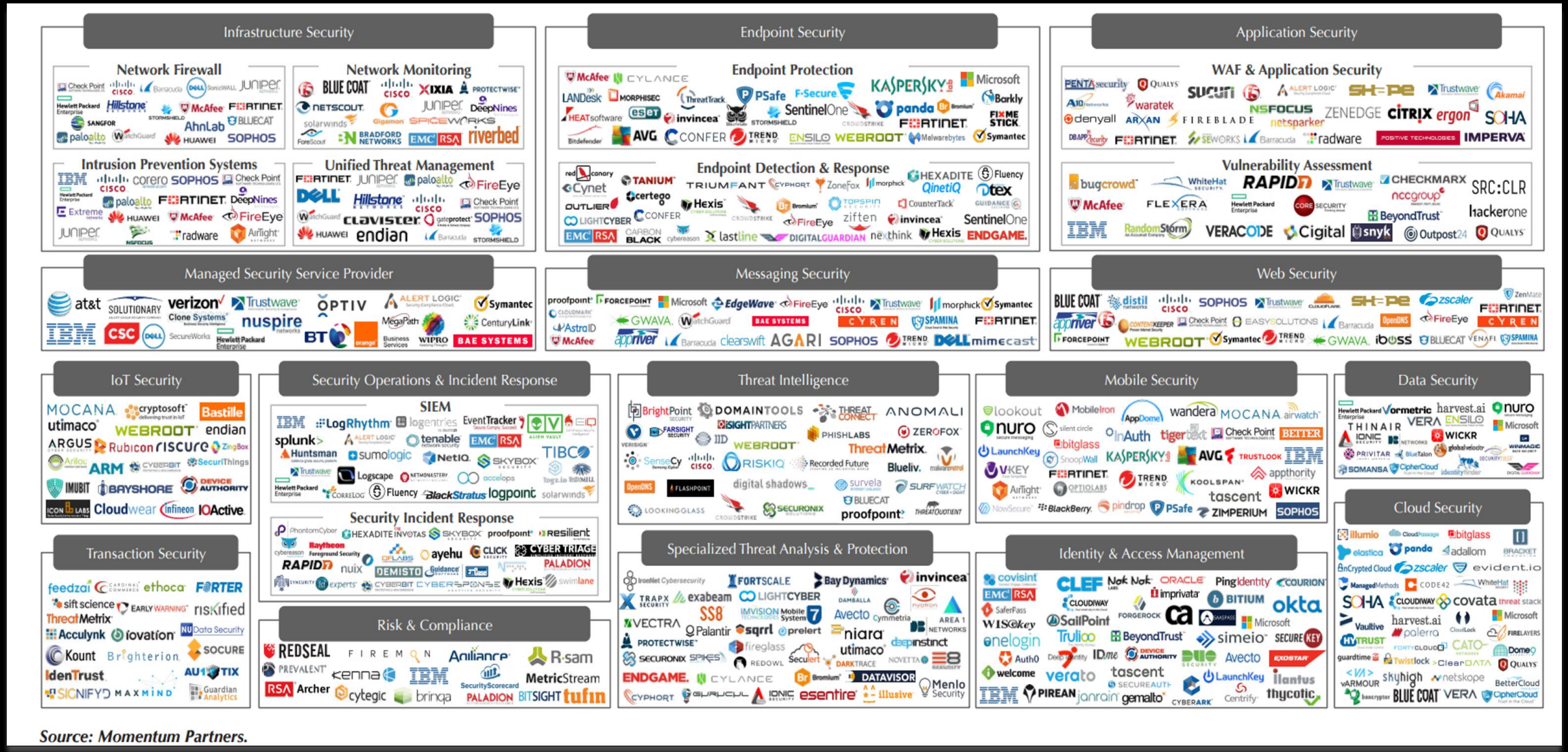
Rising Cyberthreats in Taiwan –

Building a Security Platform

Michael F Montoya
Chief Cybersecurity Officer
Microsoft Enterprise CyberSecurity Group, Asia

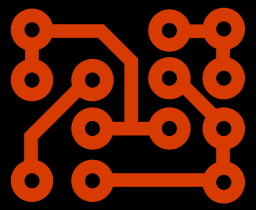
How did we end up here?

140+ Security Solutions at average Enterprise



Source: Momentum Partners.

Our traditional solutions

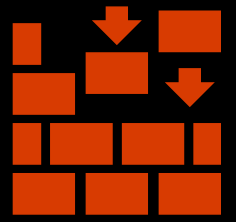


Complexity

Initial setup, fine-tuning, creating rules and thresholds/baselines can take a long time.

Prone to false positives

You receive too many reports in a day with several false positives that require valuable time you don't have.



Designed to protect the perimeter

When user credentials are stolen and attackers are in the network, your current defenses provide limited protection.

Asia cybersecurity amongst the least mature

>95%

ENTERPRISES UNKNOWINGLY HOST COMPROMISED ENDPOINTS

2X

LIKELIHOOD TO BE HACKED VS. THE GLOBAL AVERAGE

510 DAYS

TO DETECT A COMPROMISE

86% of Attacks

MINUTES FOR ATTACKERS TO COMPROMISE THE SYTEMS

55%

DETECTIONS FROM EXTERNAL SOURCE

Hard truths

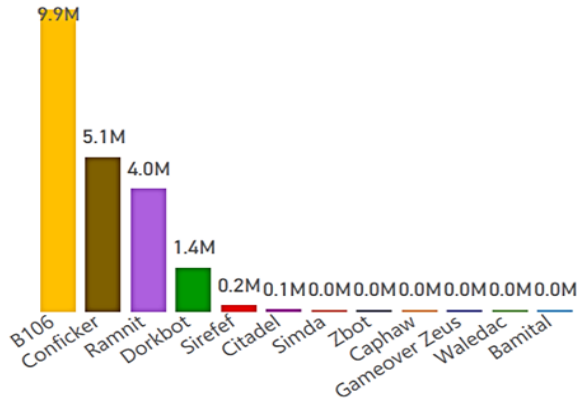
Digital Crimes Unit

15,591,784	44	229	7,397,125,721	12/1/2016	3/10/2017
Distinct IPs	Countries	Threats	Connections	Start Date	End Date

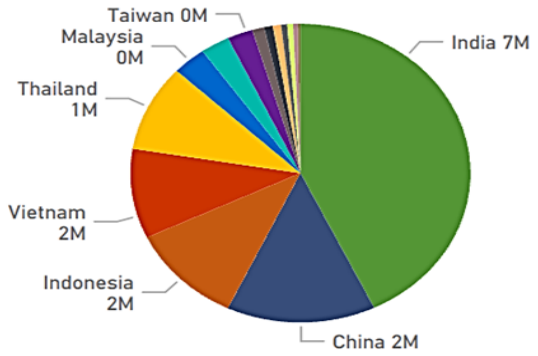
Select Area

Asia | EMEA | Latam | North America | Unknown

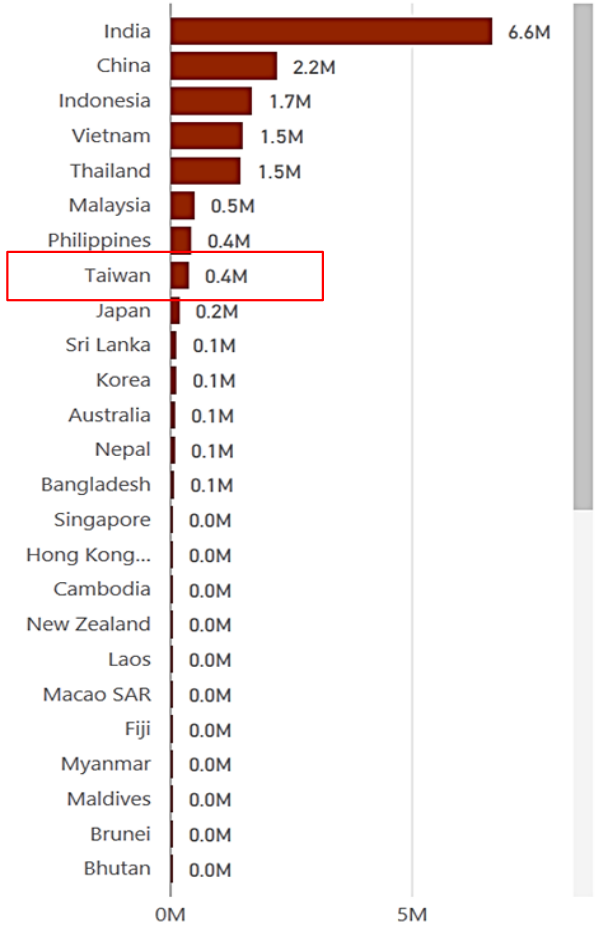
Distinct IPs by Threat



Distinct IPs by Country



Distinct IPs by Country



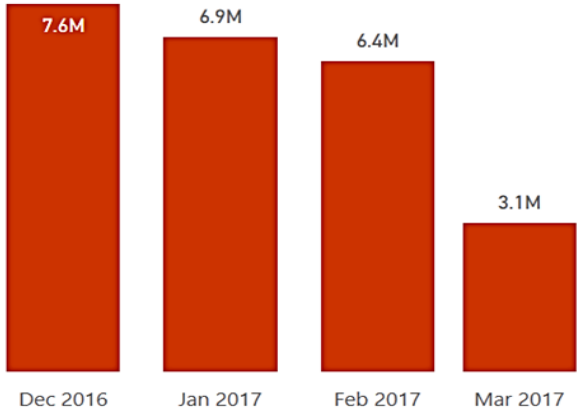
Month

Decemb... 2016 | January 2017 | February 2017 | March 2017

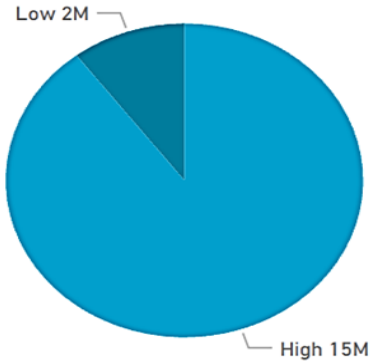
Week

1 2 3 4 5

Distinct IPs by Month



Distinct IPs by Confidence Level



Date

- 12/1/2016
- 12/2/2016
- 12/3/2016
- 12/4/2016
- 12/5/2016
- 12/6/2016
- 12/7/2016
- 12/8/2016
- 12/9/2016
- 12/10/2016
- 12/11/2016
- 12/12/2016
- 12/13/2016
- 12/14/2016
- 12/15/2016
- 12/16/2016
- 12/17/2016
- 12/18/2016
- 12/19/2016
- 12/20/2016
- 12/21/2016

Threat

- B106
- Bamital
- Caphaw
- Citadel
- Conficker
- Dorkbot
- Gameover Zeus
- Ramnit
- Rustock
- Simda
- Sirefef
- Waledac
- Zbot

Taiwan active risk

Digital Crimes Unit

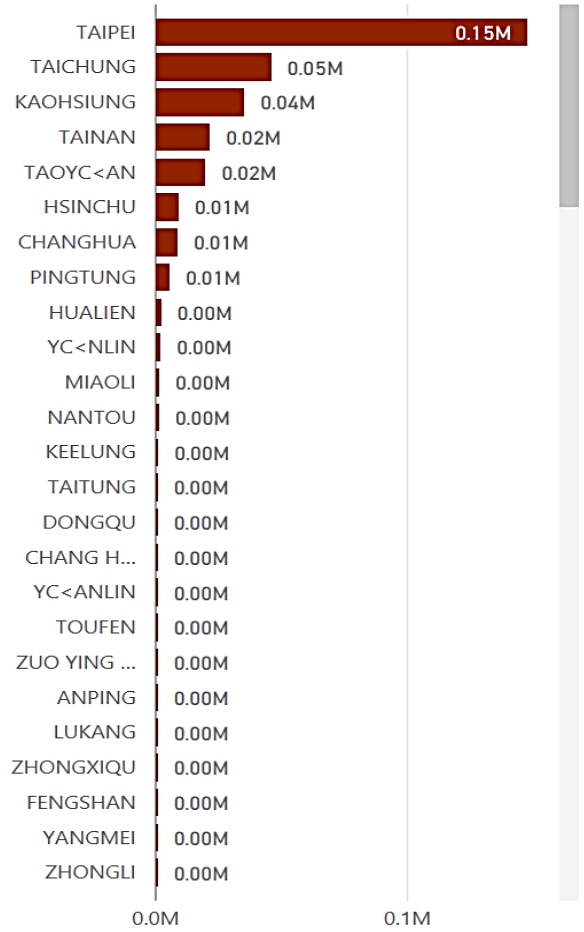
374,932	1	227	139,793,840	12/1/2016	3/10/2017
Distinct IPs	Countries	Threats	Connections	Start Date	End Date

Select Area

Asia | EMEA | Latam | North America | Unknown

Connections by Country

Distinct IPs by City



Month

Decemb... 2016 | January 2017 | February 2017 | March 2017

Week

1 2 3 4 5

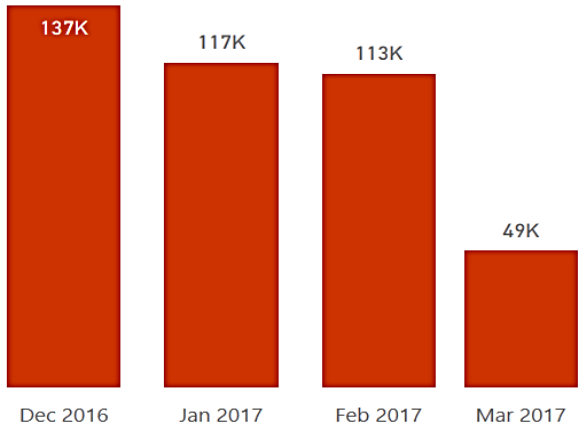
Date

- 12/1/2016
- 12/2/2016
- 12/3/2016
- 12/4/2016
- 12/5/2016

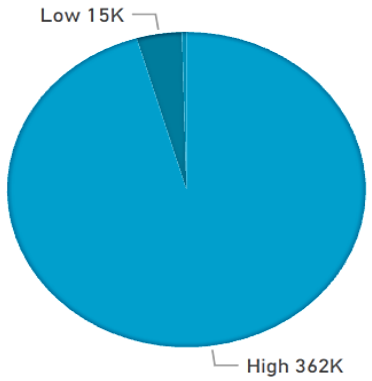
Threat

- B106
- Bamital
- Caphaw
- Citadel
- Conficker
- Dorkbot
- Gameover Zeus
- Ramnit
- Rustock

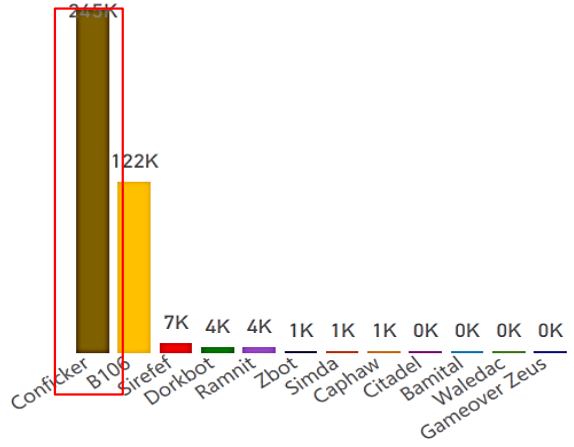
Distinct IPs by Month



Distinct IPs by Confidence Level



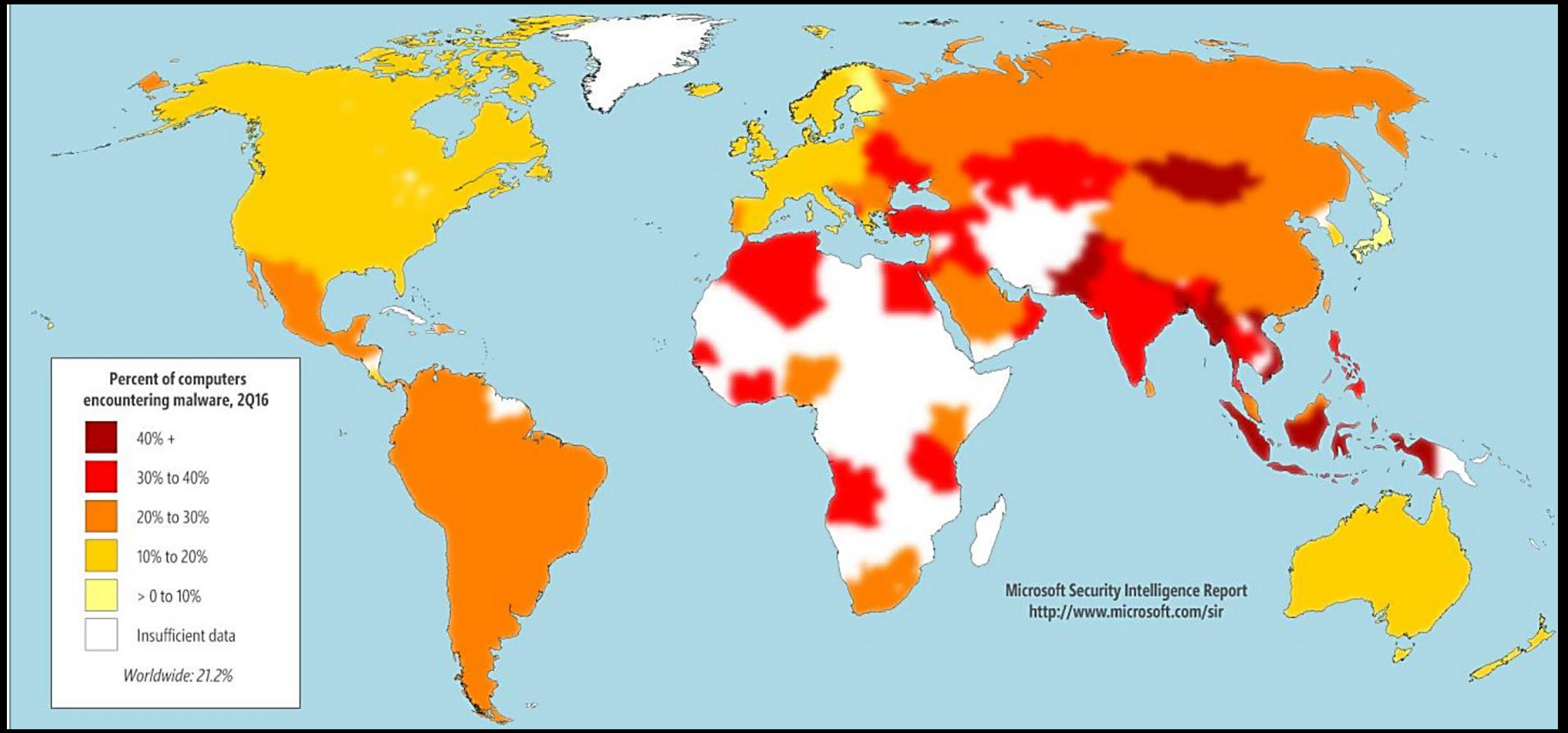
Distinct IPs by Threat



Harder facts

Global Malware Encounter Rate

Microsoft Security Intelligence Report (SIR), Volume 21

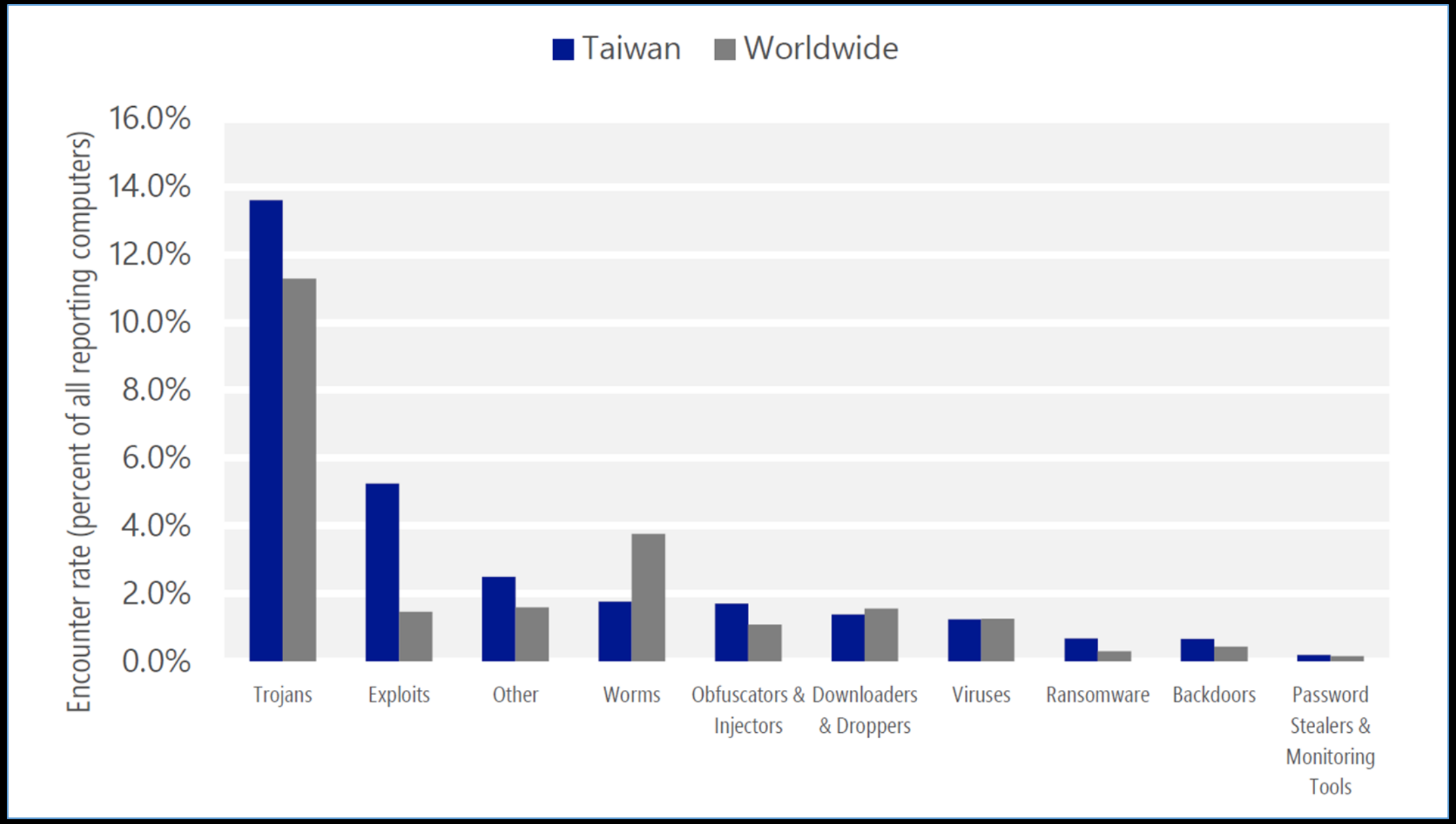


Taiwan malware

Top Active Malware in Taiwan

	Family	Most significant category
1	JS/Axpergle	Exploits
2	Win32/Spursint	Trojans
3	Win32/Rundas	Trojans
4	Win32/Dynamer	Trojans
5	Win32/Obfuscator	Obfuscators & Injectors
6	INF/Autorun	Obfuscators & Injectors
7	JS/NeutrinoEK	Exploits
8	Win32/Wpakill	Other Malware
9	HTML/Meadgive	Exploits
10	Win32/Skeeyah	Trojans

Malware encountered in Taiwan vs Global



Cybersecurity is Microsoft's #1 priority

Building a cybersecurity posture

ASSUME YOU ARE BREACHED!

1. IT **Hygiene** matters
2. No more **Antivirus**
3. **Protect** the critical **email application** vector
4. Implement an intelligence **detection platform** not dependent on signatures
5. Employ an advanced **cybersecurity response and operations**

1 Hygiene – minimum operating guidelines

Know your environment

- How many users, endpoints, network devices, data classification and location

Patching and maintenance updates

- Ensure genuine software, current versions, hotfixes and security updates

Strong password management and disc encryption

- Complex passwords and change policy, multi-factor authentication, disc encryption

Hardened Administration and Network configurations

- Hardened networks, ports, authentication and access controls

Logging

- Maintain accurate logs and reporting

2 Endpoint protect…hasta la vista Antivirus

THE **WINDOWS 10** DEFENSE STACK

PROTECT, DETECT & RESPOND

PRE-BREACH

POST-BREACH

Device protection

Device integrity

Device control

Threat resistance

SmartScreen

Windows Firewall

Microsoft Edge

Device Guard

Windows Defender

Identity protection

Windows Hello :)

Credential Guard

Information protection

BitLocker and BitLocker to Go

Windows Information Protection

Breach detection investigation & response

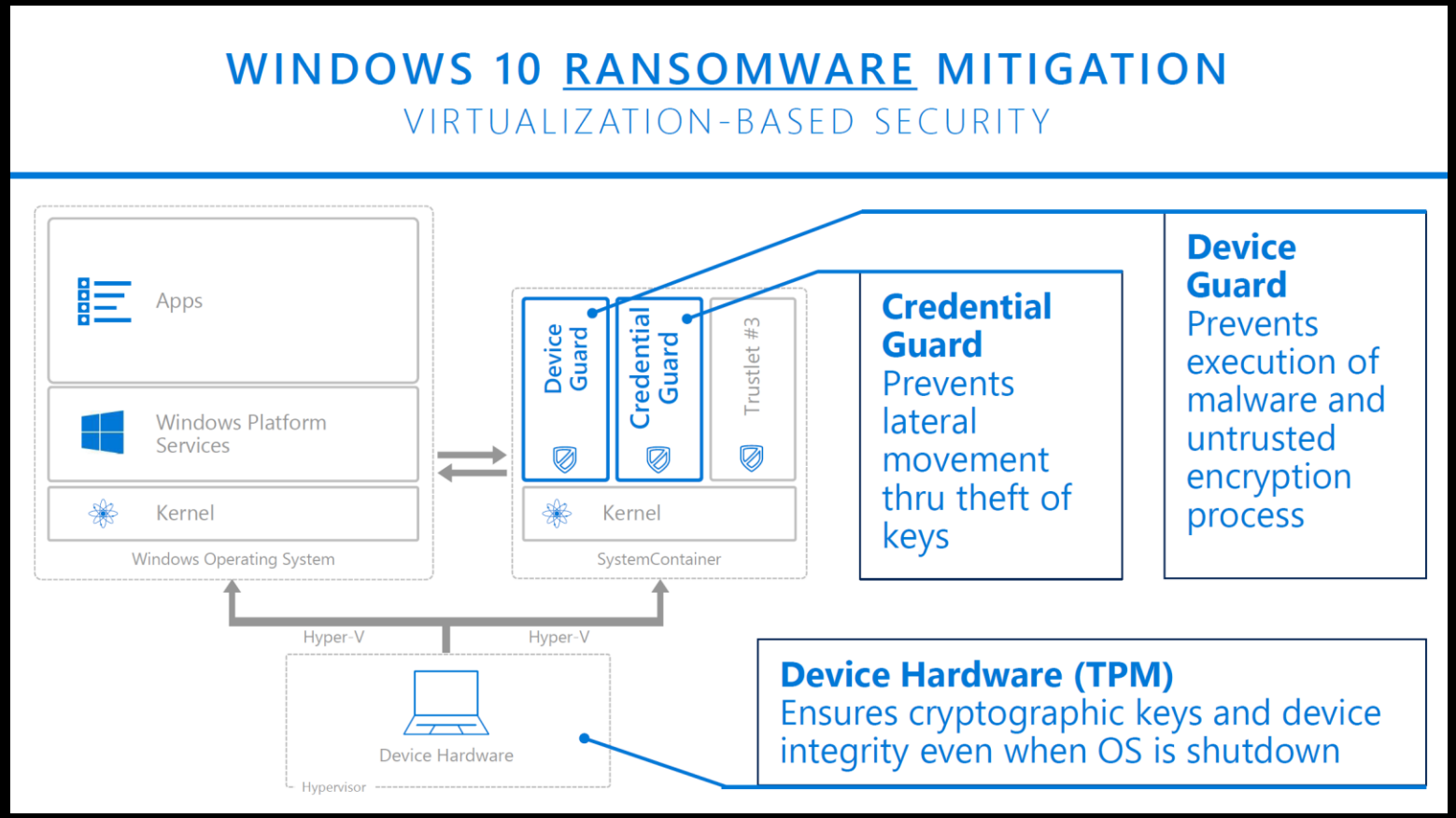
Conditional Access

Windows Defender ATP

2 Endpoint protect…hasta la vista Antivirus

- Pass the Hash (PtH) attacks are the #1 go-to tool for hackers. Used in nearly every major breach and APT type of attack
- Credential Guard uses VBS to isolate Windows authentication from Windows operating system
- Protects LSA Service (LSASS) and derived credentials (NTLM Hash)
- Fundamentally breaks derived credential theft using MimiKatz

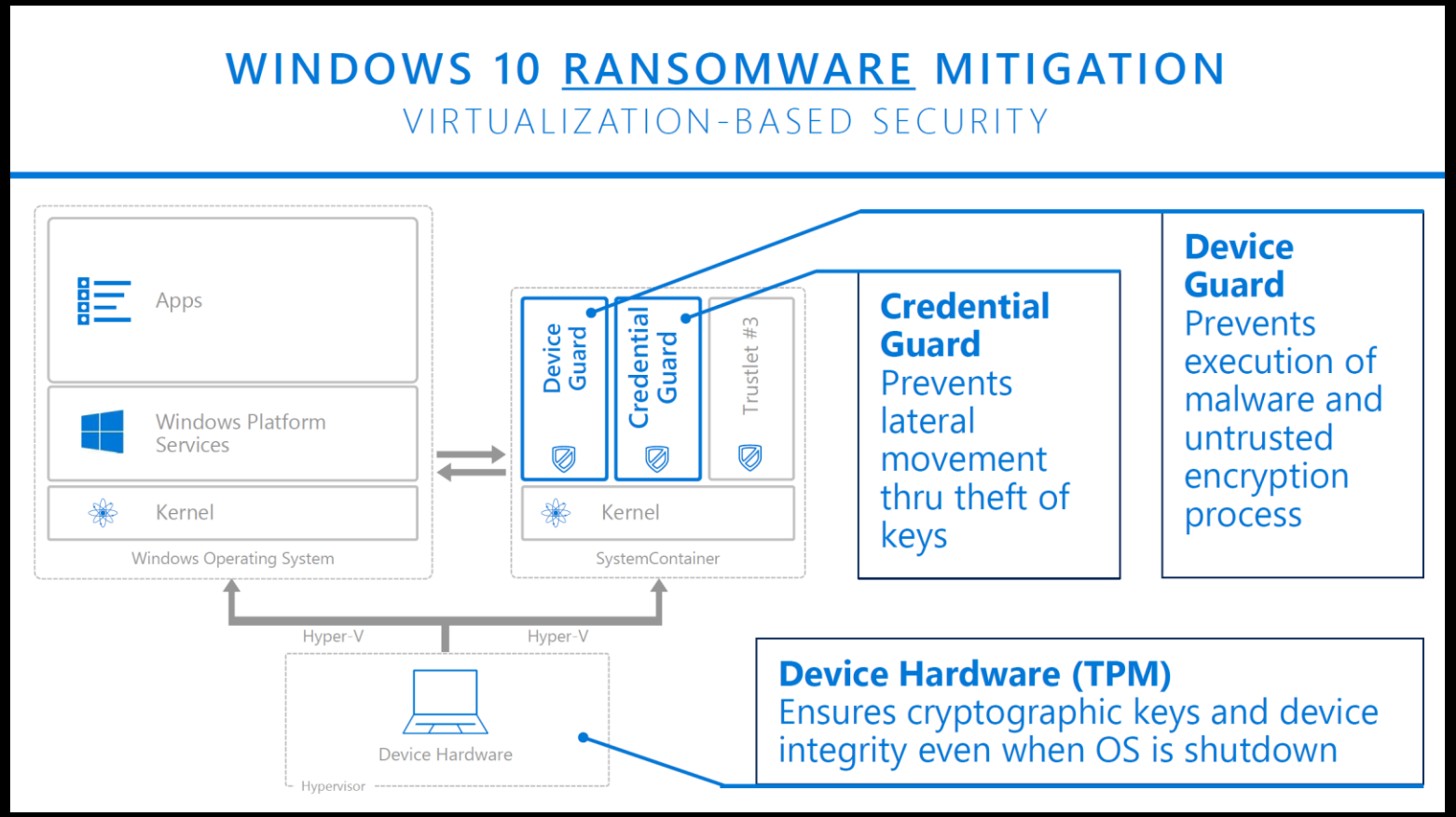
PASS THE HASH SOLUTION: **CREDENTIAL GUARD**



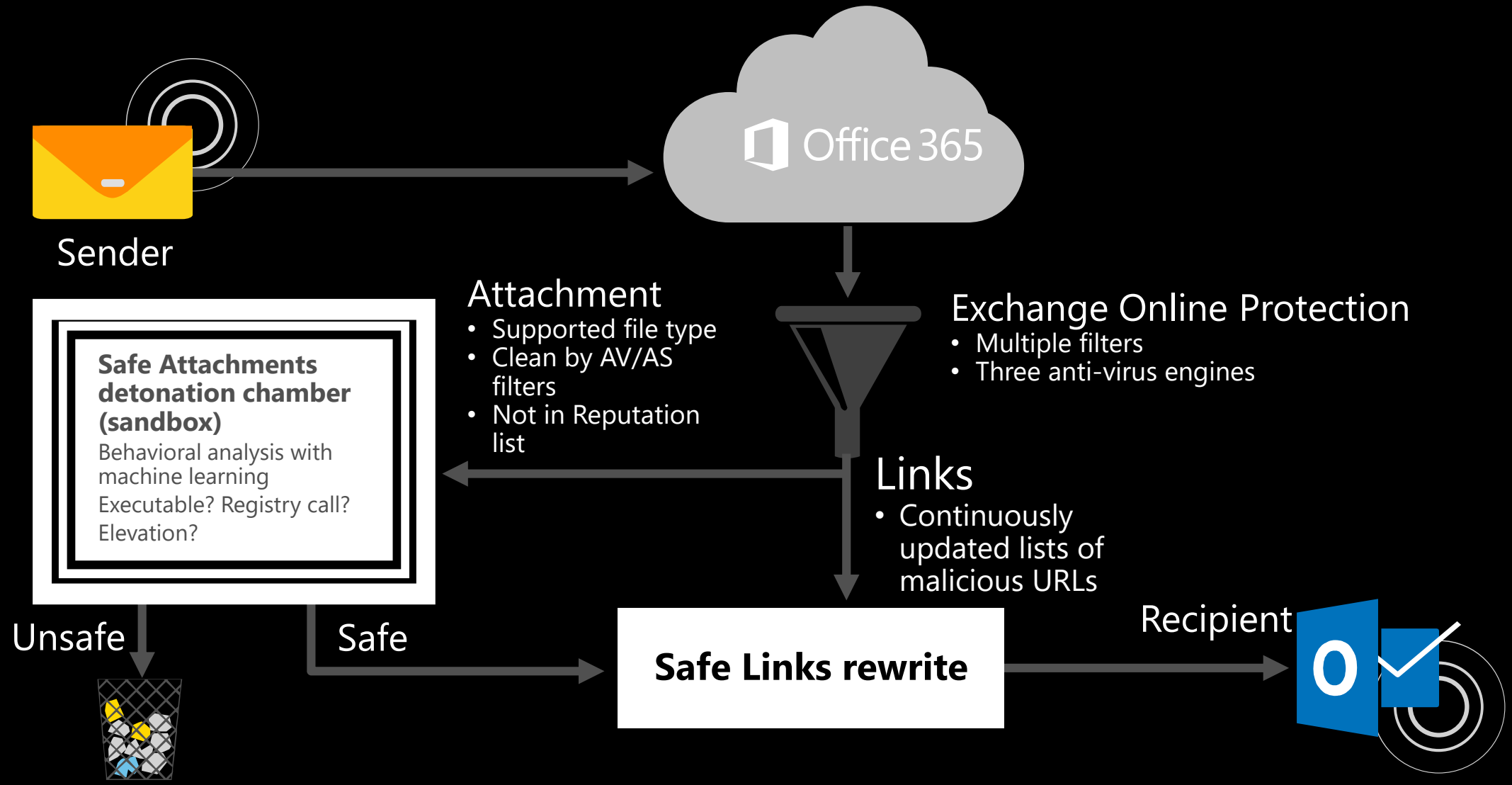
2 Endpoint protect…hasta la vista Antivirus

- Pass the Hash (PtH) attacks are the #1 go-to tool for hackers. Used in nearly every major breach and APT type of attack
- Credential Guard uses VBS to isolate Windows authentication from Windows operating system
- Protects LSA Service (LSASS) and derived credentials (NTLM Hash)
- Fundamentally breaks derived credential theft using MimiKatz

PASS THE HASH SOLUTION: **CREDENTIAL GUARD**



3 Protect email…No Phishing allowed



4 Intel platform to detect the unknown

Collecting cybersecurity data across Microsoft's global sensors

Exchange

More than **35 billion** messages scanned monthly

Daily tracking of **600,000** addresses sending spam

Windows

More than **250 million** Windows Defender users worldwide

Microsoft Security Essentials

Millions of consumers protected worldwide

Performs **billions** of malware removals per year worldwide

Microsoft System Center

Millions of computers running Microsoft enterprise anti-malware solutions

Outlook.com

More than **420 million** active users

Malicious Software Removal Tool

700 million computers reporting monthly

More than **40 billion** executions since 2005

Bing

18+ billion web-page scans per month

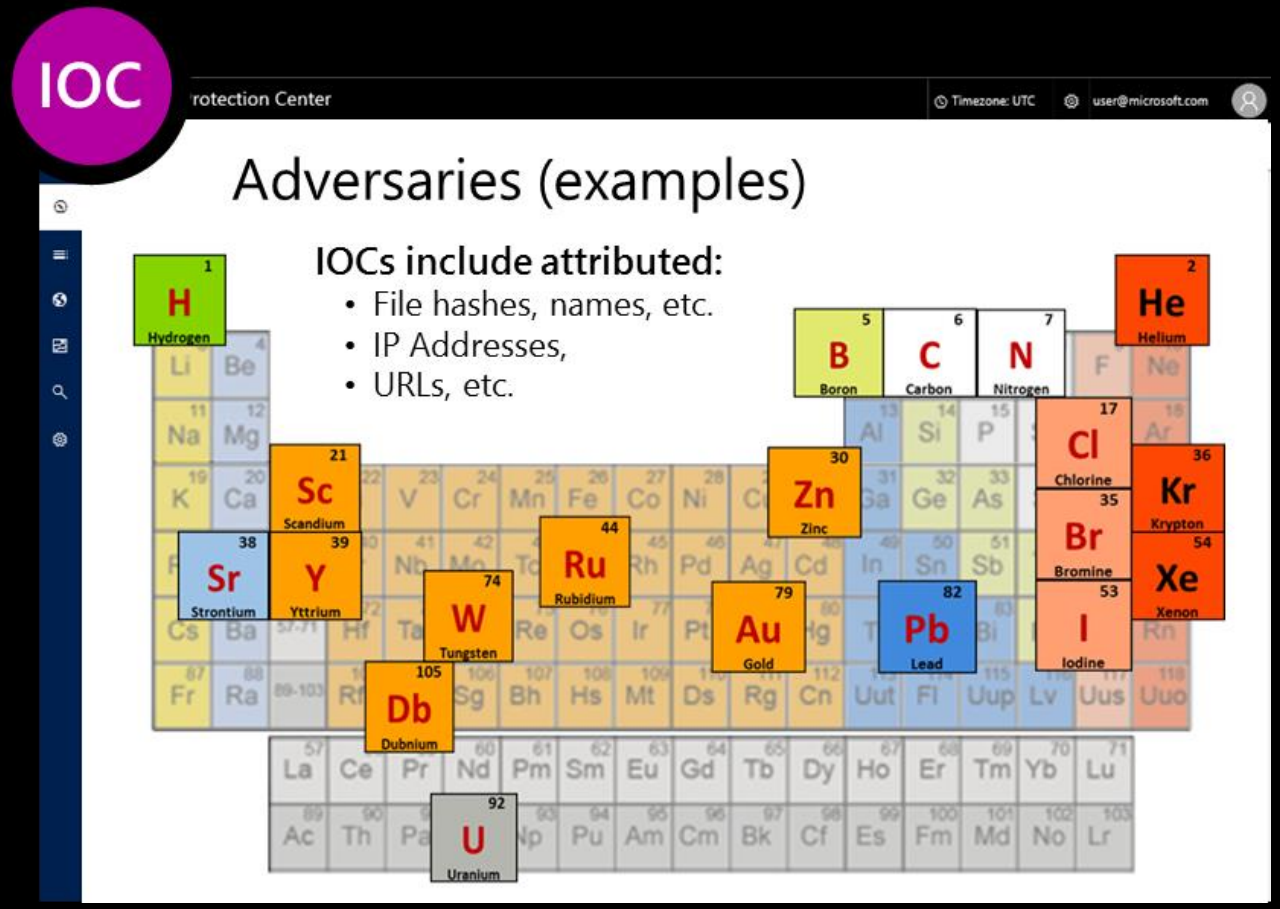
Microsoft Azure

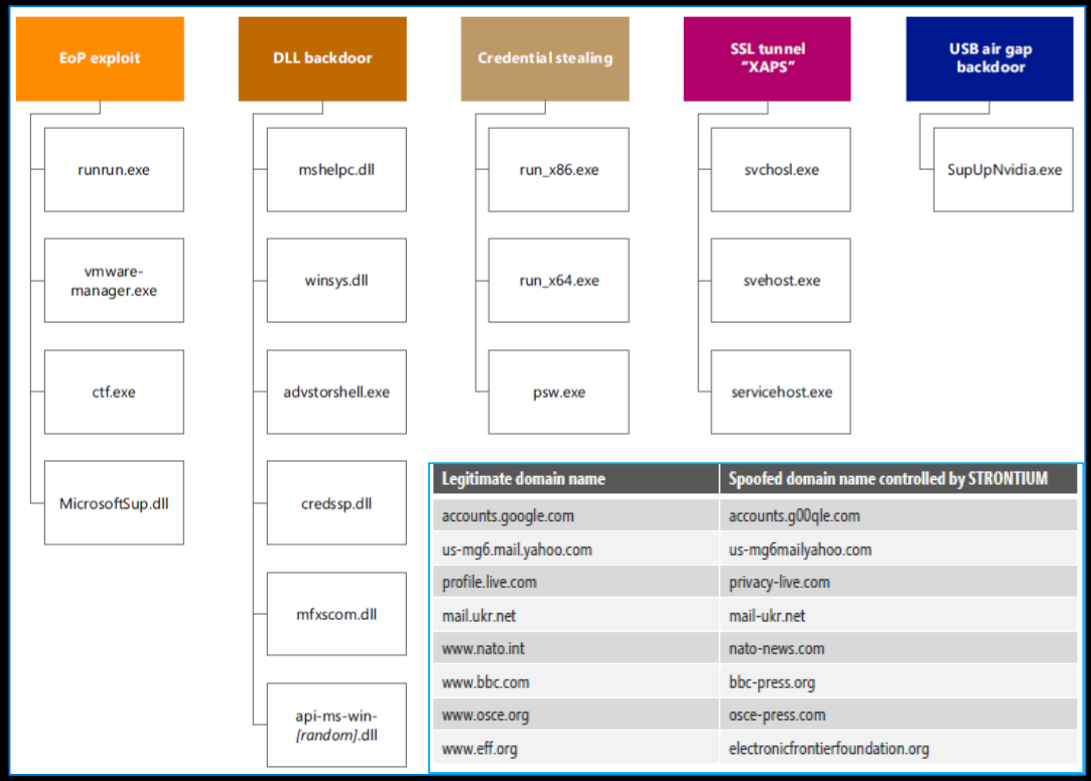
1 billion customers across enterprise and consumer segments

200+ cloud services

4 Indicators of Compromise

Monitoring "What (who) we know"
Threat Intelligence database of known adversary and campaign IOCs

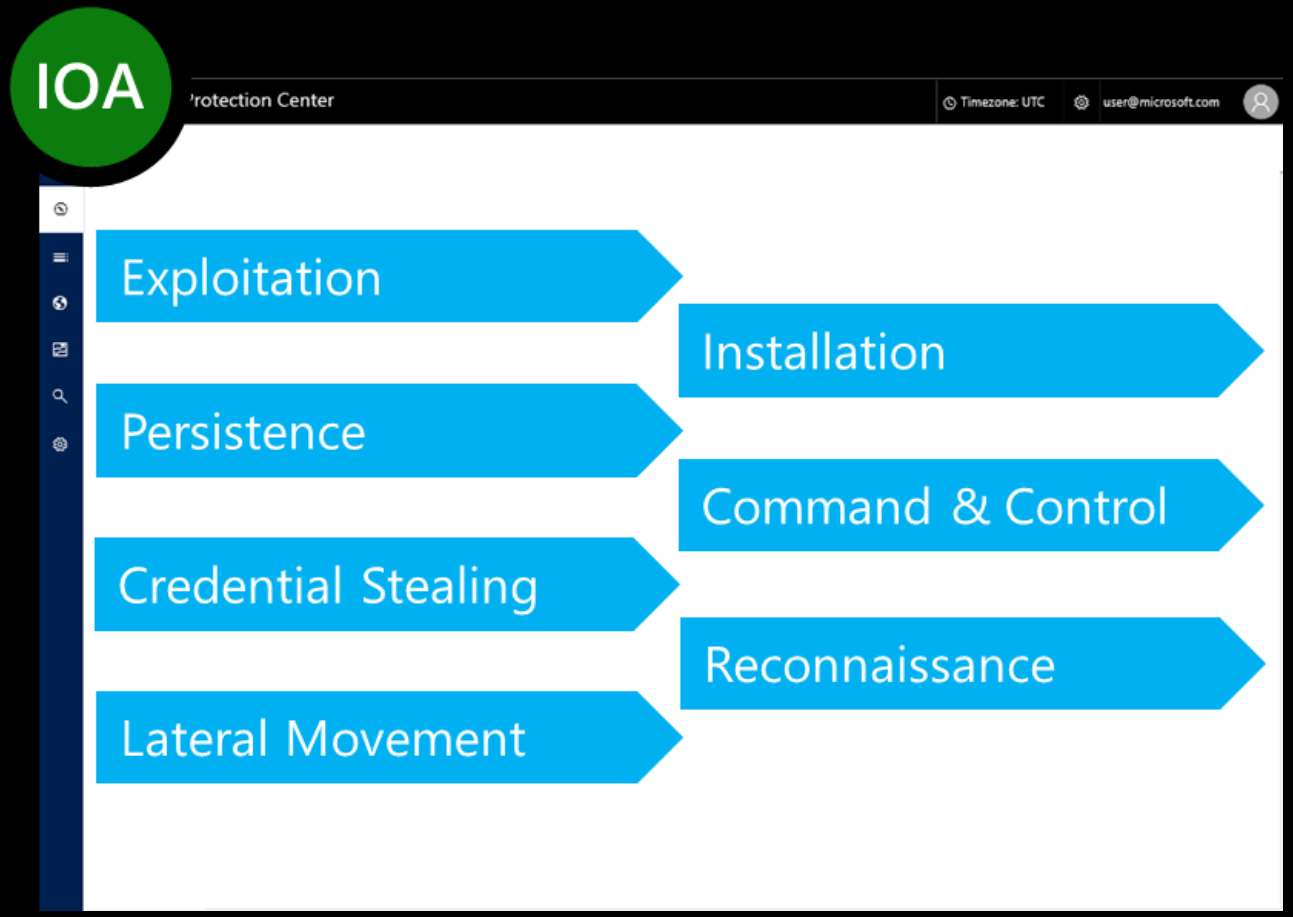




Legitimate domain name	Spoofed domain name controlled by STRONTIUM
accounts.google.com	accounts.g00qle.com
us-mg6.mail.yahoo.com	us-mg6mailyahoo.com
profile.live.com	privacy-live.com
mail.ukr.net	mail-ukr.net
www.nato.int	nato-news.com
www.bbc.com	bbc-press.org
www.osce.org	osce-press.com
www.eff.org	electronicfrontierfoundation.org

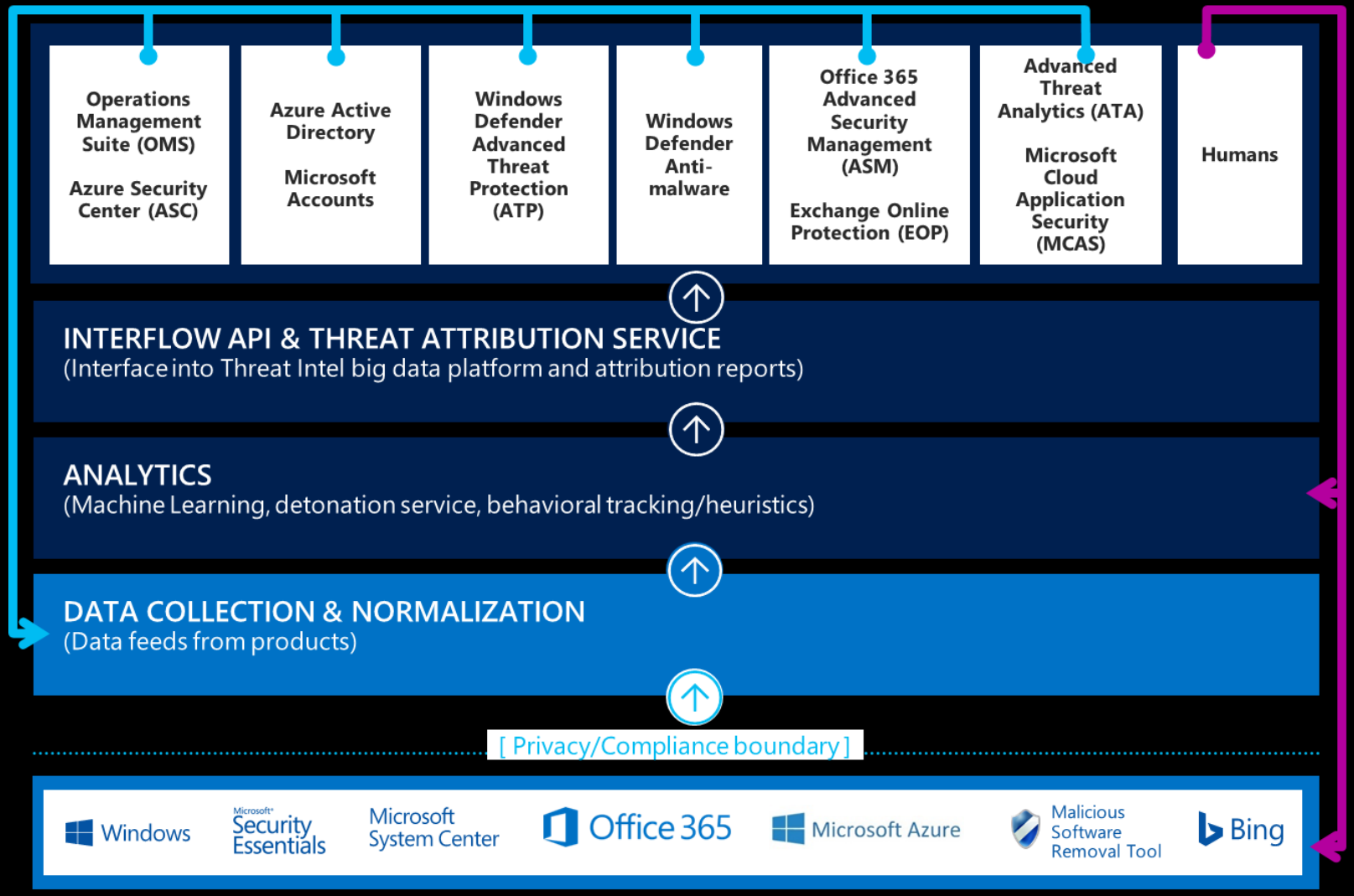
4 Indicators of Attack

Monitoring "What (whom) we don't recognize – yet"
Generic IOA Dictionary of attack-stage behaviors, tools, and techniques



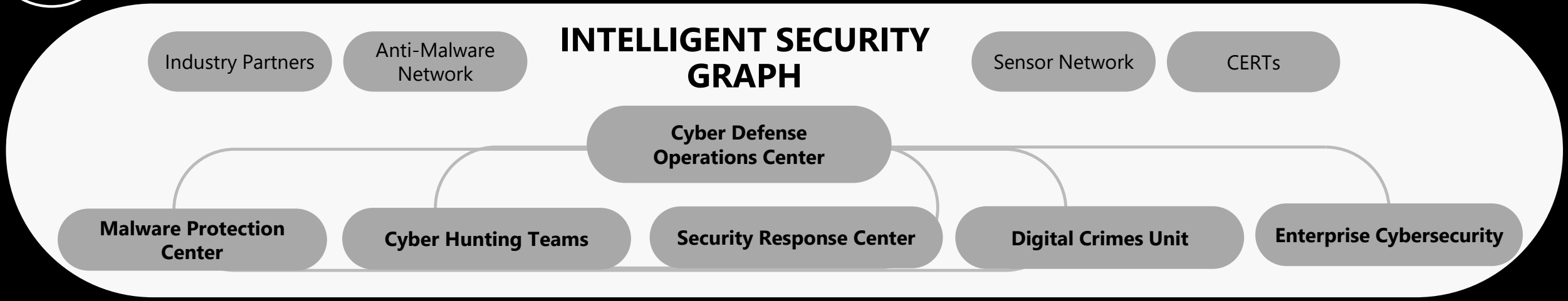
- Office dropped and ran a rare PE
- Anomalous ASEP created
- Reverse shell detected
- Variant of a HackTool
- Suspicious PowerShell invocation

4 Intel platform to detect the unknown



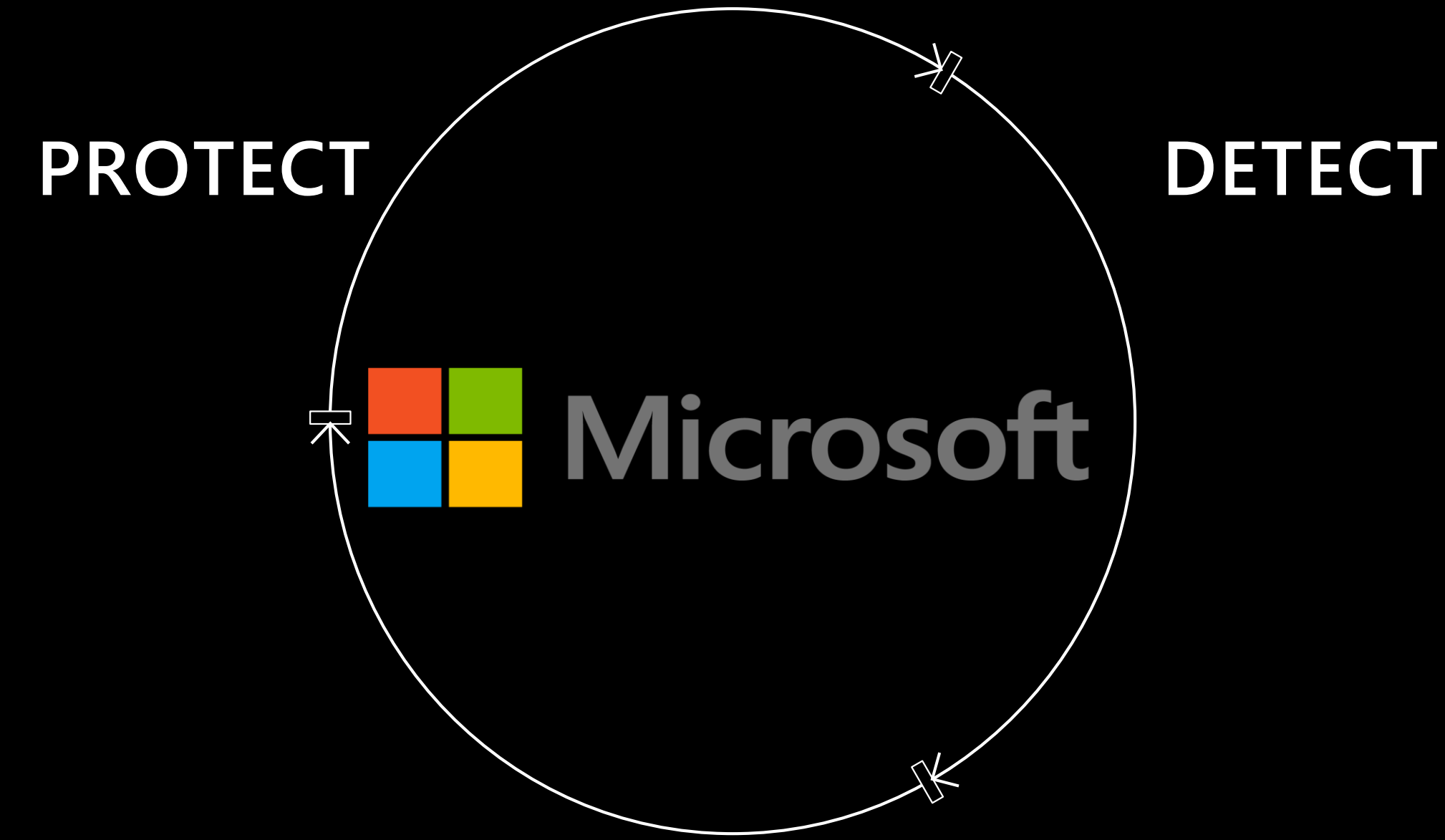
- Hunters identify attacks, and improve analytics
- Products generate their own data which feeds back into the graph
- Products use Interflow APIs to access results
- Analytics surfaces findings to help fuel new discoveries
- Data is processed
- Products send data to graph
- Products instrumented with privacy/compliance in mind

5 Advanced cybersecurity response



Augment your security operations: Continuous monitoring of your network for attacks, vulnerabilities, and persistent threats	Enterprise Threat Detection (ETD)	Persistent Adversary Detection Service
Incident Response: Investigate and disrupt suspicious events to provide a diagnosis and potential mitigations	Tactical Recovery	
	Incident Response	
	Strategic Recovery	

If not
YOU,
WHO?


PROTECT
DETECT
Microsoft
RESPOND