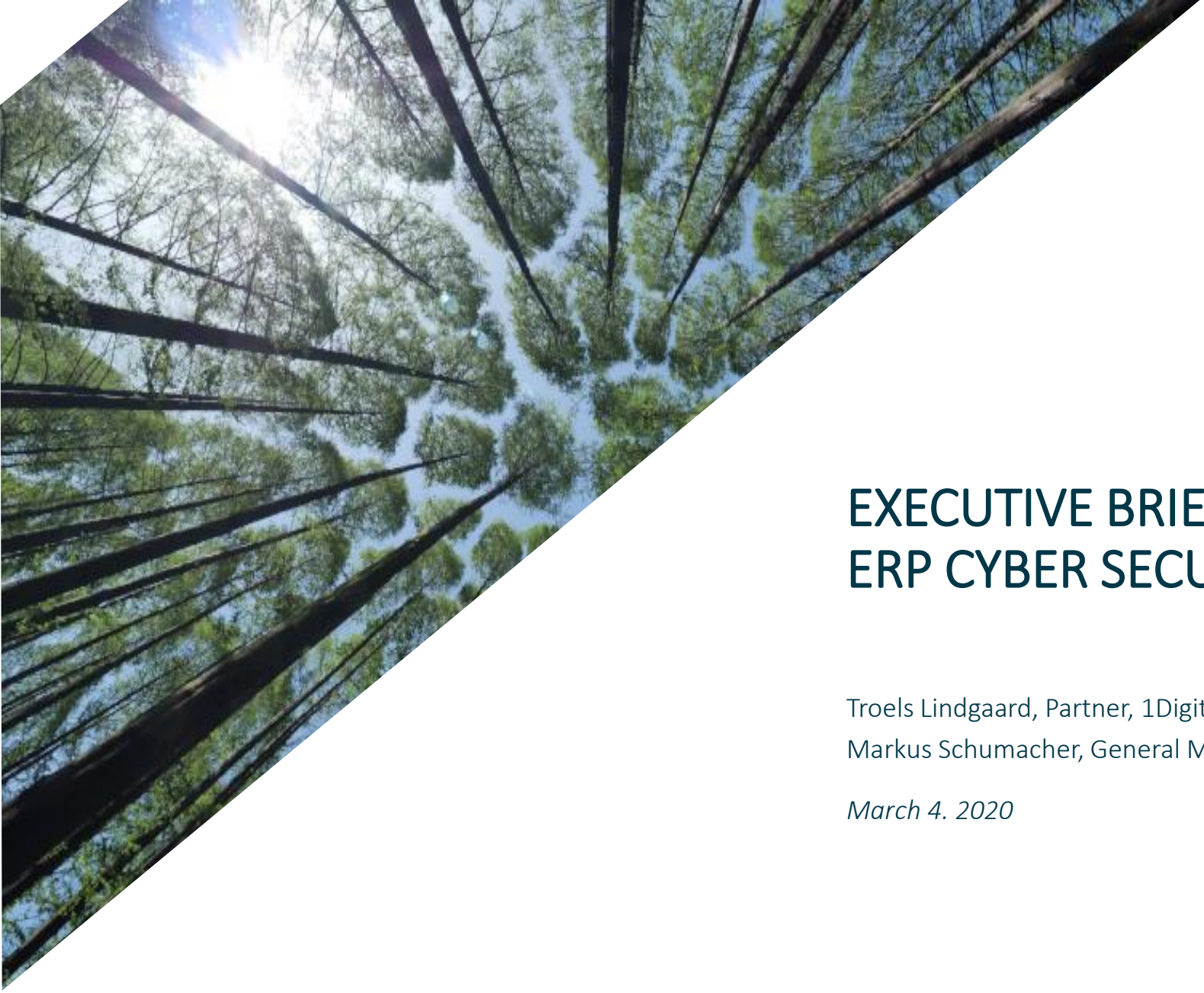


EXECUTIVE BRIEFING
ERP CYBER SECURITY

Troels Lindgaard, Partner, 1DigitalTrust
Markus Schumacher, General Manager Europe, Onapsis Inc.

March 4. 2020

AGENDA

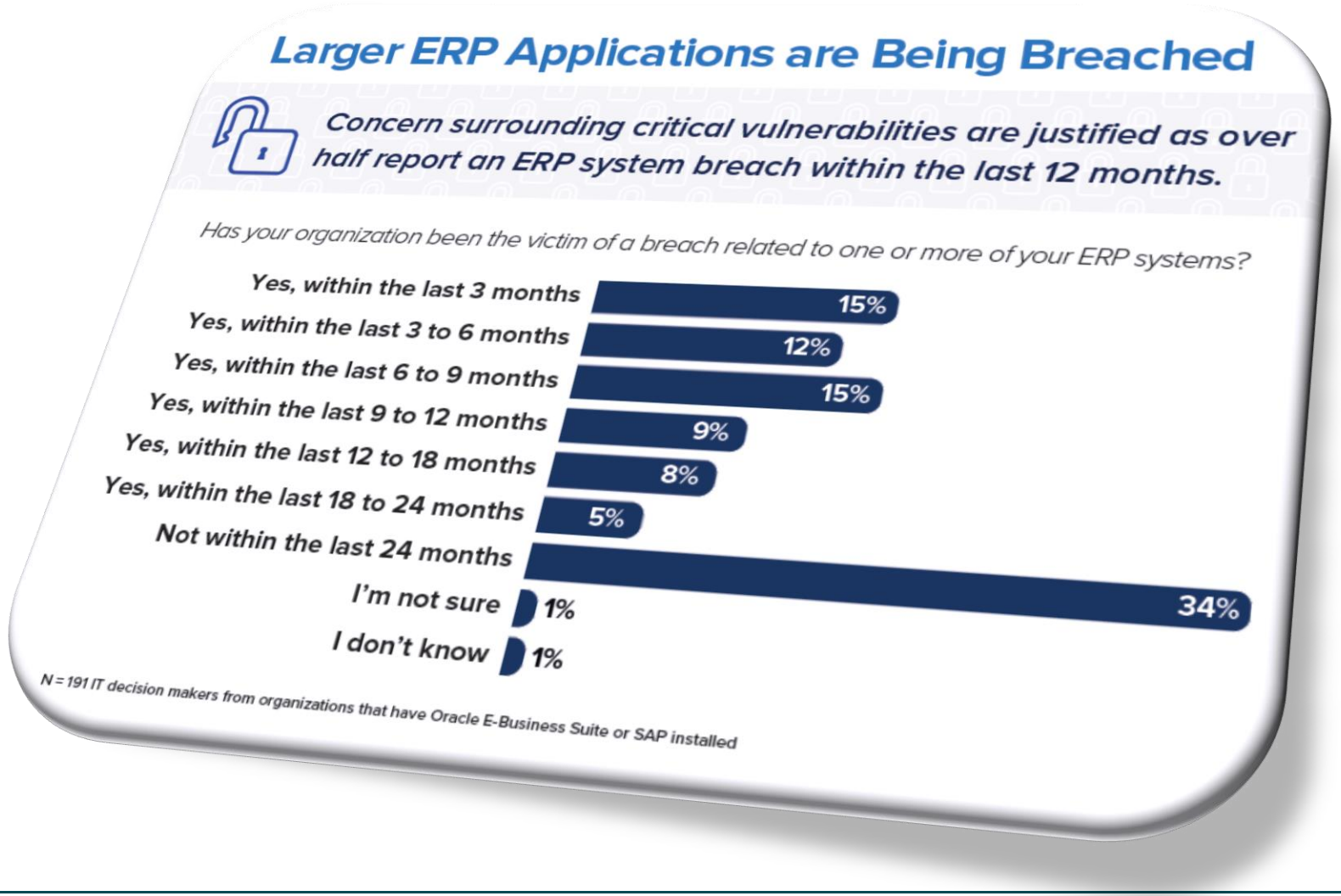
Risks

- Profit
- Share price
- Data integrity
- Operation

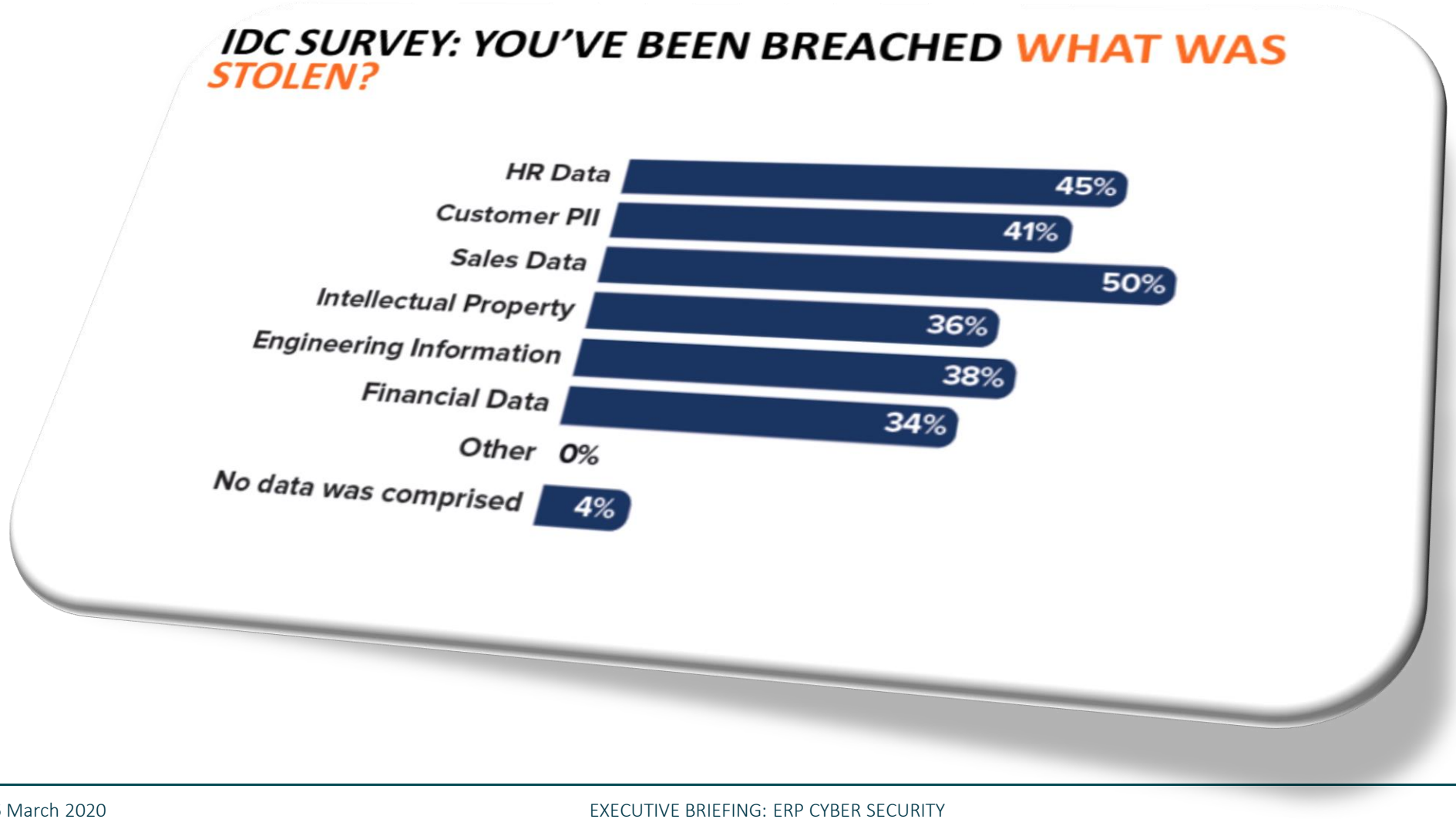
Business case

- Avoid profit loss
- Avoid share price decline
- No downtime

ERP BREACHES ARE NOT HAPPENING?



BUSINESS RISKS – DATA INTEGRITY – LOSS OF AUDIT TRAIL AND DATA RELIABILITY



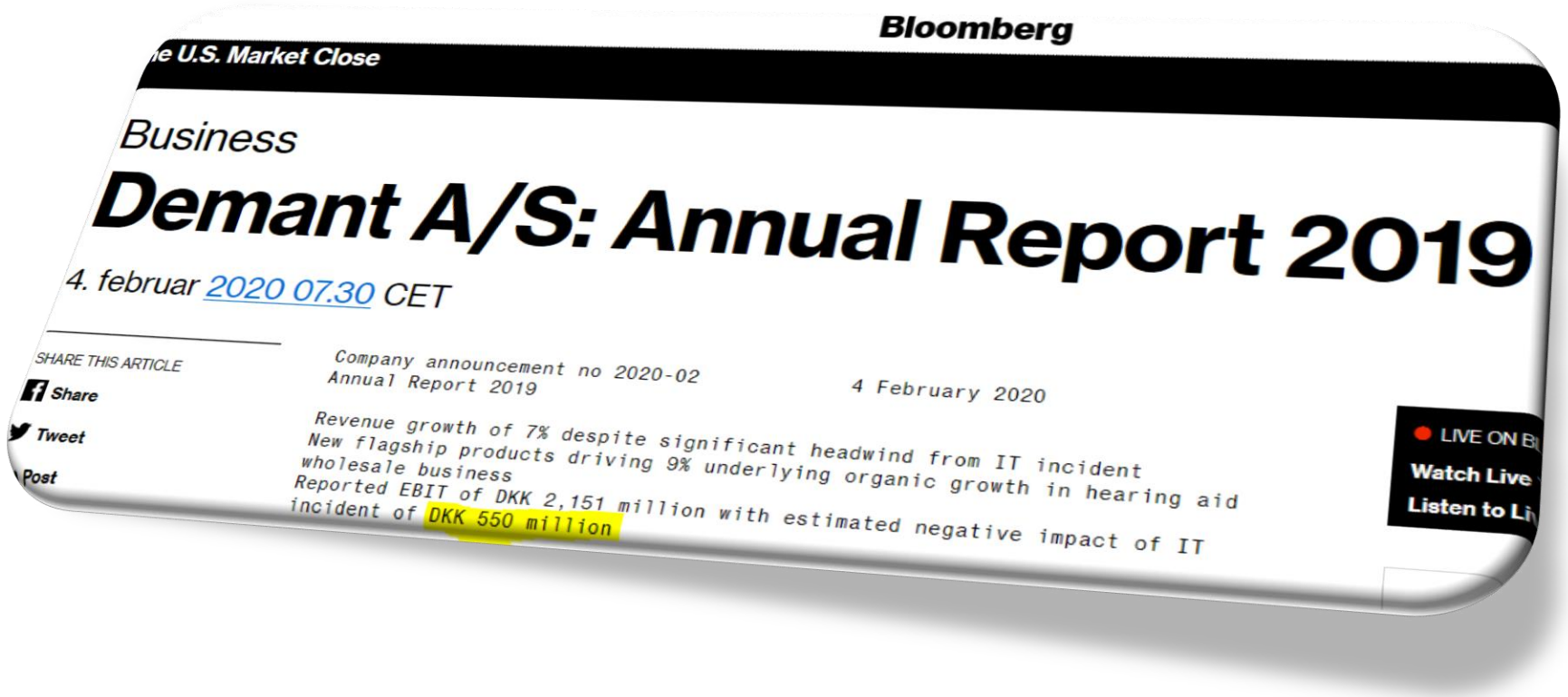
BUSINESS RISKS – PROFITS

- Profits decrease when attack is identified
  - Between 7-25% of profits

A.P. Moller – Maersk
Revenue: ~ $ 39 billion
Employees: ~ 80.000

It will also be a priority to strengthen the IT backbone and increase cyber resilience. In June, A.P. Moller - Maersk was hit by a cyber-attack that was one of the most aggressive that we and our global partners have ever experienced. The effect on profitability was USD 250-300 million, with the vast majority

8 A.P. Moller - Maersk | Annual Report 2017



Demant A/S
Revenue: ~ $ 2,22 billion
Employees: ~ 15.000

BUSINESS RISKS - SHARE PRICE

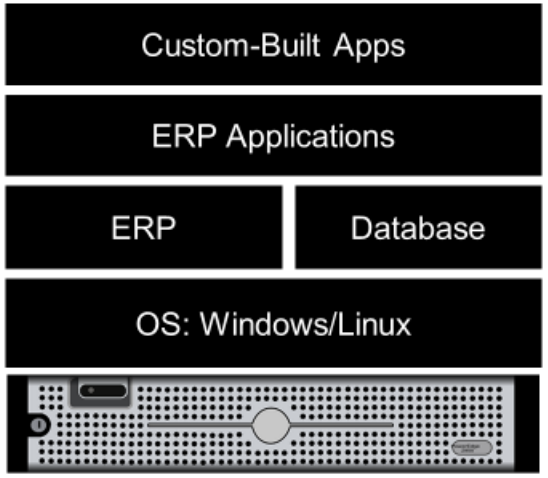
- Share price decrease
  - From 10 -30%

ISS World Services A/S
Revenue: ~ $ 10,9 billion
Employees: ~ 480.000

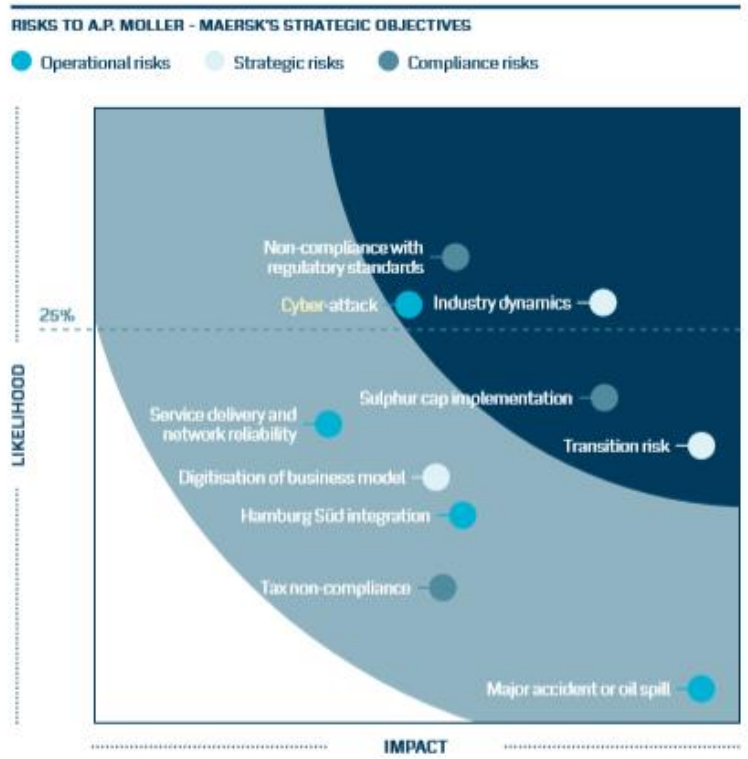
BUSINESS RISKS – NO IT SUPPORT OPERATION

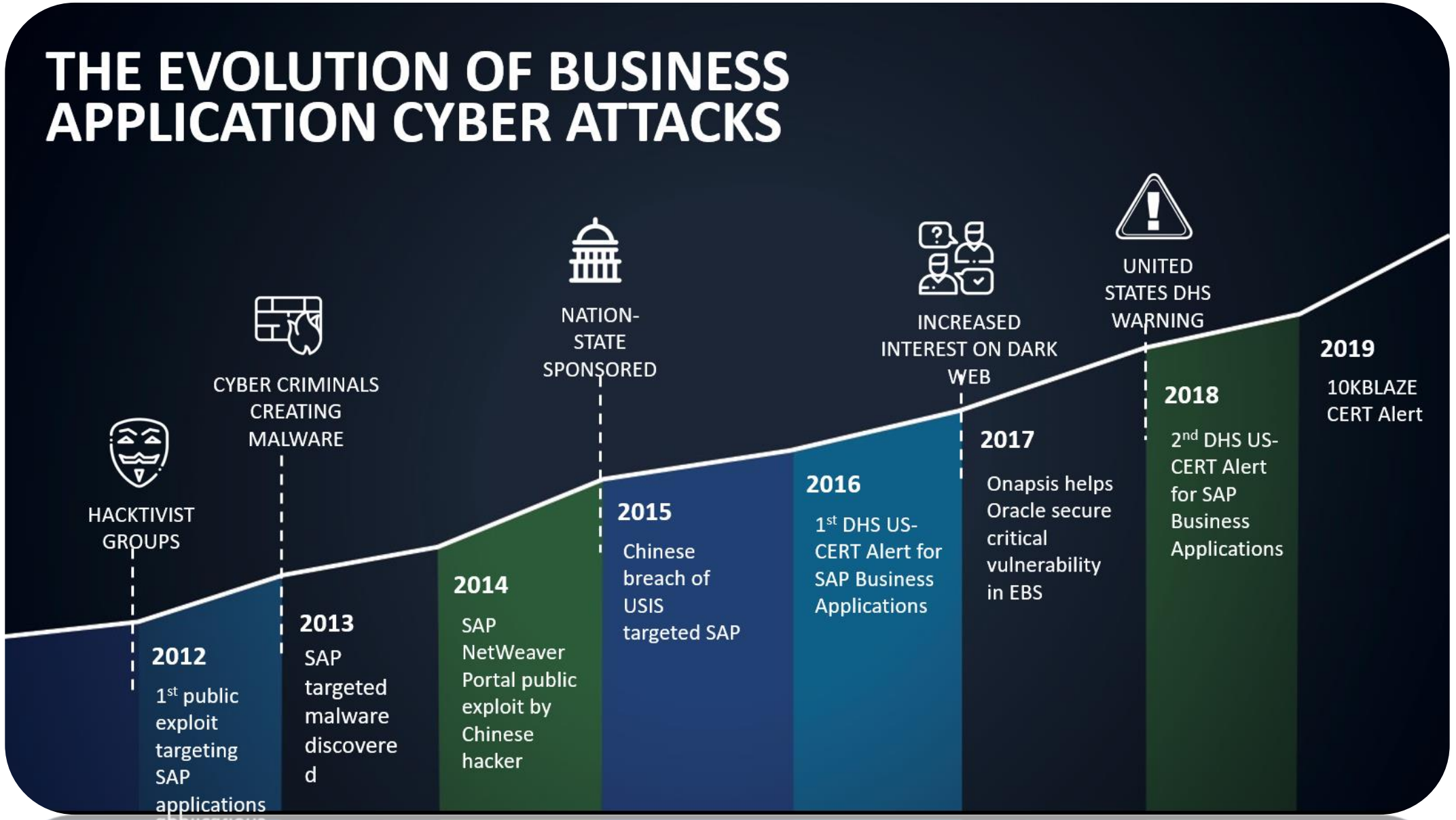
- Cyber attack has high (Highest?) impact on operation

WHAT IS ERP?
IT'S BIGGER THAN YOU THINK

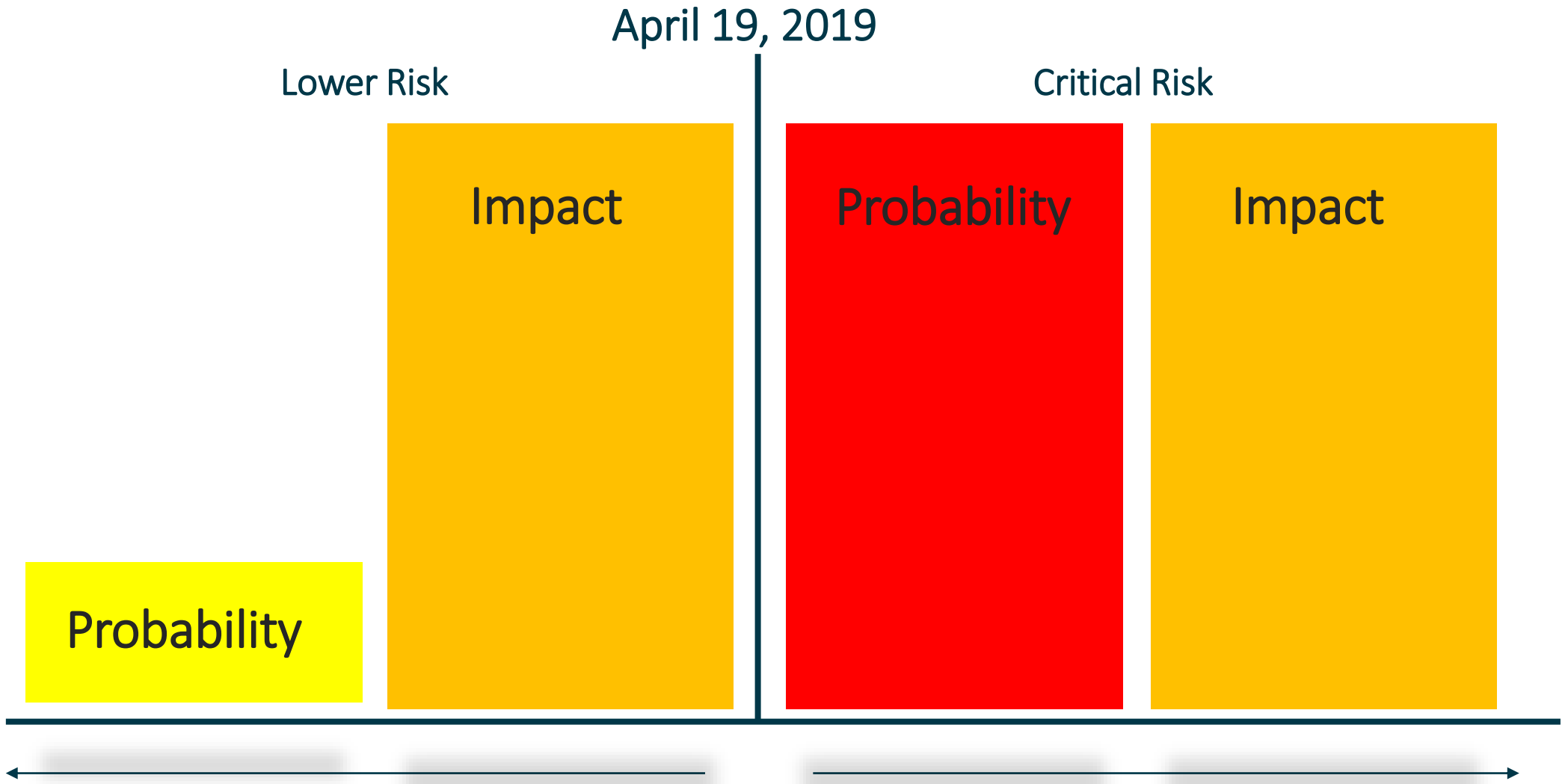


- It's not an app, it's an ecosystem
- Businesses run on SAP – critical to daily operations
- Critical business data lives there
  - PII
  - Material financial information
  - Billing/Payments
  - Pricing/Contracts
  - Banking Information
  - Intellectual Property




THE EVOLUTION OF BUSINESS APPLICATION CYBER ATTACKS
HACKTIVIST GROUPS
CYBER CRIMINALS CREATING MALWARE
NATION-STATE SPONSORED
INCREASED INTEREST ON DARK WEB
UNITED STATES DHS WARNING
2012
1st public exploit targeting SAP applications
2013
SAP targeted malware discovered
2014
SAP NetWeaver Portal public exploit by Chinese hacker
2015
Chinese breach of USIS targeted SAP
2016
1st DHS US-CERT Alert for SAP Business Applications
2017
Onapsis helps Oracle secure critical vulnerability in EBS
2018
2nd DHS US-CERT Alert for SAP Business Applications
2019
10KBLAZE CERT Alert

10KBLAZE: RISK, PROBABILITY AND IMPACT



BUSINESS CASE – AVOID PROFIT LOSS

- Average cost for ERP Cyber security protection is 0,5-1% of the profit loss

BUSINESS CASE – AVOID SHARE PRICE DECLINE

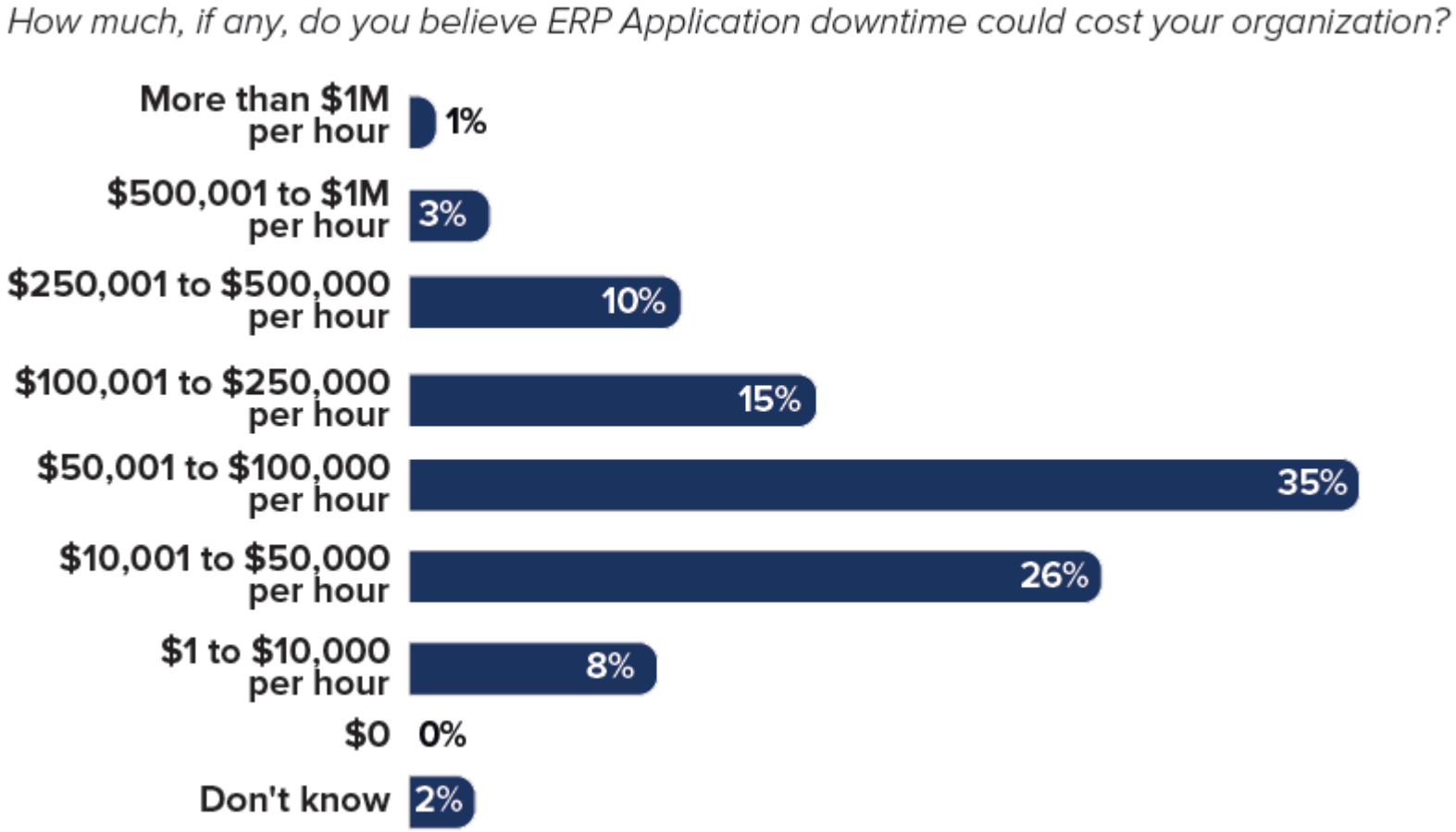
- Average cost for ERP Cyber security protection is 0,01-0,02% of the loss in market value

BUSINESS CASE – AVOID EMERGENCY AND CLEAN UP COSTS

- Average cost for ERP Cyber security protection is 0,5 - 2 % of the Emergency and clean up costs

BUSINESS CASE – NO DOWNTIME

- Cost for an ERP Cyber security system is 1-5 hours of downtime for 2/3 of companies

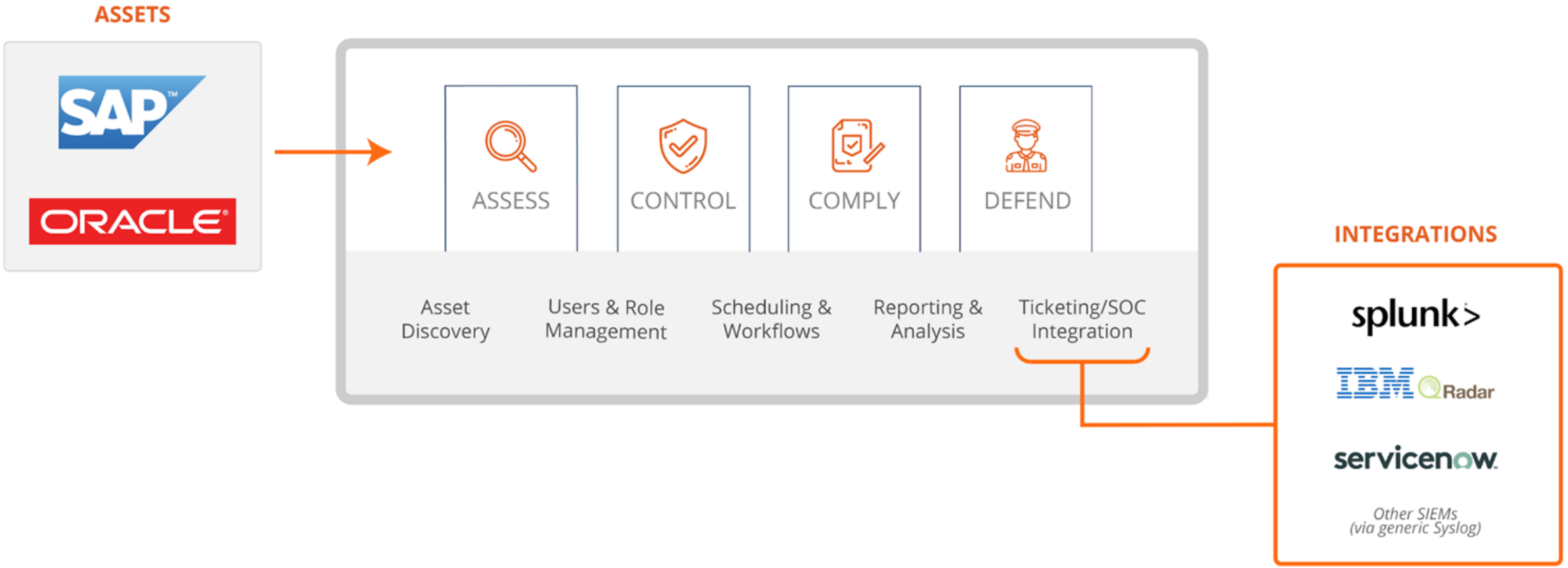


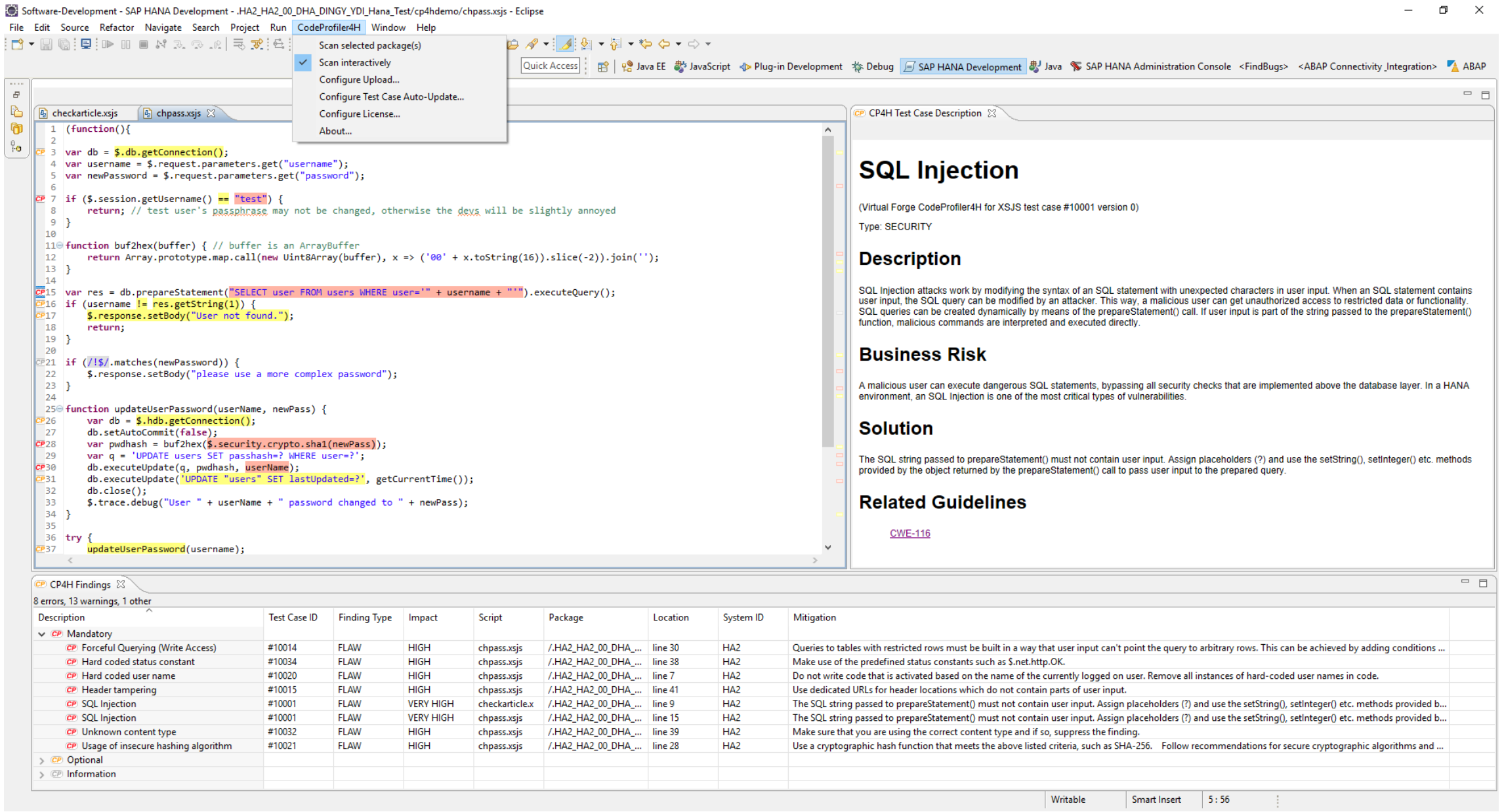
SHOULD AN ATTACK HAPPEN

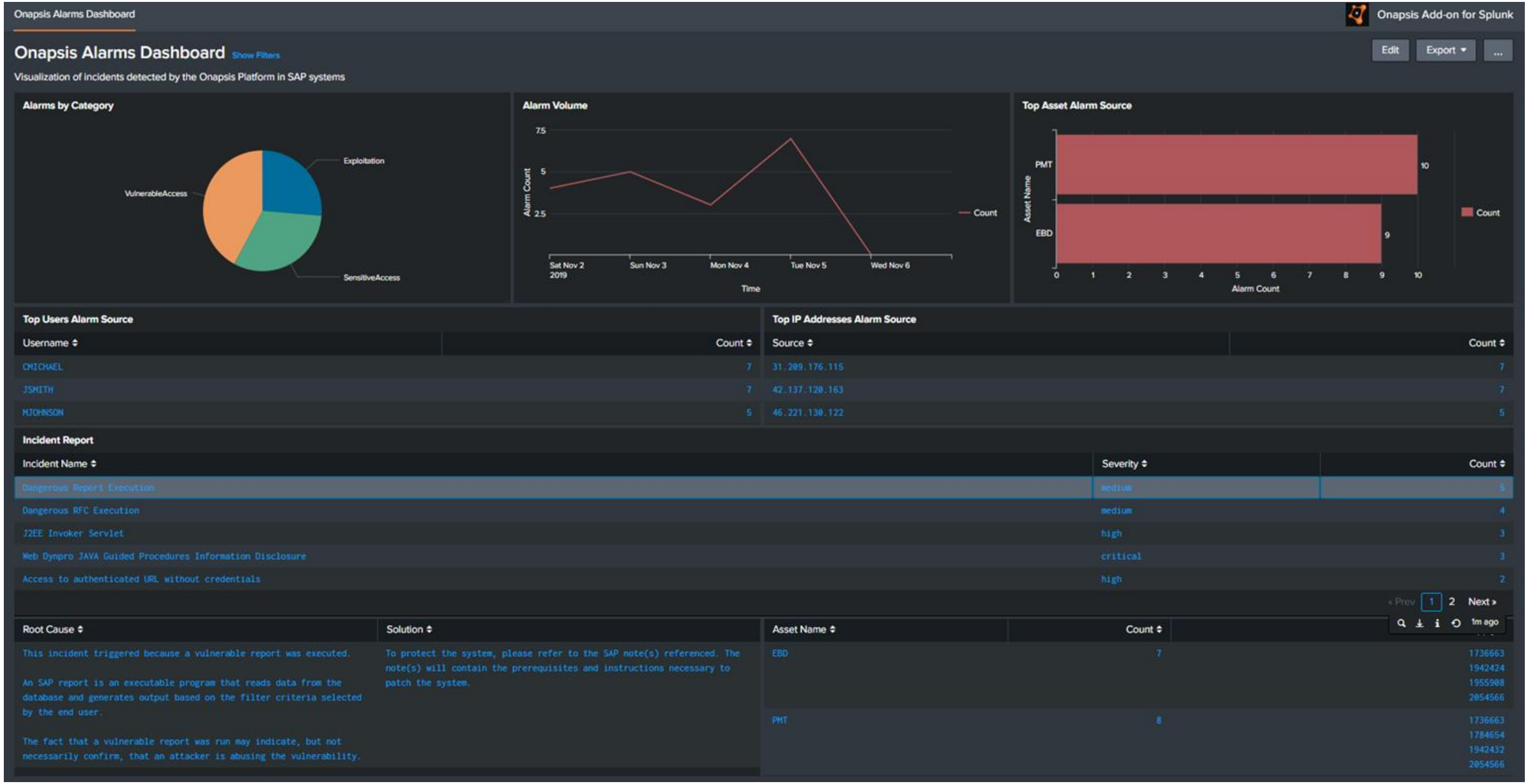
- All the risks will occur
  - Profit loss – up to 25%
  - Share price decline – up to 30%
  - Limited access to operation processes - € 100 thousands
  - Emergency and clean up costs - € millions

All the risks are calculated individually against the cost, if the combined cost of the risks are compared against the cost of running an ERP cyber security solution, which is the same for all risks, is the business case even stronger.

ONAPSIS **PLATFORM**

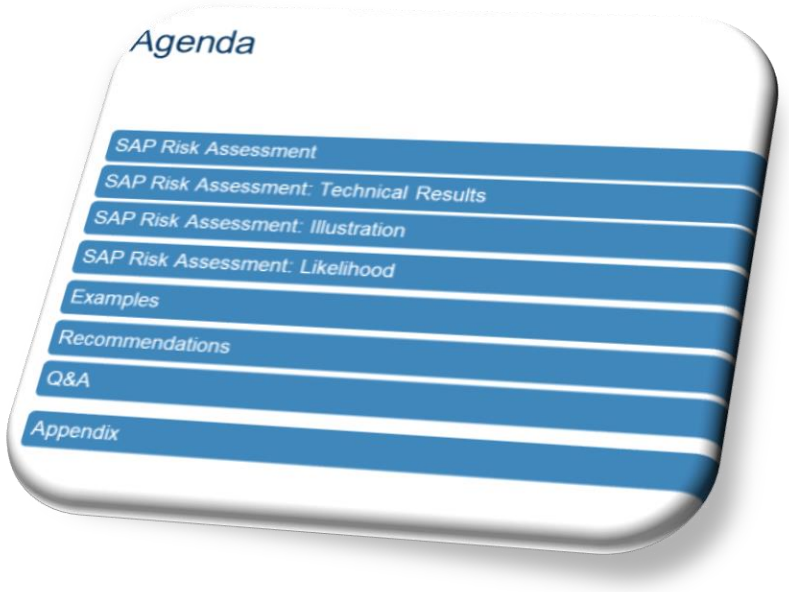



Software-Development - SAP HANA Development - .HA2_HA2_00_DHA_DINGY_YDI_Hana_Test/cp4hdemo/chpass.xsjs - Eclipse
File Edit Source Refactor Navigate Search Project Run CodeProfiler4H Window Help
Scan selected package(s)
Scan interactively
Configure Upload...
Configure Test Case Auto-Update...
Configure License...
About...
checkarticle.xsjs
chpass.xsjs
(function(){
var db = $.db.getConnection();
var username = $.request.parameters.get("username");
var newPassword = $.request.parameters.get("password");
if ($.session.getUsername() == "test") {
return; // test user's passphrase may not be changed, otherwise the devs will be slightly annoyed
}
function buf2hex(buffer) { // buffer is an ArrayBuffer
return Array.prototype.map.call(new Uint8Array(buffer), x => ('00' + x.toString(16)).slice(-2)).join('');
}
var res = db.prepareStatement("SELECT user FROM users WHERE user='" + username + "'").executeQuery();
if (username != res.getString(1)) {
$.response.setBody("User not found.");
return;
}
if (/!$/.matches(newPassword)) {
$.response.setBody("please use a more complex password");
}
function updateUserPassword(userName, newPass) {
var db = $.hdb.getConnection();
db.setAutoCommit(false);
var pwdhash = buf2hex($.security.crypto.sha1(newPass));
var q = 'UPDATE users SET passhash=? WHERE user=?';
db.executeUpdate(q, pwdhash, userName);
db.executeUpdate('UPDATE "users" SET lastUpdated=?', getCurrentTime());
db.close();
$.trace.debug("User " + userName + " password changed to " + newPass);
}
try {
updateUserPassword(username);
CP4H Test Case Description
SQL Injection
(Virtual Forge CodeProfiler4H for XSJS test case #10001 version 0)
Type: SECURITY
Description
SQL Injection attacks work by modifying the syntax of an SQL statement with unexpected characters in user input. When an SQL statement contains user input, the SQL query can be modified by an attacker. This way, a malicious user can get unauthorized access to restricted data or functionality. SQL queries can be created dynamically by means of the prepareStatement() call. If user input is part of the string passed to the prepareStatement() function, malicious commands are interpreted and executed directly.
Business Risk
A malicious user can execute dangerous SQL statements, bypassing all security checks that are implemented above the database layer. In a HANA environment, an SQL Injection is one of the most critical types of vulnerabilities.
Solution
The SQL string passed to prepareStatement() must not contain user input. Assign placeholders (?) and use the setString(), setInteger() etc. methods provided by the object returned by the prepareStatement() call to pass user input to the prepared query.
Related Guidelines
CWE-116
CP4H Findings
8 errors, 13 warnings, 1 other
Description | Test Case ID | Finding Type | Impact | Script | Package | Location | System ID | Mitigation
Mandatory
Forceful Querying (Write Access) | #10014 | FLAW | HIGH | chpass.xsjs | /.HA2_HA2_00_DHA_... | line 30 | HA2 | Queries to tables with restricted rows must be built in a way that user input can't point the query to arbitrary rows. This can be achieved by adding conditions ...
Hard coded status constant | #10034 | FLAW | HIGH | chpass.xsjs | /.HA2_HA2_00_DHA_... | line 38 | HA2 | Make use of the predefined status constants such as $.net.http.OK.
Hard coded user name | #10020 | FLAW | HIGH | chpass.xsjs | /.HA2_HA2_00_DHA_... | line 7 | HA2 | Do not write code that is activated based on the name of the currently logged on user. Remove all instances of hard-coded user names in code.
Header tampering | #10015 | FLAW | HIGH | chpass.xsjs | /.HA2_HA2_00_DHA_... | line 41 | HA2 | Use dedicated URLs for header locations which do not contain parts of user input.
SQL Injection | #10001 | FLAW | VERY HIGH | checkarticle.x | /.HA2_HA2_00_DHA_... | line 9 | HA2 | The SQL string passed to prepareStatement() must not contain user input. Assign placeholders (?) and use the setString(), setInteger() etc. methods provided b...
SQL Injection | #10001 | FLAW | VERY HIGH | chpass.xsjs | /.HA2_HA2_00_DHA_... | line 15 | HA2 | The SQL string passed to prepareStatement() must not contain user input. Assign placeholders (?) and use the setString(), setInteger() etc. methods provided b...
Unknown content type | #10032 | FLAW | HIGH | chpass.xsjs | /.HA2_HA2_00_DHA_... | line 39 | HA2 | Make sure that you are using the correct content type and if so, suppress the finding.
Usage of insecure hashing algorithm | #10021 | FLAW | HIGH | chpass.xsjs | /.HA2_HA2_00_DHA_... | line 28 | HA2 | Use a cryptographic hash function that meets the above listed criteria, such as SHA-256. Follow recommendations for secure cryptographic algorithms and ...
Optional
Information
Writable
Smart Insert
5 : 56


Onapsis Alarms Dashboard
Onapsis Add-on for Splunk
Onapsis Alarms Dashboard
Show Filters
Edit
Export
...
Visualization of incidents detected by the Onapsis Platform in SAP systems
Alarms by Category
Exploitation
VulnerableAccess
SensitiveAccess
Alarm Volume
7.5
5
2.5
Alarm Count
Count
Sat Nov 2 2019
Sun Nov 3
Mon Nov 4
Tue Nov 5
Wed Nov 6
Time
Top Asset Alarm Source
PMT
EBD
10
9
Asset Name
Count
0 1 2 3 4 5 6 7 8 9 10
Alarm Count
Top Users Alarm Source
Username
Count
CMICHAEL 7
JSMITH 7
MJOHNSON 5
Top IP Addresses Alarm Source
Source
Count
31.209.176.115 7
42.137.120.163 7
46.221.130.122 5
Incident Report
Incident Name
Severity
Count
Dangerous Report Execution medium 5
Dangerous RFC Execution medium 4
J2EE Invoker Servlet high 3
Web Dynpro JAVA Guided Procedures Information Disclosure critical 3
Access to authenticated URL without credentials high 2
« Prev 1 2 Next »
1m ago
Root Cause
Solution
This incident triggered because a vulnerable report was executed.
An SAP report is an executable program that reads data from the database and generates output based on the filter criteria selected by the end user.
The fact that a vulnerable report was run may indicate, but not necessarily confirm, that an attacker is abusing the vulnerability.
To protect the system, please refer to the SAP note(s) referenced. The note(s) will contain the prerequisites and instructions necessary to patch the system.
Asset Name
Count
EBD 7
1736663
1942424
1955908
2054566
PMT 8
1736663
1784654
1942432
2054566

CALL TO ACTION NOW: ARE YOUR ERP SYSTEMS SECURE?

- Get an assessment of your ERP system – **Business Risk Illustration** (BRI)
  - € 15.000
  - Executive Overview
    - 1) do you have known risks? and 2) next steps
    - Rules of engagement
      - Senior level commitment
      - Technical verification of findings (do we have it: yes/no)
      - Discuss outcome (risk to the business) and next steps



- Nordic ERP Cyber security campaign
  - First Nordic customer to sign up in 2020 will get 50% discount

Leading ERP Cyber security vendor for SAP and Oracle
+300 customers incl. Ericsson, Mölnlycke, Sanofi

Donnie M. Lund
E: Donnie.Lund@1digitaltrust.com
M: +45 4110 8909

Sarmad Reda
E: Sarmad.Reda@1digitaltrust.com
M: +45 5219 5118

Stefan A. Sønderup
E: Stefan.Soenderup@1digitaltrust.com
M: +45 5140 7958

Thomas Bladh
E: Thomas.Bladh@1digitaltrust.com
M: +46 70-550 49 13

Troels Lindgård
E: Troels.Lindgaard@1digitaltrust.com
M: +45 5363 5787

1DigitalTrust
Kollemosevej 40B, 2830 Virum
www.1digitaltrust.com

APPENDIX

ONAPSIS PLATFORM MARKETECTURE: ONAPSIS PACKAGES

ASSESS

- Native code, interface, transport and system assessment
- Identify misconfigurations and vulnerabilities and measure business impact
- Streamline remediation of code and system vulnerabilities

CONTROL

- Manage and control change to ensure system stability and integrity
- Lock/block changes to prevent security and compliance issues
- Automated remediation of code, configurations and vulnerabilities

COMPLY

- Define, manage and run compliance policies
- Automate the continuous process of testing and validating compliance controls
- Receive alerts on compliance failures

DEFEND

- Continuous monitoring for cyberattacks, privilege misuse and material weakness
- Investigate, respond and mitigate incidents
- Automate alarm notifications and SIEM integration

Management Functionality

Reporting & Analysis | Ticketing/SOC Integration | Scheduling & Workflows | Asset Discovery | Users & Role Management