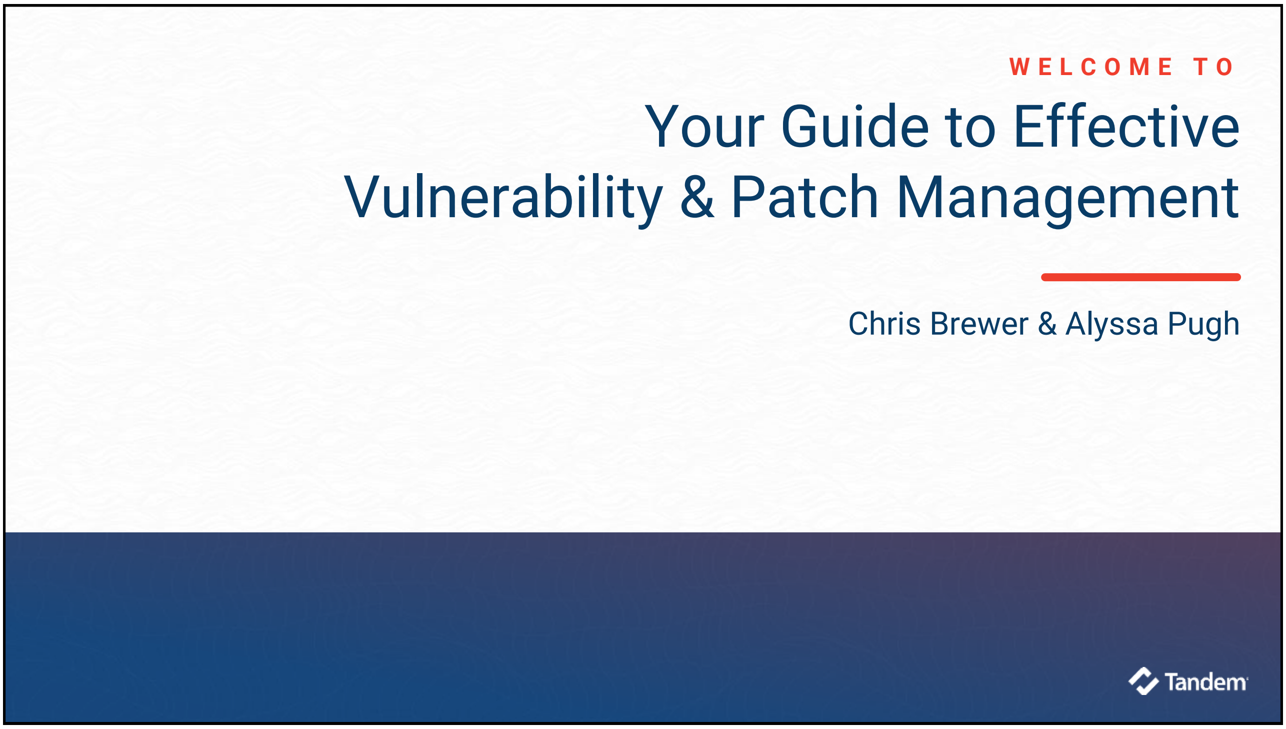


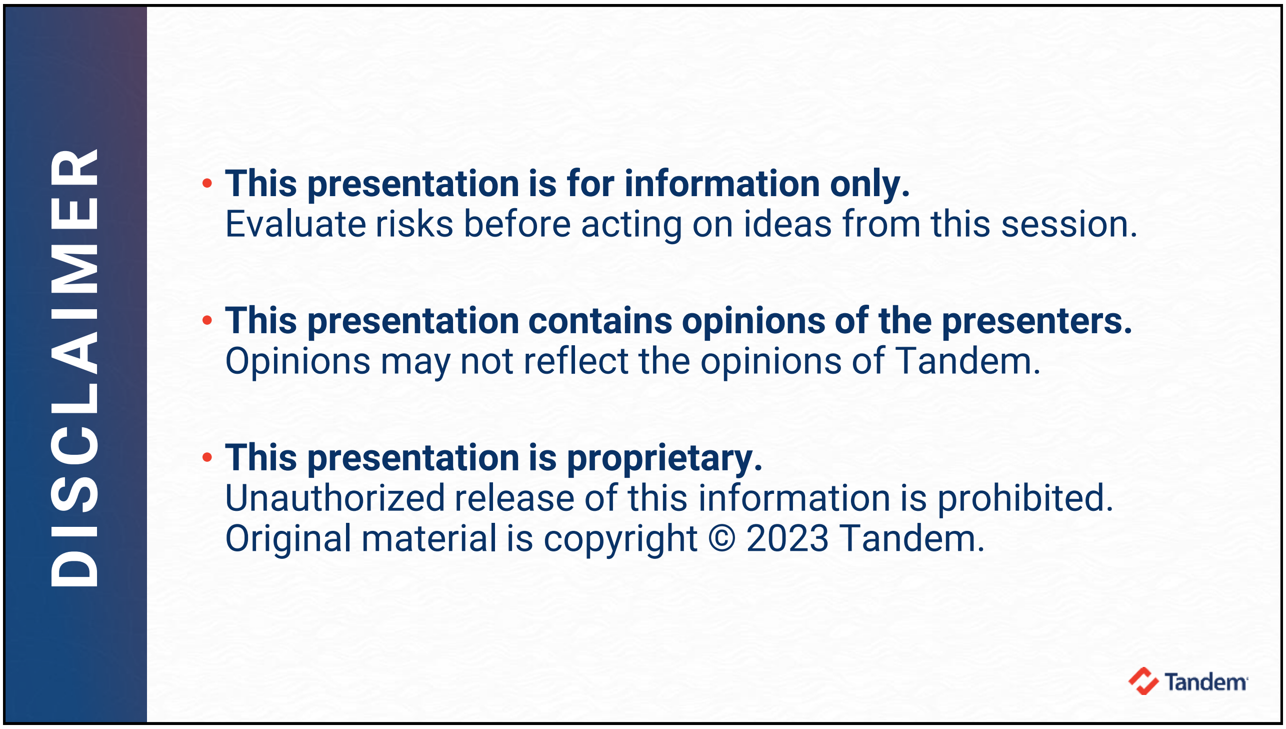
WELCOME TO

Your Guide to Effective Vulnerability & Patch Management

Chris Brewer & Alyssa Pugh

Tandem

1

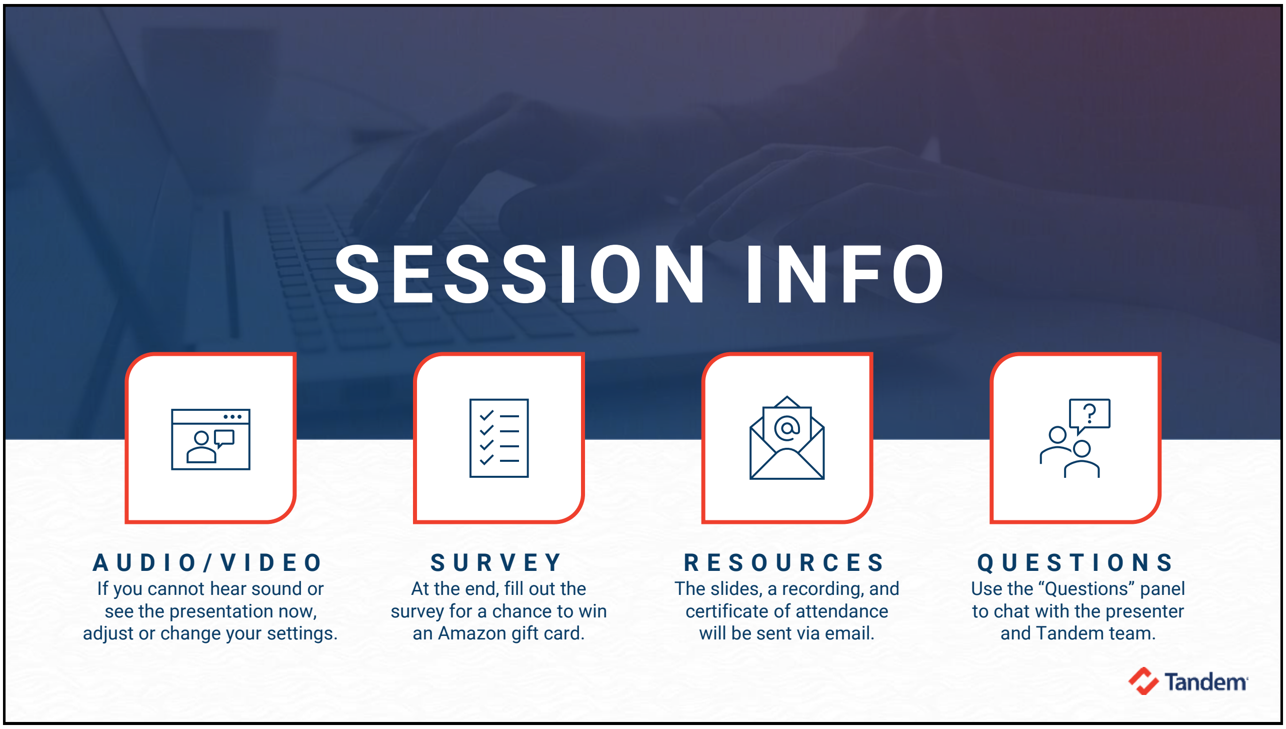


DISCLAIMER

- **This presentation is for information only.** Evaluate risks before acting on ideas from this session.
- **This presentation contains opinions of the presenters.** Opinions may not reflect the opinions of Tandem.
- **This presentation is proprietary.** Unauthorized release of this information is prohibited. Original material is copyright © 2023 Tandem.

Tandem

2



SESSION INFO

AUDIO/VIDEO
If you cannot hear sound or see the presentation now, adjust or change your settings.

SURVEY
At the end, fill out the survey for a chance to win an Amazon gift card.

RESOURCES
The slides, a recording, and certificate of attendance will be sent via email.

QUESTIONS
Use the "Questions" panel to chat with the presenter and Tandem team.

Tandem

3

- Audit Management
- Business Continuity Plan
- Compliance Management
- Cybersecurity
- Identity Theft Prevention
- Incident Management
- Internet Banking Security
- Phishing
- Policies
- Risk Assessment
- Vendor Management

Tandem™
A CoNetrix company

Tandem

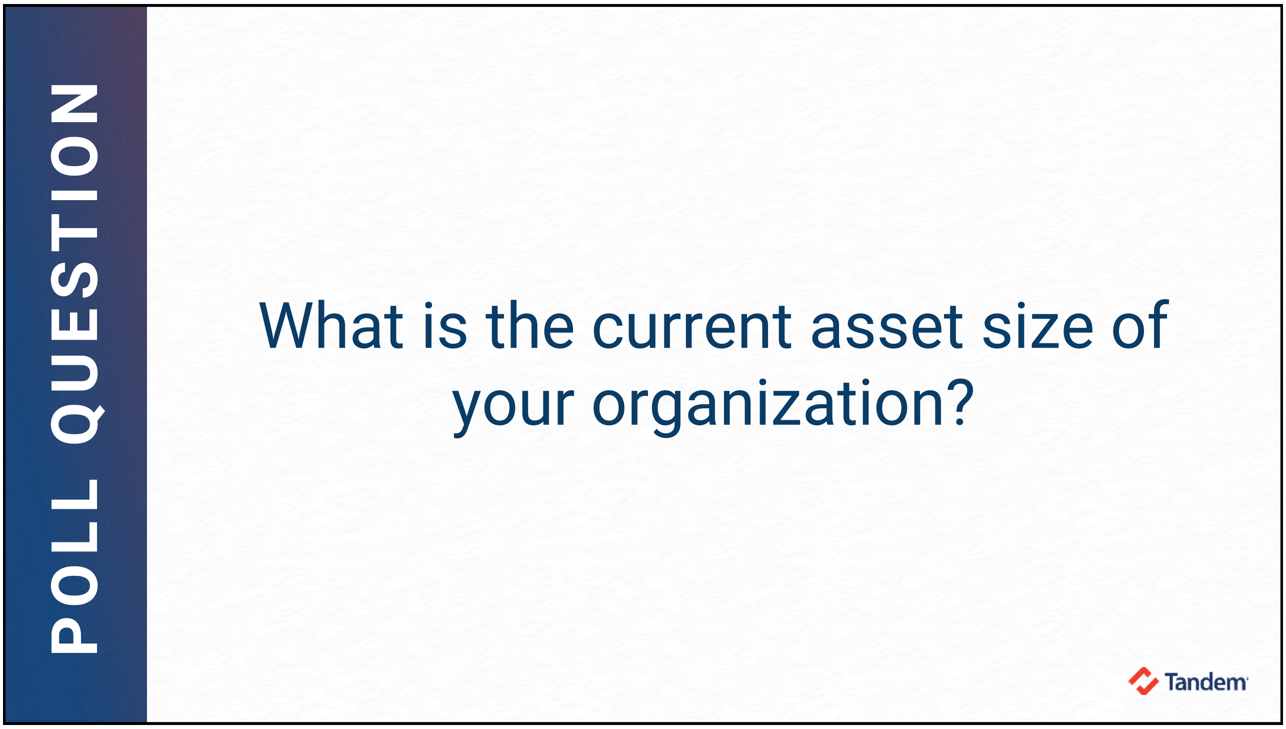
4

ABOUT THE PRESENTERS

Alyssa Pugh, CISM, Security+
GRC Content Manager
Tandem, LLC
LinkedIn.com/in/AlyssaPugh

Chris Brewer, VCP
Team Lead
CoNetrix Technology
LinkedIn.com/in/TheChrisBrewer

5



POLL QUESTION

What is the current asset size of your organization?

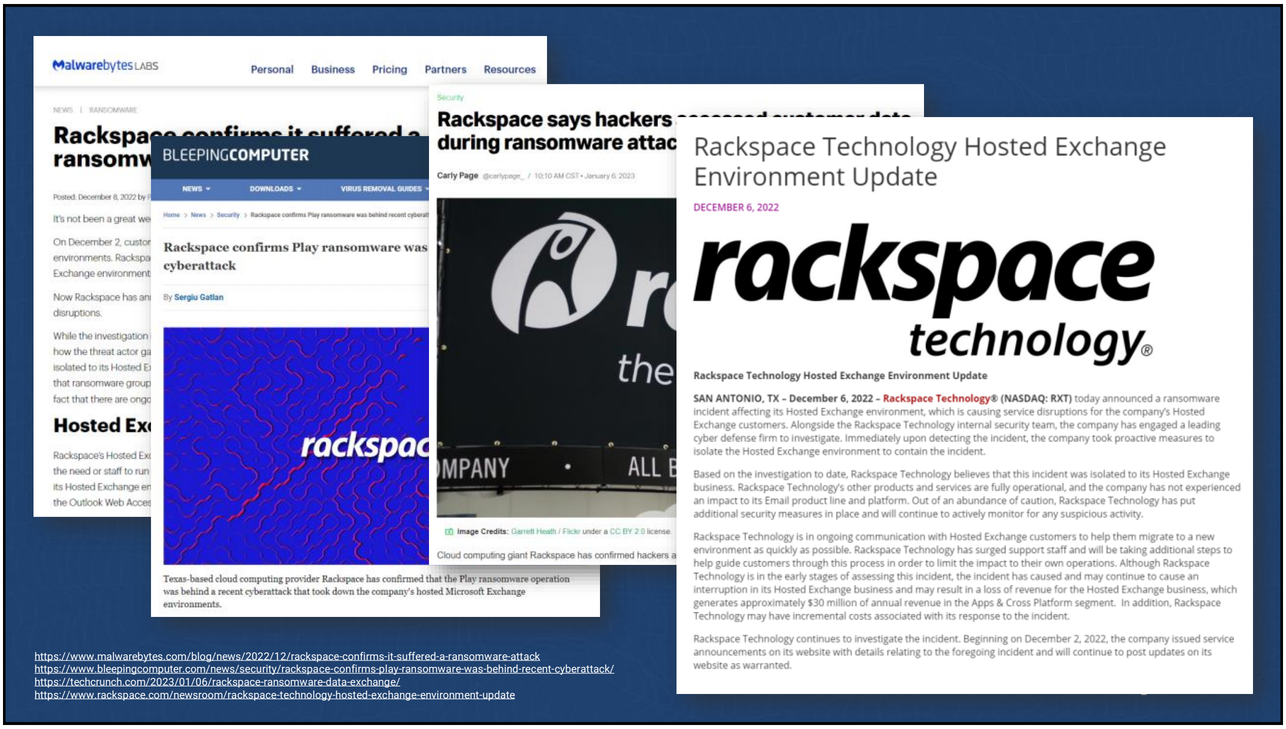
6

POLL QUESTION

How would you describe your role at your organization?

Tandem

7



Malwarebytes LABS

Personal Business Pricing Partners Resources

NEWS | RANSOMWARE

Rackspace confirms it suffered a ransomw

Posted: December 8, 2022 by

It's not been a great we

On December 2, custor environments. Rackspa Exchange environment

Now Rackspace has an disruptions.

While the investigation how the threat actor ga isolated to its Hosted E that ransomware group fact that there are ongo

Hosted Exc

Rackspace's Hosted Ex the need or staff to run its Hosted Exchange en the Outlook Web Acces

BLEEPINGCOMPUTER

NEWS DOWNLOADS VIRUS REMOVAL GUIDES

Home > News > Security > Rackspace confirms Play ransomware was behind recent cyberat

Rackspace confirms Play ransomware was cyberattack

By Sergiu Gatlan

Texas-based cloud computing provider Rackspace has confirmed that the Play ransomware operation was behind a recent cyberattack that took down the company's hosted Microsoft Exchange environments.

Security

Rackspace says hackers during ransomware attac

Carly Page @carlypage_ / 10:10 AM CST • January 6, 2023

Image Credits: Garrett Heath / Flickr under a CC BY 2.0 license.

Cloud computing giant Rackspace has confirmed hackers a

Rackspace Technology Hosted Exchange Environment Update

DECEMBER 6, 2022

rackspace technology®

Rackspace Technology Hosted Exchange Environment Update

SAN ANTONIO, TX – December 6, 2022 – Rackspace Technology® (NASDAQ: RXT) today announced a ransomware incident affecting its Hosted Exchange environment, which is causing service disruptions for the company's Hosted Exchange customers. Alongside the Rackspace Technology internal security team, the company has engaged a leading cyber defense firm to investigate. Immediately upon detecting the incident, the company took proactive measures to isolate the Hosted Exchange environment to contain the incident.

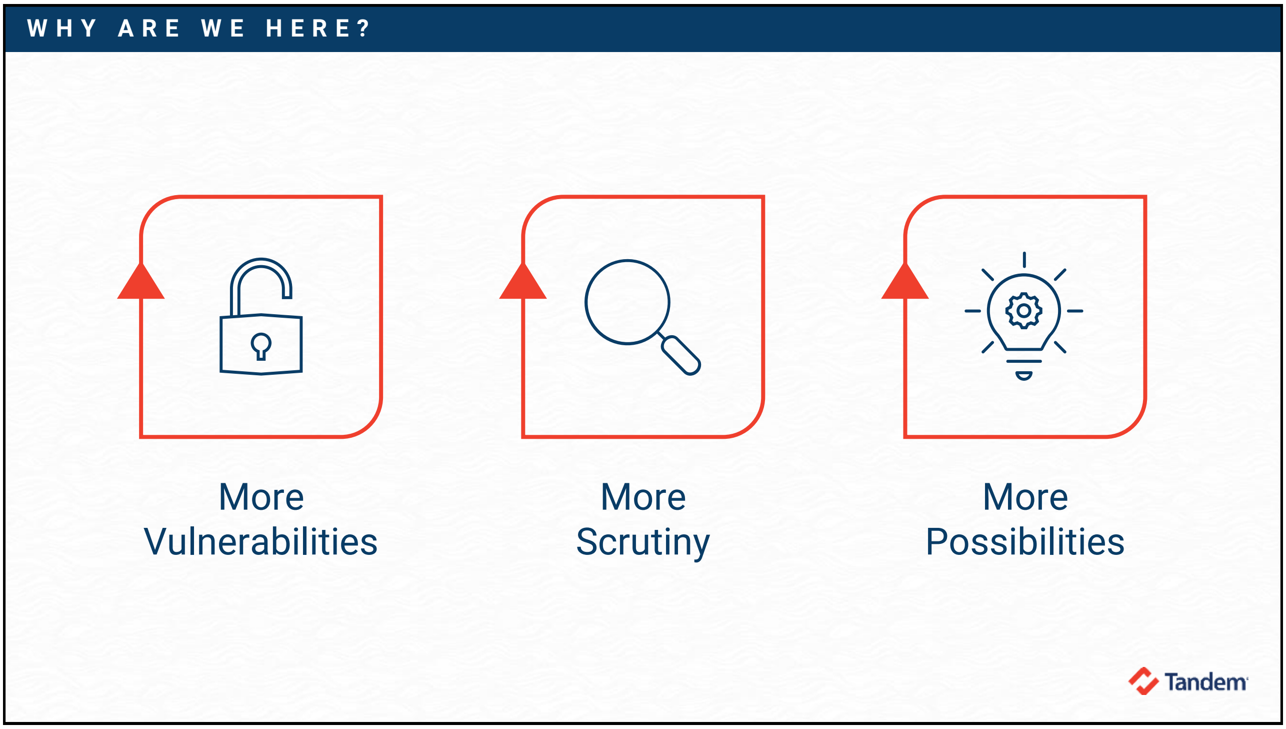
Based on the investigation to date, Rackspace Technology believes that this incident was isolated to its Hosted Exchange business. Rackspace Technology's other products and services are fully operational, and the company has not experienced an impact to its Email product line and platform. Out of an abundance of caution, Rackspace Technology has put additional security measures in place and will continue to actively monitor for any suspicious activity.

Rackspace Technology is in ongoing communication with Hosted Exchange customers to help them migrate to a new environment as quickly as possible. Rackspace Technology has surged support staff and will be taking additional steps to help guide customers through this process in order to limit the impact to their own operations. Although Rackspace Technology is in the early stages of assessing this incident, the incident has caused and may continue to cause an interruption in its Hosted Exchange business and may result in a loss of revenue for the Hosted Exchange business, which generates approximately $30 million of annual revenue in the Apps & Cross Platform segment. In addition, Rackspace Technology may have incremental costs associated with its response to the incident.

Rackspace Technology continues to investigate the incident. Beginning on December 2, 2022, the company issued service announcements on its website with details relating to the foregoing incident and will continue to post updates on its website as warranted.

https://www.malwarebytes.com/blog/news/2022/12/rackspace-confirms-it-suffered-a-ransomware-attack
https://www.bleepingcomputer.com/news/security/rackspace-confirms-play-ransomware-was-behind-recent-cyberattack/
https://techcrunch.com/2023/01/06/rackspace-ransomware-data-exchange/
https://www.rackspace.com/newsroom/rackspace-technology-hosted-exchange-environment-update

8



WHY ARE WE HERE?

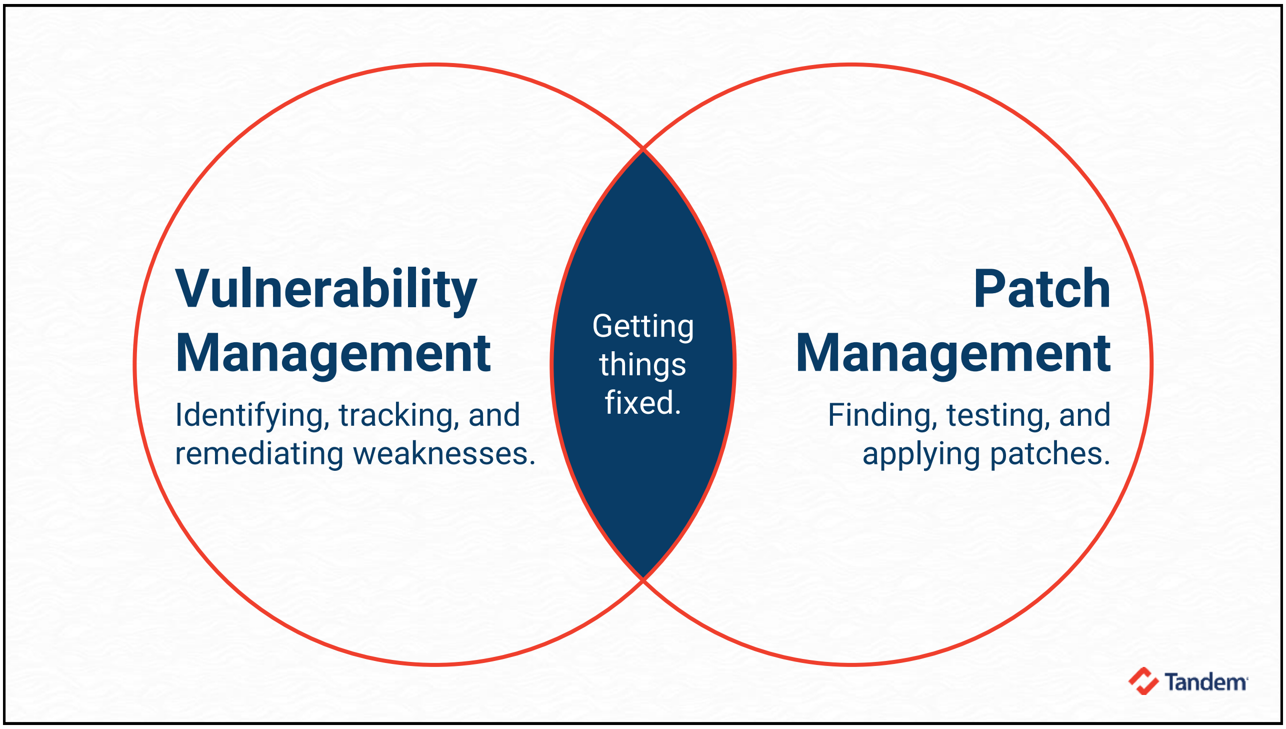
More Vulnerabilities

More Scrutiny

More Possibilities

Tandem

9



Vulnerability Management

Identifying, tracking, and remediating weaknesses.

Getting things fixed.

Patch Management

Finding, testing, and applying patches.

Tandem

10

Vulnerability Management

Tandem

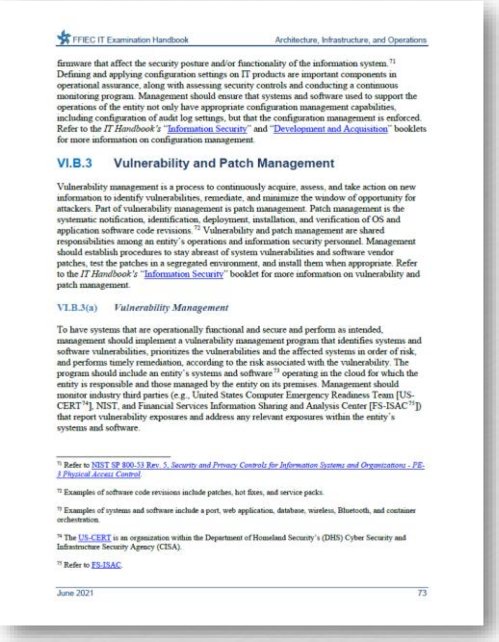
11

POLL QUESTION

How confident are you in your vulnerability management processes?

Tandem

12



FFIEC IT Examination Handbook Architecture, Infrastructure, and Operations

firmware that affect the security posture and/or functionality of the information system.[71] Defining and applying configuration settings on IT products are important components in operational assurance, along with assessing security controls and conducting a continuous monitoring program. Management should ensure that systems and software used to support the operations of the entity not only have appropriate configuration management capabilities, including configuration of audit log settings, but that the configuration management is enforced. Refer to the *IT Handbook's* "Information Security" and "Development and Acquisition" booklets for more information on configuration management.

VI.B.3 Vulnerability and Patch Management

Vulnerability management is a process to continuously acquire, assess, and take action on new information to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers. Part of vulnerability management is patch management. Patch management is the systematic notification, identification, deployment, installation, and verification of OS and application software code revisions.[72] Vulnerability and patch management are shared responsibilities among an entity's operations and information security personnel. Management should establish procedures to stay abreast of system vulnerabilities and software vendor patches, test the patches in a segregated environment, and install them when appropriate. Refer to the *IT Handbook's* "Information Security" booklet for more information on vulnerability and patch management.

VI.B.3(a) *Vulnerability Management*

To have systems that are operationally functional and secure and perform as intended, management should implement a vulnerability management program that identifies systems and software vulnerabilities, prioritizes the vulnerabilities and the affected systems in order of risk, and performs timely remediation, according to the risk associated with the vulnerability. The program should include an entity's systems and software[73] operating in the cloud for which the entity is responsible and those managed by the entity on its premises. Management should monitor industry third parties (e.g., United States Computer Emergency Readiness Team [US-CERT[74]], NIST, and Financial Services Information Sharing and Analysis Center [FS-ISAC[75]]) that report vulnerability exposures and address any relevant exposures within the entity's systems and software.

[71] Refer to NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations - PE-3 Physical Access Control*.

[72] Examples of software code revisions include patches, hot fixes, and service packs.

[73] Examples of systems and software include a port, web application, database, wireless, Bluetooth, and container orchestration.

[74] The US-CERT is an organization within the Department of Homeland Security's (DHS) Cyber Security and Infrastructure Security Agency (CISA).

[75] Refer to FS-ISAC.

June 2021 73

FFIEC BOOKLET

Architecture, Infrastructure, and Operations

Tandem

13

FFIEC AIO BOOKLET: VULNERABILITY MANAGEMENT

Acquire Information

Assess Information

Act on Information

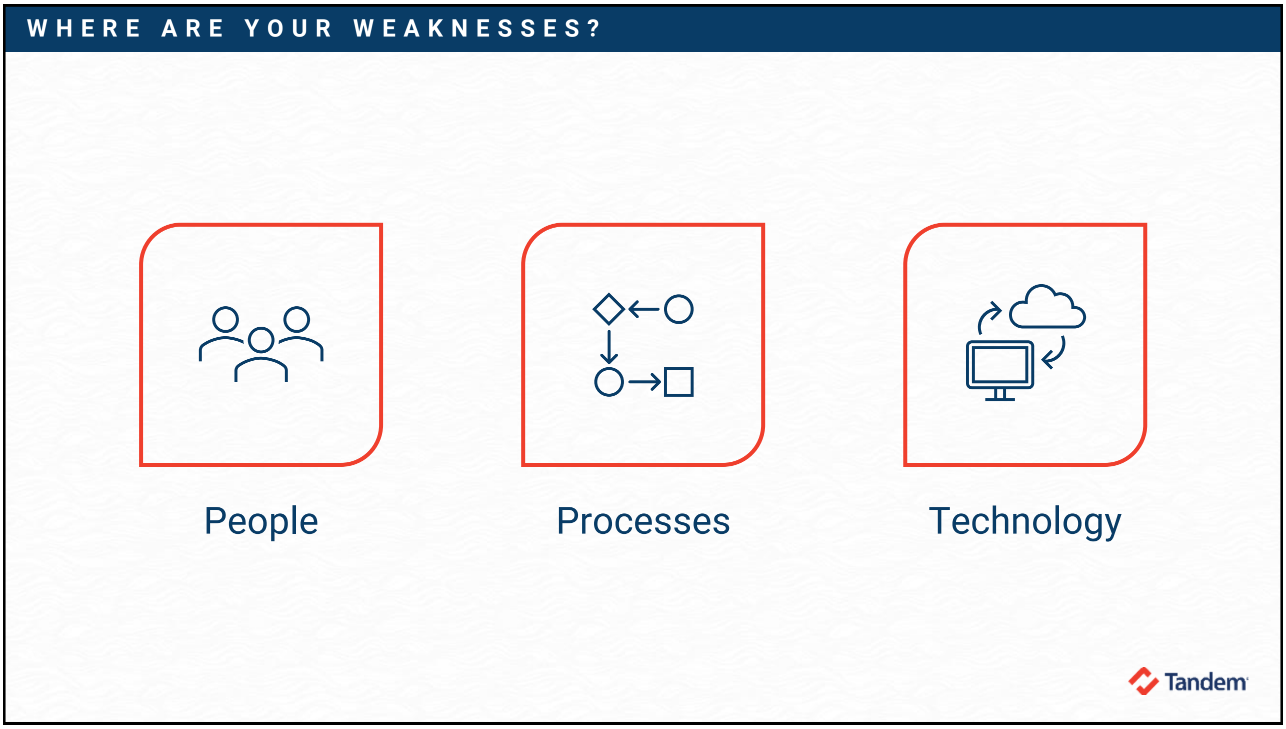
Identify Vulnerabilities

Remediate Vulnerabilities

Minimize Opportunity

Tandem

14



WHERE ARE YOUR WEAKNESSES?

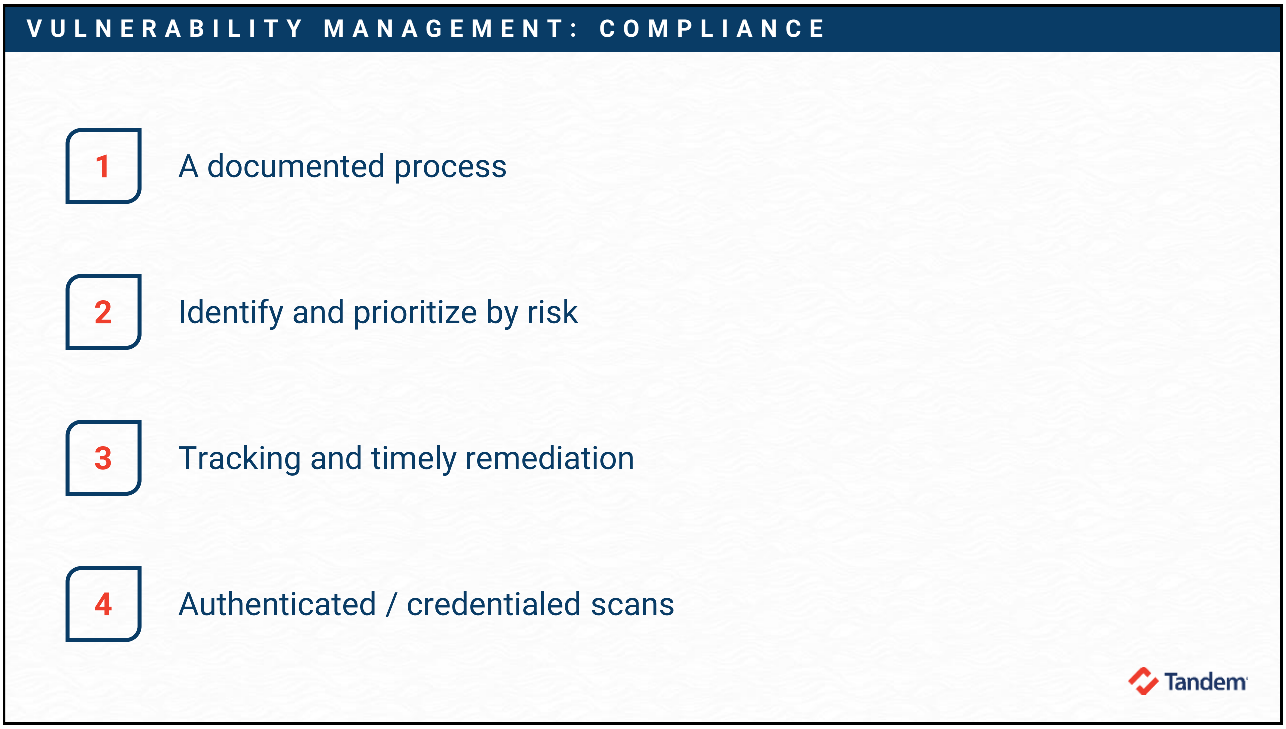
People

Processes

Technology

Tandem

15



VULNERABILITY MANAGEMENT: COMPLIANCE

1 A documented process

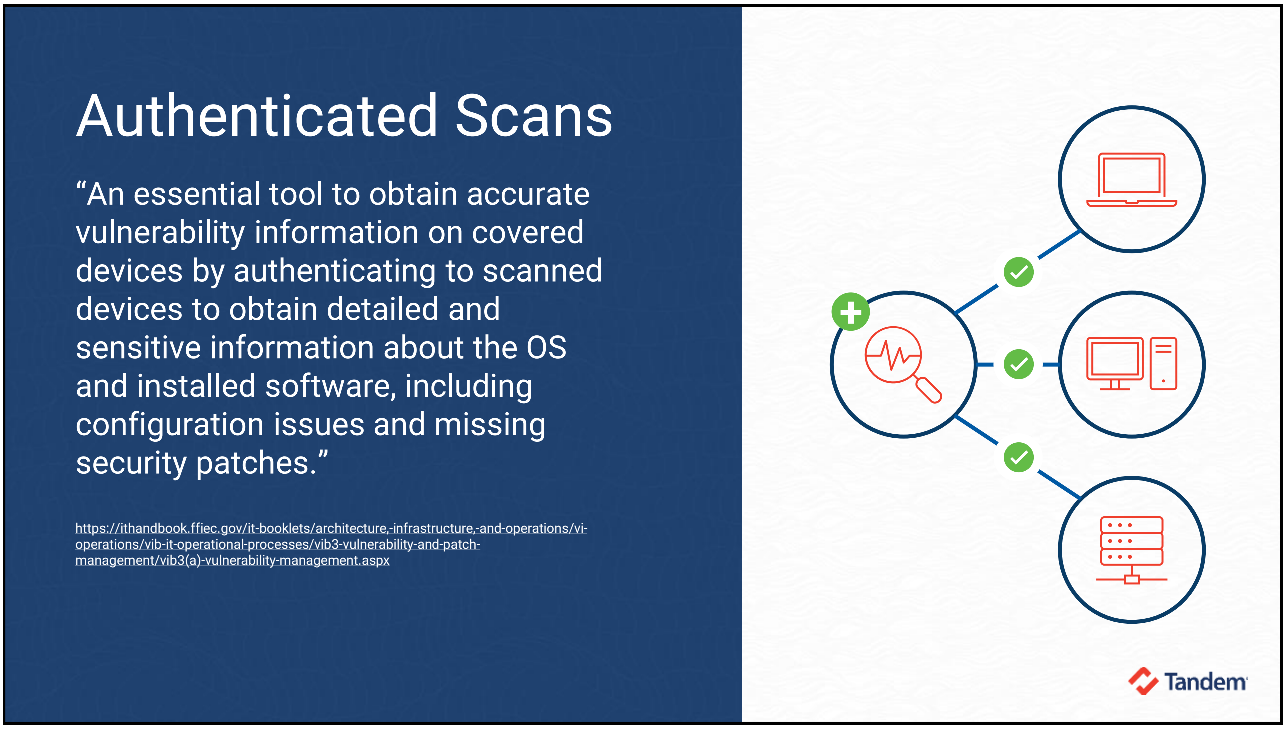
2 Identify and prioritize by risk

3 Tracking and timely remediation

4 Authenticated / credentialed scans

Tandem

16

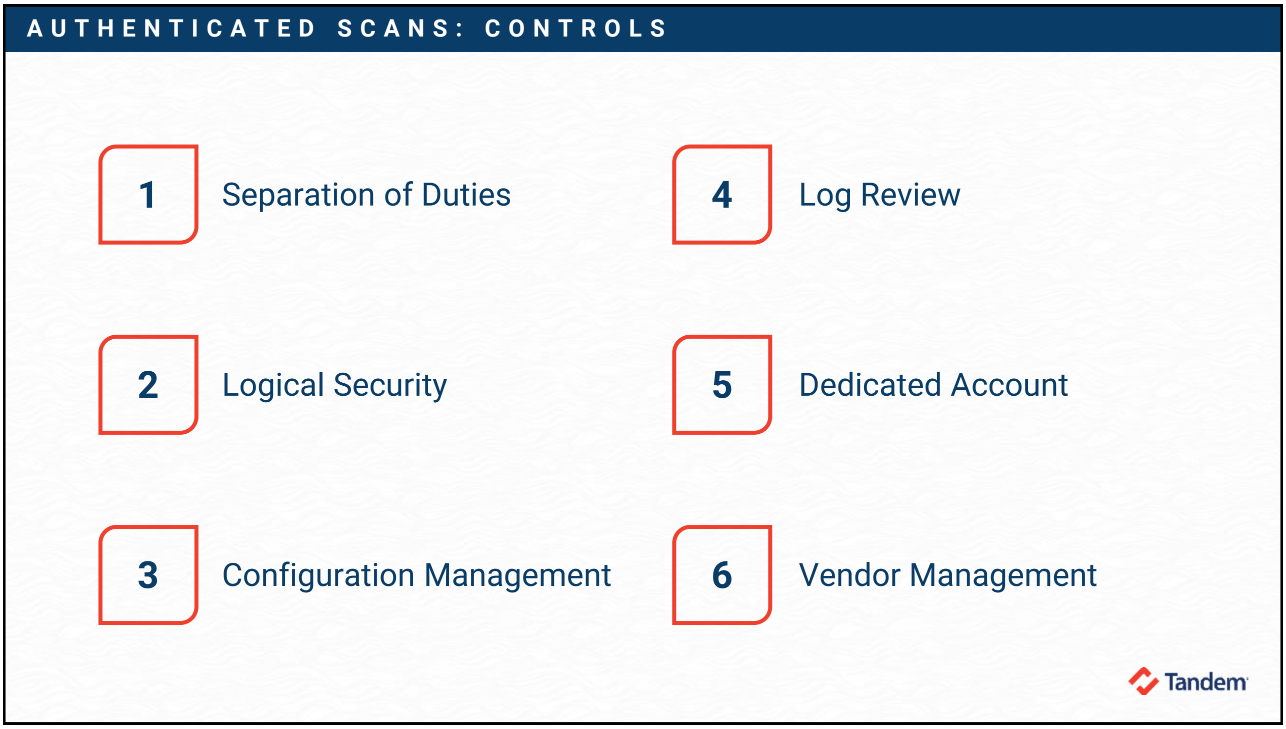


Authenticated Scans

"An essential tool to obtain accurate vulnerability information on covered devices by authenticating to scanned devices to obtain detailed and sensitive information about the OS and installed software, including configuration issues and missing security patches."

https://ithandbook.ffiec.gov/it-booklets/architecture,-infrastructure,-and-operations/vi-operations/vib-it-operational-processes/vib3-vulnerability-and-patch-management/vib3(a)-vulnerability-management.aspx

17



AUTHENTICATED SCANS: CONTROLS

1 Separation of Duties

2 Logical Security

3 Configuration Management

4 Log Review

5 Dedicated Account

6 Vendor Management

18

WHAT TO DO?

Know Your Systems

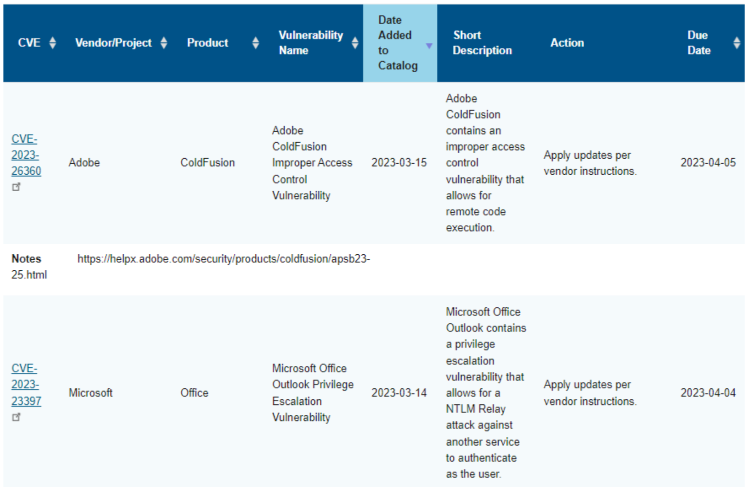
Know Your Weaknesses

Know Your Options

Tandem

19

Known Exploited Vulnerabilities Catalog



CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date
CVE-2023-26360	Adobe	ColdFusion	Adobe ColdFusion Improper Access Control Vulnerability	2023-03-15	Adobe ColdFusion contains an improper access control vulnerability that allows for remote code execution.	Apply updates per vendor instructions.	2023-04-05
Notes	https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html						
CVE-2023-23397	Microsoft	Office	Microsoft Office Outlook Privilege Escalation Vulnerability	2023-03-14	Microsoft Office Outlook contains a privilege escalation vulnerability that allows for a NTLM Relay attack against another service to authenticate as the user.	Apply updates per vendor instructions.	2023-04-04

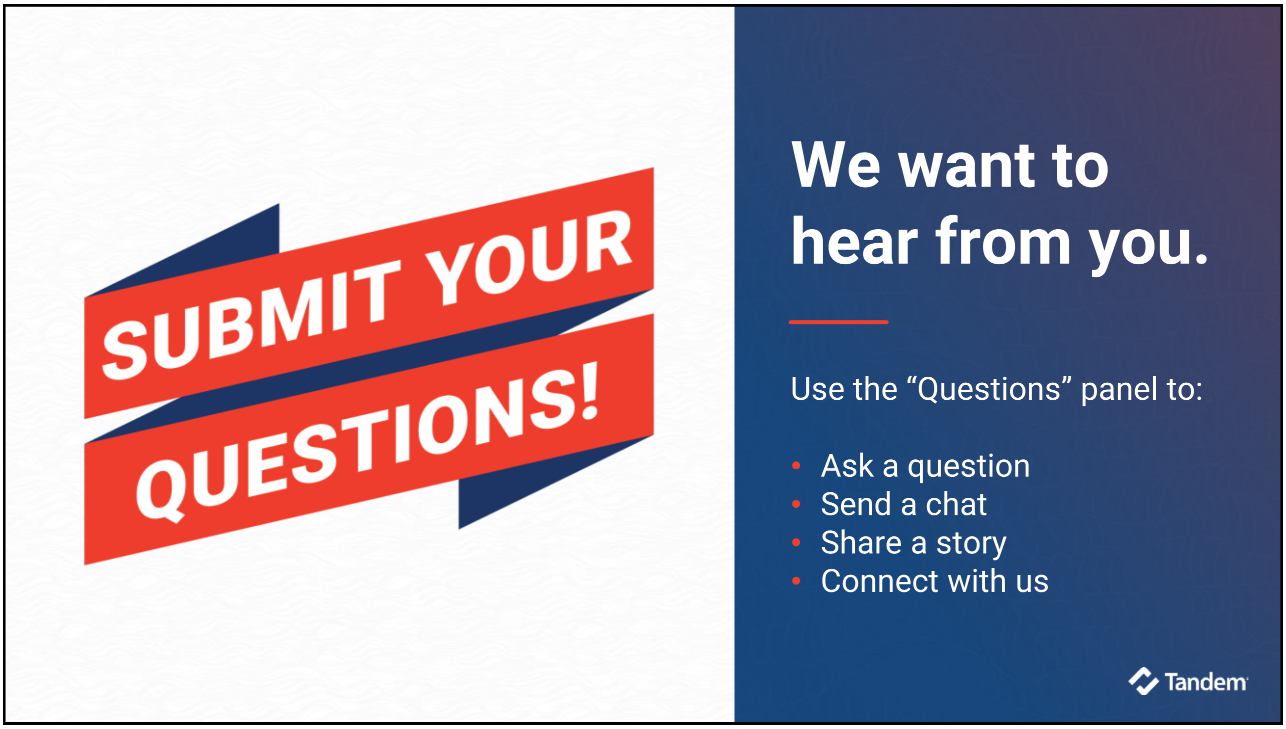
RESOURCE

CISA Known Exploited Vulnerabilities Catalog

CISA.gov/KEV

Tandem

20



SUBMIT YOUR QUESTIONS!

We want to hear from you.

Use the “Questions” panel to:

- Ask a question
- Send a chat
- Share a story
- Connect with us

Tandem

21

Patch Management

Tandem

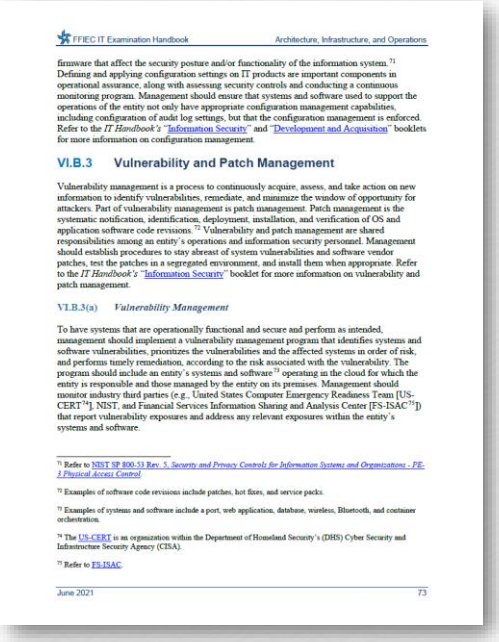
22

POLL QUESTION

How confident are you in your patch management processes?

Tandem

23



FFIEC IT Examination Handbook Architecture, Infrastructure, and Operations

firmware that affect the security posture and/or functionality of the information system.[71] Defining and applying configuration settings on IT products are important components in operational assurance, along with assessing security controls and conducting a continuous monitoring program. Management should ensure that systems and software used to support the operations of the entity not only have appropriate configuration management capabilities, including configuration of audit log settings, but that the configuration management is enforced. Refer to the *IT Handbook's* "Information Security" and "Development and Acquisition" booklets for more information on configuration management.

VI.B.3 Vulnerability and Patch Management

Vulnerability management is a process to continuously acquire, assess, and take action on new information to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers. Part of vulnerability management is patch management. Patch management is the systematic notification, identification, deployment, installation, and verification of OS and application software code revisions.[72] Vulnerability and patch management are shared responsibilities among an entity's operations and information security personnel. Management should establish procedures to stay abreast of system vulnerabilities and software vendor patches, test the patches in a segregated environment, and install them when appropriate. Refer to the *IT Handbook's* "Information Security" booklet for more information on vulnerability and patch management.

VI.B.3(a) *Vulnerability Management*

To have systems that are operationally functional and secure and perform as intended, management should implement a vulnerability management program that identifies systems and software vulnerabilities, prioritizes the vulnerabilities and the affected systems in order of risk, and performs timely remediation, according to the risk associated with the vulnerability. The program should include an entity's systems and software[73] operating in the cloud for which the entity is responsible and those managed by the entity on its premises. Management should monitor industry third parties (e.g., United States Computer Emergency Readiness Team [US-CERT[74]], NIST, and Financial Services Information Sharing and Analysis Center [FS-ISAC[75]]) that report vulnerability exposures and address any relevant exposures within the entity's systems and software.

[71] Refer to NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations - PE-3 Physical Access Control*.

[72] Examples of software code revisions include patches, hot fixes, and service packs.

[73] Examples of systems and software include a port, web application, database, wireless, Bluetooth, and container orchestration.

[74] The US-CERT is an organization within the Department of Homeland Security's (DHS) Cyber Security and Infrastructure Security Agency (CISA).

[75] Refer to FS-ISAC.

June 2021 73

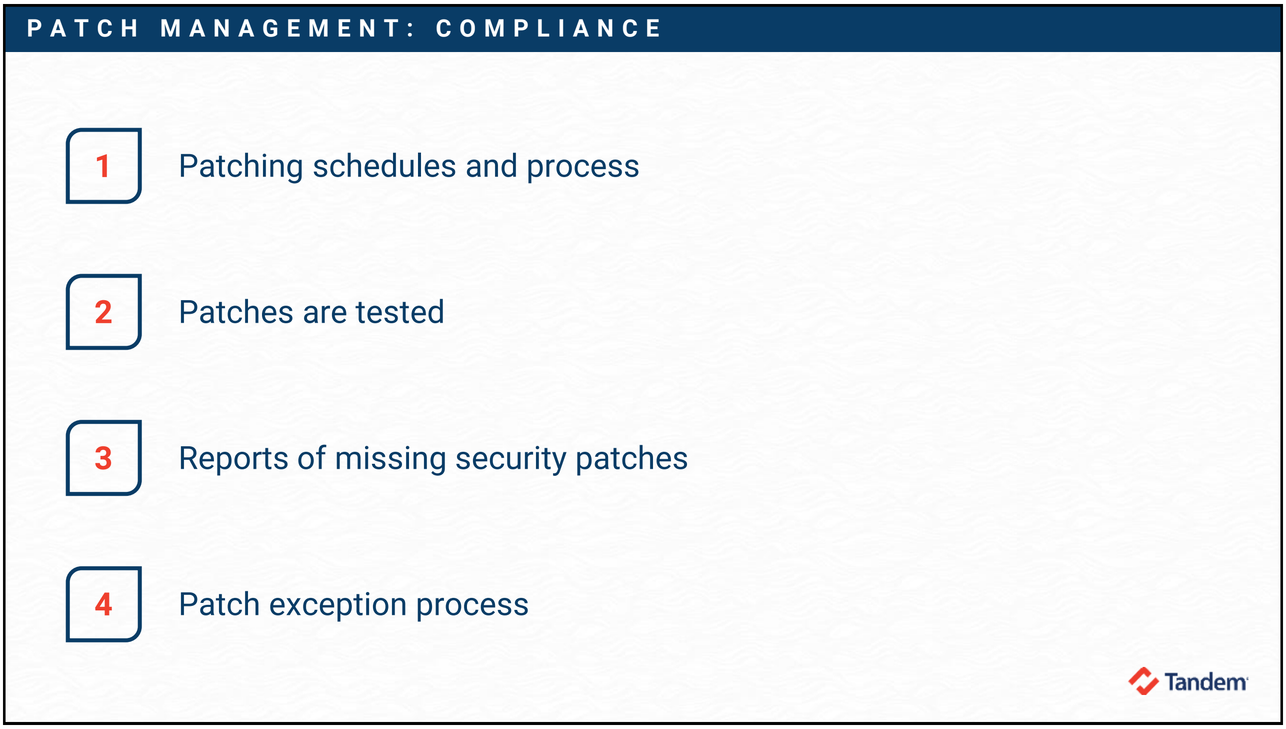
FFIEC BOOKLET

Architecture, Infrastructure, and Operations

"Part of vulnerability management is patch management. Patch Management is the systematic notification, identification, deployment, installation, and verification of OS and application software code revisions."

Tandem

24



PATCH MANAGEMENT: COMPLIANCE

1 Patching schedules and process

2 Patches are tested

3 Reports of missing security patches

4 Patch exception process

25

WHAT NEEDS PATCHED?

BOTTOM LINE

Everything

Needs Patched

26

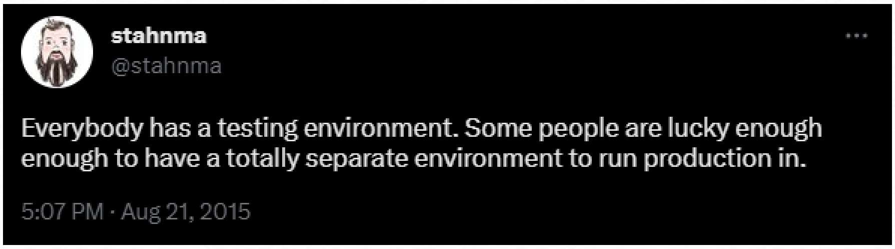
PATCH MANAGEMENT

Test

Apply

Verify

Document



stahnma
@stahnma

Everybody has a testing environment. Some people are lucky enough enough to have a totally separate environment to run production in.

5:07 PM · Aug 21, 2015

Tandem

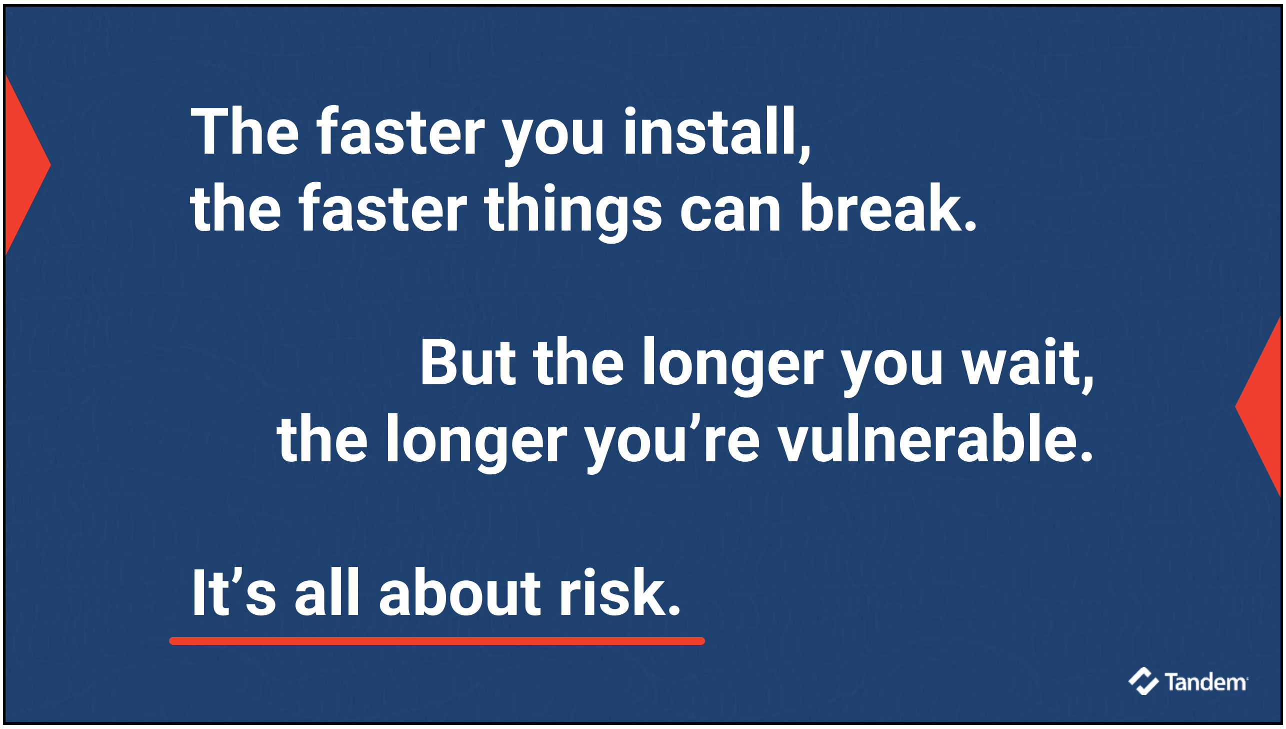
27

MICROSOFT PATCH SCHEDULE

SUN	MON	TUE	WED	THU	FRI	SAT	
			1	2	3	4	
5	6	A	8	9	10	11	Office & Non-Security Updates
12	13	B	15	16	17	18	"Patch Tuesday" Updates
19	20	C	22	23	24	25	Preview Non-Security Updates
26	27	D	29	30			

Tandem

28



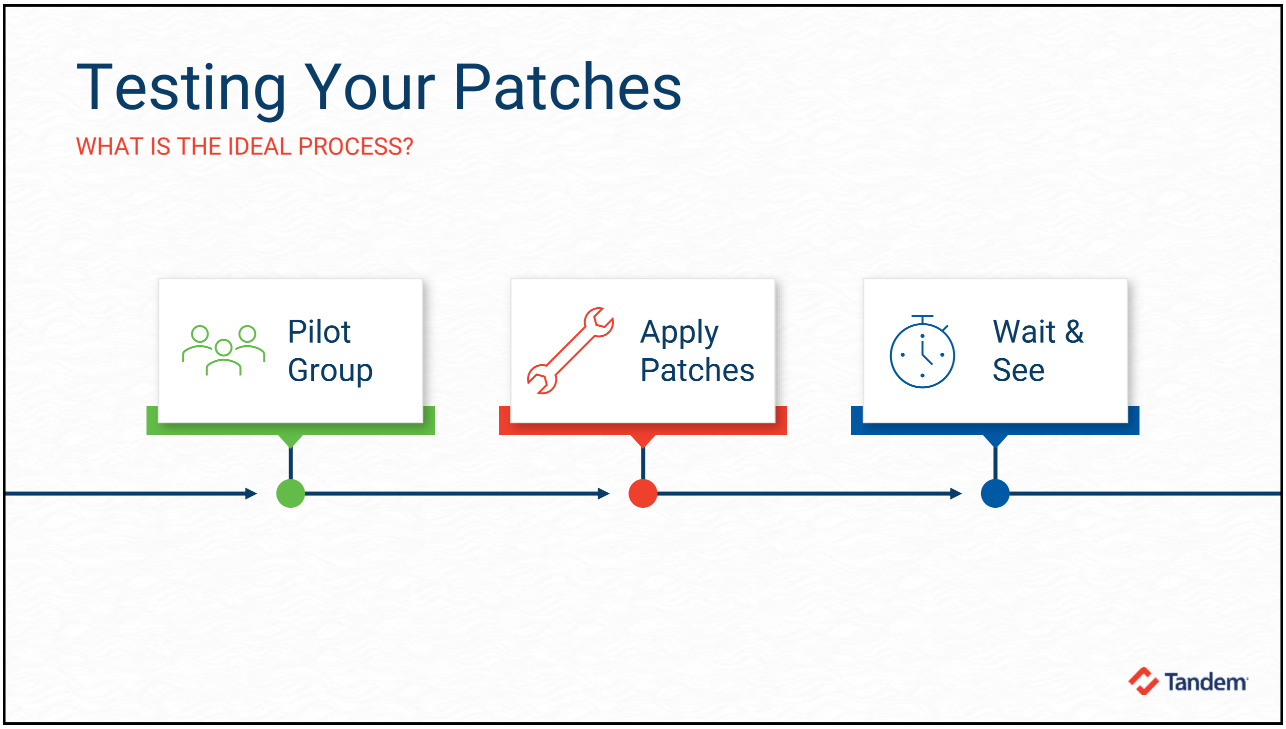
The faster you install,
the faster things can break.

But the longer you wait,
the longer you're vulnerable.

It's all about risk.

Tandem

29



Testing Your Patches

WHAT IS THE IDEAL PROCESS?

Pilot Group

Apply Patches

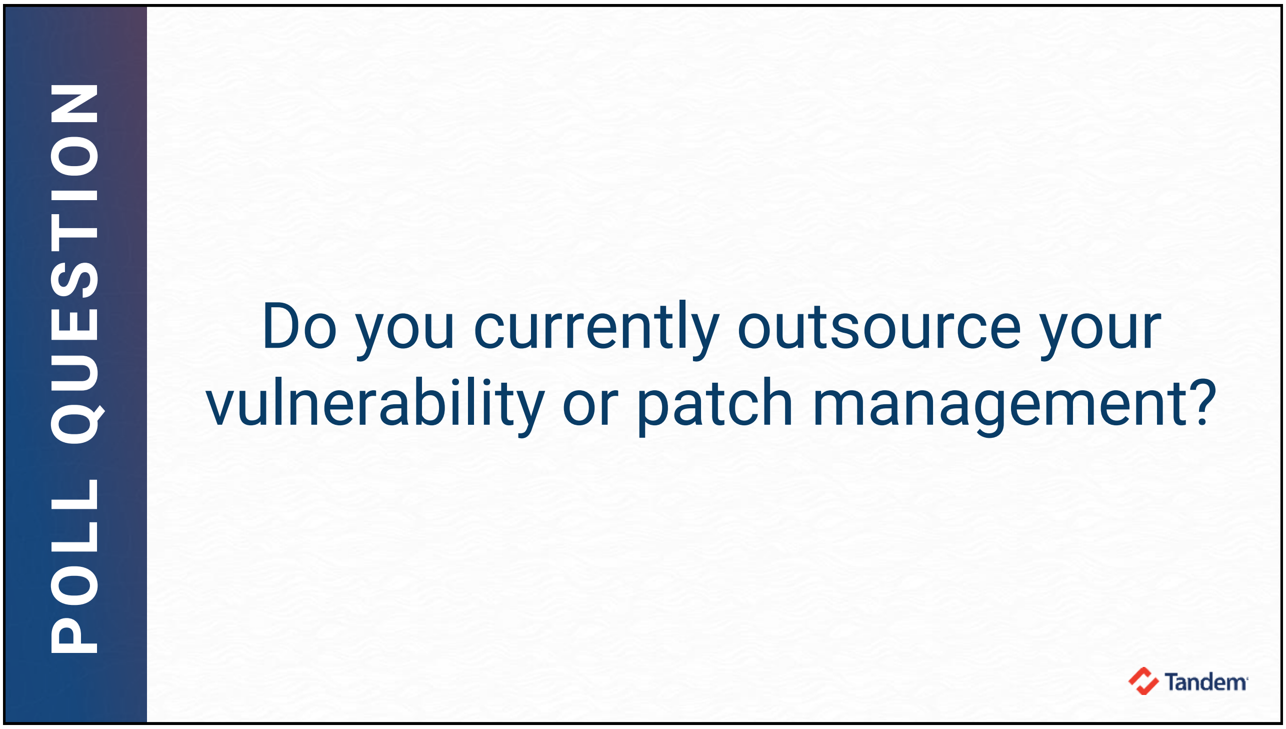
Wait & See

Tandem

30

In 2023, there is very little reason why you would not install all the patches.

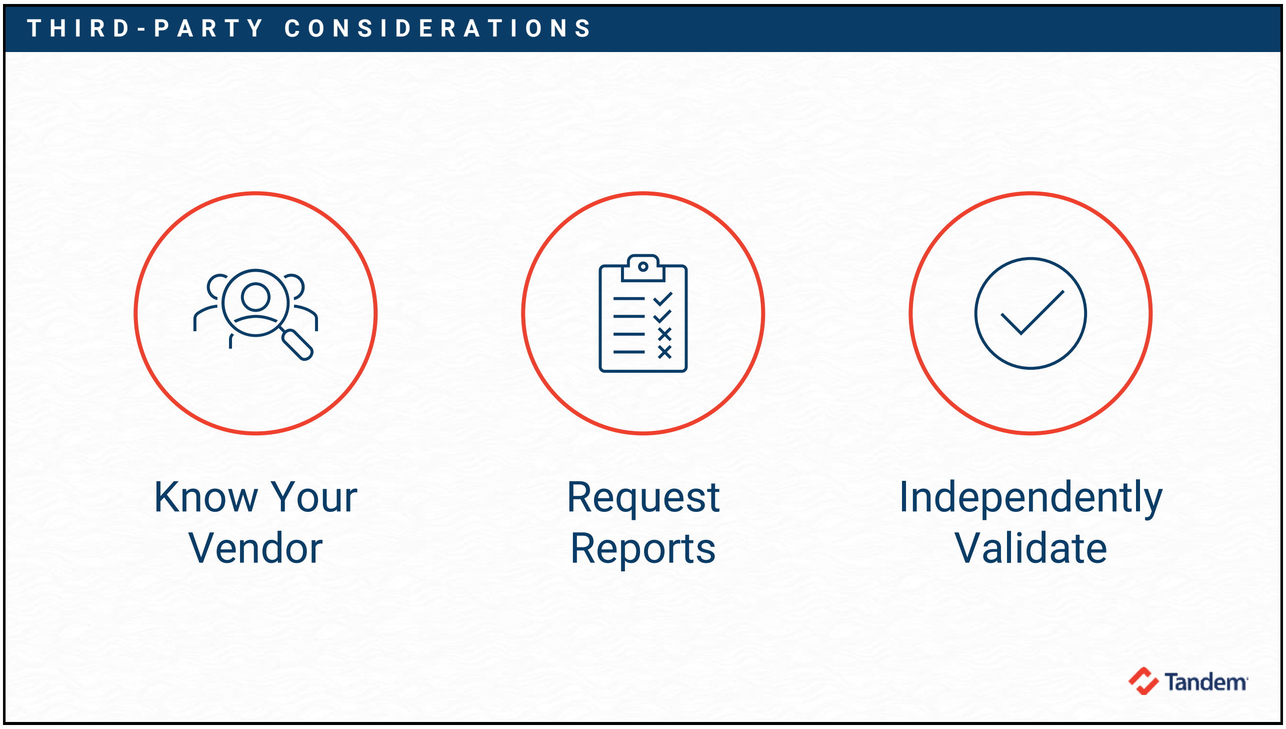
31



POLL QUESTION

Do you currently outsource your vulnerability or patch management?

32



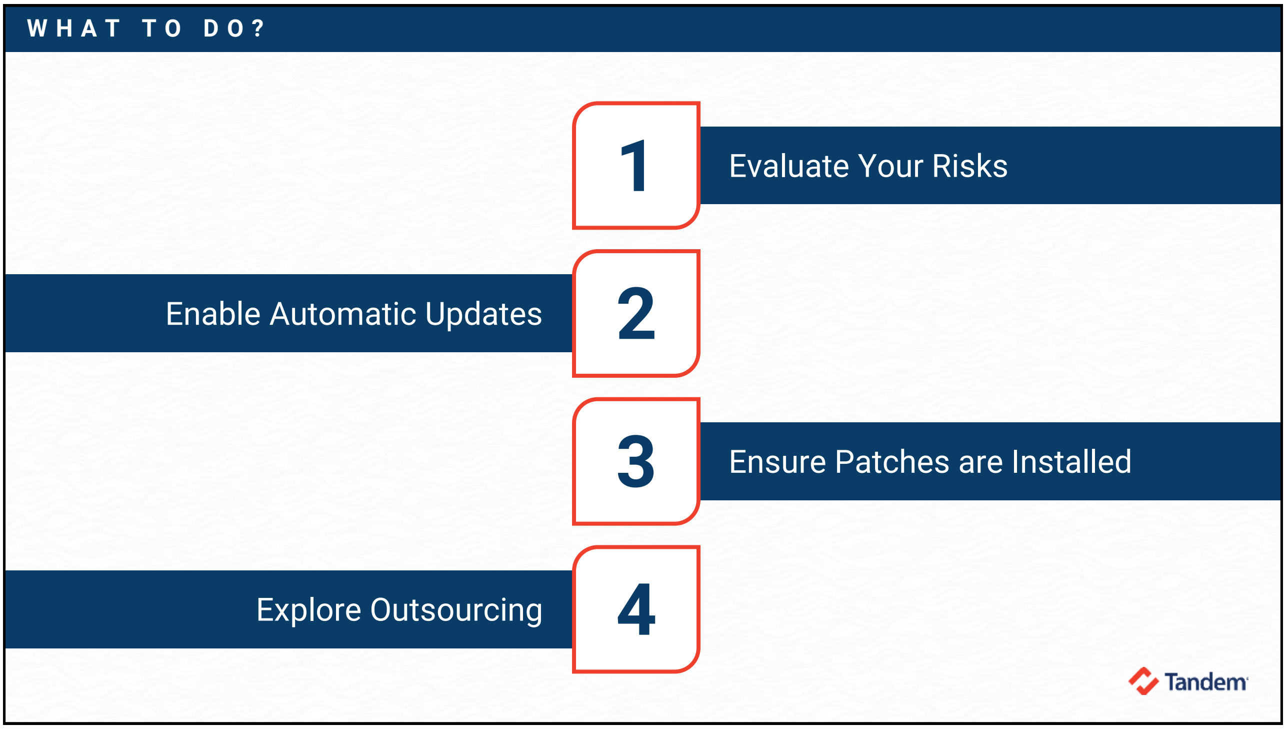
THIRD-PARTY CONSIDERATIONS

Know Your Vendor

Request Reports

Independently Validate

33



WHAT TO DO?

1 Evaluate Your Risks

2 Enable Automatic Updates

3 Ensure Patches are Installed

4 Explore Outsourcing

34

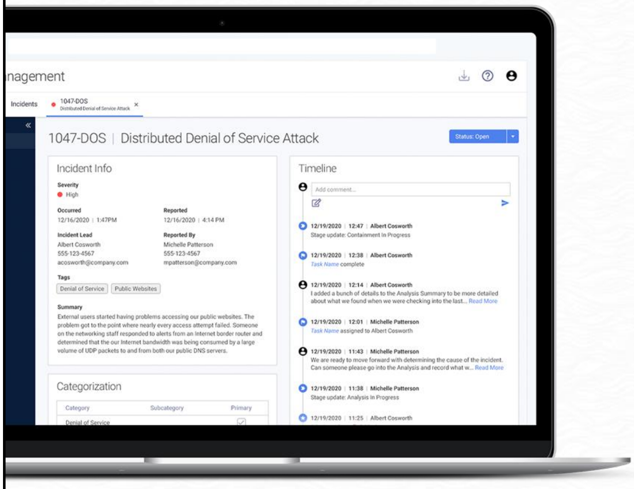
We want to hear from you.

Use the “Questions” panel to:

- Ask a question
- Send a chat
- Share a story
- Connect with us

Tandem

35



1047-DOS | Distributed Denial of Service Attack

Incident Info

Severity
● High

Occurred 12/16/2020 | 1:47PM	Reported 12/16/2020 | 4:14 PM
Incident Lead Albert Cosworth 555-123-4567 acosworth@company.com	Reported By Michelle Patterson 555-123-4567 mpatterson@company.com

Tags
Denial of Service | Public Websites

Summary
External users started having problems accessing our public websites. The problem got to the point where nearly every access attempt failed. Someone on the networking staff responded to alerts from an Internet border router and determined that the our Internet bandwidth was being consumed by a large volume of UDP packets to and from both our public DNS servers.

Categorization

Category	Subcategory	Primary
Denial of Service		✓

Timeline

Add comment...

12/19/2020 | 12:47 | Albert Cosworth
Stage update: Containment In Progress

12/19/2020 | 12:38 | Albert Cosworth
Task Name complete

12/19/2020 | 12:14 | Albert Cosworth
I added a bunch of details to the Analysis Summary to be more detailed about what we found when we were checking into the last... Read More

12/19/2020 | 12:01 | Michelle Patterson
Task Name assigned to Albert Cosworth

12/19/2020 | 11:43 | Michelle Patterson
We are ready to move forward with determining the cause of the incident. Can someone please go into the Analysis and record what w... Read More

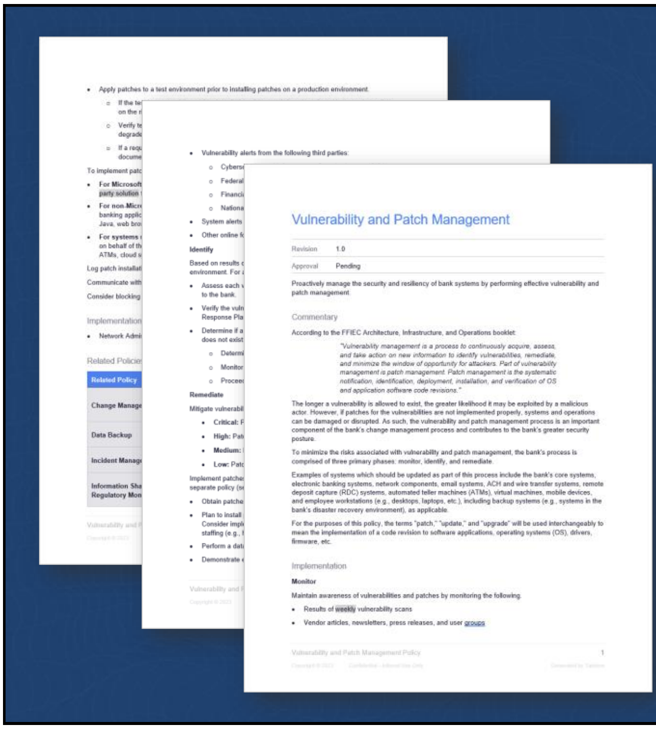
12/19/2020 | 11:38 | Michelle Patterson
Stage update: Analysis In Progress

12/19/2020 | 11:25 | Albert Cosworth

Cybersecurity Governance, Risk Management, and Compliance (GRC) Software

Tandem.App

36



Vulnerability and Patch Management

Revision	1.0
Approval	Pending

Proactively manage the security and resiliency of bank systems by performing effective vulnerability and patch management.

Commentary

According to the FFIEC Architecture, Infrastructure, and Operations booklet:

> *"Vulnerability management is a process to continuously acquire, assess, and take action on new information to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers. Part of vulnerability management is patch management. Patch management is the systematic notification, identification, deployment, installation, and verification of OS and application software code revisions."*

The longer a vulnerability is allowed to exist, the greater likelihood it may be exploited by a malicious actor. However, if patches for the vulnerabilities are not implemented properly, systems and operations can be damaged or disrupted. As such, the vulnerability and patch management process is an important component of the bank's change management process and contributes to the bank's greater security posture.

To minimize the risks associated with vulnerability and patch management, the bank's process is comprised of three primary phases: monitor, identify, and remediate.

Examples of systems which should be updated as part of this process include the bank's core systems, electronic banking systems, network components, email systems, ACH and wire transfer systems, remote deposit capture (RDC) systems, automated teller machines (ATMs), virtual machines, mobile devices, and employee workstations (e.g., desktops, laptops, etc.), including backup systems (e.g., systems in the bank's disaster recovery environment), as applicable.

For the purposes of this policy, the terms "patch," "update," and "upgrade" will be used interchangeably to mean the implementation of a code revision to software applications, operating systems (OS), drivers, firmware, etc.

Implementation

Monitor

Maintain awareness of vulnerabilities and patches by monitoring the following.

- Results of weekly vulnerability scans
- Vendor articles, newsletters, press releases, and user groups

Vulnerability and Patch Management Policy 1

Copyright © 2023 Confidential - Internal Use Only Generated by Tandem

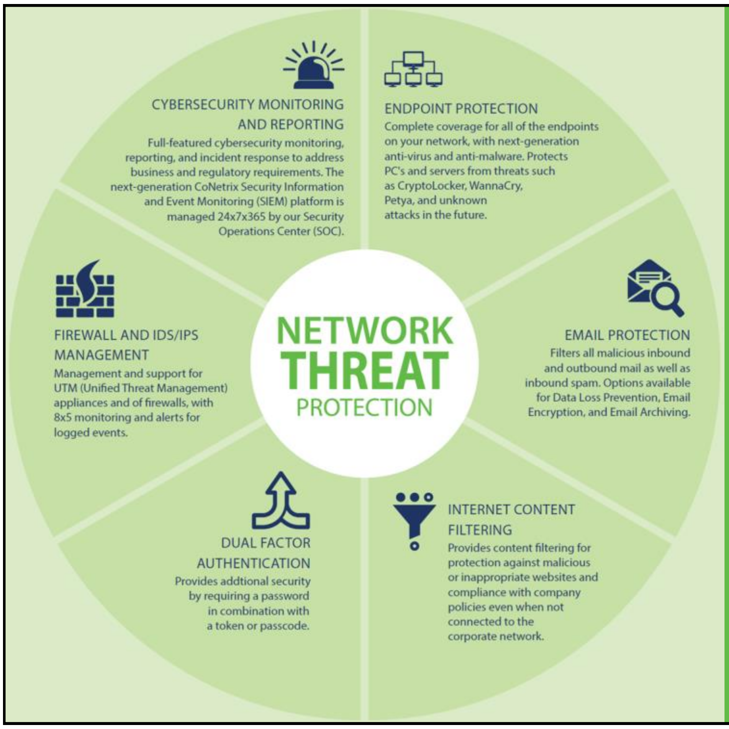
RESOURCE

Template Vulnerability and Patch Management Policy

Tandem.App/Patch-Policy-Download

Tandem

37



NETWORK THREAT PROTECTION

CYBERSECURITY MONITORING AND REPORTING

Full-featured cybersecurity monitoring, reporting, and incident response to address business and regulatory requirements. The next-generation CoNetrix Security Information and Event Monitoring (SIEM) platform is managed 24x7x365 by our Security Operations Center (SOC).

ENDPOINT PROTECTION

Complete coverage for all of the endpoints on your network, with next-generation anti-virus and anti-malware. Protects PC's and servers from threats such as CryptoLocker, WannaCry, Petya, and unknown attacks in the future.

FIREWALL AND IDS/IPS MANAGEMENT

Management and support for UTM (Unified Threat Management) appliances and of firewalls, with 8x5 monitoring and alerts for logged events.

EMAIL PROTECTION

Filters all malicious inbound and outbound mail as well as inbound spam. Options available for Data Loss Prevention, Email Encryption, and Email Archiving.

DUAL FACTOR AUTHENTICATION

Provides addtional security by requiring a password in combination with a token or passcode.

INTERNET CONTENT FILTERING

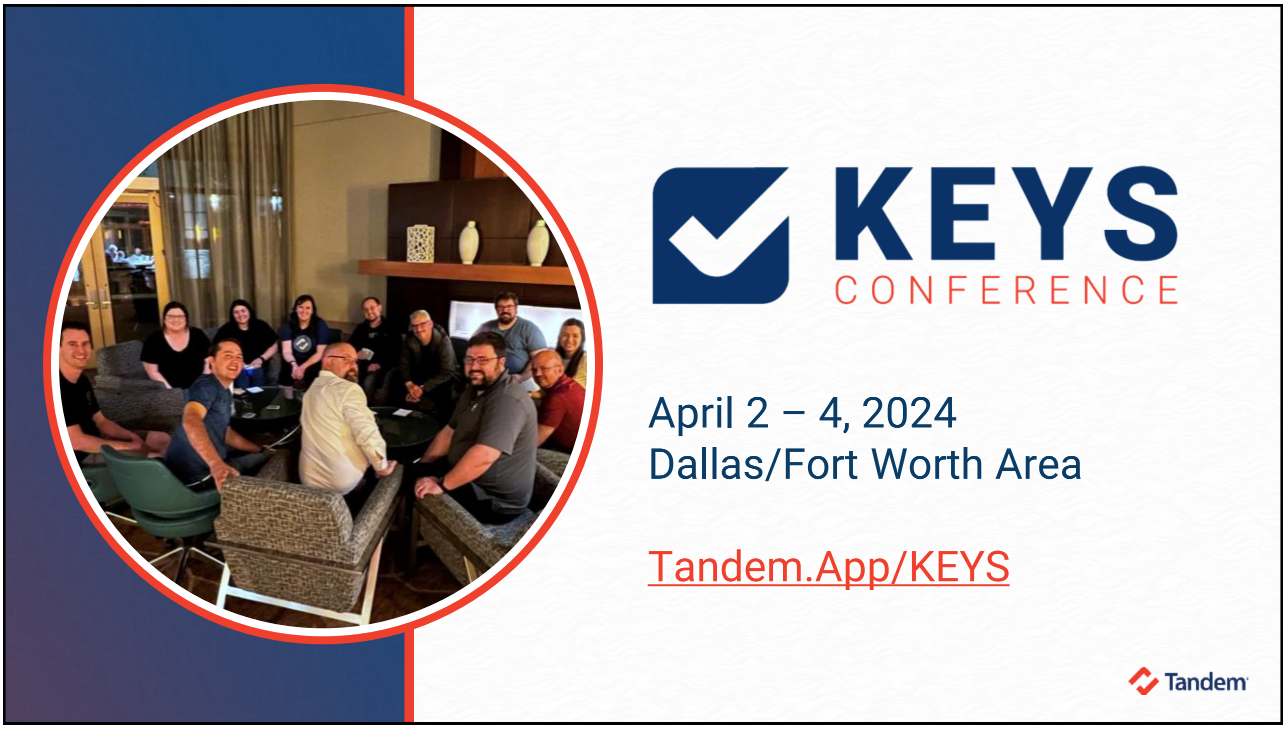
Provides content filtering for protection against malicious or inappropriate websites and compliance with company policies even when not connected to the corporate network.

CoNetrix Technology

Managed Technology Services and Network Support

CoNetrix.com/Technology

38



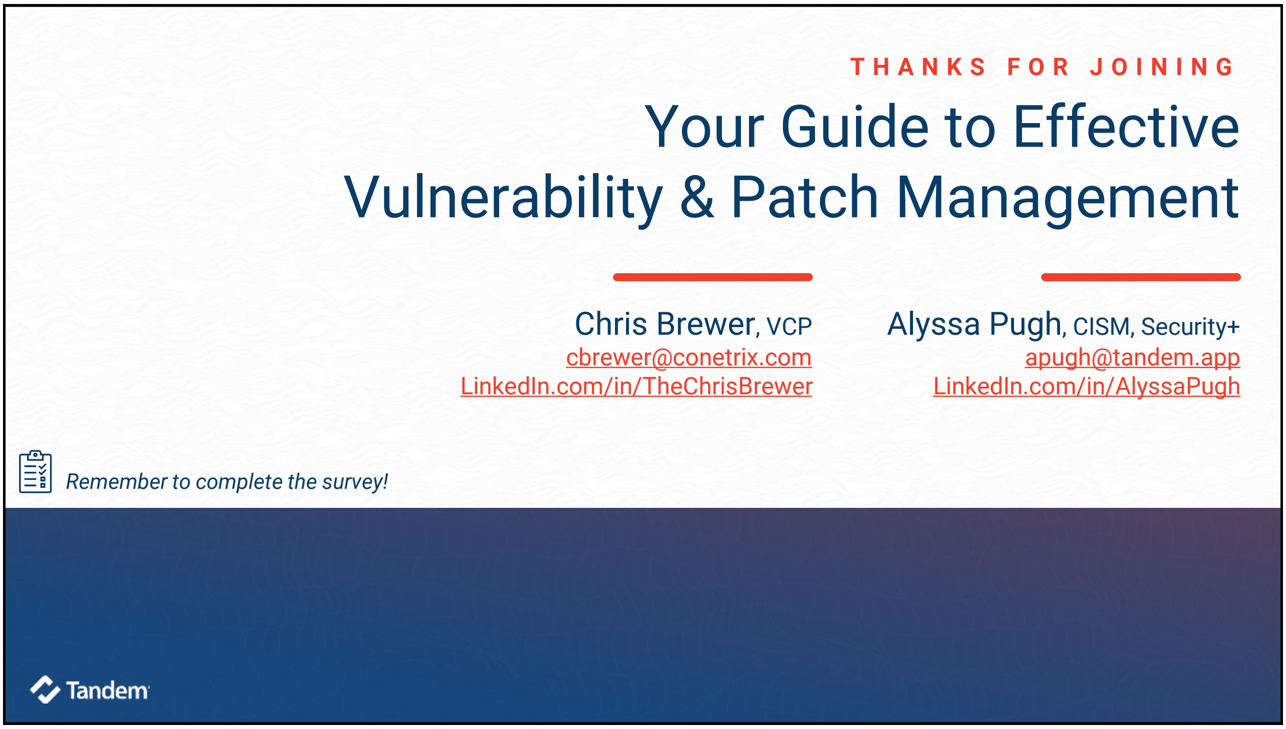
KEYS CONFERENCE

April 2 – 4, 2024
Dallas/Fort Worth Area

Tandem.App/KEYS

Tandem

39



THANKS FOR JOINING

Your Guide to Effective Vulnerability & Patch Management

Chris Brewer, VCP
cbrewer@conetrix.com
LinkedIn.com/in/TheChrisBrewer

Alyssa Pugh, CISM, Security+
apugh@tandem.app
LinkedIn.com/in/AlyssaPugh

Remember to complete the survey!

Tandem

40