SAP CYBERSECURITY BEST PRACTICES & IMPLEMENTATION CHALLENGES

Nipun Mahajan, Senior Cybersecurity Analyst, Lonza

Bill Oliver, Managing Director, SecurityBridge

Las Vegas

2024

SAPinsider

In This Session

SAP Cybersecurity the Key pillars

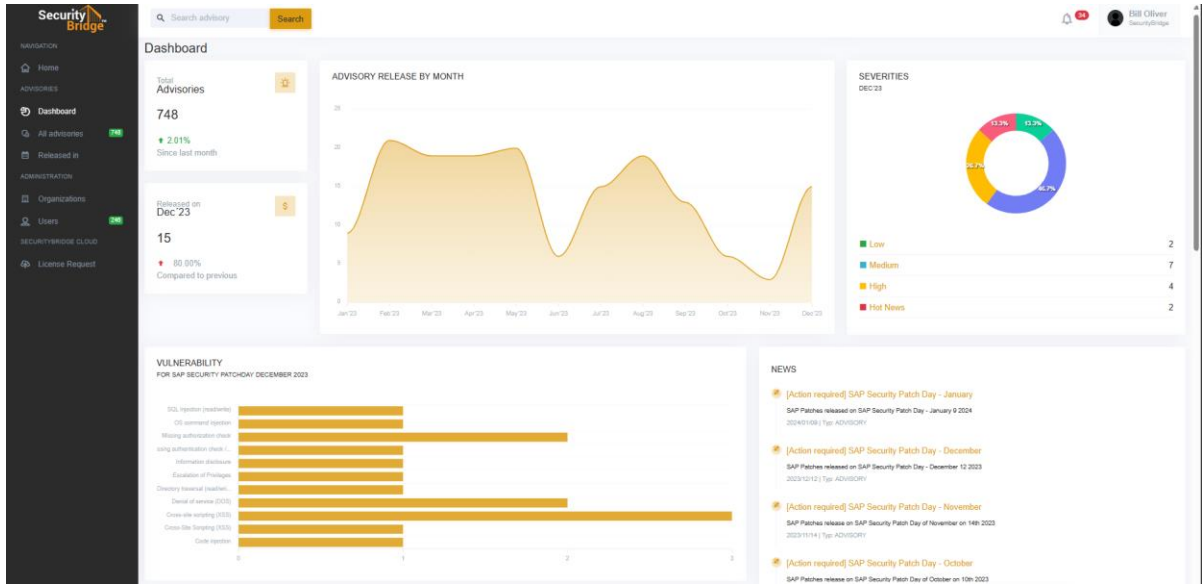
- SAP Security Position (Start Strong)
- SAP Security Patch Management
- Custom Code vulnerabilities
- Security Monitoring (Intrusion Detection)

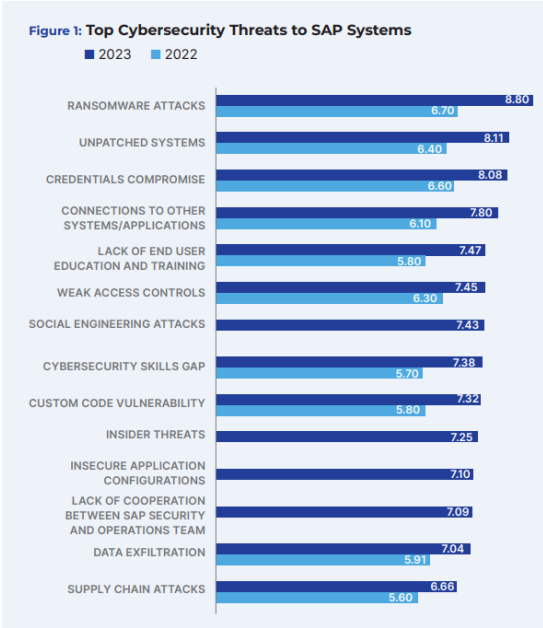
Lonza's SAP Cybersecurity Journey

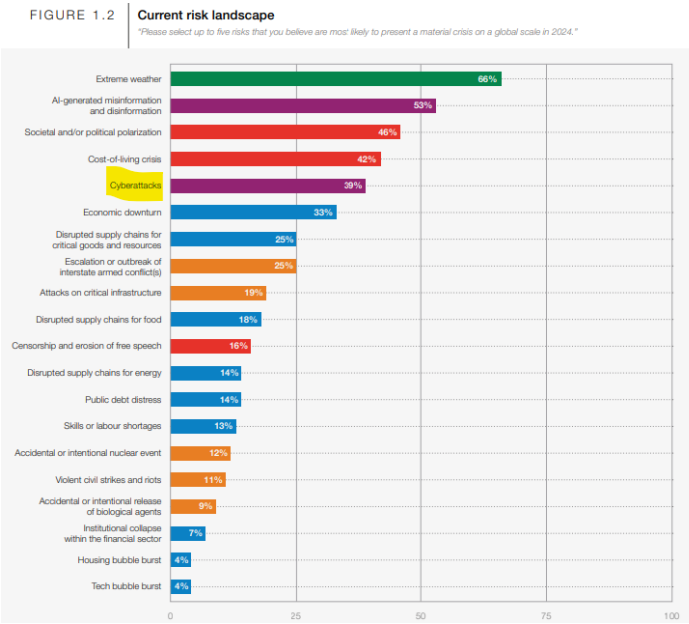
SAP Security Surroundings

Has SAP ever been breached?

- **Between mid 2020 and March 2021, 300 out of every 1500 cyber-attacks were successful in exploiting target SAP systems**
  - USIS breach, personnel records of federal employees and contractors with access to classified data
  - Critical SAP Vulnerability Allows Supply Chain Attacks
  - Critical SAP Vulnerabilities, CISA (Cybersecurity & Infrastructure Security Agency) suggests swift patching
  - In 2023, SAP has released over 160 security patches 21 of which are classified as “Hot News.” SAP recommends implementation immediately.







Source: WEF Global Risk Report 2023
Source: https://www.cpomagazine.com/cyber-security/hackers-exploit-known-sap-security-vulnerabilities-with-a-typical-cyber-attack-succeeding-in-record-time/
Source: https://sapinsider.org/research-reports/cybersecurity-threats-to-sap-systems

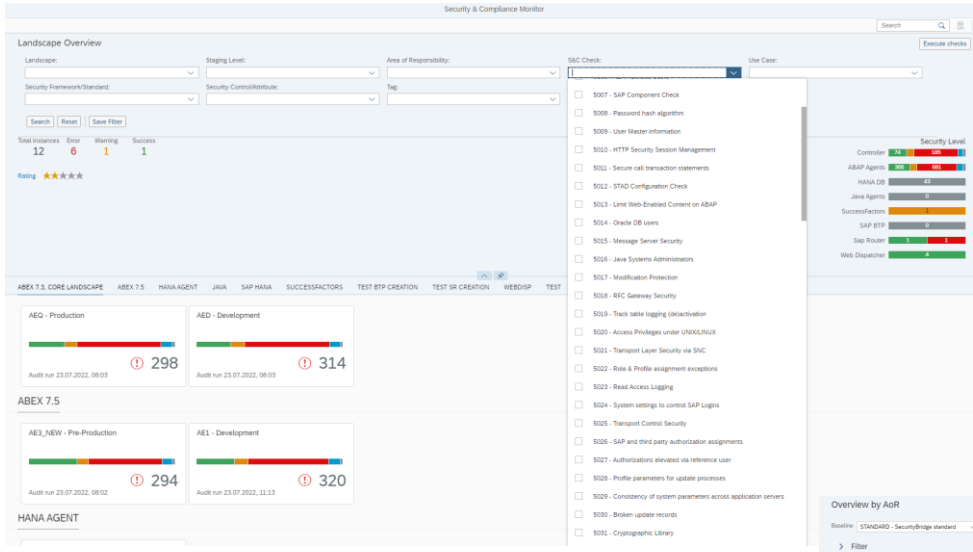
Hardening your SAP Security Position

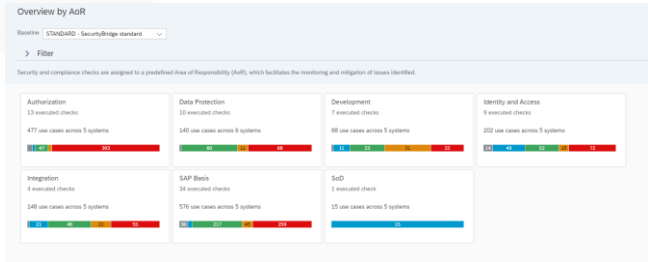
Hardening your SAP Security Position

If you have not already started hardening your SAP Security position, you need to start now. This is more than just who has access to “SAP_ALL”, who can run Profile Generator (PFCG), and what users can create and pay vendors (Segregation of Duties violations).

SAP System is so much more. A few of the many things you should look at are:

- Communication and Channel Security (RFC connections, HTTP connections, etc.)
- Internet Communications Framework
- File Systems Access Security
- Virus Scanning
- Data Storage Security (Encryption)
- Masking Data (Online presentation, Anonymization reporting)





PUBLIC
SAP HANA Platform 2.0 SPS 05
Document Version: 1.0 – 2021-05-21

SAP HANA Security Guide for SAP HANA Platform

Focused Run
The Ultimate Solution for Monitoring, Alerting, Root Cause Analysis, and Analytics

CUSTOMER/PARTNER

THE BEST RUN SAP

SAP Run Simple

Security Patch Management

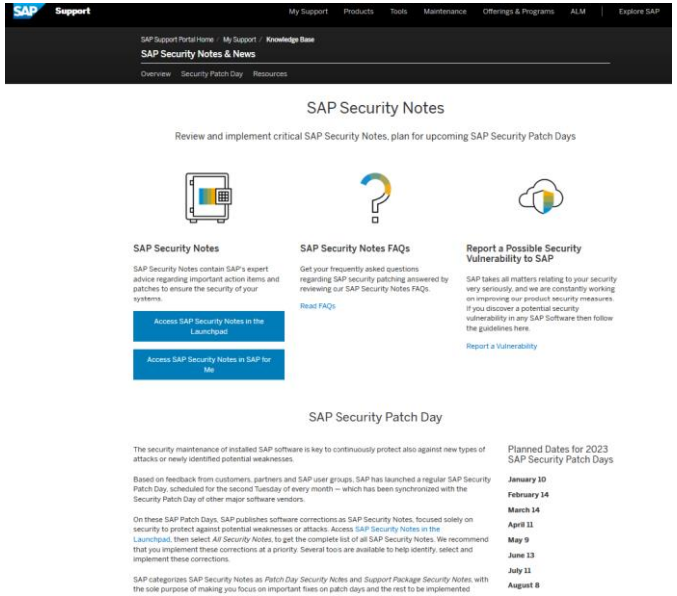
SAP Security Patch Management

For those who don't know, SAP has what we call "Patch Tuesday." On the second Tuesday of every month, SAP releases Security patches. They break them up into four categories: Hot News, High, Medium, and Low.

In 2023, SAP has released over 160 security patches 21 of which are classified as "Hot News." SAP recommends implementation immediately.

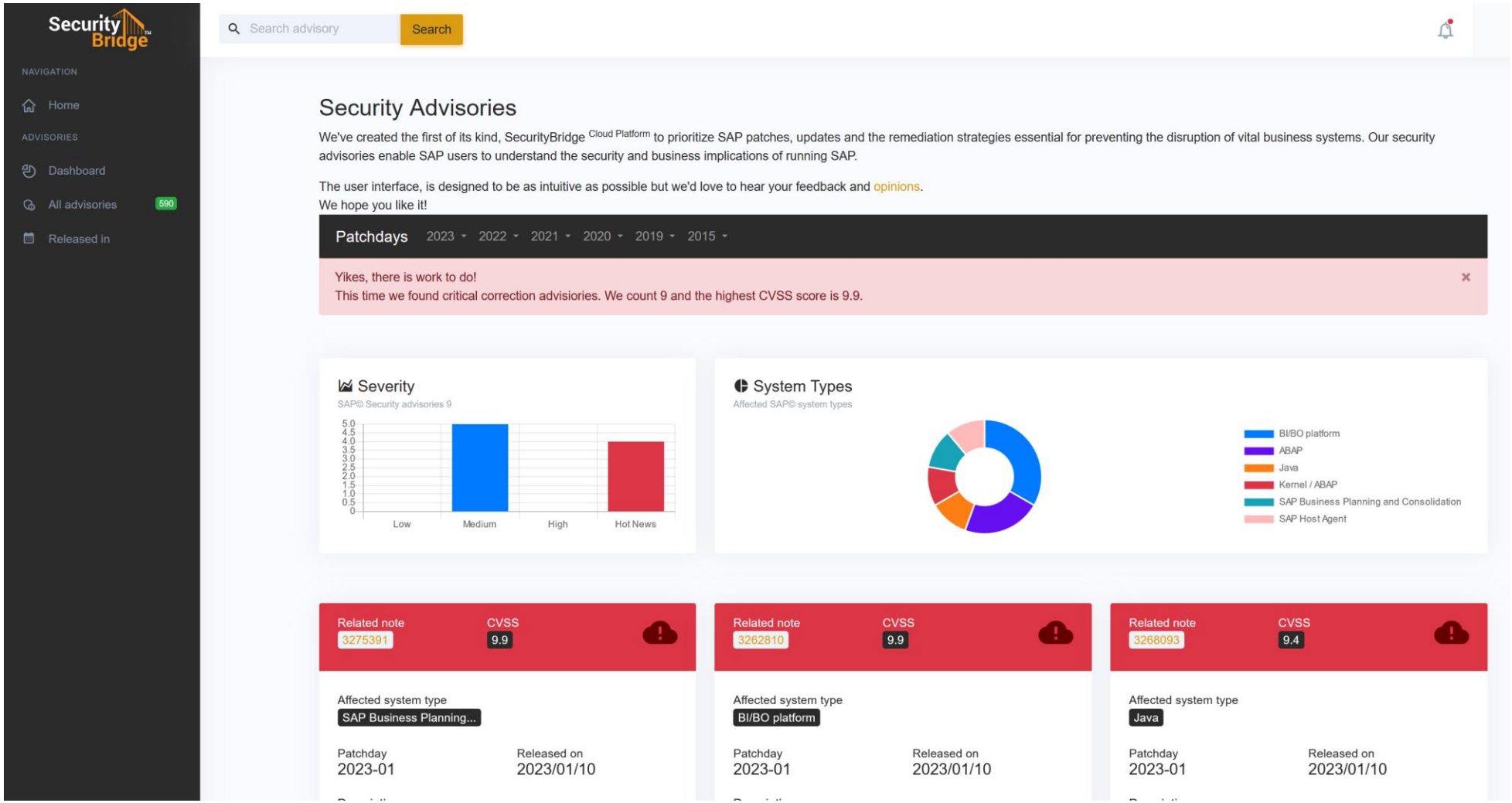
While it is up for debate on how quickly you need to install these patches. The key is not to leave this to your "Yearly Service Pack install and testing rollout." I have seen suggestions for the timing to implement Security notes anywhere from 15 days (Hot News – Highest Security impact) to 180 days (Low Security impact). The key is faster the better.

Note Category	Priority	Implementation Timing	Deadline	Deadline Notes / Comments
Hot News	Very High	15 days	30 days	Based on Risk Potential
Security Notes	High	30 days	60 days	
	Medium	90 days	180 days	
	Low	180 days	N/A	Aligned to maintenance/support release planning and implementation



Security Advisories

Cloud.SecurityBridge.com



Custom code Vulnerabilities

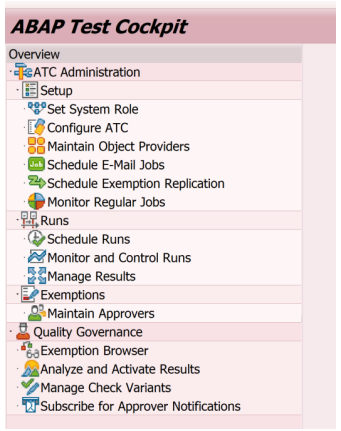
Custom Code Vulnerabilities

Now that we know how SAP fixes code (Patch Management), the question becomes, *"How are you going to fix all that custom ABAP you have been doing over the years that have security issues?*"

"Are you actually reviewing your custom code for Security defects?" If not (a common response is "What is a Code Scan?"), then you need to start now.

A few things to look for:

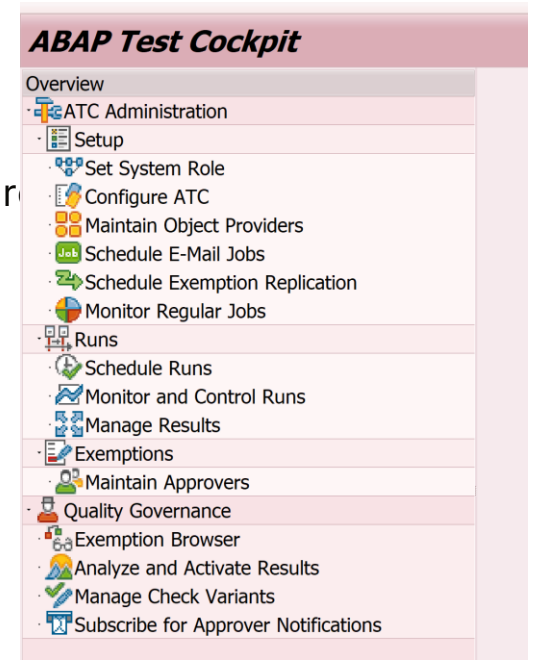
- *SQL Injections*
- *Missing Authority checks*
- *Backdoor Injections*
- *Mass data deletion*
- *Key SAP Programs/function modules that should not be in Custom Code*
- *Test programs still in production*
- *Directory Traversal*

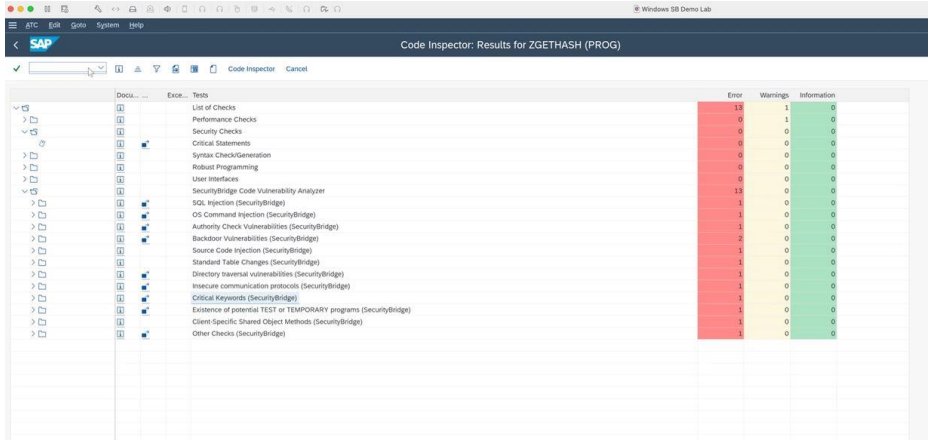


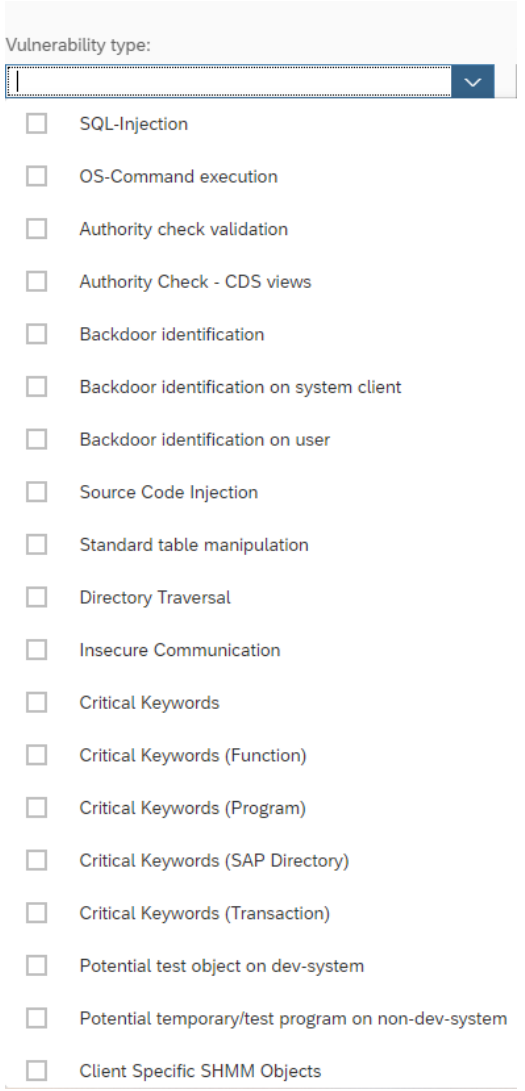
Custom Code Vulnerabilities

Scanning custom code to ensure security risks are identified and addr

fully integrated within the SAP standard development process.







Security Monitoring

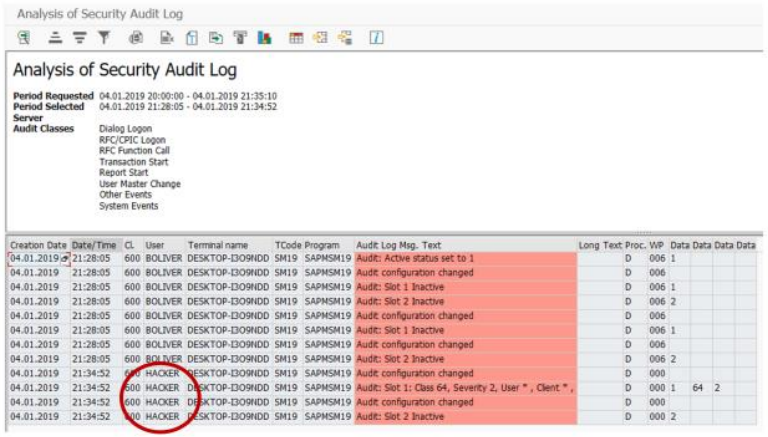
Security Monitoring

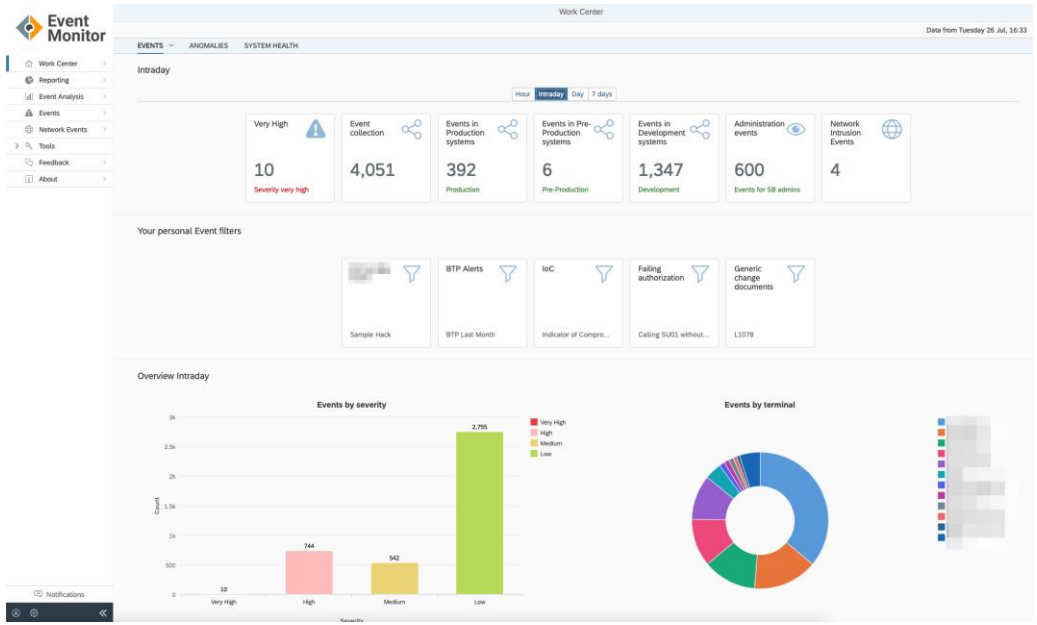
Monitoring what is happening right now in your SAP systems is something that every organization needs to be doing.

You need to look at this from an “I’ve been hacked” perspective.

While it’s important to monitor who ran what transactions in SAP and who created what POs, etc. your security team needs to know more about what’s happening in your SAP systems, which includes (but not limited to):

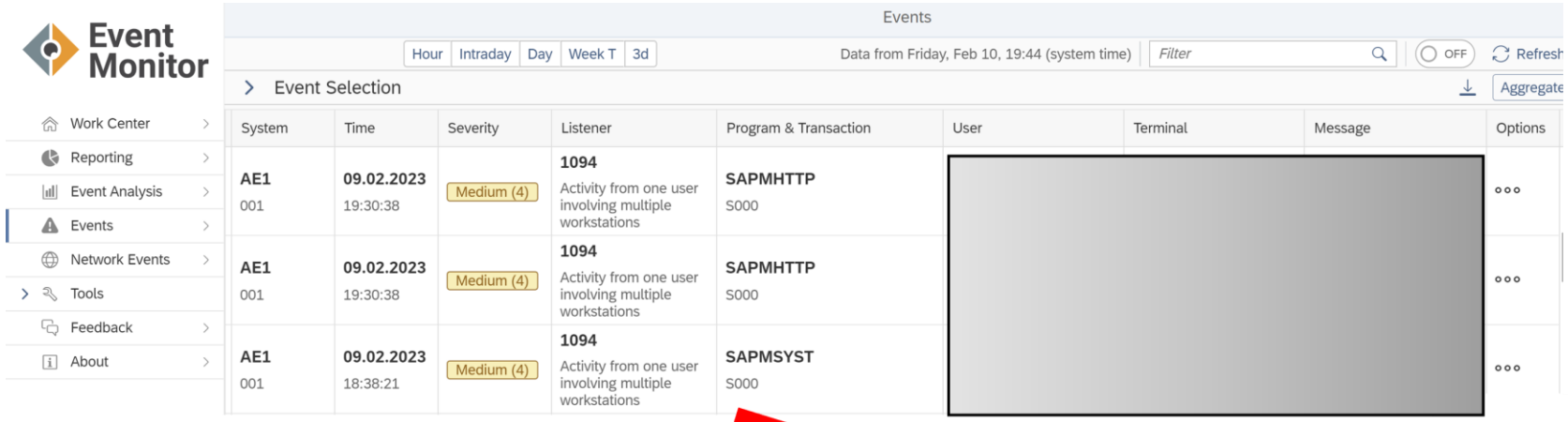
- Failed Logins from unknown accounts
- Debugging activated (in production systems)
- Security Audit Log changes (turn off, change scope of logging, etc.)
- Download critical tables
- Mass changes to critical tables
- Digital signature error
- RFC Callback rejected
- Suspicious HTTP calls

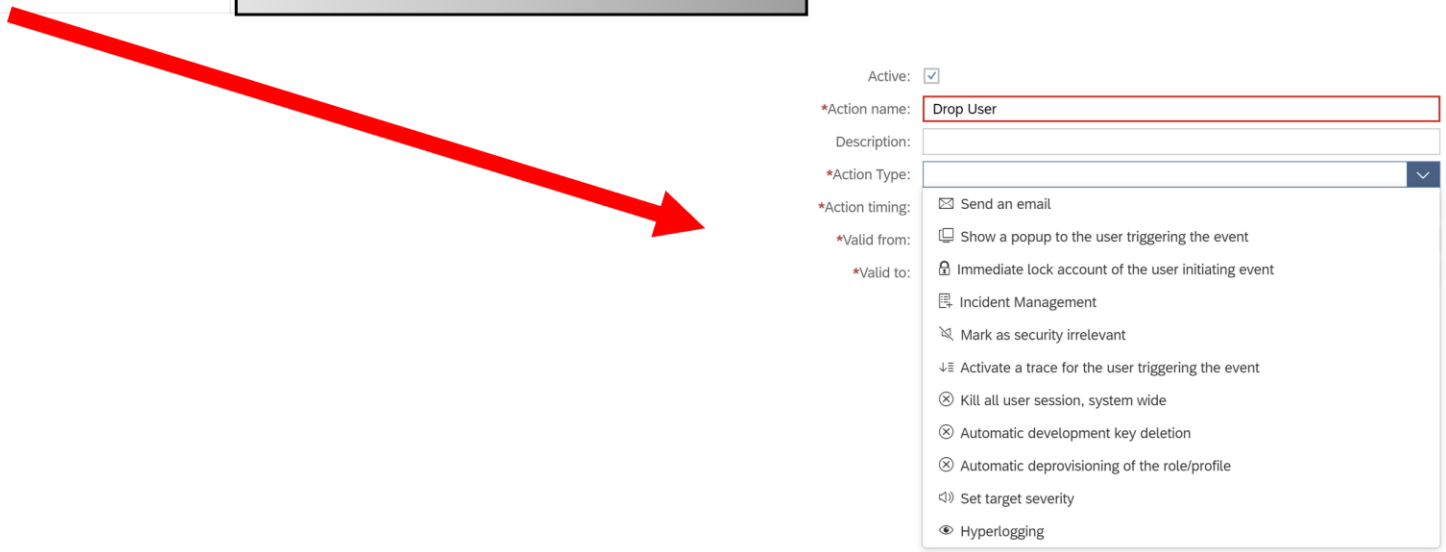




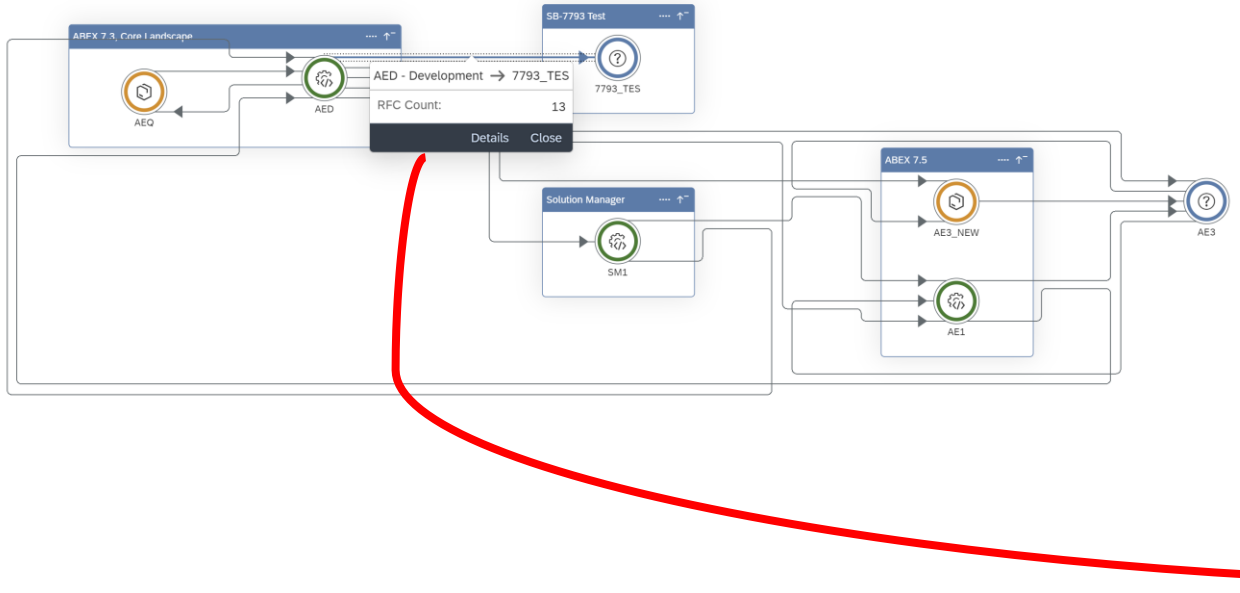
Now what ?

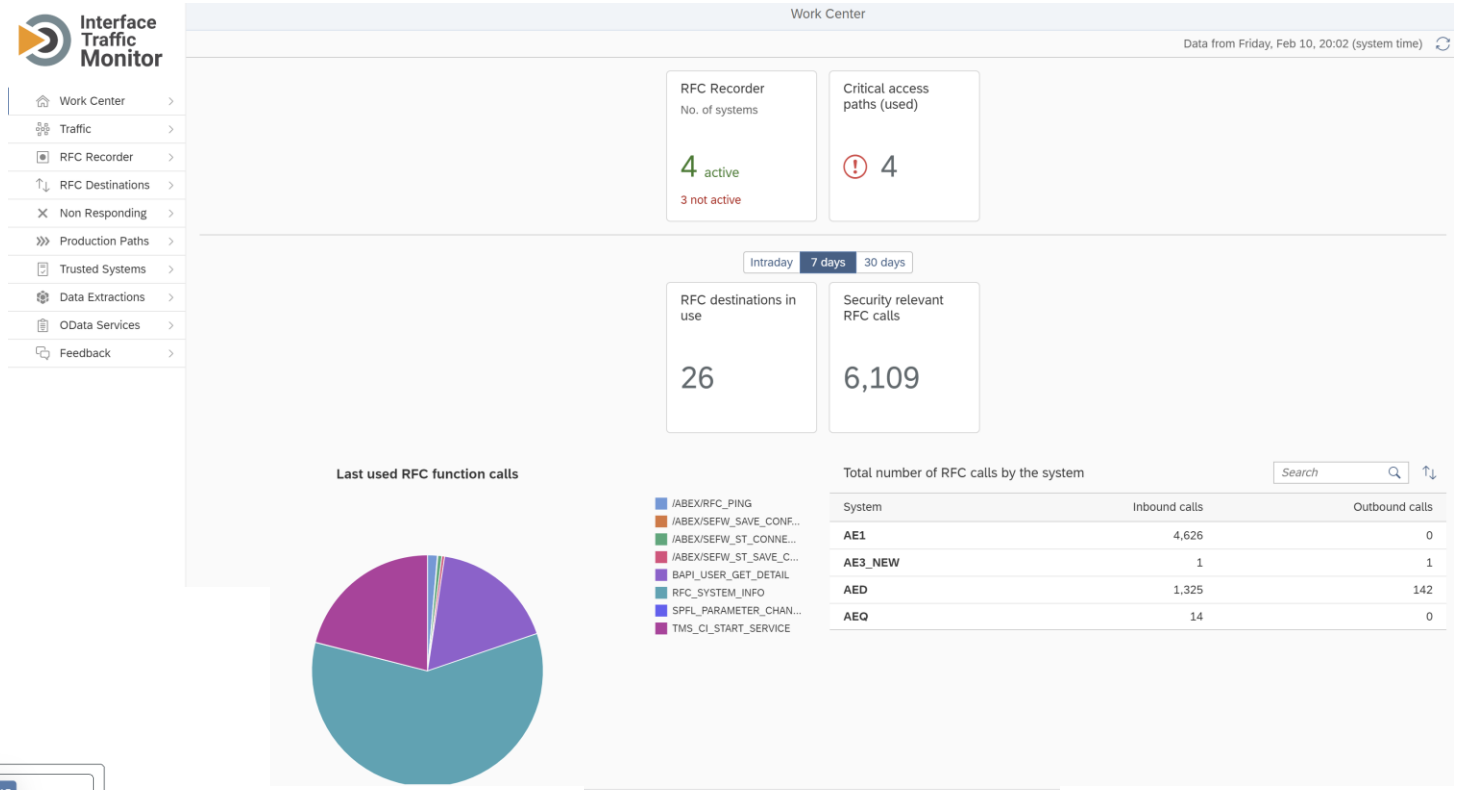
There will be times you don't want to just see it happen; you want to take action !

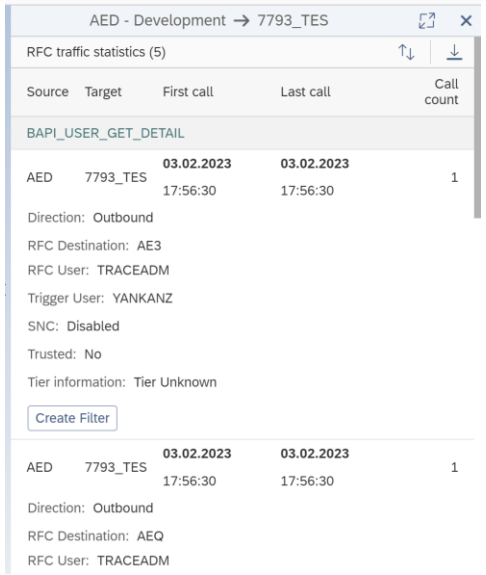




Where is all my data going ?



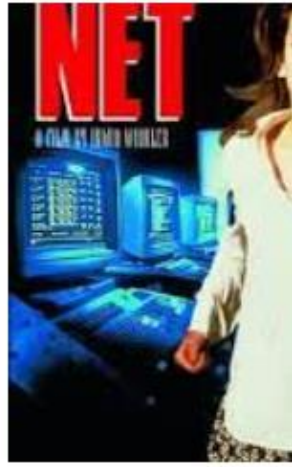


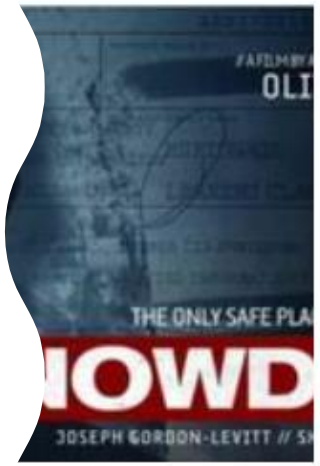


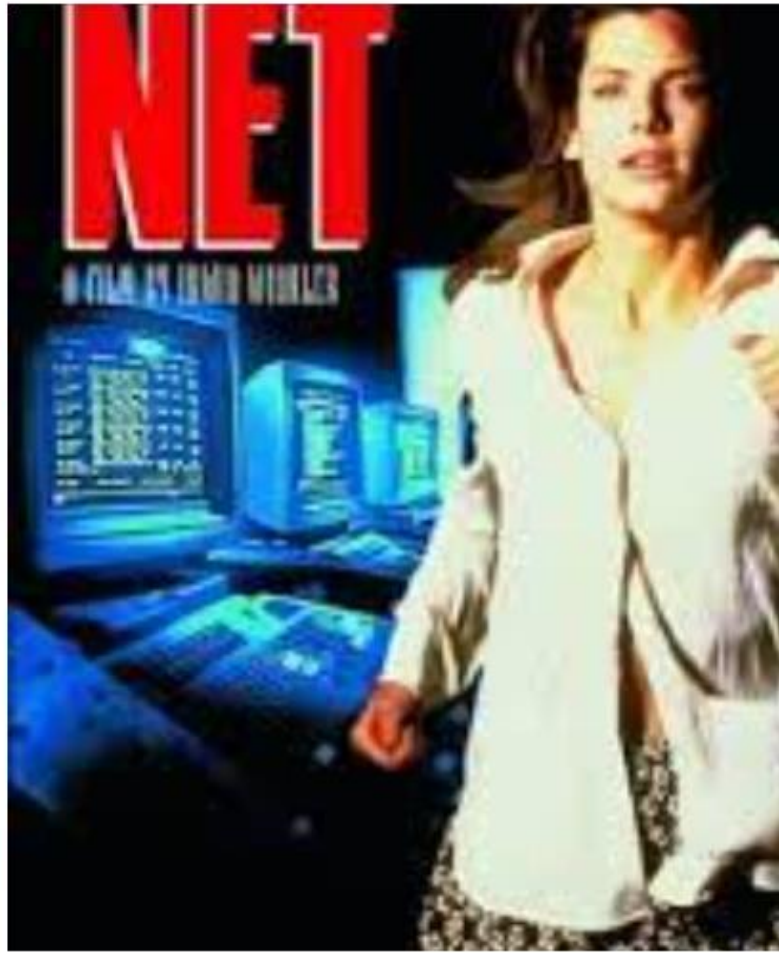
Lonza’s

SAP Cybersecurity Journey

Interested in Cybersecurity ?







Depth and Breadth

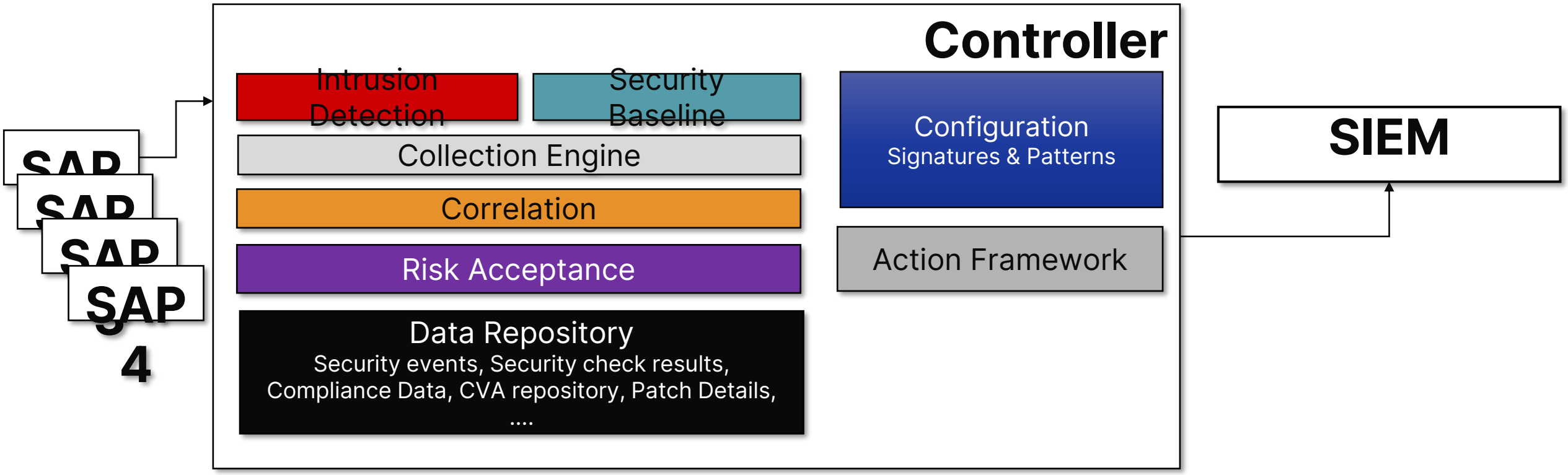
Cybersecurity

Identity and Access Management

Data Protection and Privacy

Risk and Compliance

Implementation at Lonza



Event Monitor

Security & Compliance

Patch Management

Code Vulnerability Analyzer

Implementation Challenges

Sync with system owners
Identifying critical data, obsolete clients, automated processes.

Low disk space
SAP Security Audit logs consume disk space.

Flooding SIEM solution
Approx. 10,000+ events recorded per day.

Remediation of vulnerable ABAP code
Multiple lines of vulnerable ABAP code.
Testing ABAP code changes is time consuming.

Remediation of vulnerable RFC connections
Testing authorizations for RFC connections is time consuming

Implementing Patches & Security notes
Involvement of multiple teams depending on security notes

Baby Steps

Dave Ramsey's Financial University

"Baby Steps to Financial Security"

What about SAP Cybersecurity?

Baby Step 1 – Know your System

Inventory Tracking

- Determine complete inventory of SAP systems.
- Determine Operating System , databases, application servers associated with SAP systems.
- Determine SAP system landscape, systems and clients with critical data to prioritize risk management.

Review existing policies for data lifecycle management, risk management, disaster recovery, incident management..

Review impact of activation of the SAP security audit log including disk space with appropriate stakeholders.

Baby Step 2 - Baselines

Create an SAP Security Baseline with minimum recommended security requirements for ABAP, JAVA, HANA and Cloud based SAP Systems.

Create a policy for risk assessment of vendor software or tools related to SAP.

Create a policy to validate any new SAP systems against SAP security baselines.

Baby Step 3 – System Monitoring

Create a policy for Incident management for SAP.

Approach to Implement System Monitoring

1st Phase - Detect Privilege escalation

Activate listeners to determine unauthorized changes to user master data.

Activate listeners to determine unauthorized changes to system configuration.

Push security events to SIEM system for 24/7 monitoring.

2nd Phase – Detect Lateral Movement

Activate listeners to record RFC traffic for critical calls.

Create filters to reduce noise for known traffic

3rd Phase - Detect data leakage

Activate listeners to record download of critical data

Baby Step 4 – Interface Management

Create a policy which includes minimum security requirements for applications which require interface to SAP.

Create a policy which includes minimum security requirements for creation of RFC users.

Determine and remediate vulnerable RFC connections.

Baby Step 5 – Security & Compliance Management

Implement security configurations changes as per minimum security requirements provided in SAP Security baseline.

Implement MFA for critical transactions and Power users

Educate end users on SAP Cyber hygiene and fraud prevention

Baby Step 6 – ABAP Code Vulnerability

- Create a policy for data lifecycle management of ABAP code.
- Create a policy for remediation of vulnerable code.
- Provide training to developers to remediate vulnerable code
- Approach to Code Vulnerability Scan
  - Plan remediation of ABAP vulnerabilities identified using SAST tool.
  - Scan future transports for code vulnerabilities.
- Activate listeners to monitor dynamically generated programs in non-development systems.

Baby Step 7 – Patch Management

Create a policy for implementation of Security patches and notes.

Approach to implement Patch Management

1st Phase – Identification

Review status of implementation of SAP patches & security notes.

2nd Phase – Remediation

Setup monthly meetings to review and implement SAP security notes

Develop remediation plan to patch SAP systems.

Where to Find More Information

https://www.securityweek.com/critical-sap-vulnerability-allows-supply-chain-attacks/

- Critical SAP Vulnerability Allows Supply Chain Attacks

https://www.abex.io/advisory

- SAP Security Advisories

SAP Cybersecurity interview with ChatGPT (sapinsider.org)

https://www.cybersecuritydive.com/news/sap-vulnerabilities-urgent-patching/618647/

- Critical SAP Vulnerabilities spur CISA, researcher pleas for urgent patching

Global Risks Report 2024 | World Economic Forum | World Economic Forum (weforum.org)

- Global Risk Report 2024 – World Economic Forum

https://securitybridge.com/security-news/what-is-the-sap-cyber-risk-appetite/

- What is Cyber Risk Appetite

https://www.cpomagazine.com/cyber-security/hackers-exploit-known-sap-security-vulnerabilities-with-a-typical-cyber-attack-succeeding-in-record-time/

- Hackers exploit SAP security vulnerabilities to bypass compliance control and commit fraud

Key Points to Take Home

You are the target; bad people want in!

Hackers are getting in, and the IoT is just going to make that easier

Monitoring what's going on (you will learn more about your SAP system then you ever imagined)

Communication is key – management must understand the risk

Patch Management (Security) no more later/back burner

Custom code is a risk – you need to make sure you have it covered

You need to know where you stand – the first step is always the hardest – **BABY STEPS**

Thank you! Any Questions?

Bill Oliver - bill.oliver@securitybridge.com

https://twitter.com/_securitybridge

https://de.linkedin.com/company/securitybridge

Nipun Mahajan - nipun.mahajan@lonza.com

Please remember to complete your session evaluation.

SAPinsider

SAPinsider.org

PO Box 982Hampstead, NH 03841

SAPinsider comprises the largest and fastest growing SAP membership group with more than 800,000 members worldwide.