Vyhodnocování hrozeb a zabezpečení v cloudu

Zdeněk Jiříček
National Technology Officer
Microsfot Czech Republic

Microsoft

CYBER: NOVÉ VÝZVY

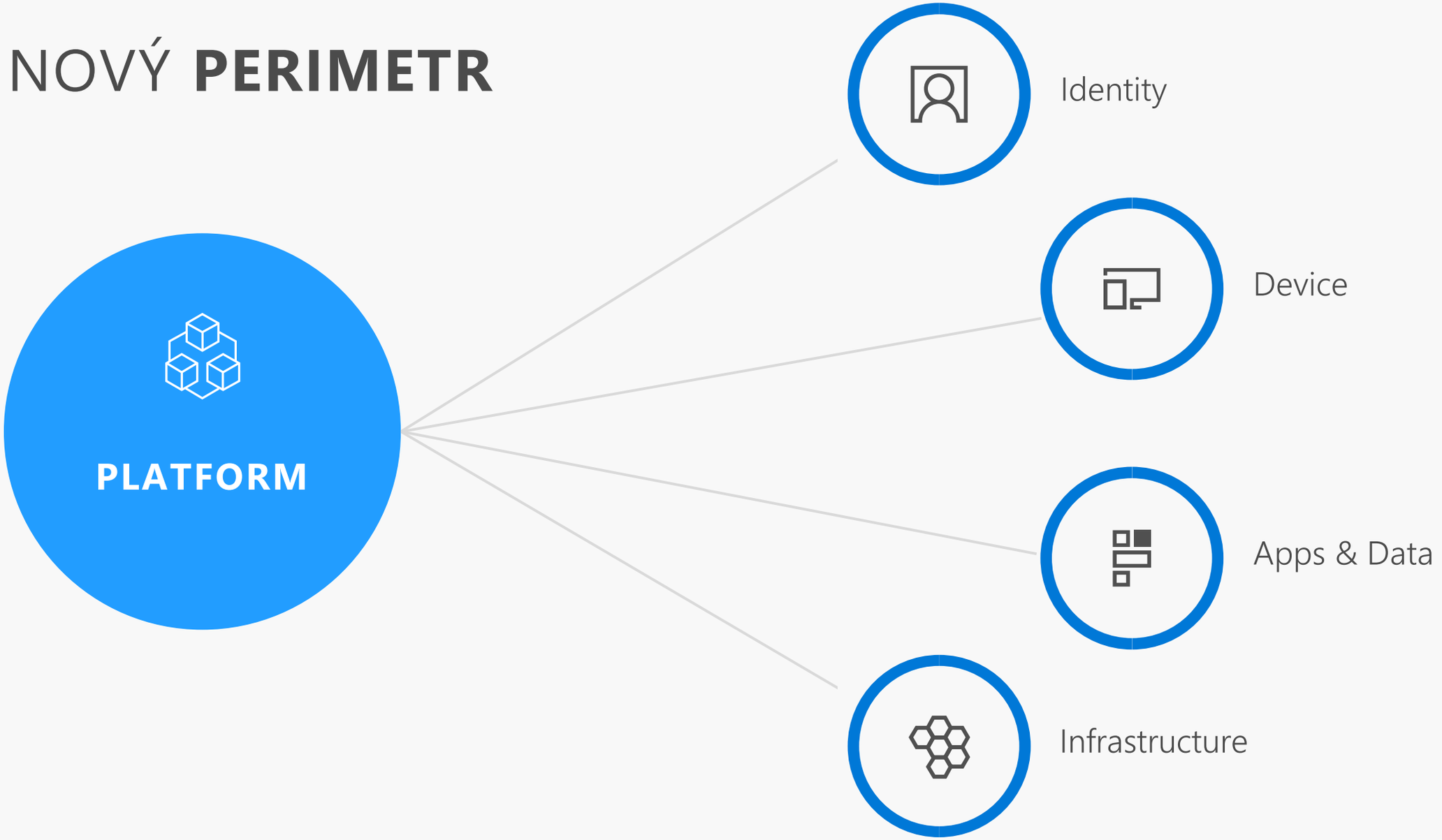
160 MIL. uniklých osobních záznamů

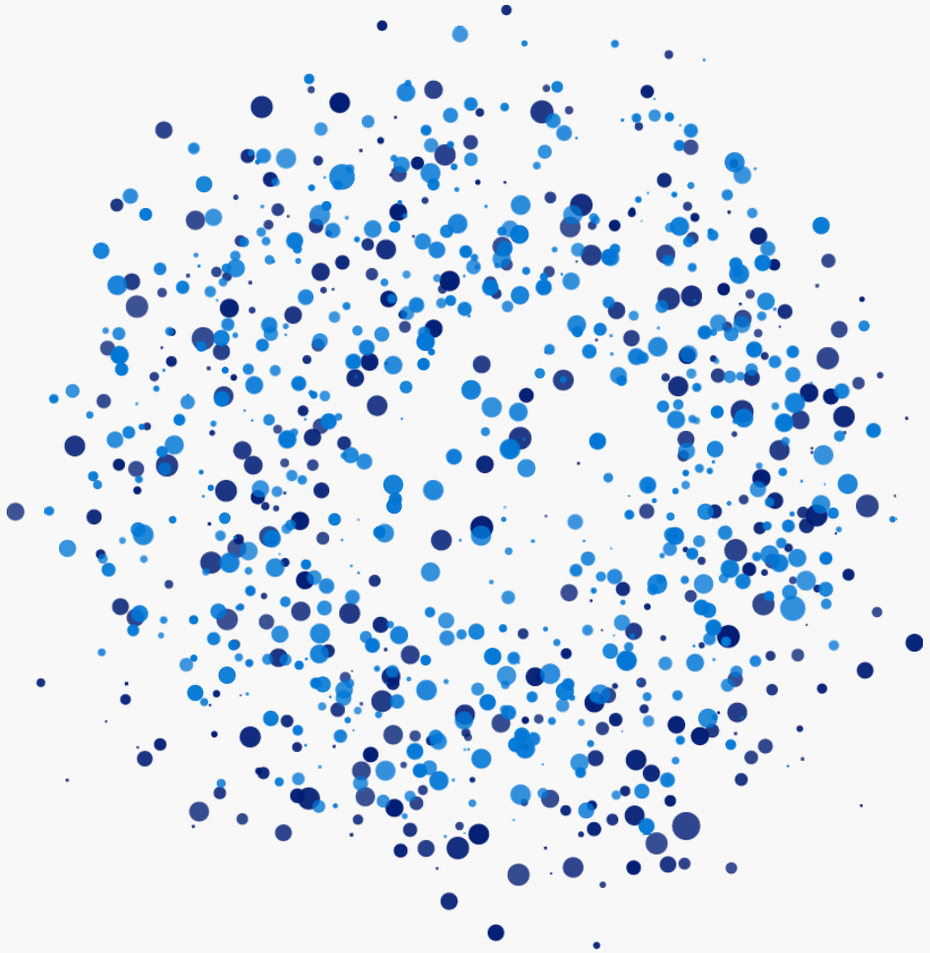
229 DNÍ mezi průnikem a detekcí

$3 MIL. prům. ztráty pro business / případ

NÁŠ CELKOVÝ PŘÍSTUP

NOVÝ **PERIMETR**





VSTUPY PRO **THREAT INTELLIGENCE**

300B user authentications each month

1B Windows devices updated

200B emails analyzed for spam and malware

18B web pages scanned by Bing each month

Zabezpečení díky analytice

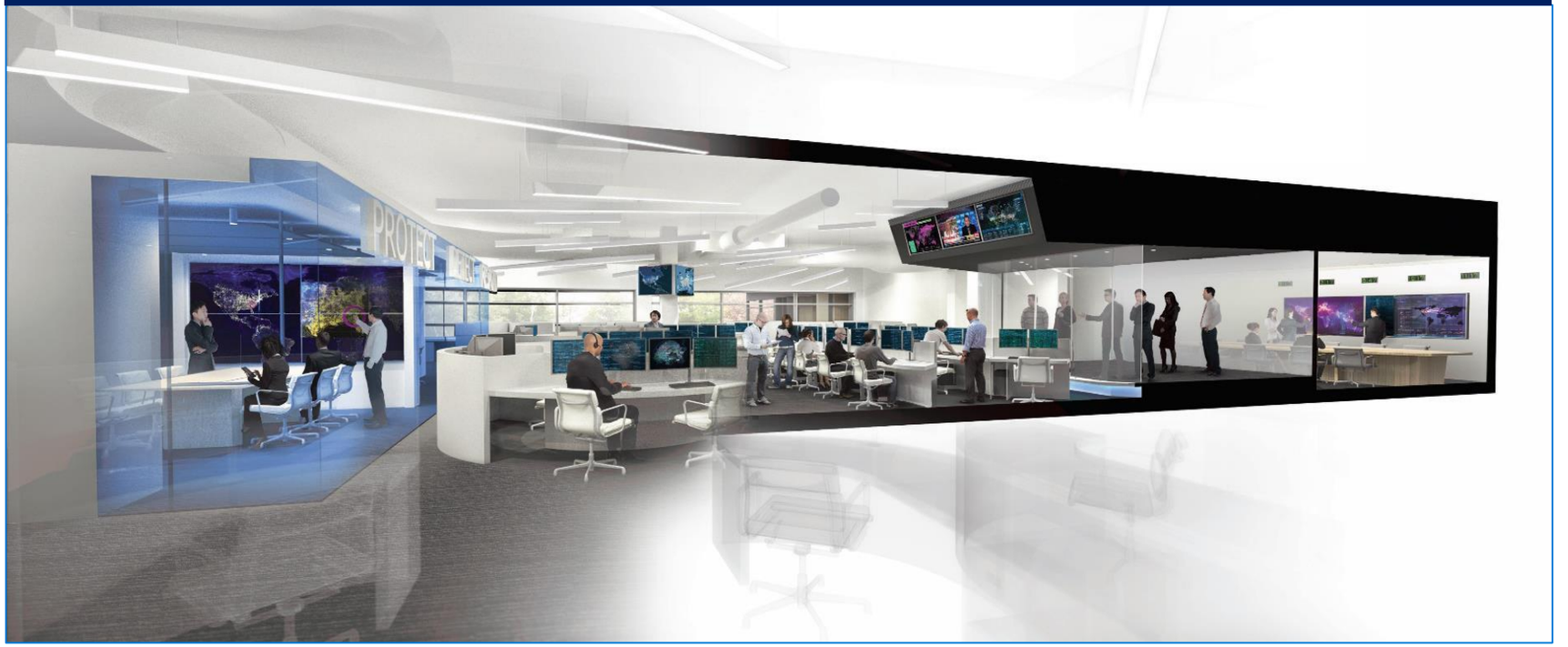
Ochrana pro naše zákazníky,

pro naše cloudové služby,

i pro ostatní spotřebitele

Narůstající hrozby vyžadují novou koordinaci:

Cyber Defense Operations Center



- Digital Crimes Unit
- Microsoft Security Response Center
- Microsoft Threat Intelligence Center
- Office 365
- Microsoft Azure
- Windows & Devices Group

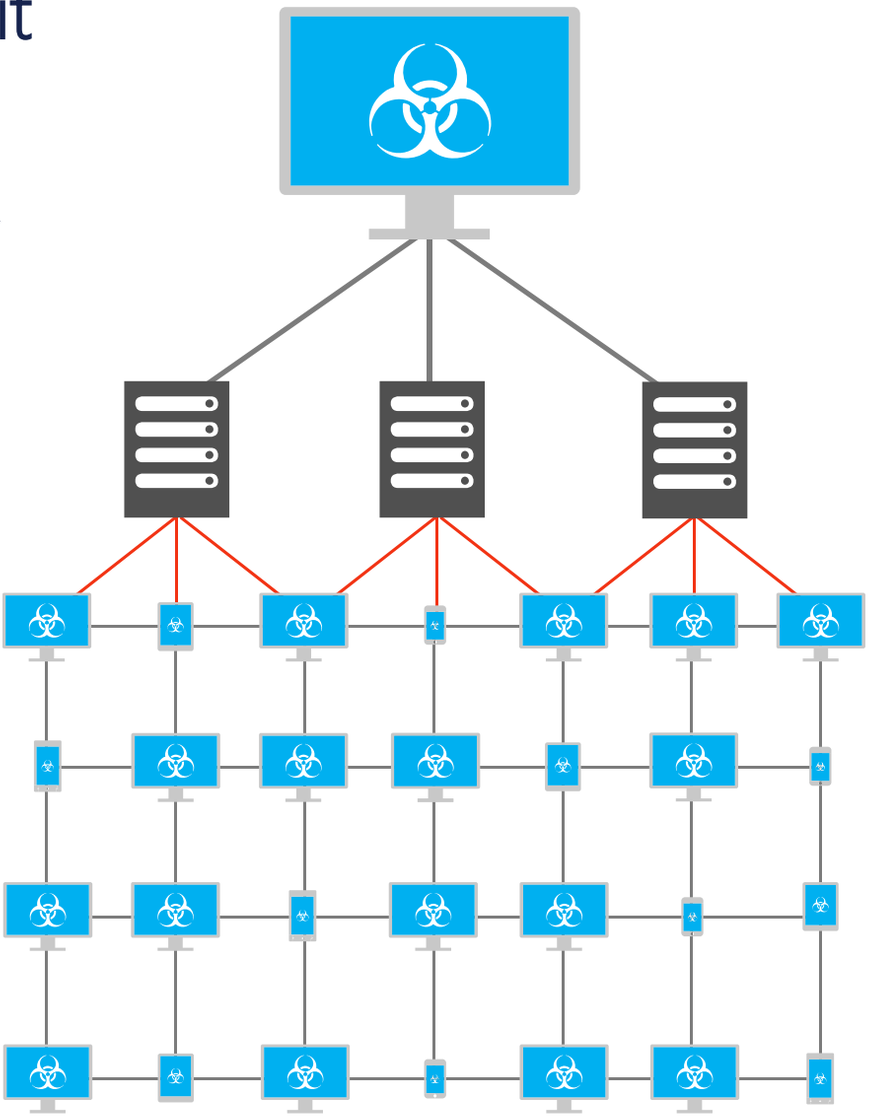
Eliminovat Malware

Spolupracujeme s vyšetřovateli a soukromým sektorem na rozrušení zločinných sítí

Microsoft Digital Crimes Unit

vyšetřuje, přebírá IP adresy kompromitovaných serverů, a organizuje globální partnerství proti zločinu na Internetu

Informujeme CERTy a ISP aby mohli správně reagovat



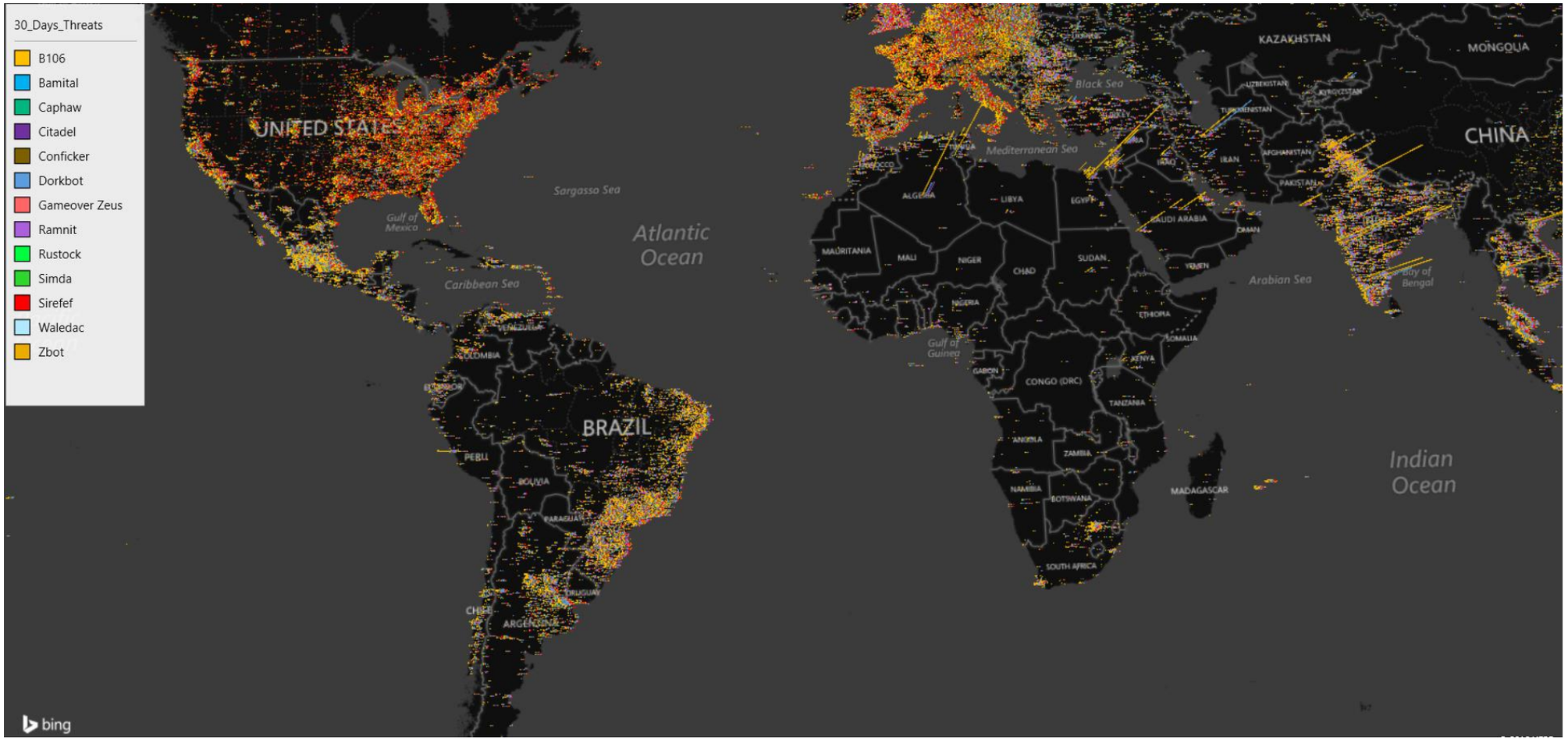
Cyber Threat Intelligence Program

Vyhodnotíme 50-100 milionů podezřelých IP adres denně

300 mil. - 1 mld. připojení denně

Objem se neustále mění

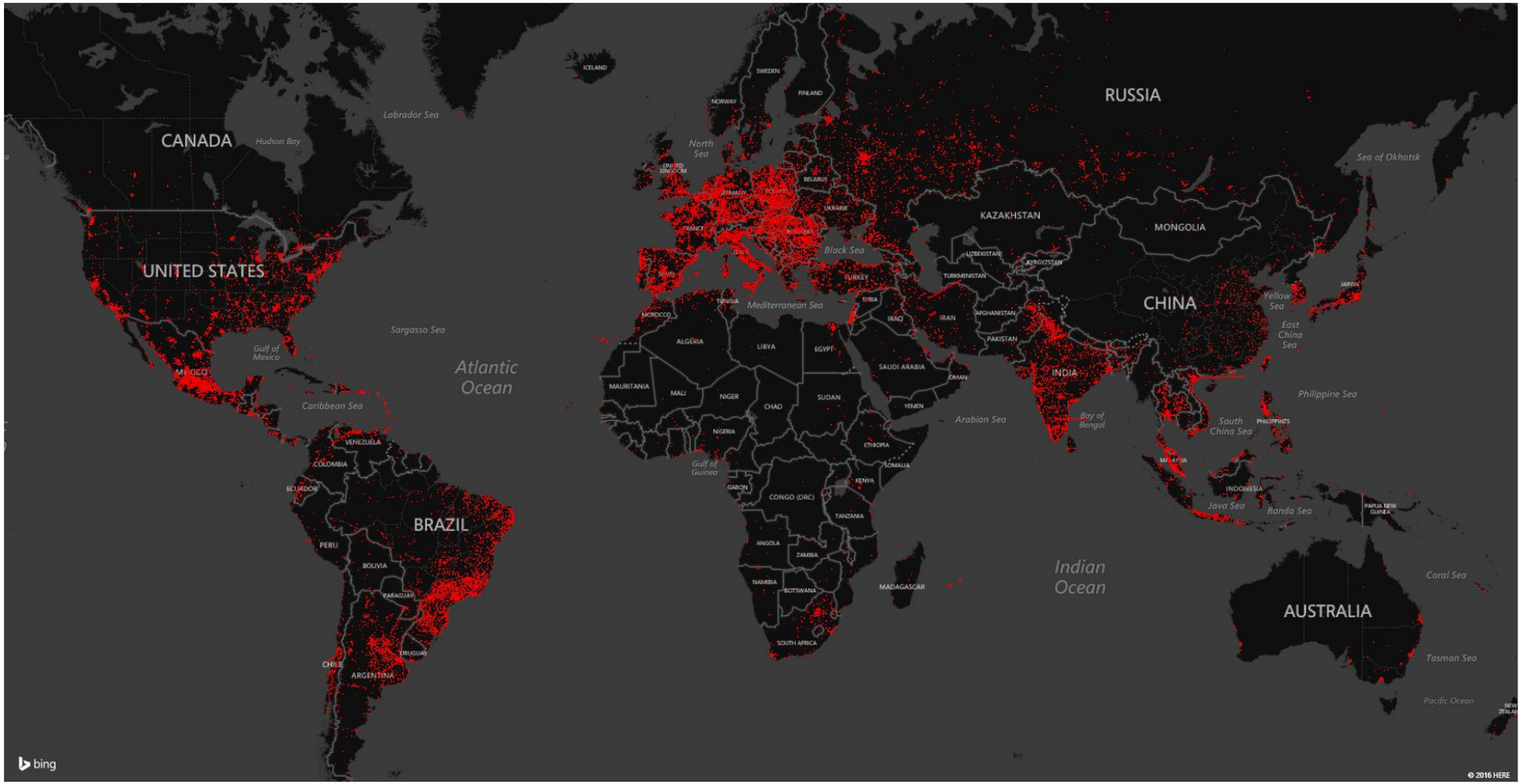
Actionable Threat Intelligence - data získaná z rozrušených botnetů



Dorkbot Operation
December 2015

Dorkbot malware spreads, steals, distributes and disables

Over 15 mil. infected IP addresses found



DCU Azure Architecture

Transforming data into intelligent action

Data at Rest

Data in Motion

Cortana Intelligence Suite

Machine Learning | Advanced Analytics

Azure Machine Learning
Azure HDInsight
Azure Data Lake Analytics
Azure Stream Analytics

Big Data Stores

Azure Data Lake
Azure SQL Data Warehouse

Information Management

Azure Data Factory
Azure Event Hubs

Data Subscribers

Microsoft Products
Microsoft Services
Governments, ISPs and others

Dashboards | Visualizations

Office 365
Power BI
Kibana*
Elastic Search*

*Open source software

Bezpečnostní inovace: nejdříve v cloudu

Ochrana emailu a dokum. v Office 365

- Advanced Threat Protection
  - Safe Links / Safe Attachments
- O365 Advanced Encryption
  - Šifrování s hlavním klíčem pod kontrolou zákazníka
- Advanced Security Mgmt.
  - Akvizice izraelské fy Adallom
  - Auditní stopa uživatelů v cloudu
  - Detekce podezřelých aktivit na bázi abnormalit

Ochrana virtuálních strojů

- Azure Disk Encryption
  - Šifrování celých VM
  - Autentizace spuštění VM
- Antimalware for Azure
  - Strojové učení v reálném čase
- Azure Security Center
  - Dashboard, který sám upozorňuje na slabiny VM
- Azure Informat. Protection
  - Nástroj pro klasifikaci a ochranu informací (dat)

Ochrana databází

- Transparent Data Encryption
  - Šifrování s hlavním klíčem pod kontrolou zákazníka
- SQL „Always Encrypted“
  - Šifrování vybraných sloupců pod úplnou kontrolou zákazníka
- SQL Threat Detection
  - Ochrana proti SQL injections

Nástroje cloudu pro IT zákazníka

Microsoft Advanced Threat Analytics (ATA)… link (Aug. 2015)

- Cíl: zachytit abnormality na základě analýzy AD traffic a SIEM záznamů
- Profiluje normální chování uživatelů min. 3 týdny, vytváří šablony
- Vyhodnocuje abnormality, „Pass The Hash“, lateral movement, neautorizované změny

System Center Operations Mgmt Suite: navíc IP Threat Intelligence

- Ověřuje jestli on-premise PC‘s nebo servery se připojují k nakaženým IP adresám (web serverům)
- Informace z Microsoft Threat Intelligence Center (MSTIC) a od třetích stran
- Centralizovaný pohled na statistiku pokusů připojit se na špatné IP adresy

Microsoft EMS, Azure AD Premium

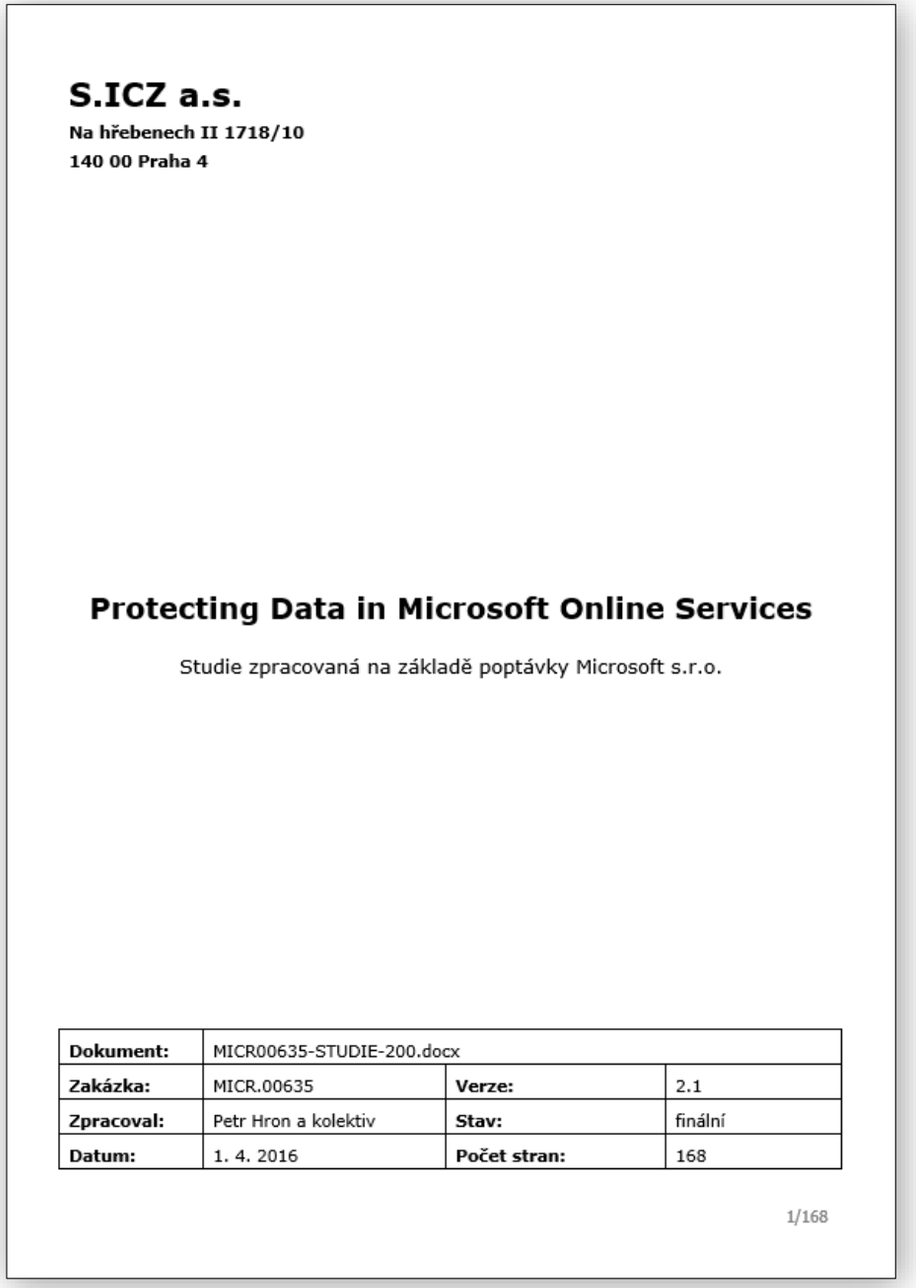
- Zaznamenává a varuje, pokud se přes Azure AD loguje IP adresa kterou máme na rizikovém seznamu

Zabezpečení dat v cloudu

Jak splnit požadavky vyhlášky č. 316/2014 Sb (VoKB)

- Příloha 1.: požadavky na důvěrnost, integritu, dostupnost dat

Studie S.ICZ a.s.: podklad pro analýzu rizik a zabezpečení dat v Office 365 (SaaS) a Microsoft Azure (IaaS/PaaS)



S.ICZ a.s.
Na hřebenech II 1718/10
140 00 Praha 4

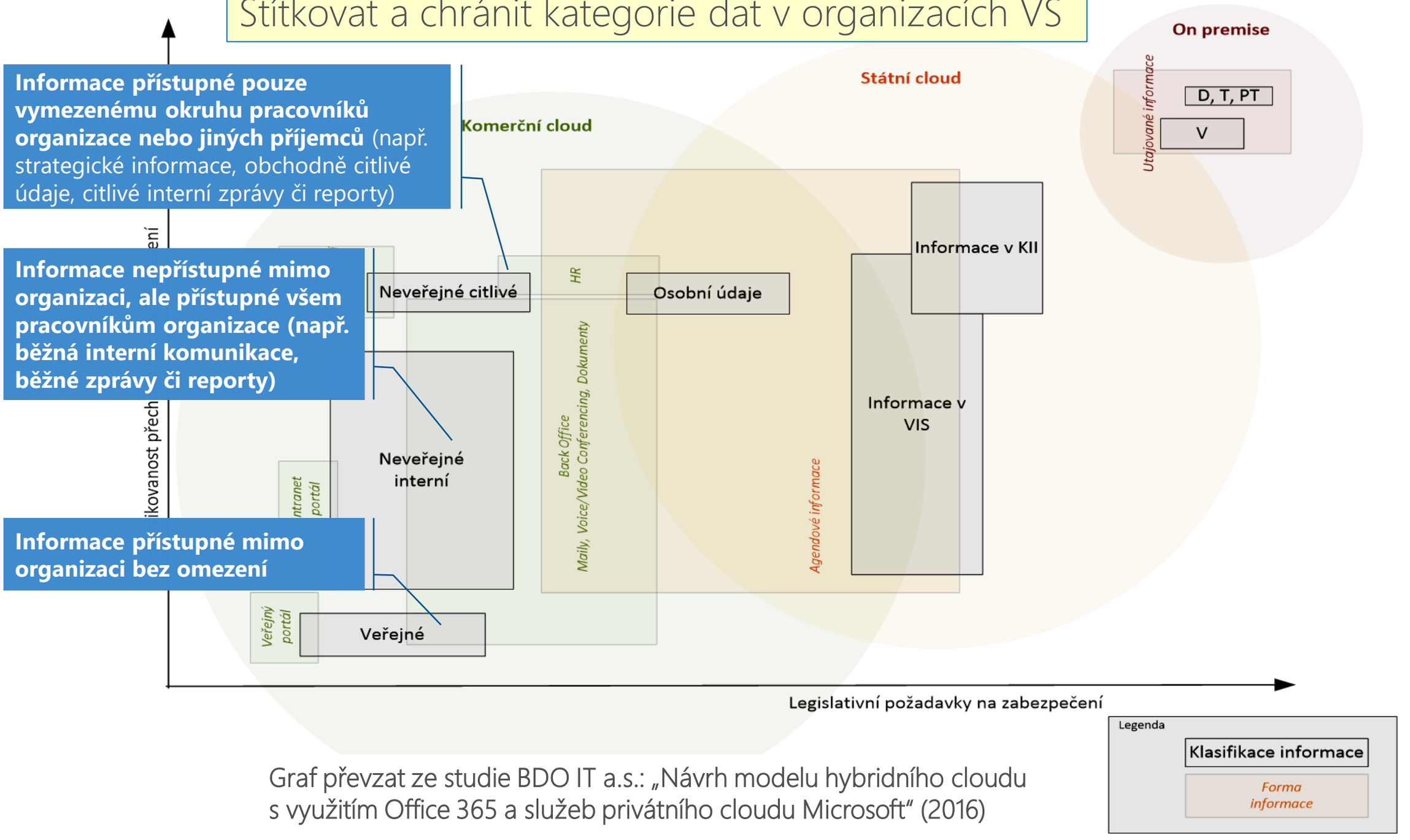
Protecting Data in Microsoft Online Services

Studie zpracovaná na základě poptávky Microsoft s.r.o.

Dokument:	MICR00635-STUDIE-200.docx		
Zakázka:	MICR.00635	**Verze:**	2.1
Zpracoval:	Petr Hron a kolektiv	**Stav:**	finální
Datum:	1. 4. 2016	**Počet stran:**	168

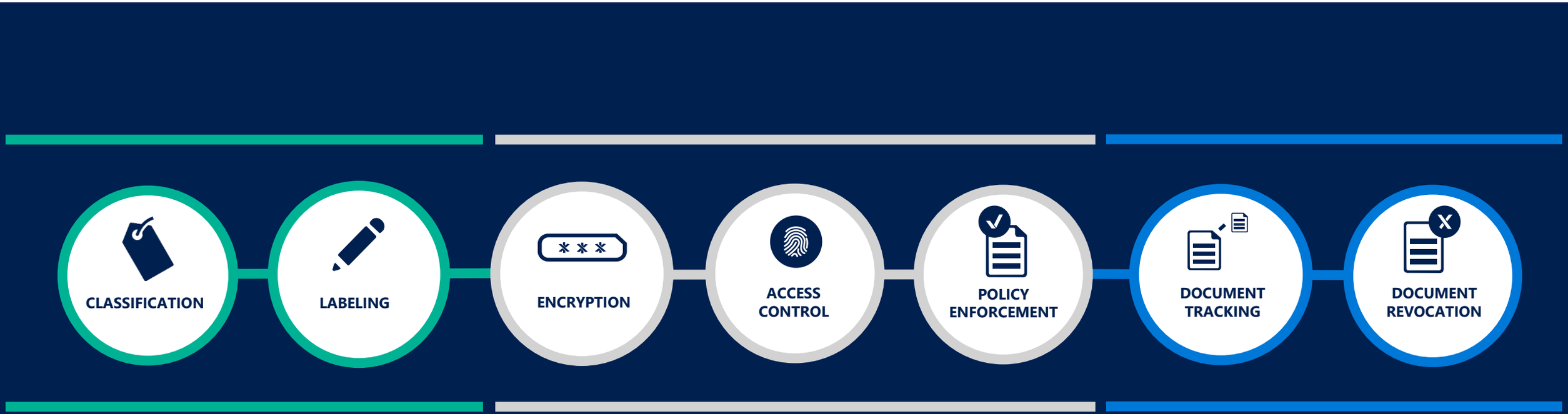
1/168

Štítkovat a chránit kategorie dat v organizacích VS



Graf převzat ze studie BDO IT a.s.: „Návrh modelu hybridního cloudu s využitím Office 365 a služeb privátního cloudu Microsoft" (2016)

Jak realizovat klasifikaci a ochranu dokumentů?



Klasifikace a štítkování

Protect

Monitoring a Response

Data nositelem perimetru: Azure RM

Azure Information Protection

Classification & labeling

Celý životní cyklus dokumentu

Protec… …nitor & …spond

Partnerské řešení: AEC DocTag

WINDOWS 10: KROMĚ OBRANY NYNÍ MYSLÍME I NA **MOŽNOST PRŮNIKU**

PRE-BREACH → POST-BREACH

Device protection	Identity protection	Information protection	Threat resistance	Breach detection investigation & response
				
Device Health Attestation	Built-in 2FA	Device protection / Drive encryption	SmartScreen	**Windows Defender Advanced Threat Protection (ATP)**
Device Guard	Account lockdown	Windows Information Protection	AppLocker	
Device Control	Credential Guard	Conditional access	Device Guard	
Security policies	Windows Hello :)		Windows Defender	
			Network/Firewall	

InPrivate | Seville - Dashboard

seville.windows.com

Windows Security Center | Dashboard

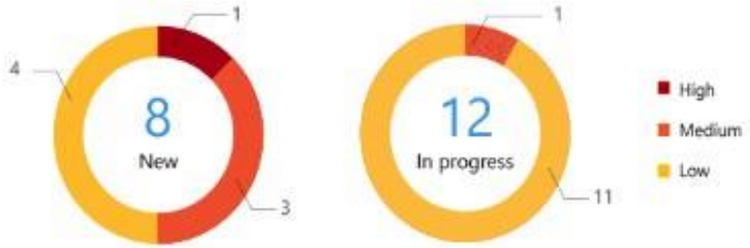
Timezone: UTC | Analyst@SevilleContoso.onmicrosoft.com

- Dashboard
- Alerts Queue
- Machines View

File | Search (File, IP, URL, Machine)

ATP alerts

All time



Latest ATP alerts

Go to all alerts

Feb 18 18:07:01	NeroBlaze attack detected	High
Feb 18 11:54:02	Outlook dropped and executed a PE file	Medium
Feb 18 14:34:00	A suspicious Powershell commandline was executed	Medium
Feb 18 13:01:09	A reverse shell was detected	Medium

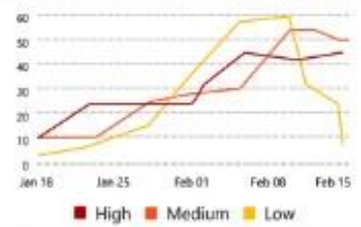
Top machines with ATP alerts

Go to machine view

CONT-LIZBEAN	1	3	1
CONT-LILYJARVIS	0	0	1
CONT-RODGERANDR	0	0	1
CONT-ERICGAYLOR	0	0	1

ATP alert trends

30 days



ATP alerts mapping

30 days

High severity malware

All time

Ransomware	5	1	12
Backdoor	7	0	16
Exploit	35	3	52
Trojan	17	0	25

Machines reporting

30 days

Status

Service status	✓
Total machines reporting	3,547
Open message center	

Machine

Cont-LizBean-X1

Domain: Contoso.org
OS: windows10

Machine IP Addresses

Last external IP: 40.122.164.91
Last internal IP: 10.0.0.13

Machine Reporting

First seen: 6 days ago
Last seen: 6 minutes ago

Alerts related to this machine

02.23.2016	NeroBlaze attack detected	Command And Control	New
02.23.2016	A port scanning tool was detected	Suspicious Activity	New
02.23.2016	A potential reverse shell has been detected	Command And Control	New
02.23.2016	Anomaly detected in ASEP registry Software\Microsoft\Windows\CurrentVersion\Run	Persistence	New
02.23.2016	A suspicious Powershell commandline was executed on the machine	Lateral Movement	New
02.23.2016	Outlook dropped and executed a PE file.	Suspicious Activity	New

Machine in organization

Filter by: All Behaviors

Description	Details
02.21.2016	

NeroBlaze attack detected

NeroBlaze	NeroBlaze attack detected	02.23.2016 16:39:42	*Today*	Command And Control	cont-lizbean-x1

NEROBLAZE

Introduction

Active since 2007, NeroBlaze is an activity group that has been used primarily to target government bodies, diplomatic institutions and political advisors. Frequent use of zero-day vulnerabilities, spear-phishing and a number of other distribution methods, makes NeroBlaze a highly resilient threat.

Interests

We have seen NeroBlaze target government agencies, diplomatic institutions, and military organizations/installations in NATO member states, and certain Eastern European countries. We have also observed it target organizations associated with political activism in central Asia.

Tools, tactics, and processes

NeroBlaze seeks out victim information through open-source intelligence and social media interaction. It uses simple spear phishing attacks to obtain victims' email account credentials, compiling information for further attacks. It uses email accounts from generic email providers in order to imitate the email provider to disguise the spear phishing emails as a notification from the generic email provider, such as 'a privacy alert.' NeroBlaze persistently sends spear phishing attacks over many months to the same victims.

NeroBlaze attacks higher-value targets with emails that contain lures designed to take control of the victims' machines. NeroBlaze uses a breadth of tactics using lure emails that include:

- URLs to websites containing zero-day exploits
- URLs to websites that use social engineering techniques that cause the victim to download malware
- Document attachments that contain zero-day exploits

NeroBlaze usually packages these emails into a lure that might be interesting to the victim. NeroBlaze tries to provide credibility to these emails by associating the sender with a real organization.

Note: NeroBlaze appears to have resources to acquire many zero-day exploits that cover a wide range of software products for these attacks.

After a successful attack, NeroBlaze proceeds to get a foothold onto the victim's network. This includes making use of malware backdoors and VPN clients to achieve persistent network access. NeroBlaze has also been observed using Kali Linux (a penetration testing Linux distribution) on the victim's network for further exploration of the victim's computer. Lateral movement is also commonly used through pass-the-hash and credential dumping using publicly available tools, such as Mimikatz.

Exfiltration of information from the victim's network can happen through dedicated command and control (C2) infrastructure. NeroBlaze attempts to disguise this traffic through domain names that are associated with common tasks on the network, such as updates and malware checks. On rare instances, we have observed that NeroBlaze uses legitimate servers, such as local SMTP mail servers, to extract information. Overall, NeroBlaze tries to blend into the network traffic to avoid suspicion.

Areas affected

Recommended defenses

- Use the latest, up-to-date operating system and software versions with latest security mitigations
- Conduct enterprise software security awareness training, and build awareness about malware infection prevention
- Institute second factor authentication
- Prepare your network to be forensically ready
- Keep personnel and personal data private
- Lock down privacy settings on social profiles
- Keep systems and software fully updated

Dismiss

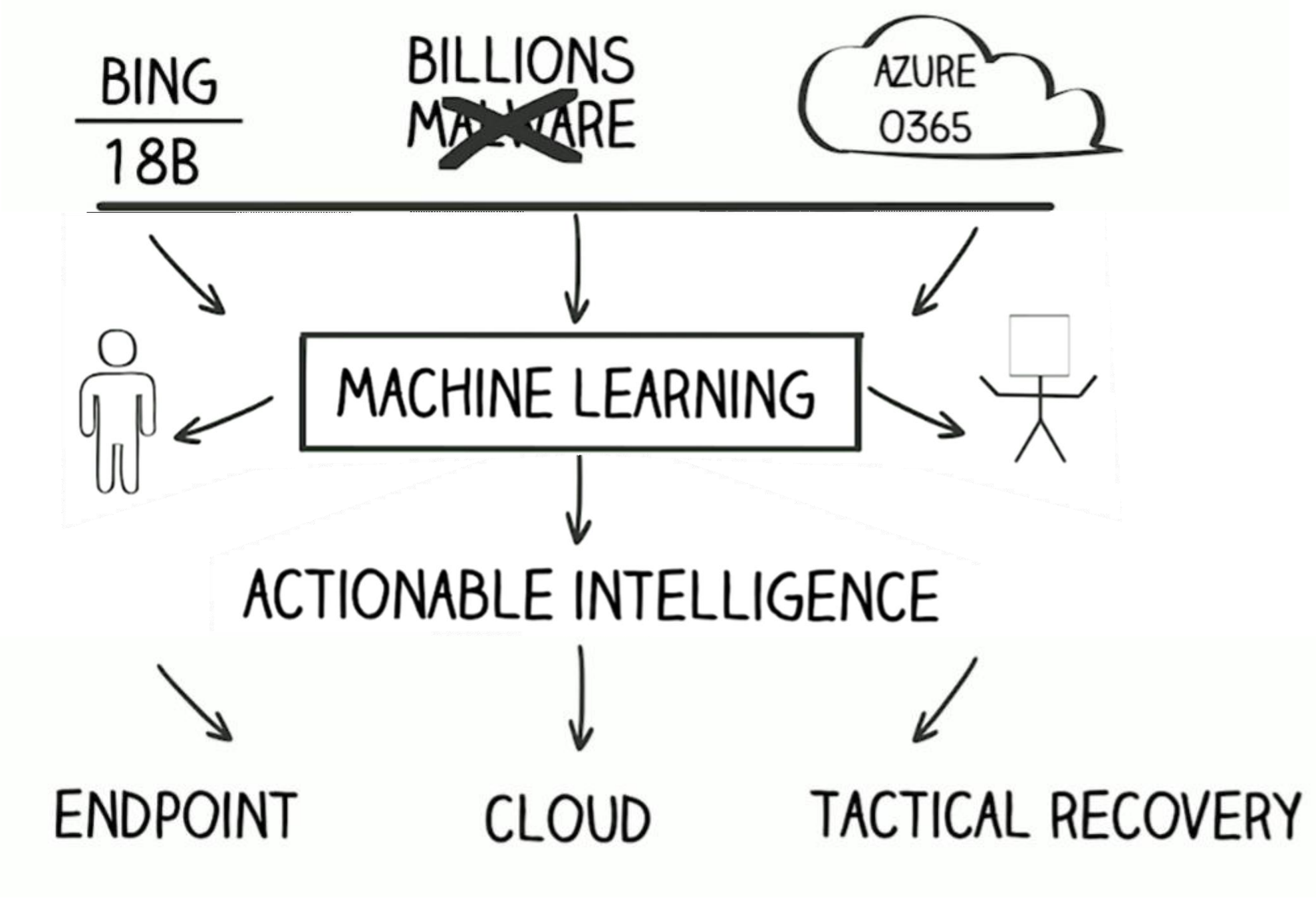
More info about this alert

A set of behaviors likely associated with the NeroBlaze adversary was detected on this machine.

Recommended Actions

New

1. Contact your Incident Response team. NOTE: If you don't have an Incident Response team, contact the Microsoft Consulting Services (MCS)


BING
18B
BILLIONS
AZURE
O365
MACHINE LEARNING
ACTIONABLE INTELLIGENCE
ENDPOINT
CLOUD
TACTICAL RECOVERY

Děkuji za pozornost!

Zdeněk Jiříček
National Technology Officer
zdenekj@microsoft.com