SAPinsider

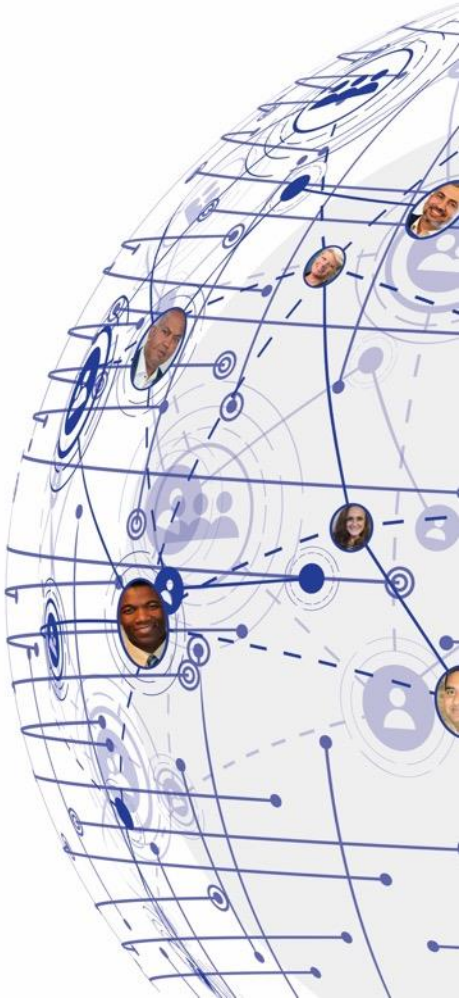
Secure Your SAP Environment - Improve Security And Reduce Operational Risks

Markus Gürtler – B1 Systems

Alan Clarke – SUSE

What We'll Cover

- SAP Security today – what's different from before?
- How to improve the security for your SAP environment
- Security of the Linux operating system layer
- Security 'Best Practices'
- Demonstration of typical attack vectors
- Outlook - what's important for tomorrow?
- Wrap-up



B1 SYSTEMS @ SAP

- Founded in 2004, >150 Consultants & Trainers
- **SAP on Linux Consulting, Training & Support**
- 365/24/7 Operations for SAP infrastructures
- SUSE **Partner for almost 20 years**
- Based in Germany, world-wide active

IT Security for SAP today – what's different from before?

Security in the age of digital transformation

- Digital transformation creates new security relevant targets
- Espionage, sabotage & data theft have higher impacts, due to
  - increasing amounts of sensitive digital data
  - increasing dependencies of our society, economy and politics on digital infrastructures
- Steady increasing number of security incidents world-wide
- New geo-political situation heavily influences number of cyber attacks (“cyber war”)
- Successful cyber-attacks on critical infrastructure can have serious consequences
- Increased need for data sovereignty

Causes of – and for - concern

In 2020, 86% of breaches were financially driven with 10% motivated by espionage,

45% featured hacking, 17% malware and 22% phishing

(Source – Verizon)

The average cost of a data breach is $3.86 million as of 2020 and $5.85 million in the financial services market

(Sources – IBM, Varonis)

The average ransomware payment rose 33% in 2020 over 2019 to $111,605

(Source - Fintech News)

The average cost of a malware attack on a company is $2.6 million

(Source – Accenture)

Global cybercrime-related damage costs is predicted to exceed $10 trillion by 2025

(Source - Cybersecurity Ventures)

https://www.verizon.com/business/resources/reports/2020-data-breach-investigations-report
https://www.verizon.com/business/resources/executivebriefs/2020-dbir-executive-brief.pdf
https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf
https://www.fintechnews.org/the-2020-cybersecurity-stats-you-need-to-know/ - February 16th 2020
https://www.accenture.com/us-en/insights/security/invest-cyber-resilience - November 3rd 2021
https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ - November 13th 2020

Cyber Attacks - Recent Years

2020 – Twitter
Attack – 130 accounts targeted Elon Musk, Past Presidents
Result – $121,000 in Bitcoin via nearly 300 transactions

2020 – Marriott
Attack – Data security breach
Result – >5.2 million hotel guests data exposed

2021 – LinkedIn
Attack – Data security breach
Result – >90% of user base had their data exposed

2021 – Crypto.com
Attack – Data security breach
Result – Crypto-currency theft of >$33 million

https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html
https://ermprotect.com/blog/top-10-data-breaches-so-far-in-2022/

SAP systems are worthwhile targets

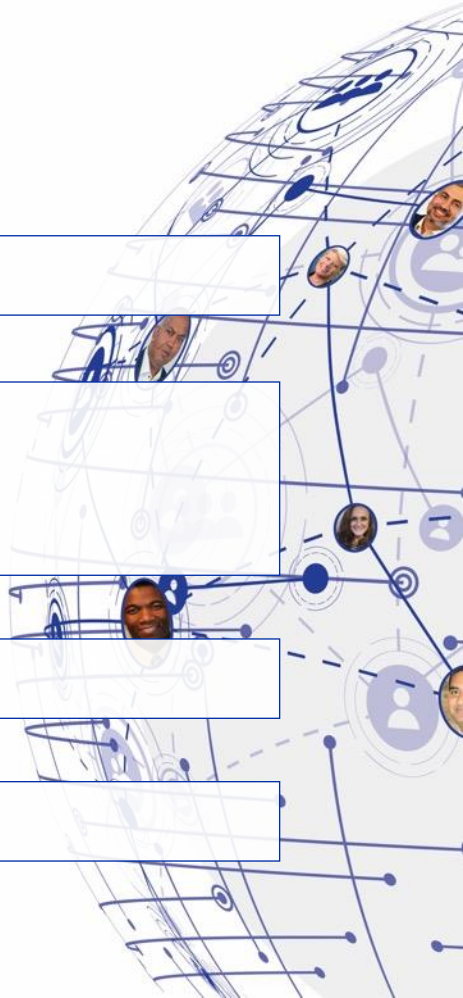
SAP systems often form the digital heart of an enterprise

Espionage, sabotage & data-theft targeted on SAP systems can have serious economical consequences for an organization

- Data-theft: Loss of possibly business-critical data
- Espionage: Attacks directed on specific business-critical information
- Sabotage: Consequences of longer downtimes or successful ransomware attacks

Central SAP systems like a central ERP system stores business-critical data

Investments into security of SAP landscapes are minimal compared to possible created costs in case of a successful cyber-attack



An increasing awareness for SAP security

- SAP security was always important, but companies often put it on low-priority in the past
- Security awareness for SAP came in several waves and slowly increased in average over time
- Today there is a completely different mindset giving SAP security the attention it deserves

How to improve the security for your SAP environment

Two dimensions of IT security

Organizational

- Inventory control
- Data protection
- Account management
- Role management
- Audit log management
- etc.

Technology

- Operating system security
- Application software security
- Network security
- Endpoint device security
- Endpoint security
- etc.

IT security requires a holistic approach

The 18 Center-of-Internet-Security (CIS) Critical Security Controls

CIS Control 1: Inventory and Control of Enterprise Assets

CIS Control 2: Inventory and Control of Software Assets

CIS Control 3: Data Protection

CIS Control 4: Secure Configuration of Enterprise Assets and Software

CIS Control 5: Account Management

CIS Control 6: Access Control Management

CIS Control 7: Continuous Vulnerability Management

CIS Control 8: Audit Log Management

CIS Control 9: Email and Web Browser Protection

CIS Control 10: Malware Defenses

CIS Control 11: Data Recovery

CIS Control 12: Network Infrastructure Management

CIS Control 13: Network Monitoring and Defense

CIS Control 14: Security Awareness and Skills Training

CIS Control 15: Service Provider Management

CIS Control 16: Application Software Security

CIS Control 17: Incident Response Management

CIS Control 18: Penetration Testing

Technology Example
SAP S/4HANA stack in the cloud

1 SAP Application & Database Layer
SAP HANA & SAP Application Server ABAP, SAProuter, etc.

- SAP Application security (e.g. user and role management, MFA)
- SAP Database security (e.g. data volume encryption, administrative security)

2 Operating System Layer
Linux (SUSE Linux Enterprise Server for SAP Applications)

- Operating System security hardening
- Operating System patching
- SAP patching
- Security auditing

3 Cloud Infrastructure Layer
Azure, GCP, AWS, private cloud

- Network security (firewalls & intrusion detection)
- Firewall (as a service), IDS (as a service)
- Restricted privileges for dangerous operations via cloud API's

Security of the Operating System layer

The Role of the Operating System

Most common attack vectors on SAP systems are

- getting user access to SAP applications
- getting administrative access to SAP databases
- **getting access to the Operating System of SAP applications & databases**
- or a combination of the three above

Almost all SAP workloads today run on Enterprise Linux operating systems

The operating system is a critical layer and each SAP system needs an operating system, regardless of whether an on-premises or cloud deployment

Command-line access via a privileged Linux user + additional SAP credentials lead to full access and control of an SAP system

Breaking into a SAP Server on the OS level

Server operating systems are one of the most common targets for hacker attacks

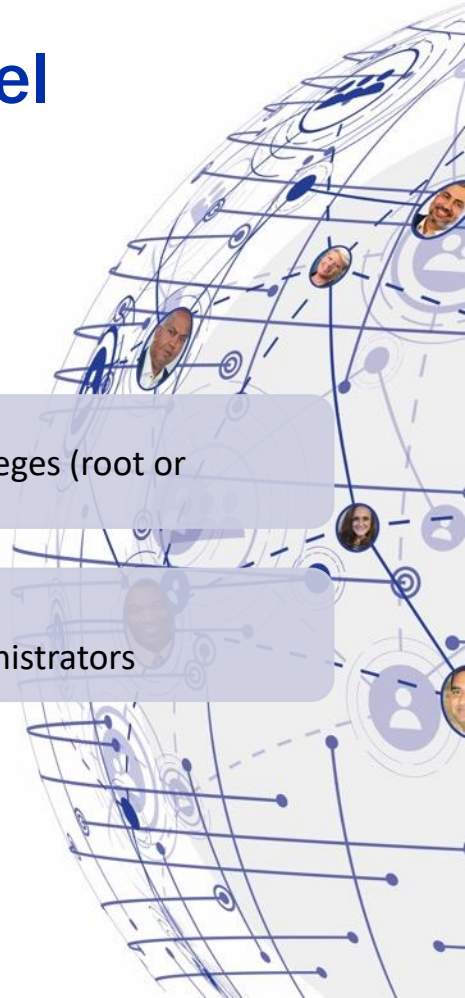
Attacks to an OS can come…..

- … from outside of a system to break into it
- … and/or on the system to gain more privileges (root or <sid>adm user)

Attacks may…..

- exploit vulnerabilities of the software stack
- use stolen user credentials, e.g. from administrators

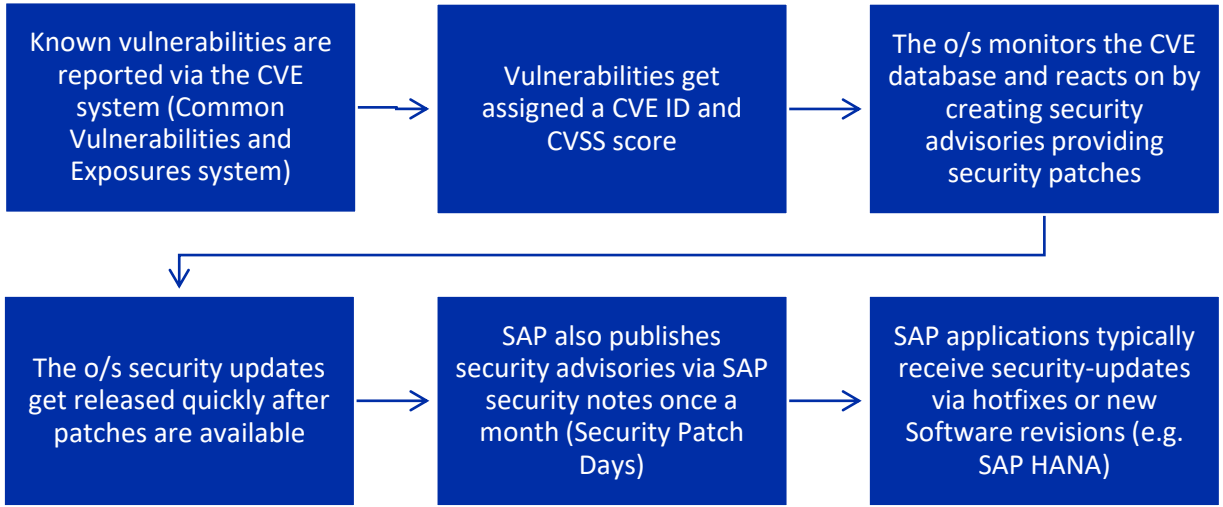
Goal is to gain sufficient privileges to access an SAP application on the OS level (i.e. become root or <sid>adm user)



The ‘Must Have’ Security Features of an Enterprise Linux Operating System for SAP Environments

- Security certifications like FIPS-140-2, CC EAL 4+, STIG & more
- Guarantees of security patches across the whole release cycle
- Kernel Live Patching allowing installing security fixes without downtime
- Security frameworks and auditing frameworks
- Firewall for SAP HANA
- OS Security Hardening for Guide for SAP & Best Practice Guides
- Outlook: Pre-hardened cloud SLE images (including SLES for SAP)

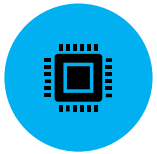
Vulnerabilities and security patches – how it works…



Note - other third-party software (like backup or monitoring software) might have different processes

Patching, Live Patching and Seamless Maintenance

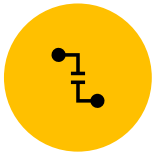
Security patches often require downtime of SAP systems



Strategies to minimize downtime during security updates

Implement live kernel patching *(apply kernel security fixes with no downtime)*

The SAP-certified Linux o/s High Availability solution for SAP S/4HANA should support seamless maintenance procedures

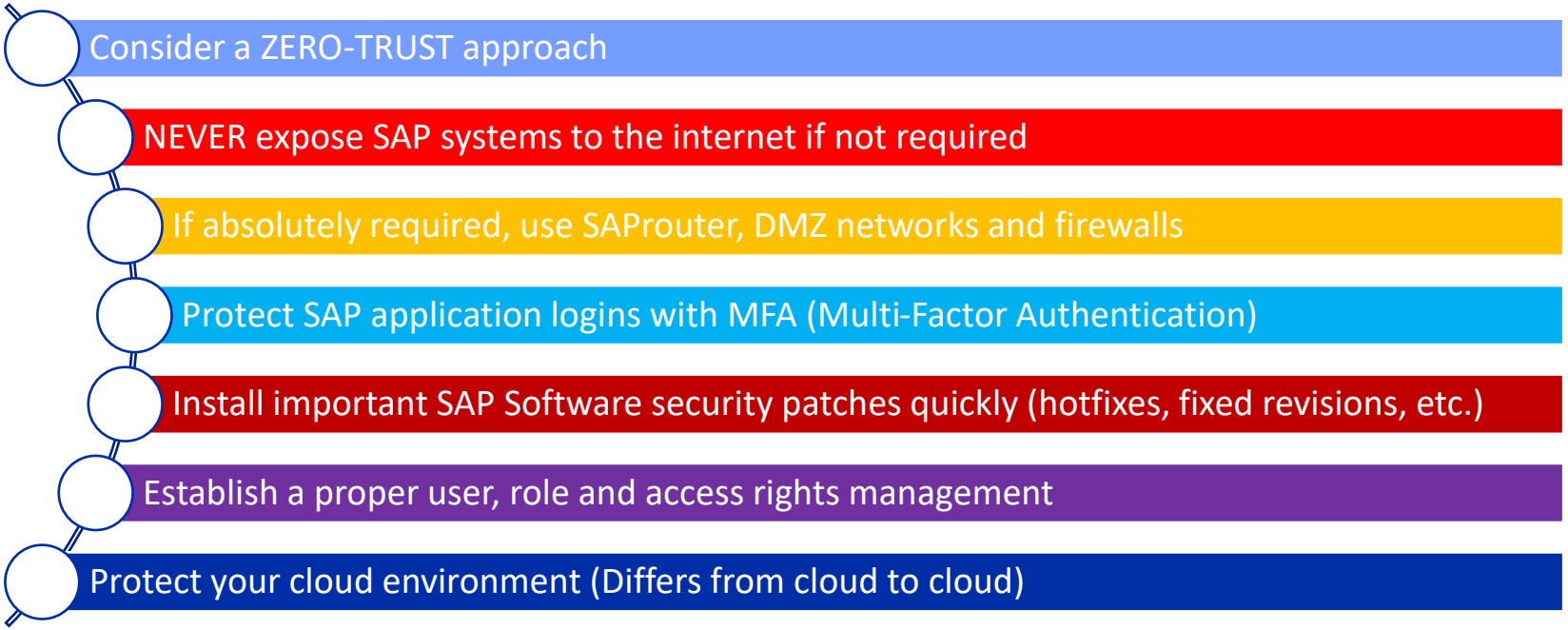


Security patches should be distributed locally, e.g. through the Linux o/s management console

Security Best-Practices

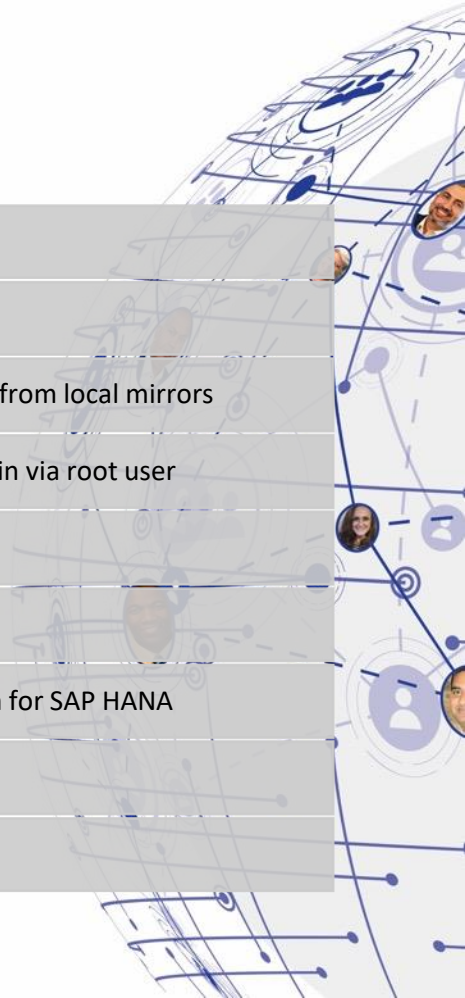
Security Best Practices

SAP landscape generic



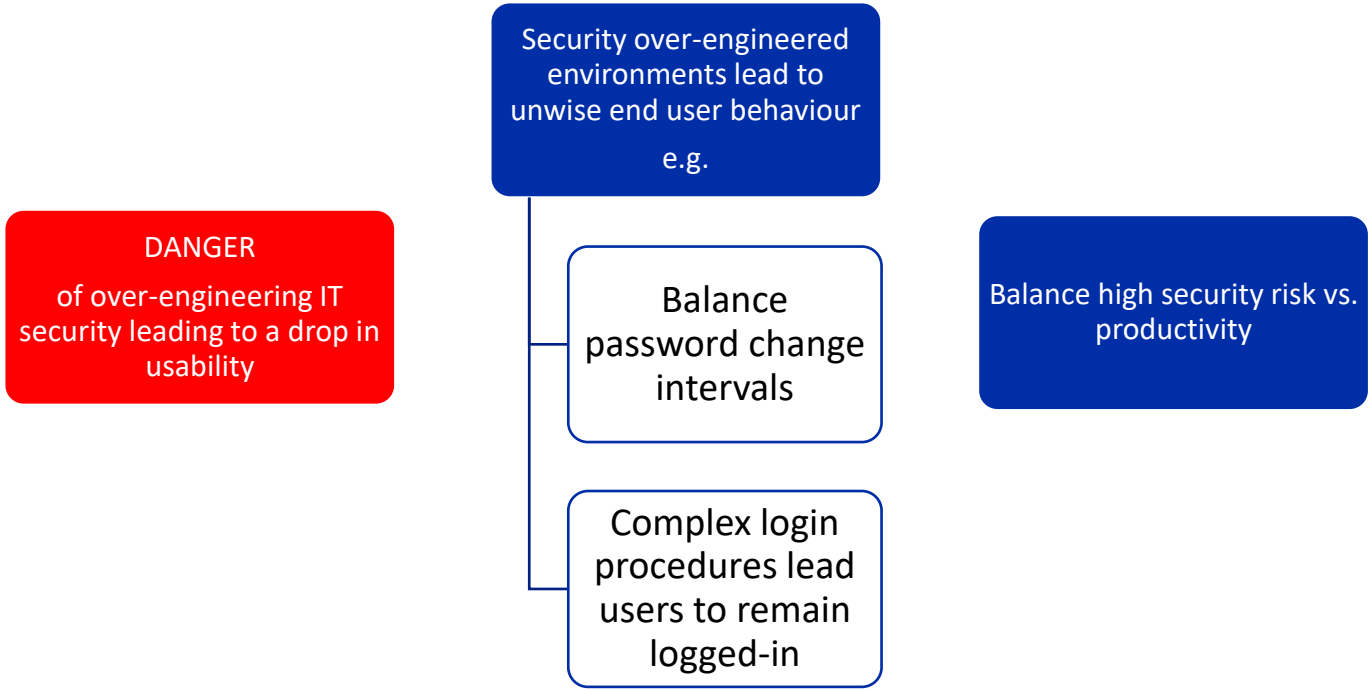
Security Best Practices
Operating System Level

Best Practices	Follow the SAP-certified enterprise Linux Security Best-Practices
Updates	Keep SAP servers always up-to-date (use live-patching to reduce downtimes)
Prohibit	Don’t allow SAP PROD or QA systems to access the Internet directly, get updates from local mirrors
Authenticate	Only allow ssh public/private key-authentication, disallow passwords, disable login via root user
Monitor	Monitor changes made on the system
Audit	Use audit functionality and forward security event logs to a SIEM
Enable	Enable data-volume-encryption, data-redo-log encryption and backup encryption for SAP HANA
Encrypt	Use storage encryption to protect against physical data theft
Protect	Use the SAP HANA firewall to better protect against remote server attacks



Security Best Practices

Find the right balance between security & usability



Investments in SAP Security

- Balance organizational security and security technology investments
- Zero-trust approach = higher investments…but also leads to significantly improved security
- Obtain help from specialized third parties (if necessary) to deal with the high complexity
- Security requires investments on a regular basis
  - Security frameworks must regularly be adapted to latest developments
  - Perform regular SAP security audits and penetration tests (e.g. annually)
  - New SAP systems should be configured with high security standards in mind
- Open Source Software - a cost-effective alternative to expensive commercial tools & appliances

Demonstration of typical attack vectors

Classic attack vector
(simplified example)

Social engineering
Find out details about employees & organization

Attack employees end-devices
e.g. by sending manipulated emails

Hijack end-devices & steal data
e.g. by installing backdoors, keyloggers, etc

Break into the local network
e.g. via VPN and stolen account data

Learn about SAP systems
e.g. gather information about SAP portals

Login to SAP systems
e.g. explore & copy data

Explore and copy data
Using standard tools like browser or SAP GUI

Start a ransomware attack
on the compromised end-devices

Classic attack vector
(simplified example)

Security awareness trainings & data protection policies

User security trainings

Endpoint devices security, patched systems

Multifactor-authentication, intrusion detection

Intrusion detection, information obfuscation (e.g. DNS records)

Multi-factor authentication

Security auditing & logging

Endpoint device security

Classic attack vector targeting the Operating System
(simplified example)

Social engineering
Find out details about employees & organization

Get account data (ideally admins)
e.g. by leading employees to faked login portals

Break into to the local network
e.g. by misusing remote-working capabilities

Learn the SAP landscape
e.g. gather information, try to find HANA DB's

Scan for security vulnerabilities
e.g. weak passwords, non-SAP services, etc.

Break into a server on OS level
e.g. using a remote exploit

Gain enhanced privileges
e.g. use local exploits

Copy, destroy or encrypt data
e.g. copy SAP HANA data files

Classic attack vector targeting the Operating System
(simplified example)

Security awareness trainings & data protection policies

Security-aware users and admins

Multifactor authentication

Intrusion detection, data obfuscation (e.g. DNS records)

Intrusion detection, intrusion prevention, firewalls,

Break into a server on OS level
e.g. using a remote exploit

Installation of most current security patches

e.g. use local exploits

Data volume encryption & co., security auditing & logging, SIEM

Modern attack vector targeting the Operating System

(simplified example)

Social engineering
Find out details about SAP Adminstrators

Attack admin's end-devices
e.g. by sending manipulated emails

Hijack an admins end-device
e.g. by installing a backdoor, keylogger, etc.

Record data from the admin
e.g. gather information about SAP environment

Misuse admin capabilities
e.g. ssh-keys, jump-hosts, access restrictions

Login to SAP HANA host as admin
using the admins account data

Manipulate regular system backup
requires some knowledge about SAP backups

Copy, destroy or encrypt data
e.g. manipulating SAP HANA data files

Modern attack vector targeting the Operating System

(simplified example)

Social engineering

Security aware administrators

Security awareness trainings & data protection policies

Hijack an admins end-device

e.g. by installing a backdoor, keylogger, etc.

Endpoint device security, patched system, security sensitive admin

e.g. gather information about SAP environment

Regular need to change passwords / pass-phrases, regular revisit access restrictions

Login to SAP

Security auditing & logging, SIEM

Manipulate

Configuration change monitoring

backups

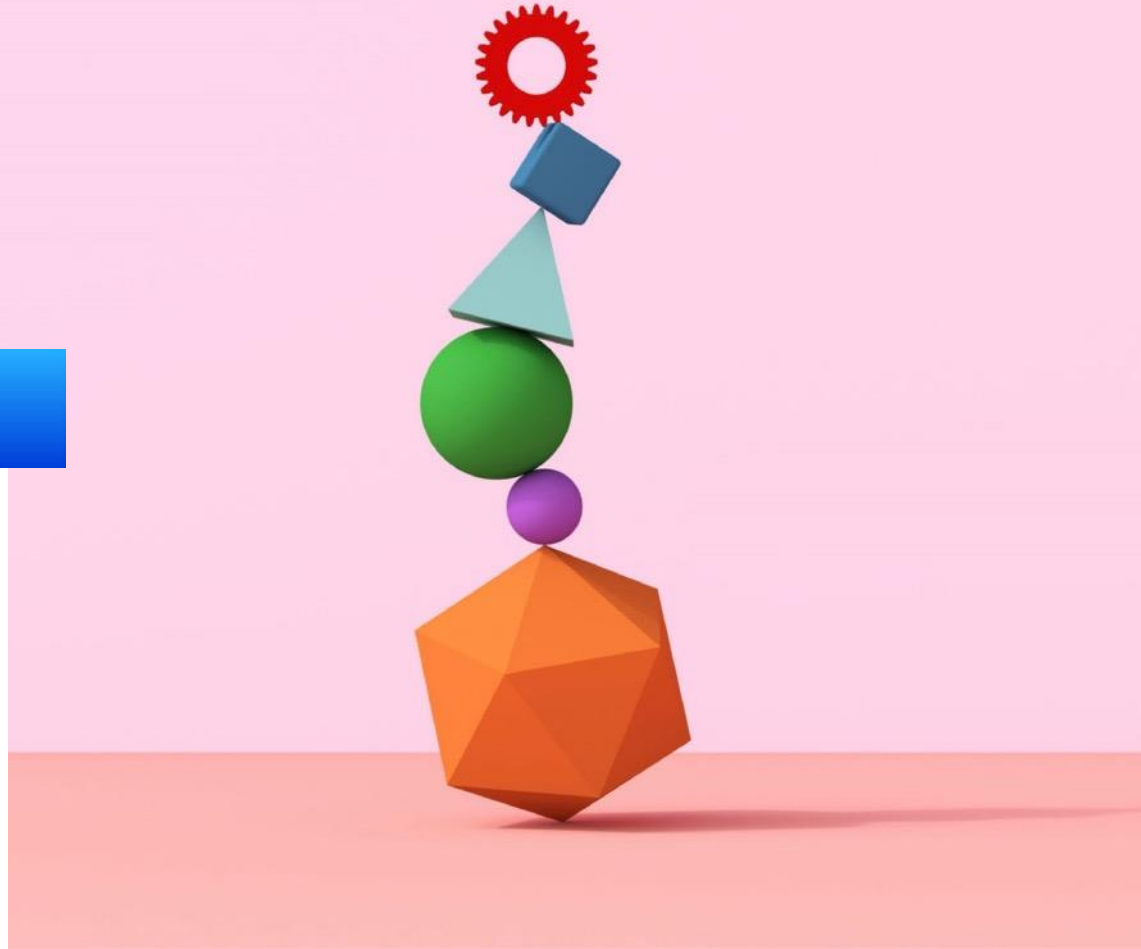
Data volume encryption & Co., security auditing & logging, SIEM

Outlook: What's important for tomorrow

What's important tomorrow?

- Dealing with security requirements on steadily increasing complexity of SAP landscapes
- Increasing data sovereignty (e.g. a sovereign cloud for mission-critical SAP systems)
- Security for containerized SAP applications & Kubernetes (e.g. NeuVector)
- Stronger focus on security of API's for SAP applications
- Improved security concepts with a new generation of containerized Linux operating systems (e.g. SUSE Adoptable Linux Platform)

Wrap Up



Where to find more information

- Operating System Security Hardening Guide for SAP HANA on SLES 15
  https://documentation.suse.com/sbp/sap/pdf/OS_Security_Hardening_Guide_for_SAP_HANA_SLES15_color_en.pdf

- SUSE Security
  https://www.suse.com/de-de/support/security/

- SAP HANA Security
  https://www.sap.com/products/technology-platform/hana/features/security.html

Key Points to Take Home

IT Security for SAP more critical than ever

Higher degree of digitalization

Increasing number of directed and undirected attacks

Security requires a holistic approach

Must every aspect of an IT environment, technically and organizational

The o/s layer of SAP Software stacks is a prime target

Ranked 2nd after SAP applications and databases

Ensure your chosen SAP-certified enterprise Linux operating system ships with security features built-in and take advantage of live kernel patching to limit unplanned downtime

External partners can help to improve your SAP security

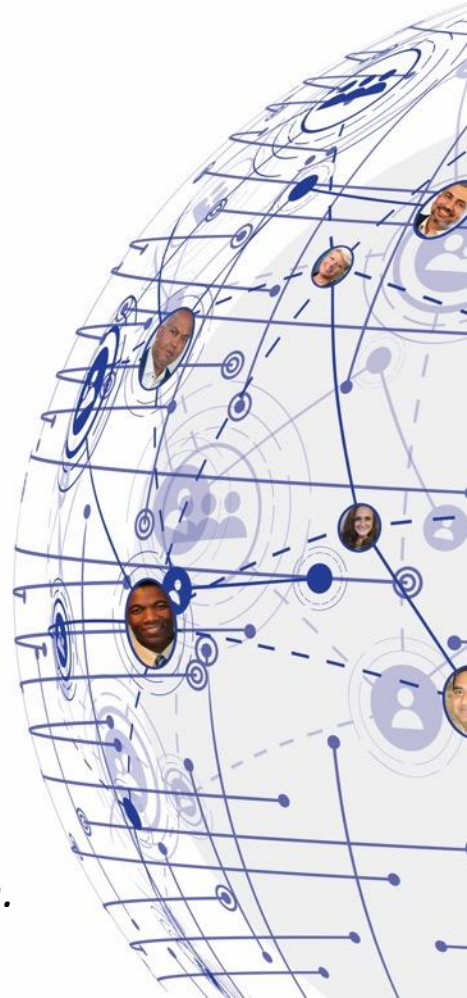
Thank you! Any Questions?

Alan Clarke

alan.clarke@suse.com

Markus Gürtler

markus.guertler@b1-systems.de



Please remember to complete your session evaluation.

SAPinsider

PO Box 982Hampstead, NH 03841

DART Methodology

DART Methodology

Drivers (D)

These are macro level events that are impacting an organization. They can be both external and internal and require the implementation of strategic plans, people, processes and systems.

- High total cost of ownership (TCO) of legacy ERP systems
- Need for continuous innovation
- (Shortening of product lifecycles and demand for more customized products, services and pricing models)

Actions (A)

These are strategies that companies can implement to address the drivers impact on the business. These are the integration of people, process and technology.

- Create a sustainable digital innovation strategy that enables your company to identify new revenue streams, lower costs, and improve current products and services
- Deploy a cloud based or hybrid business architecture to minimize costs and maximize speed to market
- Prioritize specific business processes for intelligent automation based on ROI and cost models
- Modernize your reporting, dashboard, and insights strategy to provide more real-time and high-value views into your business

Requirements (R)

These are business and process level requirements to support the strategies.

- Faster consumer-driven innovation via real-time customer insights
- KPIs and ROI model for business process improvement and business impact measures
- Self-service reporting and analytics
- Platform for custom product and pricing configuration
- Strong data cleansing, data management, and data governance practices
- Elimination of long deployment and upgrade cycles
- Elimination of complex patching and testing cycles
- Business and IT team buy-in for next level ERP via a bottom-up business case
- A clear owner to manage advancement of ERP

Technologies (T)

These are technology and systems related requirements that enable the business requirements and support the overall strategies that the company is taking.

- On-premise and cloud-based ERP deployment models
- Mobile and responsive-based UI
- Highly integrated financial planning and management solution
- Rich developer framework for customizing and extending both cloud and on premise applications
- Powerfully integrated advanced analytics and visualization tools
- Integrated financial, sales and operational planning solutions
- Best-in-class Cloud and on-premise middleware solutions
- End-to Customer data management
- Customer profiling and intelligence

VIDEO CONFERENCING GUIDELINES

PLAN AHEAD TO AVOID DISTRACTIONS

ENVIRONMENT

CAMERA POSITIONING

Camera should be centered at or above eye-level, maintain eye contact with the camera

PROPER LIGHTING

Present in a well-lit room with the light facing towards you, avoiding windows behind or next to you

RECOMMENDED BACKGROUND

Bookshelves or neutral pictures make for distraction-free natural backgrounds

PRESENTATION

PREPARATION

Test platform, internet connection, microphone, speakers and video

WHEN TO MUTE

Be sure to mute your microphone when you are not speaking and unmute when necessary

DRESS/OUTFIT

Dress professionally, wearing the same outfit you would in a face-to-face presentation

WARNINGS

TYPING ETIQUETTE

Try not to type while presenting

EATING

Do not eat while presenting and avoid drinking where possible

INTERRUPTIONS

Minimize interruptions such as muting your cell phone and closing your door

MOVEMENT

Avoid a lot of movement, including hand gestures that may stutter the video