ONAPSIS

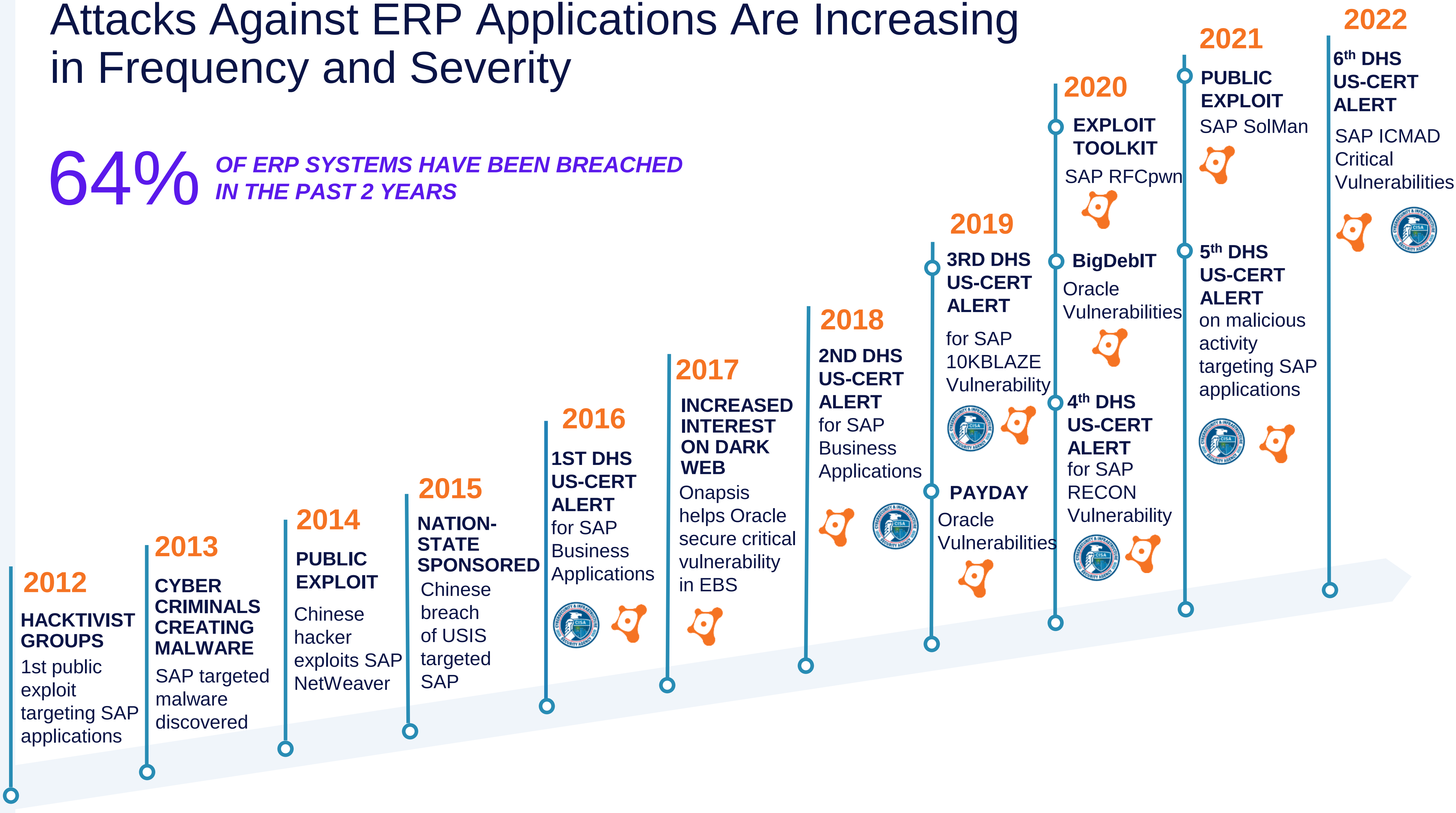
ERP Security 101: 5 Things Every Leader & Organization Should Be Doing to Secure ERP

ASUG OHIO CHAPTER EVENT

Doug Miller – Strategic Account Manager
Hector Espinoza – Senior Sales Engineer

Attacks Against ERP Applications Are Increasing in Frequency and Severity

64% *OF ERP SYSTEMS HAVE BEEN BREACHED IN THE PAST 2 YEARS*



2012
HACKTIVIST GROUPS
1st public exploit targeting SAP applications

2013
CYBER CRIMINALS CREATING MALWARE
SAP targeted malware discovered

2014
PUBLIC EXPLOIT
Chinese hacker exploits SAP NetWeaver

2015
NATION-STATE SPONSORED
Chinese breach of USIS targeted SAP

2016
1ST DHS US-CERT ALERT
for SAP Business Applications

2017
INCREASED INTEREST ON DARK WEB
Onapsis helps Oracle secure critical vulnerability in EBS

2018
2ND DHS US-CERT ALERT
for SAP Business Applications

2019
3RD DHS US-CERT ALERT
for SAP 10KBLAZE Vulnerability

PAYDAY
Oracle Vulnerabilities

2020
EXPLOIT TOOLKIT
SAP RFCpwn

BigDebIT
Oracle Vulnerabilities

4th DHS US-CERT ALERT
for SAP RECON Vulnerability

2021
PUBLIC EXPLOIT
SAP SolMan

5th DHS US-CERT ALERT
on malicious activity targeting SAP applications

2022
6th DHS US-CERT ALERT
SAP ICMAD Critical Vulnerabilities

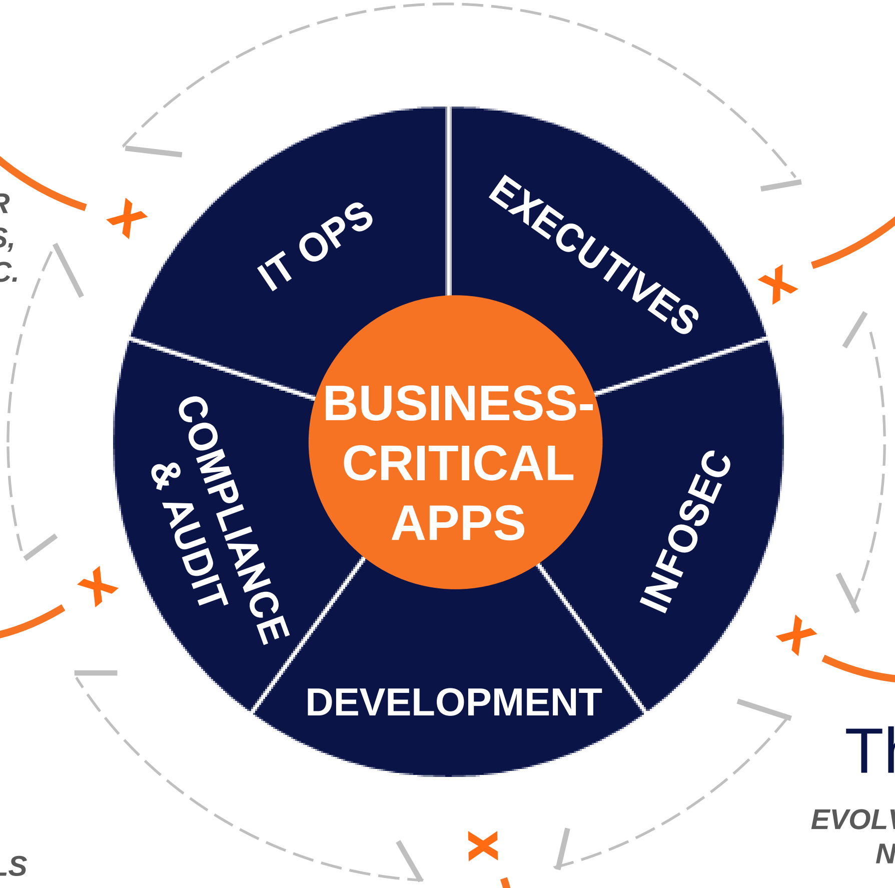
Modern Enterprises Are Facing a Perfect Storm of Complexity...

Cloud

EVAPORATING THE PERIMETER TO ENABLE REMOTE WORKERS, PARTNERS, SUPPLY CHAIN, ETC.

Digital Transformation

FREQUENTLY FAVORING EXPEDIENCY NOT SECURITY



Compliance

DRIVING STRICTER AND MORE COMPLEX CONTROLS

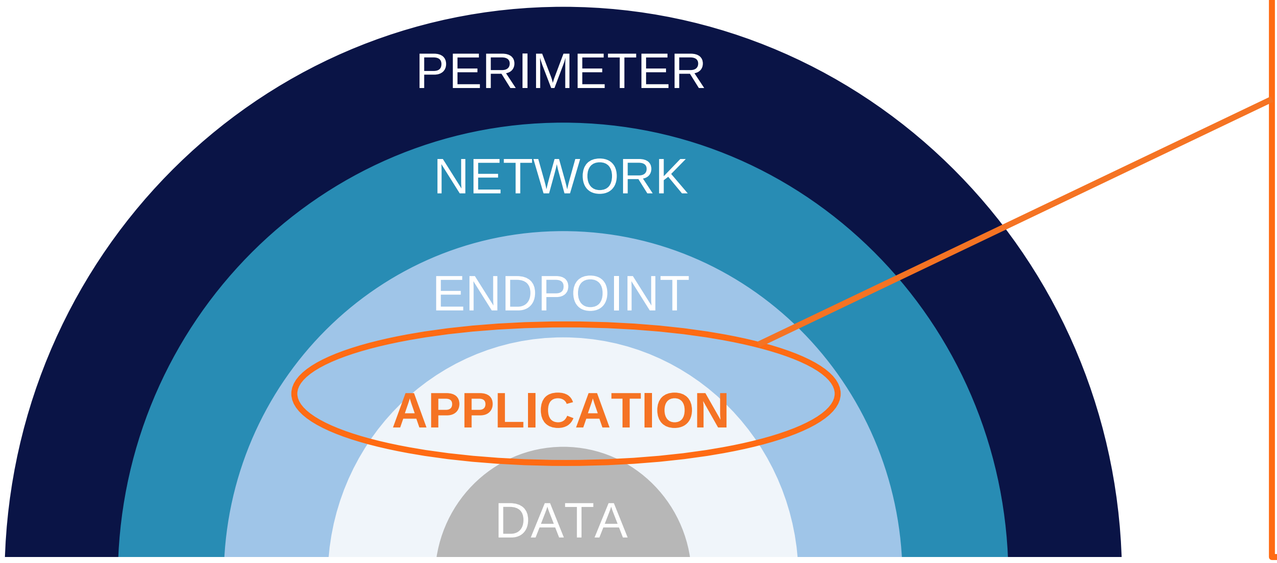
Threat Actors

EVOLVED TO TARGET MULTIPLE, NEW ATTACK VECTORS

Constant Change

DISRUPTING BUSINESS OPERATIONS

…And Are Overly Reliant on **Traditional Defense-in-Depth** Models That Surround But Don’t Secure ERP Systems



- **Attacks on the application layer** are the #1 concern of CIOs, YoY
- **Over 70%** say their application portfolio has become **more vulnerable** in the past year
- Almost **two-thirds of organizations have a backlog** of app vulnerabilities

https://www.whitesourcesoftware.com/wp-content/media/2021/04/whitesource-ponemon-research-report.pdf

This Means We May Have a Gap with Understanding The **True Risk** to Our ERP Systems…and Our Organization

Vulnerabilities?

- ERP systems are frequently managed by other teams, with little to no visibility for InfoSec
- More processes moving to SaaS applications
- Increasing reliance on code or apps developed by contracted third-parties

Threat Monitoring?

- No meaningful monitoring of ERP, with little to no visibility for the SOC
- Reliance on manual log reviews to identify threat activity in ERPs
- No ability to establish compensating controls

Code Security?

- Security is frequently “bolt on” and not “built in”
- Reliance on manual code reviews
- Problems aren’t identified until they hit production

What Happens If You Don’t Fix This?

Data Loss or Breach

74% Of breaches involved access to privileged account[1]

28% Of breaches are due to missing application patches[2]

System Outages

52% Of security events caused operational outage that affected productivity[3]

over $50k/ hour Average cost of ERP application downtime[4]

Compliance Findings

$5M Average yearly cost of business disruption due to non-compliance[5]

$2M Average yearly cost of fines and penalties due to non-compliance[5]

Project Delays

52% Of cloud migrations are delayed due to security concerns[6]

Reputation Damage

7.3% Average decrease in stock price following a security breach[7]

[1] Centrify
[2] DarkReading
[3] Fortinet
[4] Onapsis
[5] Ascent
[6] TechRepublic
[7] Forbes

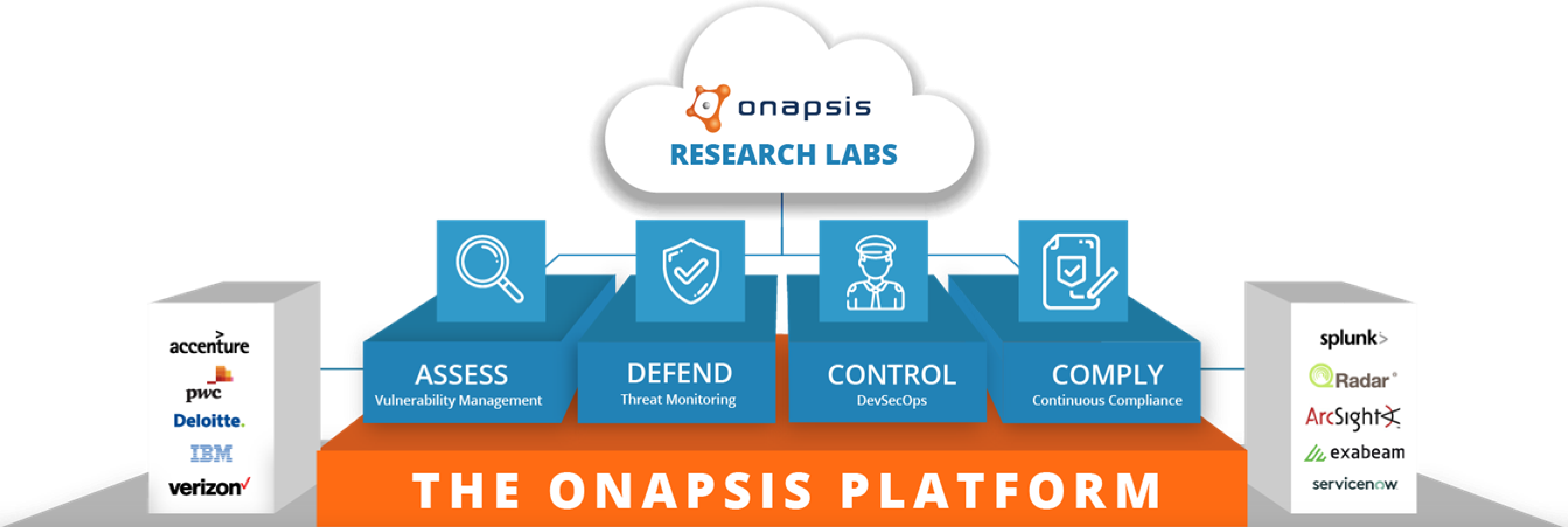
Some Questions to Ask Yourself…

- ❑ Do you have a true understanding of your real risk profile for your organization?
- ❑ Are you getting any / the right visibility into your ERP applications, such as SAP or Oracle, to help you manage risk and secure the business?
- ❑ Does your organization’s security team have the right resources who can understand “the language of ERPs”?
- ❑ Has continuous monitoring of threats (both internal and external) in the ERP application been properly established?
- ❑ Have you determined what tools should be implemented to monitor specific financial reporting systems?
- ❑ Do you have a schedule for reviewing and implementing critical security patches for your ERP applications?
- ❑ Are cybersecurity controls established for the customized code used in ERP applications for reporting?
- ❑ Is there mapping in place for key cybersecurity controls to regulation frameworks (e.g., SOX, PCI, GDPR)
- ❑ Are Audit, InfoSec and IT teams able to continually assess and test these controls to provide the right level of assurance?

…And Five Things To Do Today

1. Treat Business-Critical Apps Like OT Critical Infrastructure
2. Timely Patch Management
3. Continuous Monitoring of Vulnerabilities and Threats to Your ERP Applications
4. Secure Your Custom Code in ERP Applications
5. Commit to Control and Governance

The Onapsis Platform - Visibility and Tools To Protect Your ERP



> “Prior to using Onapsis, we were **prioritizing simple fixes and ignoring critical vulnerabilities**, of which we identified 600 in 2018. Since we started using Onapsis, we’ve **remediated 90% of those critical vulnerabilities**, and 70% of the 10,000+ total we initially discovered.” - *F100 Biotech*

> “Saves time identifying, prioritizing, and remediating security vulnerabilities. **Enables security generalists** to ensure Basis is properly maintaining SAP systems.” – F100 Tech Manufacturer

STAY AHEAD OF EVER-EVOLVING CYBERSECURITY THREATS WITH THE WORLD’S LEADING THREAT RESEARCH ON BUSINESS-CRITICAL APPLICATIONS

ONAPSIS RESEARCH LABS

- Onapsis products automatically updated with latest threat intel and security guidance
- Receive advanced notification on critical issues and improved configurations
- Get pre-patch protection ahead of scheduled vendor updates

Discovered

1,000+

zero-day vulnerabilities in business-critical apps

25%

Of critical SAP Security Notes in 2021 were influenced by Onapsis Research Labs

6

US DHS critical alerts based on our research

17

Patents, 8 issued & 9 pending

Knowledgebase of

10,000+

vulnerabilities and attacks on business applications

Fortune 500 Utility Company

COMPANY

2K Employees

$2B revenue

INDUSTRY

Energy

> ***Onapsis removes the mystery around SAP security by increasing visibility.*** *We can see ...misconfigurations, missing patches or unusual user activity - what risk they post and how to fix them*
>
> *- CISO*

CHALLENGE: A labor intensive patch and vulnerability management process created visibility and security gaps within SAP for a small team

SOLUTION: Onapsis Assess and Defend to scan and continuously monitor its SAP environment for vulnerabilities, misconfigurations, missed patches, and new threats.

RESULT: Gained visibility into SAP, including activity of third party contractors; streamlined and automated the patch and vulnerability management process, allowing the team to scale and refocus

Thank You!

@onapsis

linkedin.com/company/onapsis

ONAPSIS.COM