Ihre E-Mail. Herr Hammel sagte beim CIO Roundtable, dass Unternehmen, die nur an einer Zertifizierung interessiert sind für NoMonkey nicht die Zielgruppe seien.

Da wir zunächst "nur" die TISAX Zertifizierung anstreben ist eine Zusammenarbeit aktuell von keinem Interesse. Bei Bedarf melde ich mich.

Danke und Gruß

Mit freundlichen Grüßen / Best regards,

Head of IT



# Understand your attack surface in SAP before others do – Hope is NOT a strategy!



## **Run Secure - Together!**

**Jochen Fischer** 

**Co-Founder & CEO of NO MONKEY** 

Email: jochen.fischer@no-monkey.com

Mobile: +49 160 908 22 618

www.no-monkey.com

