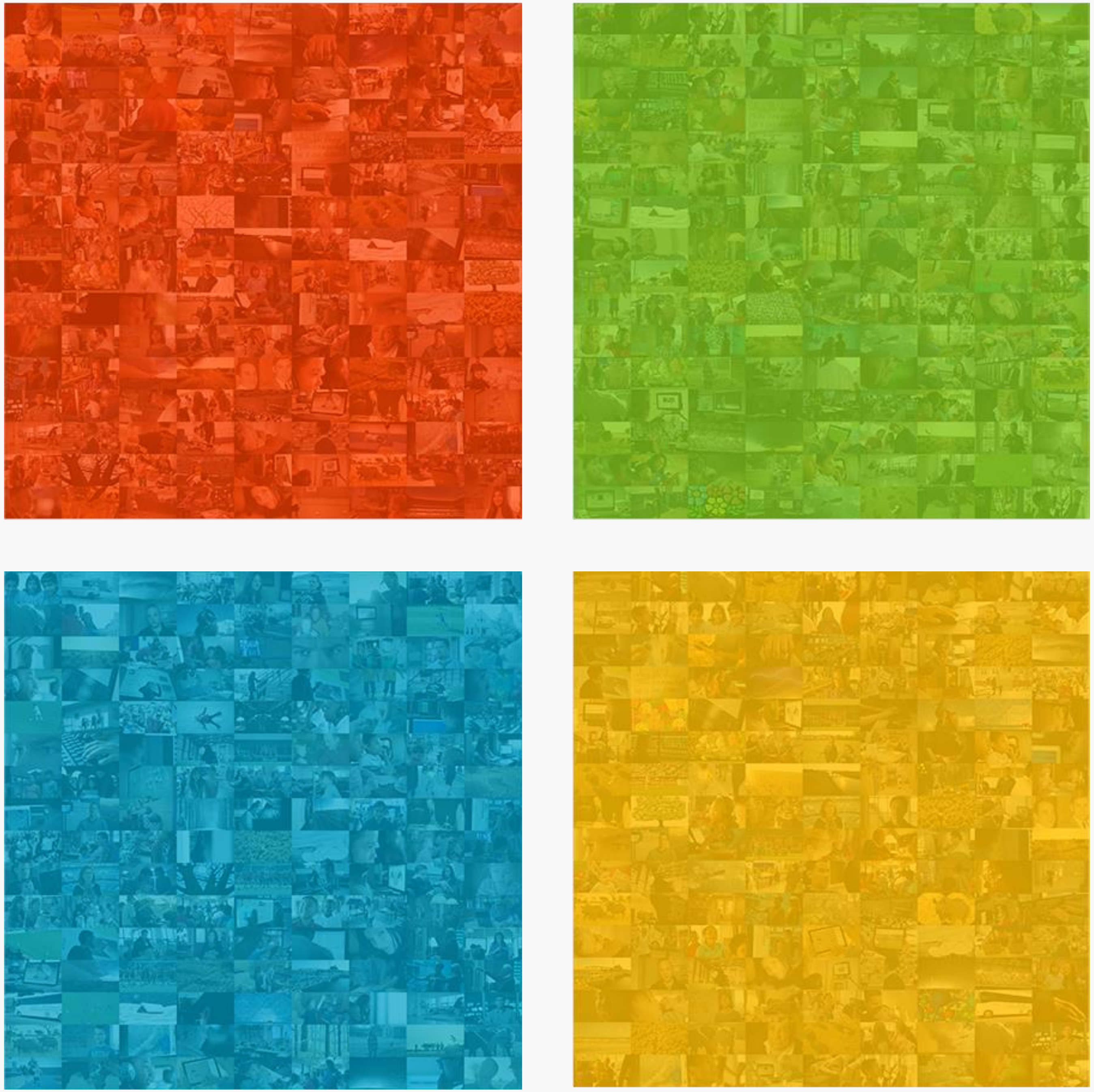
Microsoft

Security Update is Critical

Fred Sheu
NTO, Microsoft Hong Kong

Microsoft's mission

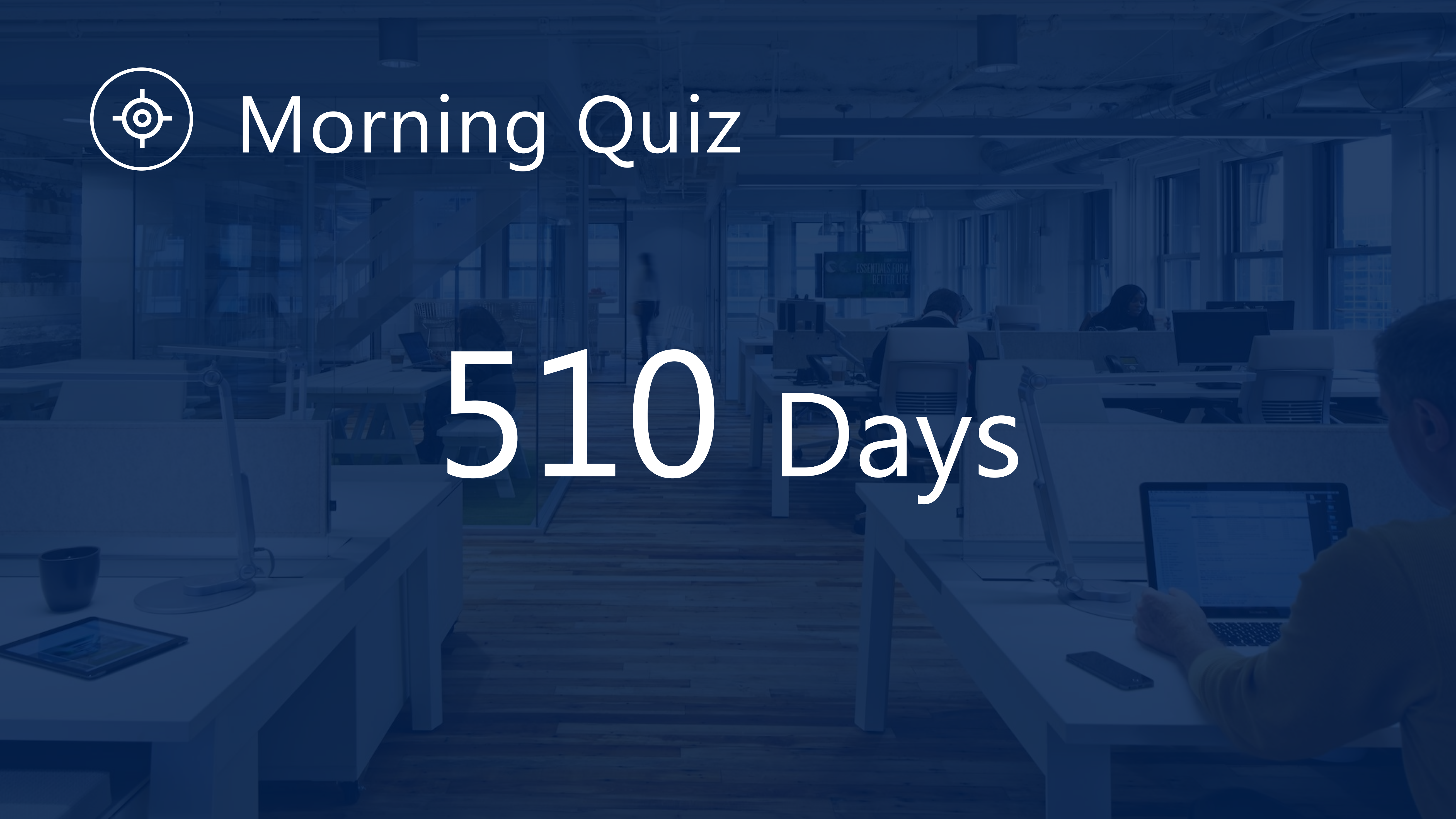
Empower every person and every organization on the planet to achieve more



Microsoft

“People will only use technology they trust.”

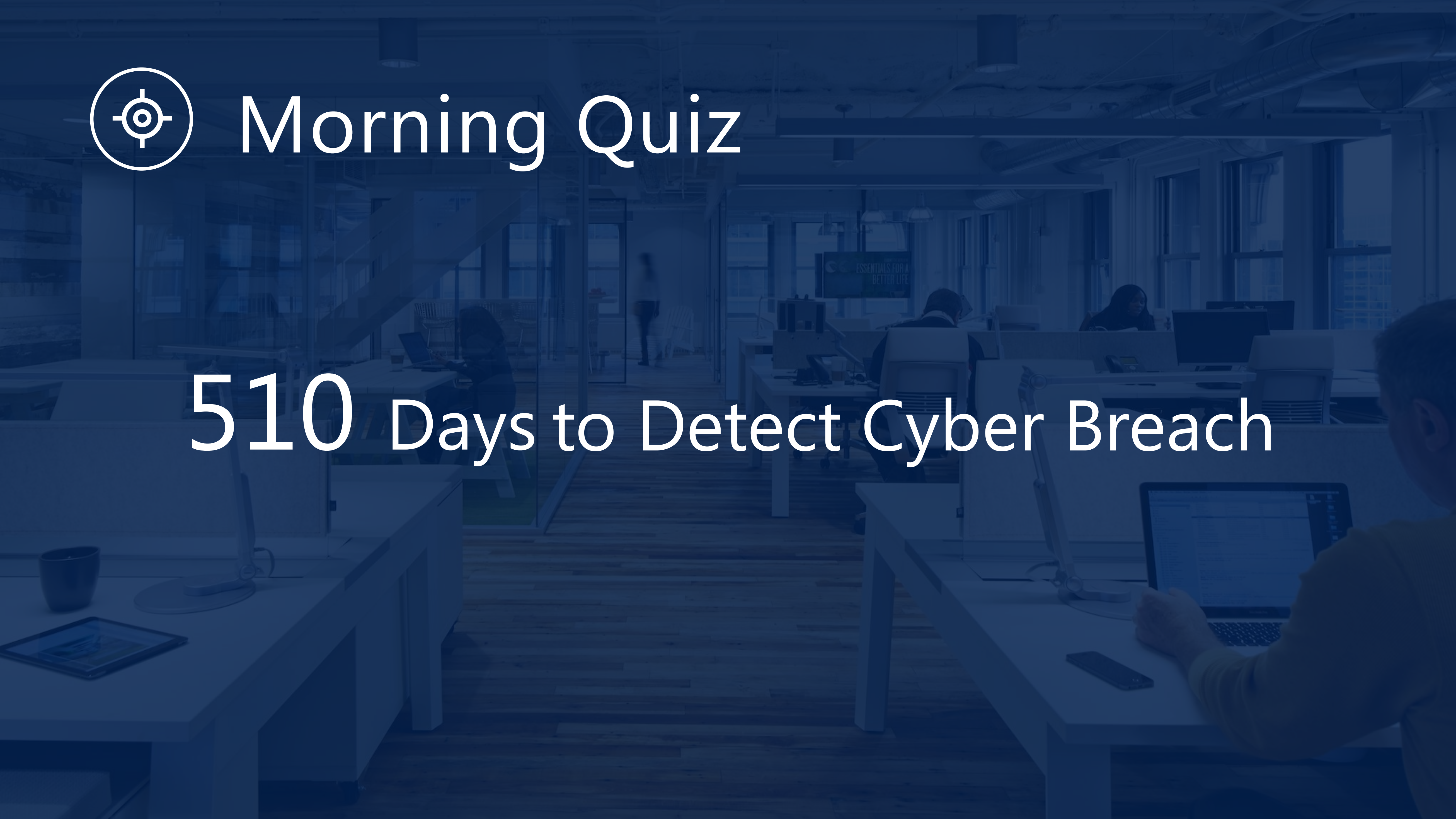
Brad Smith
President & Chief Legal Officer
Microsoft Corporation



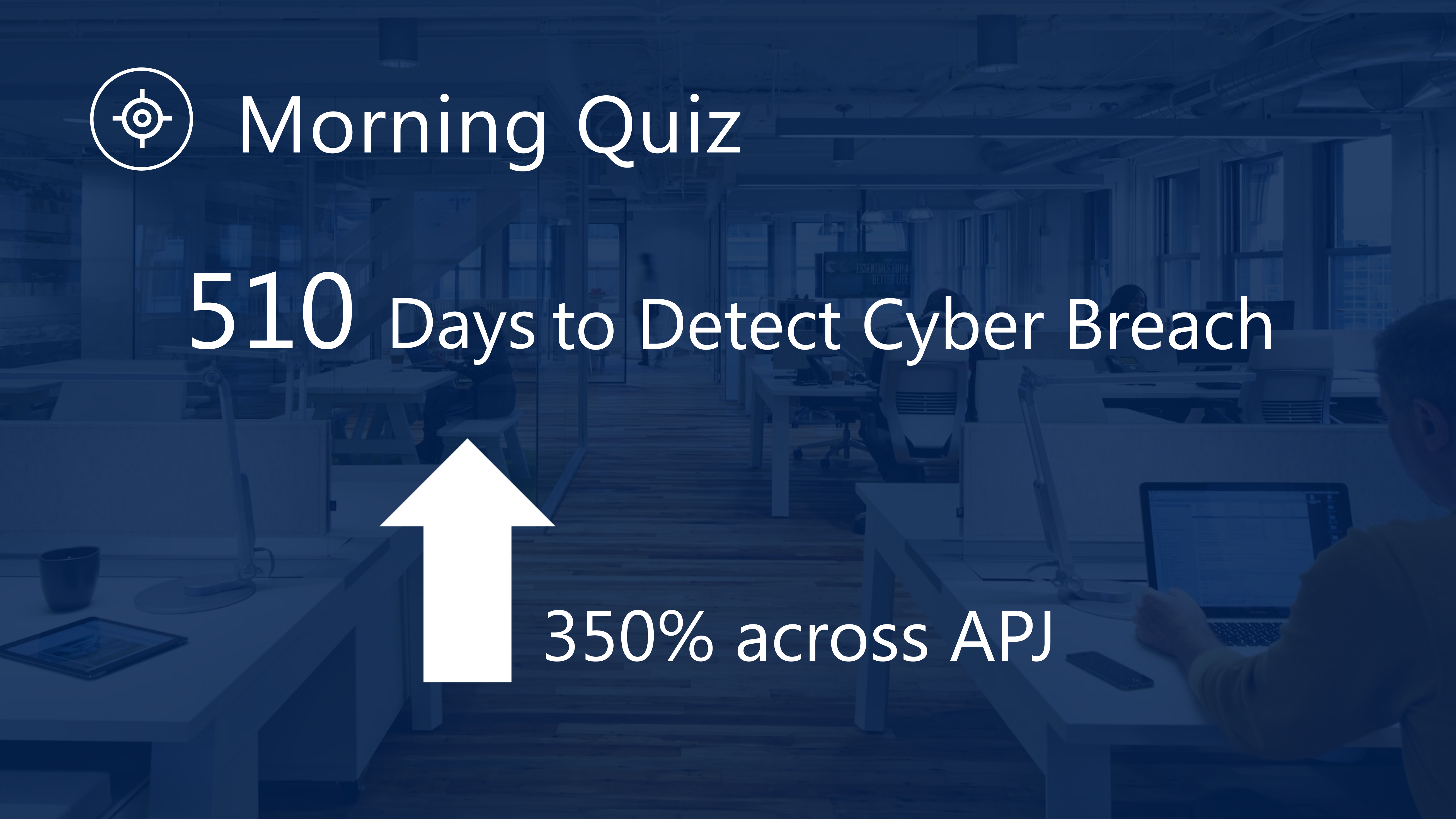
Morning Quiz

510 Days

Morning Quiz



510 Days to Detect Cyber Breach

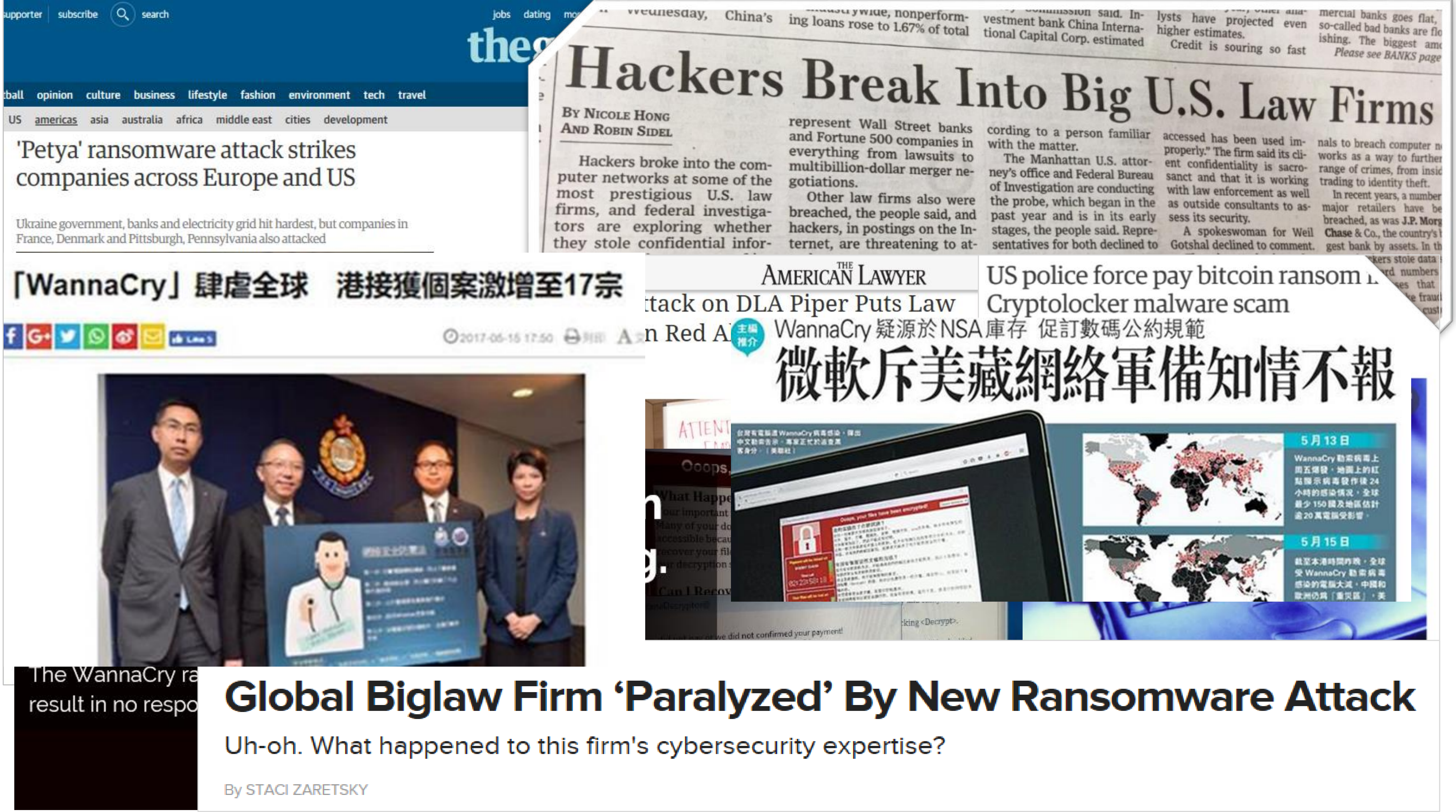


Morning Quiz

510 Days to Detect Cyber Breach

↑ 350% across APJ

The global impact of ransomware



upporter subscribe search jobs dating mo

theg

tball opinion culture business lifestyle fashion environment tech travel

US americas asia australia africa middle east cities development

'Petya' ransomware attack strikes companies across Europe and US

Ukraine government, banks and electricity grid hit hardest, but companies in France, Denmark and Pittsburgh, Pennsylvania also attacked

Wednesday, China's ... industrywide, nonperforming loans rose to 1.67% of total ... Commission said. Investment bank China International Capital Corp. estimated ... lysts have projected even higher estimates.

Credit is souring so fast ... mercial banks goes flat, so-called bad banks are flo ishing. The biggest amo

Please see BANKS page

Hackers Break Into Big U.S. Law Firms

By Nicole Hong And Robin Sidel

Hackers broke into the computer networks at some of the most prestigious U.S. law firms, and federal investigators are exploring whether they stole confidential infor- ... represent Wall Street banks and Fortune 500 companies in everything from lawsuits to multibillion-dollar merger negotiations.

Other law firms also were breached, the people said, and hackers, in postings on the Internet, are threatening to at- ... cording to a person familiar with the matter.

The Manhattan U.S. attorney's office and Federal Bureau of Investigation are conducting the probe, which began in the past year and is in its early stages, the people said. Representatives for both declined to ... accessed has been used improperly." The firm said its client confidentiality is sacrosanct and that it is working with law enforcement as well as outside consultants to assess its security.

A spokeswoman for Weil Gotshal declined to comment. ... nals to breach computer n works as a way to further range of crimes, from insid trading to identity theft.

In recent years, a number major retailers have be breached, as was J.P. Morg Chase & Co., the country's b gest bank by assets. In th ... kers stole data ... rd numbers ... ses that ... e fraud ... cust

「WannaCry」肆虐全球　港接獲個案激增至17宗

2017-06-15 17:50

THE AMERICAN LAWYER

ttack on DLA Piper Puts Law

n Red A

US police force pay bitcoin ransom i Cryptolocker malware scam

主編推介

WannaCry疑源於NSA庫存 促訂數碼公約規範

微軟斥美藏網絡軍備知情不報

台灣有電腦遭WannaCry病毒感染，彈出中文勒索告示，專家正忙於追查黑客身分。（美聯社）

5月13日

WannaCry勒索病毒上周五爆發，地圖上的紅點顯示病毒發作後24小時的感染情況，全球最少150國及地區估計逾20萬電腦受影響。

5月15日

截至本港時間昨晚，全球受WannaCry勒索病毒感染的電腦大減，中國和歐洲仍為「重災區」，美

Ooops, your files have been encrypted!

What Happe

our important

Many of your do

accessible becau

ecover your fil

ur decryption s

Can I Recov

we did not confirmed your payment!

king <Decrypt>.

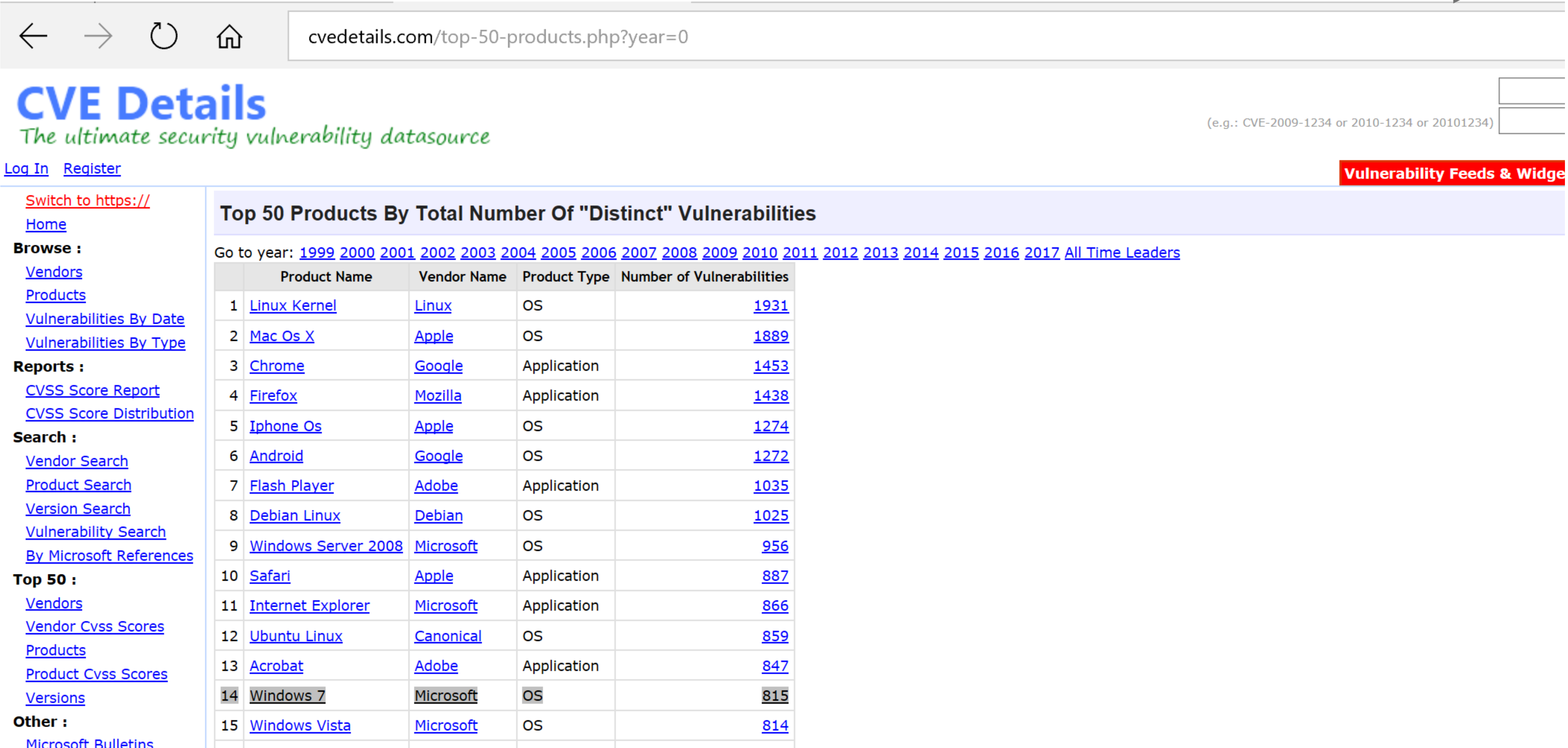
The WannaCry ra result in no respo

Global Biglaw Firm 'Paralyzed' By New Ransomware Attack

Uh-oh. What happened to this firm's cybersecurity expertise?

By STACI ZARETSKY

Software with highest vulnerabilities



cvedetails.com/top-50-products.php?year=0

CVE Details

The ultimate security vulnerability datasource

Log In Register

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Vulnerability Feeds & Widge

Switch to https://

Home

Browse :

- Vendors
- Products
- Vulnerabilities By Date
- Vulnerabilities By Type

Reports :

- CVSS Score Report
- CVSS Score Distribution

Search :

- Vendor Search
- Product Search
- Version Search
- Vulnerability Search
- By Microsoft References

Top 50 :

- Vendors
- Vendor Cvss Scores
- Products
- Product Cvss Scores
- Versions

Other :

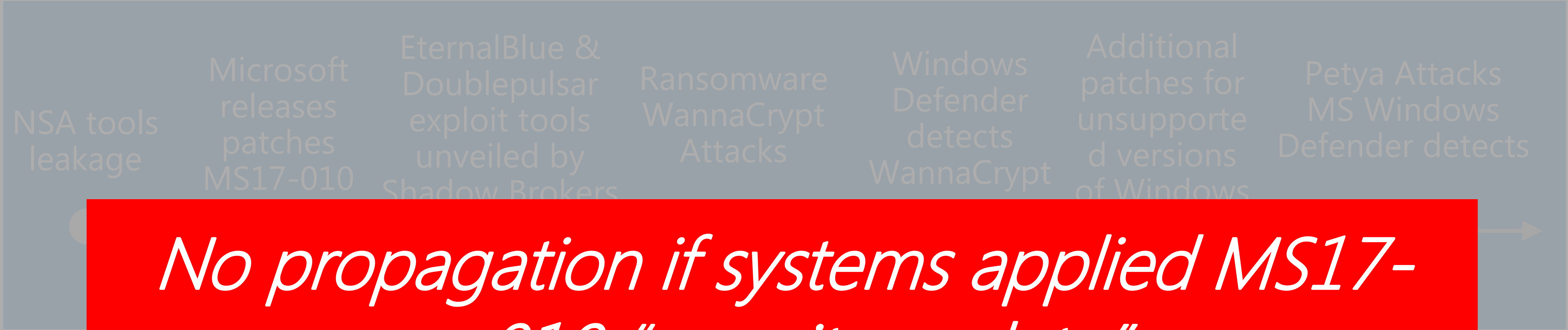
- Microsoft Bulletins

Top 50 Products By Total Number Of "Distinct" Vulnerabilities

Go to year: 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 All Time Leaders

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Linux Kernel	Linux	OS	1931
2	Mac Os X	Apple	OS	1889
3	Chrome	Google	Application	1453
4	Firefox	Mozilla	Application	1438
5	Iphone Os	Apple	OS	1274
6	Android	Google	OS	1272
7	Flash Player	Adobe	Application	1035
8	Debian Linux	Debian	OS	1025
9	Windows Server 2008	Microsoft	OS	956
10	Safari	Apple	Application	887
11	Internet Explorer	Microsoft	Application	866
12	Ubuntu Linux	Canonical	OS	859
13	Acrobat	Adobe	Application	847
14	Windows 7	Microsoft	OS	815
15	Windows Vista	Microsoft	OS	814

WannaCrypt and Petya – Timeline & facts


NSA tools leakage

Microsoft releases patches MS17-010

EternalBlue & Doublepulsar exploit tools unveiled by Shadow Brokers

Ransomware WannaCrypt Attacks

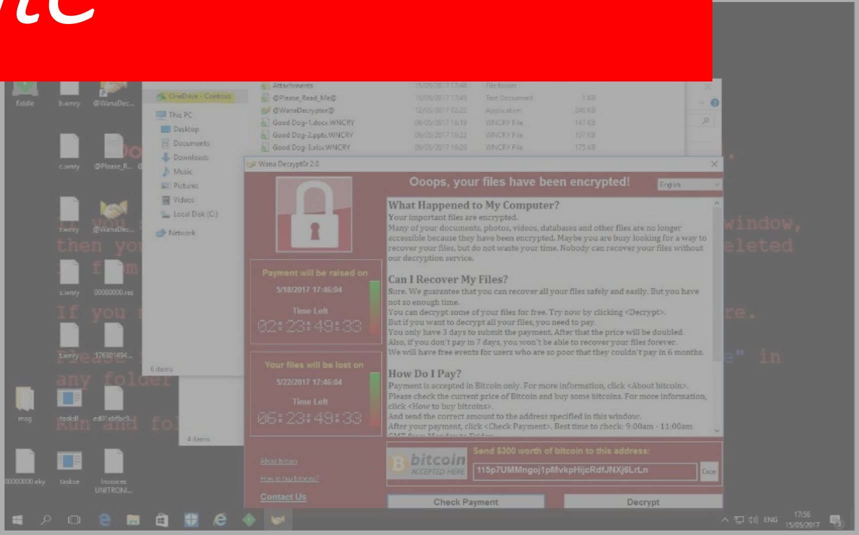
Windows Defender detects WannaCrypt

Additional patches for unsupported versions of Windows

Petya Attacks MS Windows Defender detects

No propagation if systems applied MS17-010 "security update"

- G
- Targeting Windows 7 or below
- Leveraged Windows SMB v.1 vulnerability to spread
- Encrypted files (WannaCry) or crashed OS (Petya)
- Demand payment by Bitcoin (approx. US$300 – 600)
- No propagation for systems applied MS17-010 security update


Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on 5/18/2017 17:46:04 Time Left 02:23:49:33

Your files will be lost on 5/22/2017 17:46:04 Time Left 06:23:49:33

Send $300 worth of bitcoin to this address: 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

YOUR

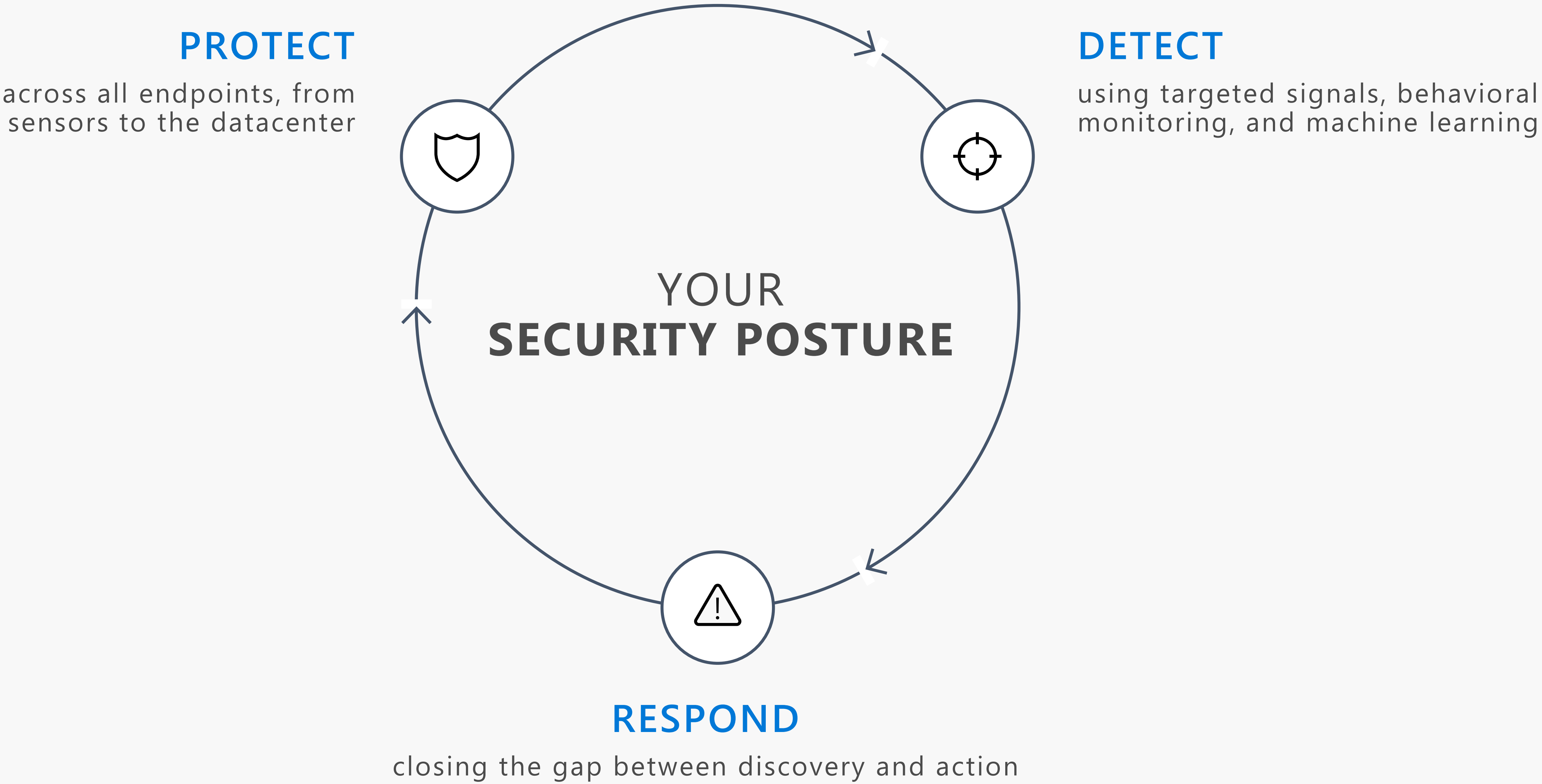
IT ENVIRONMENT

YOUR

IT ENVIRONMENT

YOUR
IT ENVIRONMENT

YOUR
OPPORTUNITY



YOUR

SECURITY POSTURE

PROTECT

across all endpoints, from
sensors to the datacenter

DETECT

using targeted signals, behavioral
monitoring, and machine learning

RESPOND

closing the gap between discovery and action

MICROSOFT TECHNICAL SECURITY NOTIFICATIONS

Free Monthly Security Update Email Alerts

Security-related software updates and notification of re-released security updates

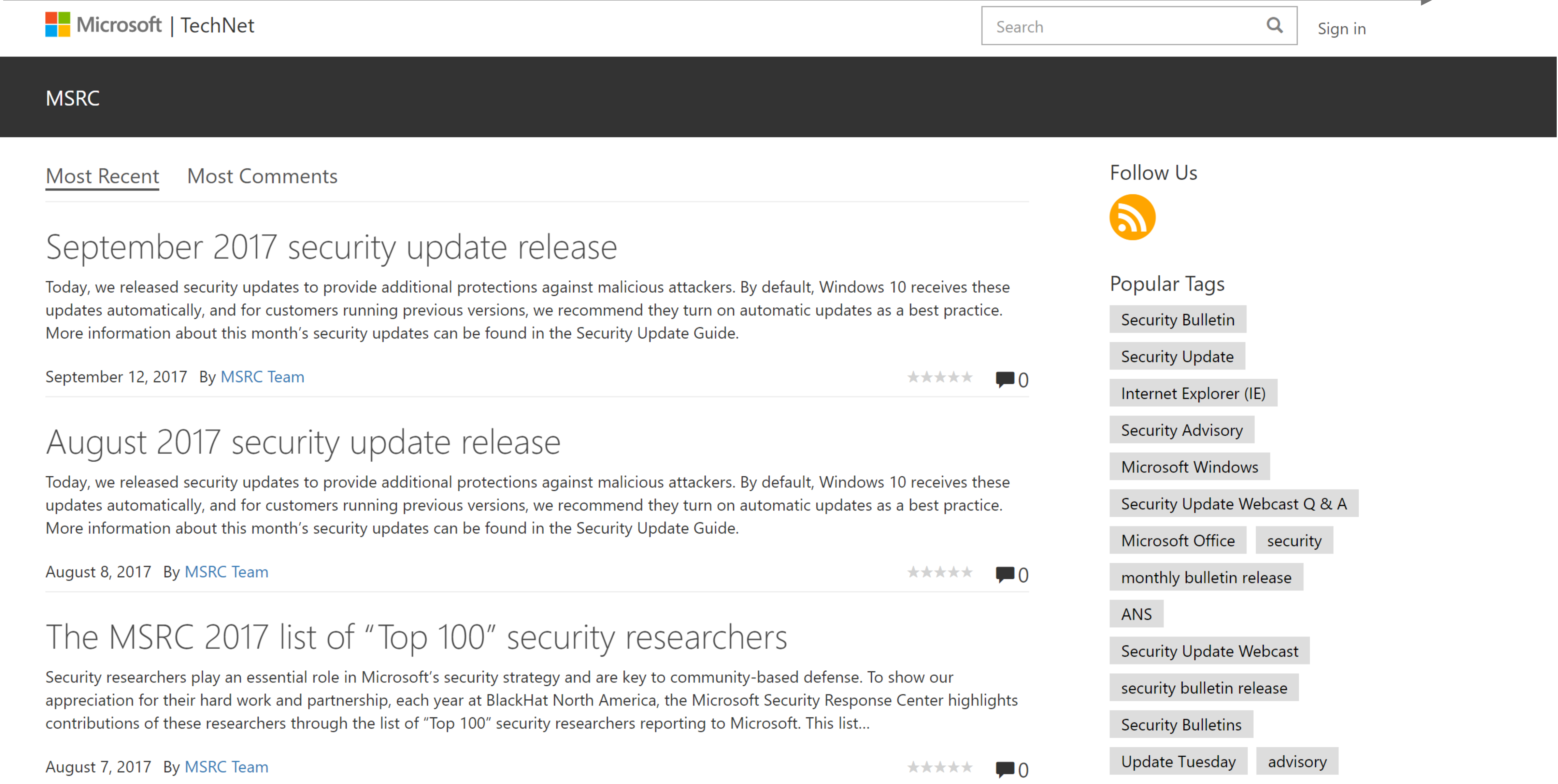
Security Advisories Alerts

issues that may not be classified as vulnerabilities and may not require a security bulletin

Microsoft Security Response Center (MSRC) Blog Alerts

Provide a real-time way for the MSRC to communicate with customers

Microsoft Security Response Center (MSRC) Blog Alerts



September 2017 security update release

Today, we released security updates to provide additional protections against malicious attackers. By default, Windows 10 receives these updates automatically, and for customers running previous versions, we recommend they turn on automatic updates as a best practice. More information about this month's security updates can be found in the Security Update Guide.

September 12, 2017 By MSRC Team ★★★★★ 0

August 2017 security update release

Today, we released security updates to provide additional protections against malicious attackers. By default, Windows 10 receives these updates automatically, and for customers running previous versions, we recommend they turn on automatic updates as a best practice. More information about this month's security updates can be found in the Security Update Guide.

August 8, 2017 By MSRC Team ★★★★★ 0

The MSRC 2017 list of "Top 100" security researchers

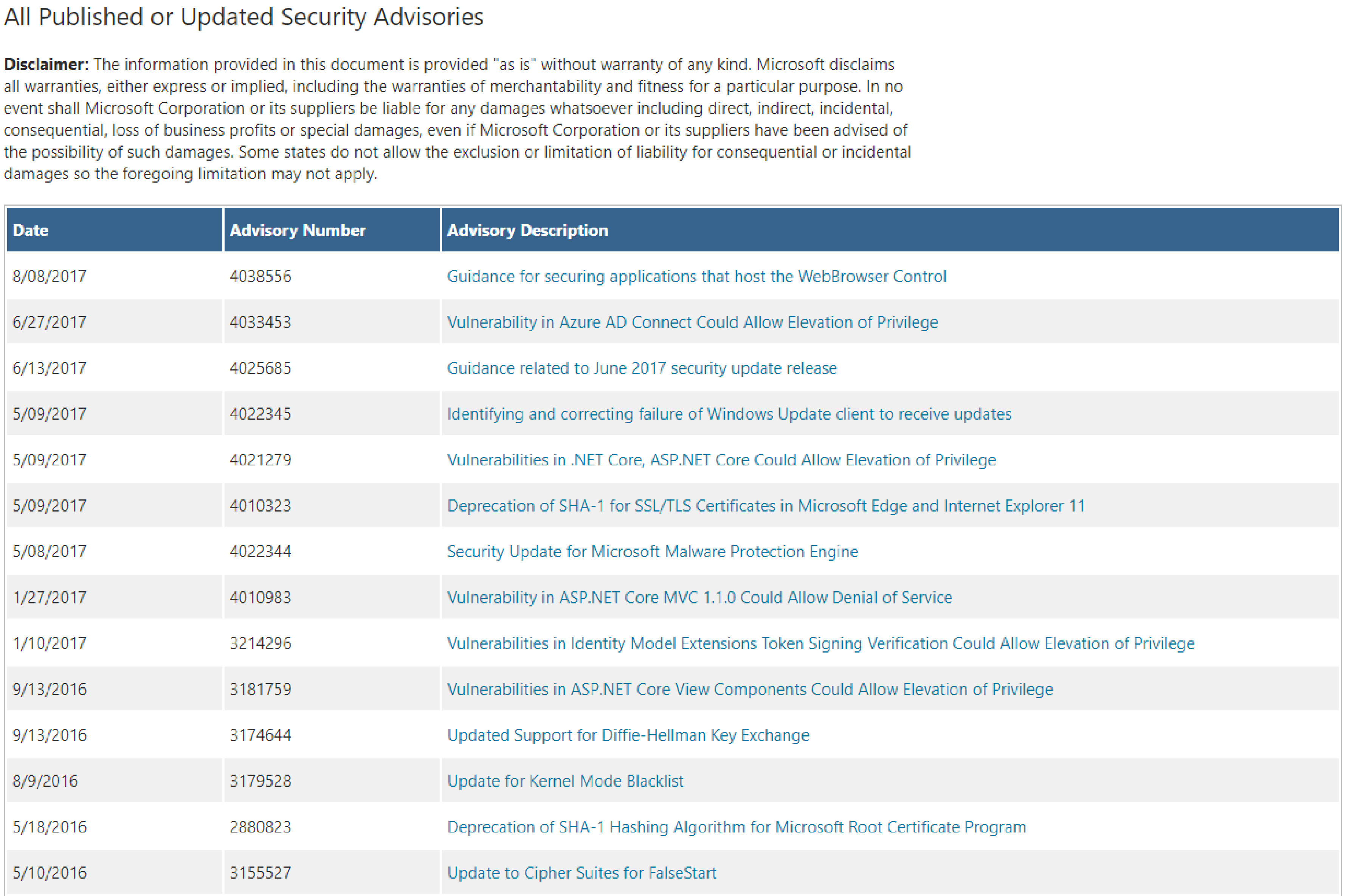
Security researchers play an essential role in Microsoft's security strategy and are key to community-based defense. To show our appreciation for their hard work and partnership, each year at BlackHat North America, the Microsoft Security Response Center highlights contributions of these researchers through the list of "Top 100" security researchers reporting to Microsoft. This list...

August 7, 2017 By MSRC Team ★★★★★ 0

Popular Tags

- Security Bulletin
- Security Update
- Internet Explorer (IE)
- Security Advisory
- Microsoft Windows
- Security Update Webcast Q & A
- Microsoft Office
- security
- monthly bulletin release
- ANS
- Security Update Webcast
- security bulletin release
- Security Bulletins
- Update Tuesday
- advisory

Security Advisories Alerts



All Published or Updated Security Advisories

Disclaimer: The information provided in this document is provided "as is" without warranty of any kind. Microsoft disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Microsoft Corporation or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Microsoft Corporation or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Date	Advisory Number	Advisory Description
8/08/2017	4038556	Guidance for securing applications that host the WebBrowser Control
6/27/2017	4033453	Vulnerability in Azure AD Connect Could Allow Elevation of Privilege
6/13/2017	4025685	Guidance related to June 2017 security update release
5/09/2017	4022345	Identifying and correcting failure of Windows Update client to receive updates
5/09/2017	4021279	Vulnerabilities in .NET Core, ASP.NET Core Could Allow Elevation of Privilege
5/09/2017	4010323	Deprecation of SHA-1 for SSL/TLS Certificates in Microsoft Edge and Internet Explorer 11
5/08/2017	4022344	Security Update for Microsoft Malware Protection Engine
1/27/2017	4010983	Vulnerability in ASP.NET Core MVC 1.1.0 Could Allow Denial of Service
1/10/2017	3214296	Vulnerabilities in Identity Model Extensions Token Signing Verification Could Allow Elevation of Privilege
9/13/2016	3181759	Vulnerabilities in ASP.NET Core View Components Could Allow Elevation of Privilege
9/13/2016	3174644	Updated Support for Diffie-Hellman Key Exchange
8/9/2016	3179528	Update for Kernel Mode Blacklist
5/18/2016	2880823	Deprecation of SHA-1 Hashing Algorithm for Microsoft Root Certificate Program
5/10/2016	3155527	Update to Cipher Suites for FalseStart

Microsoft Secure

Ensuring security to enable your digital transformation through a comprehensive platform, unique intelligence, and broad partnerships

Microsoft

Microsoft Secure

Ensuring security to enable your digital transformation through a comprehensive platform, unique intelligence, and broad partnerships

Useful Link

Microsoft