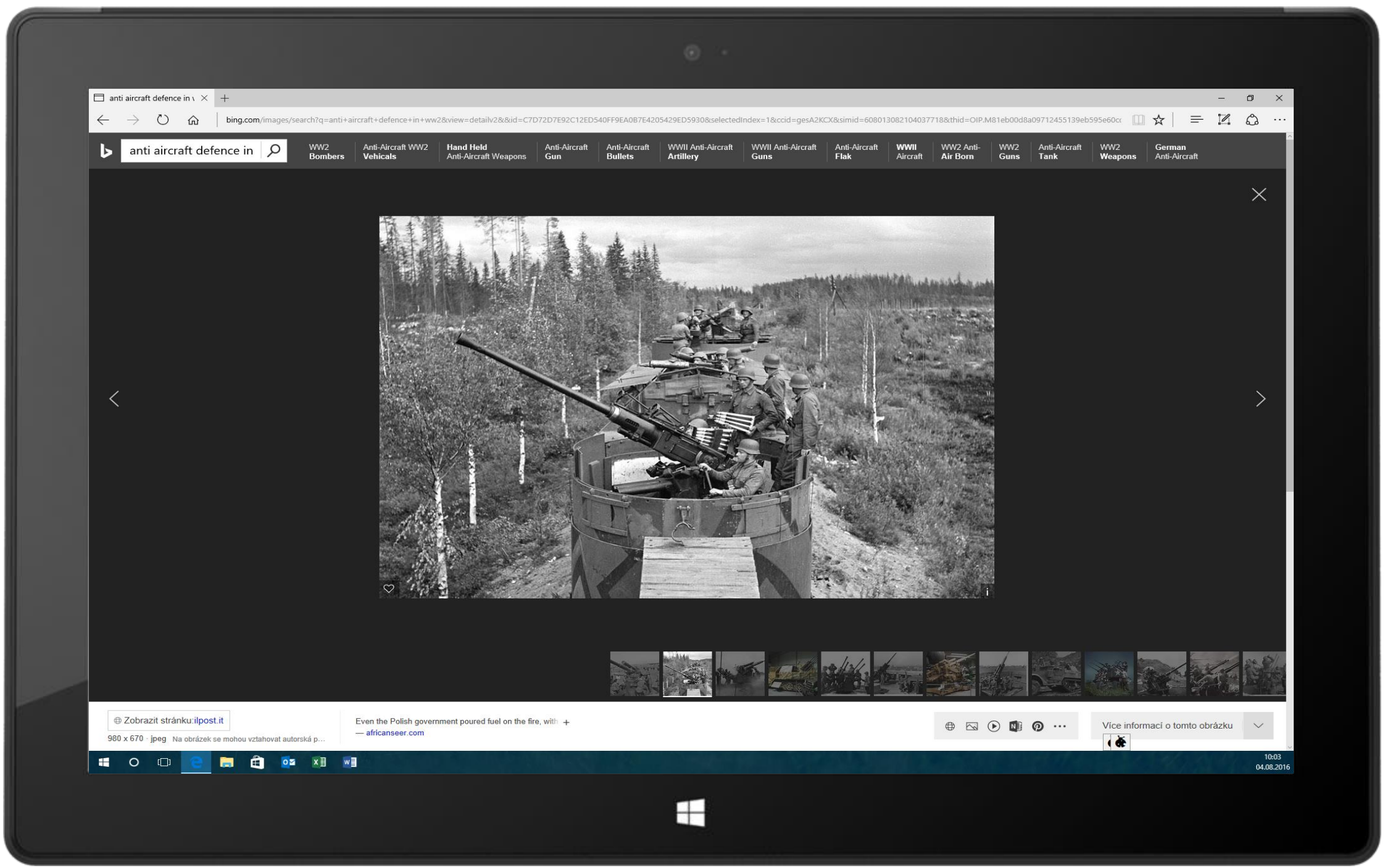
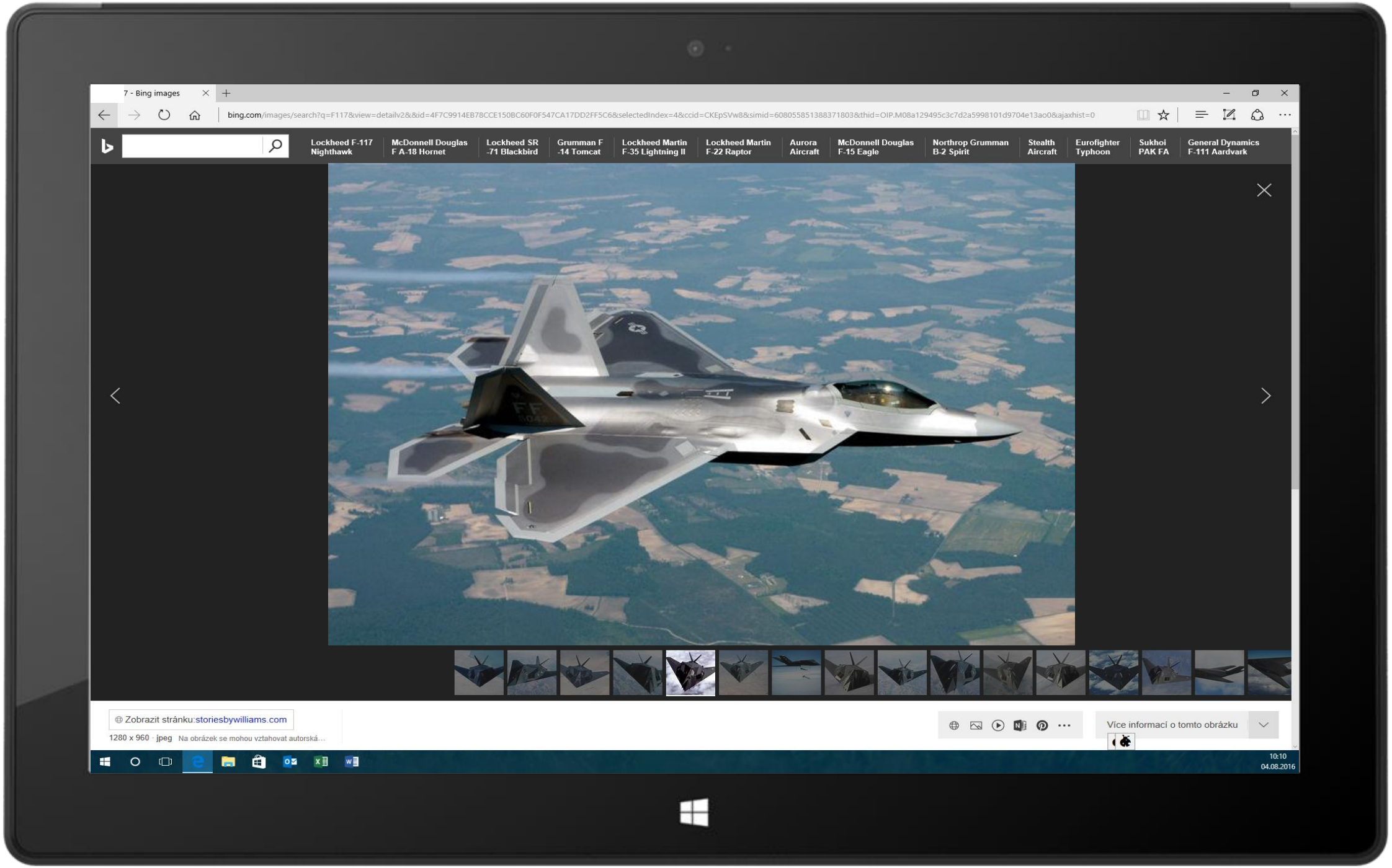
Microsoft

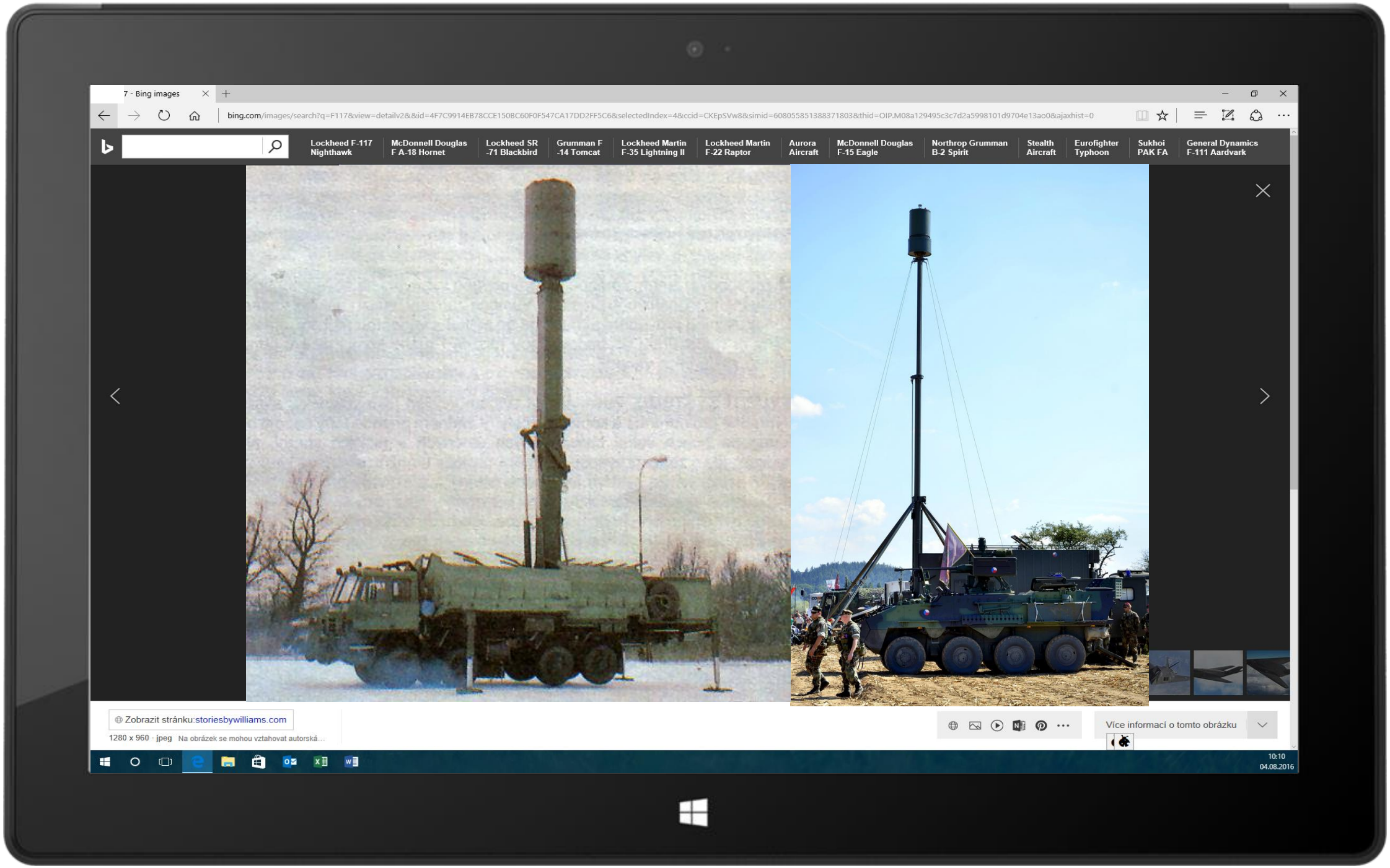
Využití Cloud AI pro ochranu, detekci a reakci na moderní hrozby

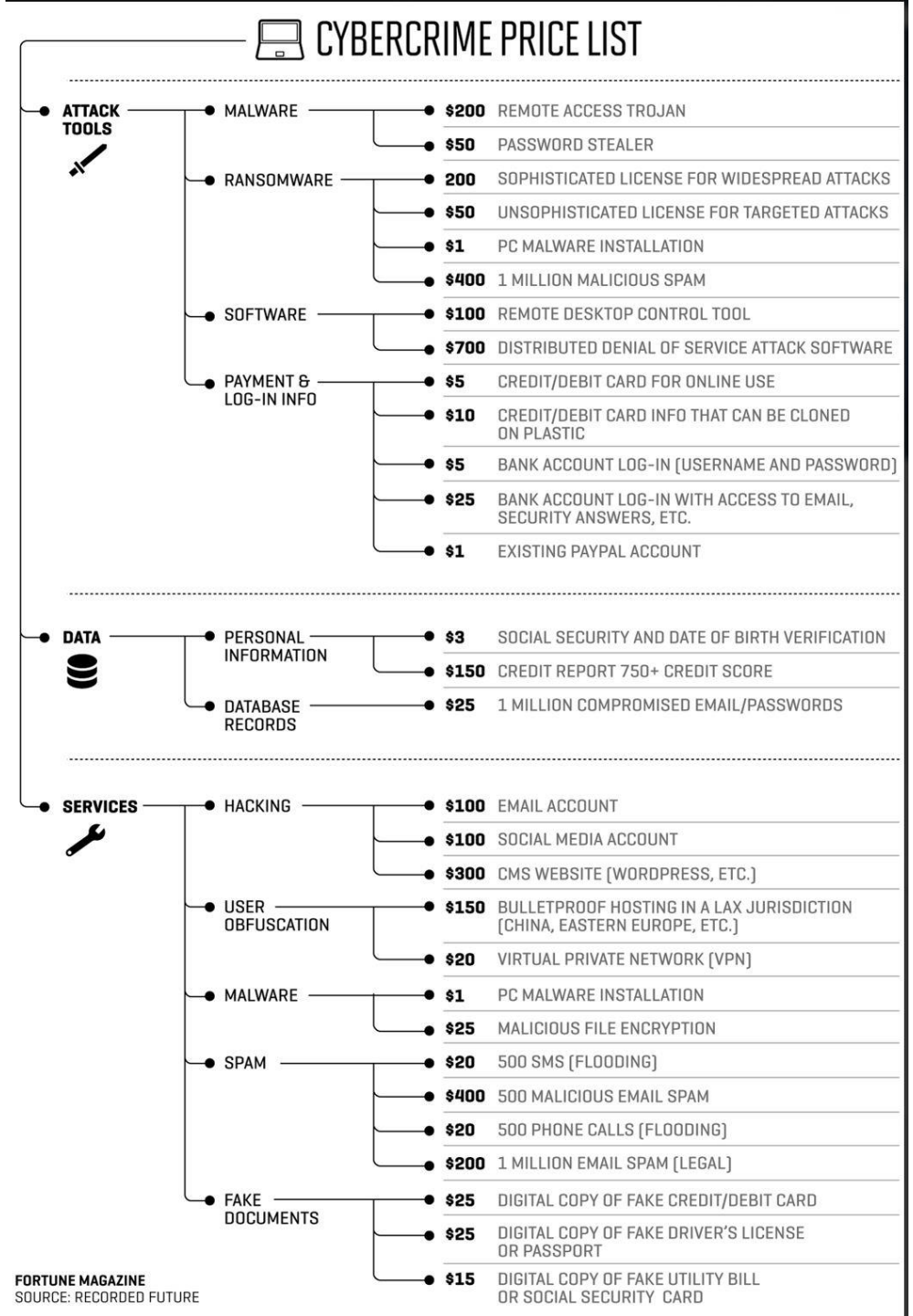
Jan Pilař
Technology Solutions Professional – Modern Desktop

Windows


anti aircraft defence in
bing.com/images/search?q=anti+aircraft+defence+in+ww2&view=detailv2&&id=C7D72D7E92C12ED540FF9EA0B7E4205429ED5930&selectedIndex=1&ccid=gesA2KCX&simid=608013082104037718&thid=OIP.M81eb00d8a09712455139eb595e60c
anti aircraft defence in
WW2 Bombers
Anti-Aircraft WW2 Vehicals
Hand Held Anti-Aircraft Weapons
Anti-Aircraft Gun
Anti-Aircraft Bullets
WWII Anti-Aircraft Artillery
WWII Anti-Aircraft Guns
Anti-Aircraft Flak
WWII Aircraft
WW2 Anti-Air Born
WW2 Guns
Anti-Aircraft Tank
WW2 Weapons
German Anti-Aircraft
Zobrazit stránku:ilpost.it
980 x 670 · jpeg Na obrázek se mohou vztahovat autorská p…
Even the Polish government poured fuel on the fire, with +
— africanseer.com
Více informací o tomto obrázku
10:03
04.08.2016


7 - Bing images
bing.com/images/search?q=F117&view=detailv2&&id=4F7C9914EB78CCE150BC60F0F547CA17DD2FF5C6&selectedIndex=4&ccid=CKEpSVw8&simid=608055851388371803&thid=OIP.M08a129495c3c7d2a5998101d9704e13ao0&ajaxhist=0
Lockheed F-117 Nighthawk
McDonnell Douglas F A-18 Hornet
Lockheed SR -71 Blackbird
Grumman F -14 Tomcat
Lockheed Martin F-35 Lightning II
Lockheed Martin F-22 Raptor
Aurora Aircraft
McDonnell Douglas F-15 Eagle
Northrop Grumman B-2 Spirit
Stealth Aircraft
Eurofighter Typhoon
Sukhoi PAK FA
General Dynamics F-111 Aardvark
Zobrazit stránku:storiesbywilliams.com
1280 x 960 · jpeg Na obrázek se mohou vztahovat autorská…
Více informací o tomto obrázku
10:10
04.08.2016


7 - Bing images
bing.com/images/search?q=F117&view=detailv2&&id=4F7C9914EB78CCE150BC60F0F547CA17DD2FF5C6&selectedIndex=4&ccid=CKEpSVw8&simid=608055851388371803&thid=OIP.M08a129495c3c7d2a5998101d9704e13ao0&ajaxhist=0
Lockheed F-117 Nighthawk
McDonnell Douglas F A-18 Hornet
Lockheed SR -71 Blackbird
Grumman F -14 Tomcat
Lockheed Martin F-35 Lightning II
Lockheed Martin F-22 Raptor
Aurora Aircraft
McDonnell Douglas F-15 Eagle
Northrop Grumman B-2 Spirit
Stealth Aircraft
Eurofighter Typhoon
Sukhoi PAK FA
General Dynamics F-111 Aardvark
Zobrazit stránku:storiesbywilliams.com
1280 x 960 · jpeg Na obrázek se mohou vztahovat autorská…
Více informací o tomto obrázku
10:10
04.08.2016


CYBERCRIME PRICE LIST
ATTACK TOOLS
MALWARE
$200 REMOTE ACCESS TROJAN
$50 PASSWORD STEALER
RANSOMWARE
200 SOPHISTICATED LICENSE FOR WIDESPREAD ATTACKS
$50 UNSOPHISTICATED LICENSE FOR TARGETED ATTACKS
$1 PC MALWARE INSTALLATION
$400 1 MILLION MALICIOUS SPAM
SOFTWARE
$100 REMOTE DESKTOP CONTROL TOOL
$700 DISTRIBUTED DENIAL OF SERVICE ATTACK SOFTWARE
PAYMENT & LOG-IN INFO
$5 CREDIT/DEBIT CARD FOR ONLINE USE
$10 CREDIT/DEBIT CARD INFO THAT CAN BE CLONED ON PLASTIC
$5 BANK ACCOUNT LOG-IN (USERNAME AND PASSWORD)
$25 BANK ACCOUNT LOG-IN WITH ACCESS TO EMAIL, SECURITY ANSWERS, ETC.
$1 EXISTING PAYPAL ACCOUNT
DATA
PERSONAL INFORMATION
$3 SOCIAL SECURITY AND DATE OF BIRTH VERIFICATION
$150 CREDIT REPORT 750+ CREDIT SCORE
DATABASE RECORDS
$25 1 MILLION COMPROMISED EMAIL/PASSWORDS
SERVICES
HACKING
$100 EMAIL ACCOUNT
$100 SOCIAL MEDIA ACCOUNT
$300 CMS WEBSITE (WORDPRESS, ETC.)
USER OBFUSCATION
$150 BULLETPROOF HOSTING IN A LAX JURISDICTION (CHINA, EASTERN EUROPE, ETC.)
$20 VIRTUAL PRIVATE NETWORK (VPN)
MALWARE
$1 PC MALWARE INSTALLATION
$25 MALICIOUS FILE ENCRYPTION
SPAM
$20 500 SMS (FLOODING)
$400 500 MALICIOUS EMAIL SPAM
$20 500 PHONE CALLS (FLOODING)
$200 1 MILLION EMAIL SPAM (LEGAL)
FAKE DOCUMENTS
$25 DIGITAL COPY OF FAKE CREDIT/DEBIT CARD
$25 DIGITAL COPY OF FAKE DRIVER'S LICENSE OR PASSPORT
$15 DIGITAL COPY OF FAKE UTILITY BILL OR SOCIAL SECURITY CARD
FORTUNE MAGAZINE
SOURCE: RECORDED FUTURE

Využití AI v oblasti ochrany

Windows Defender ATP

Proč AI v oblasti ochrany?

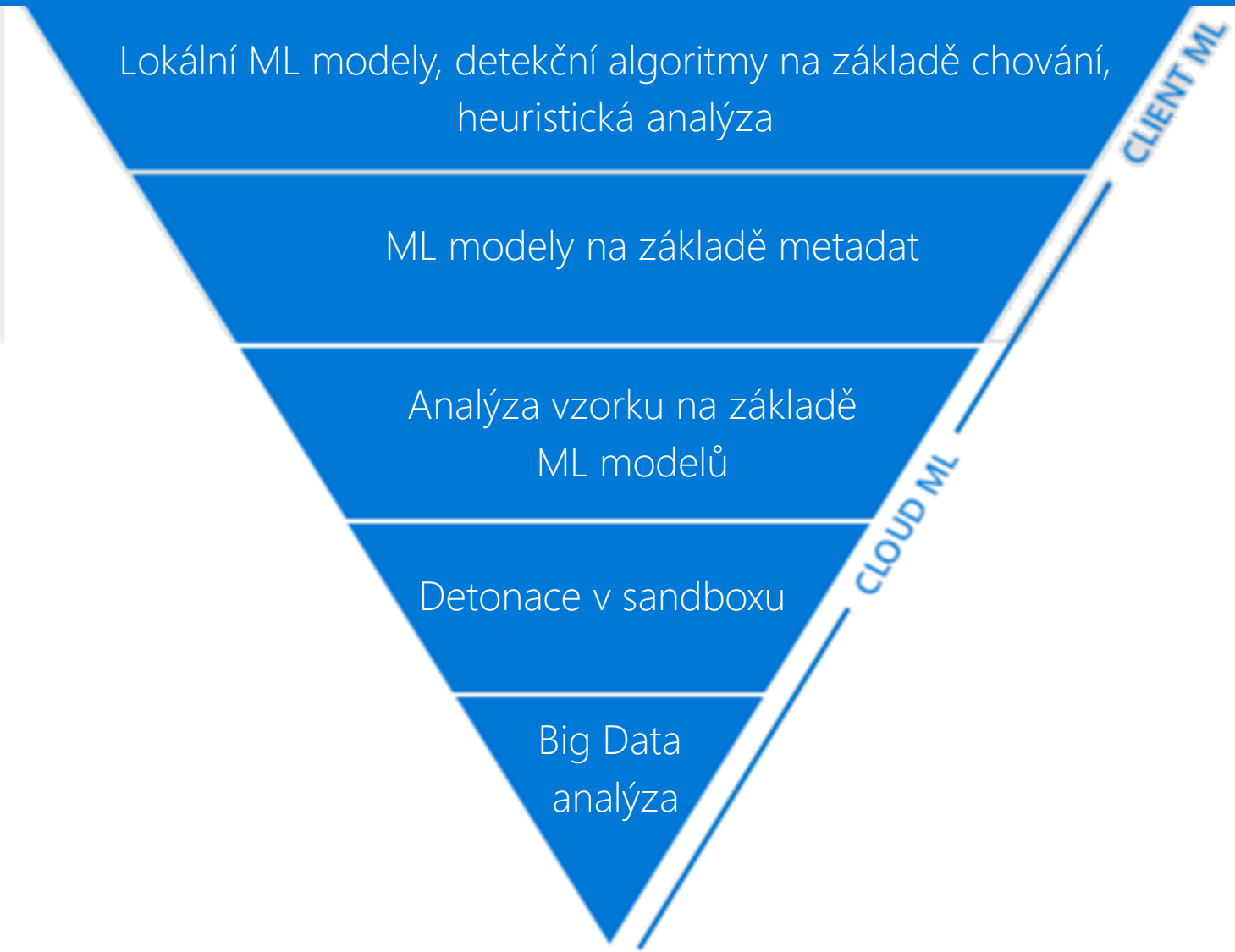
Windows Defender
Cloud-Based
Protection

Command
& Control

Uživatel 1

Uživatel 2

Útočník



Ochrana v řádu milisekund

Většina běžného malware je blokována pomocí vysoce přesné Detekce Windows Defender AV

Ochrana v řádu milisekund

Machine Learning pravidla hodnotí podezřelé spustitelné soubory na základě metadat odeslaných Windows Defender AV

Ochrana v řádu sekund

Kopie podezřelého spustitelného souboru je nahrána za účelem inspekce pomocí „Multi-Class Machine Learning“

Ochrana v řádu sekund

Podezřelý soubor je spuštěn v sandboxu v rámci dynamické analýzy Pomocí „Multi-Class Machine Learning“

Ochrana v řádu hodin

Machine Learning modely a expertní pravidla porovnávají signály ze sítě sensorů k automatické klasifikaci hrozeb

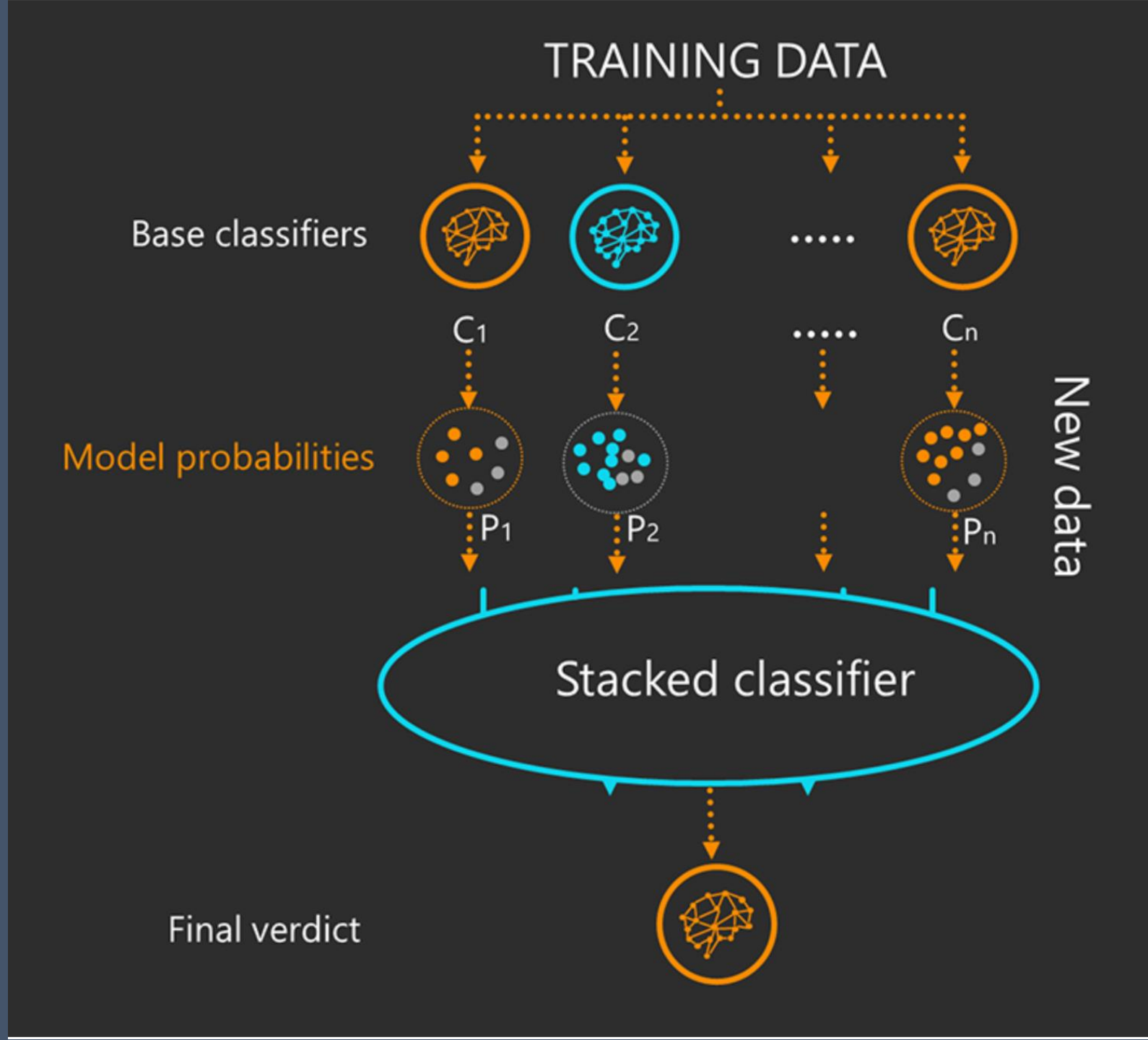
Microsoft

	Feature Set	Learner	# of Features	
Client models	PE properties	Fast tree ensemble	10K+ features	PE
Cloud models	Researcher expertise	Boosted tree ensemble	190K+ features	JavaScript
	Behavioral	Boosted tree ensemble	6M+ features	
Full file content models	Fuzzy hash 1	Random forest	512+ features	VBScript
	Fuzzy hash 2	SDCA	10M+ features	PDF
	Static, dynamic, and contextual	Averaged perceptron	16M+ features	
File detonation models	Researcher expertise, fuzzy hash	Averaged perceptron	12M+ features	Macro
	File emulation	Multiclass DNN	150K+ features	
	File detonation	Multiclass DNN	10M+ features	

Windows

Microsoft

Windows



AV-TEST Product Review and Certification Report – May-Jun/2018

During May and June 2018 we continuously evaluated 16 endpoint protection products using settings as provided by the vendor. We always used the most current publicly-available version of all products for the testing. They were allowed to update themselves at any time and query their in-the-cloud services. We focused on realistic test scenarios and challenged the products against real-world threats. Products had to demonstrate their capabilities using all components and protection layers.

Microsoft

Windows Defender Antivirus

Version 4.12
Platform Windows 10 (64 bit)
Report 182374
Date May-Jun/2018

Website ›
Archive ›

Protection

Protection against malware infections
(such as viruses, worms or Trojan horses)
More information

	Industry average	May	June
Protection against 0-day malware attacks, inclusive of web and e-mail threats (Real-World Testing) 225 samples used	100%	100%	100%
Detection of widespread and prevalent malware discovered in the last 4 weeks (the AV-TEST reference set) 5,565 samples used	100%	100%	100%
Protection Score		6.0/6.0	

Využití AI v oblasti detekce

Windows Defender ATP

Proč AI v oblasti detekce?

Proč AI v oblasti detekce?

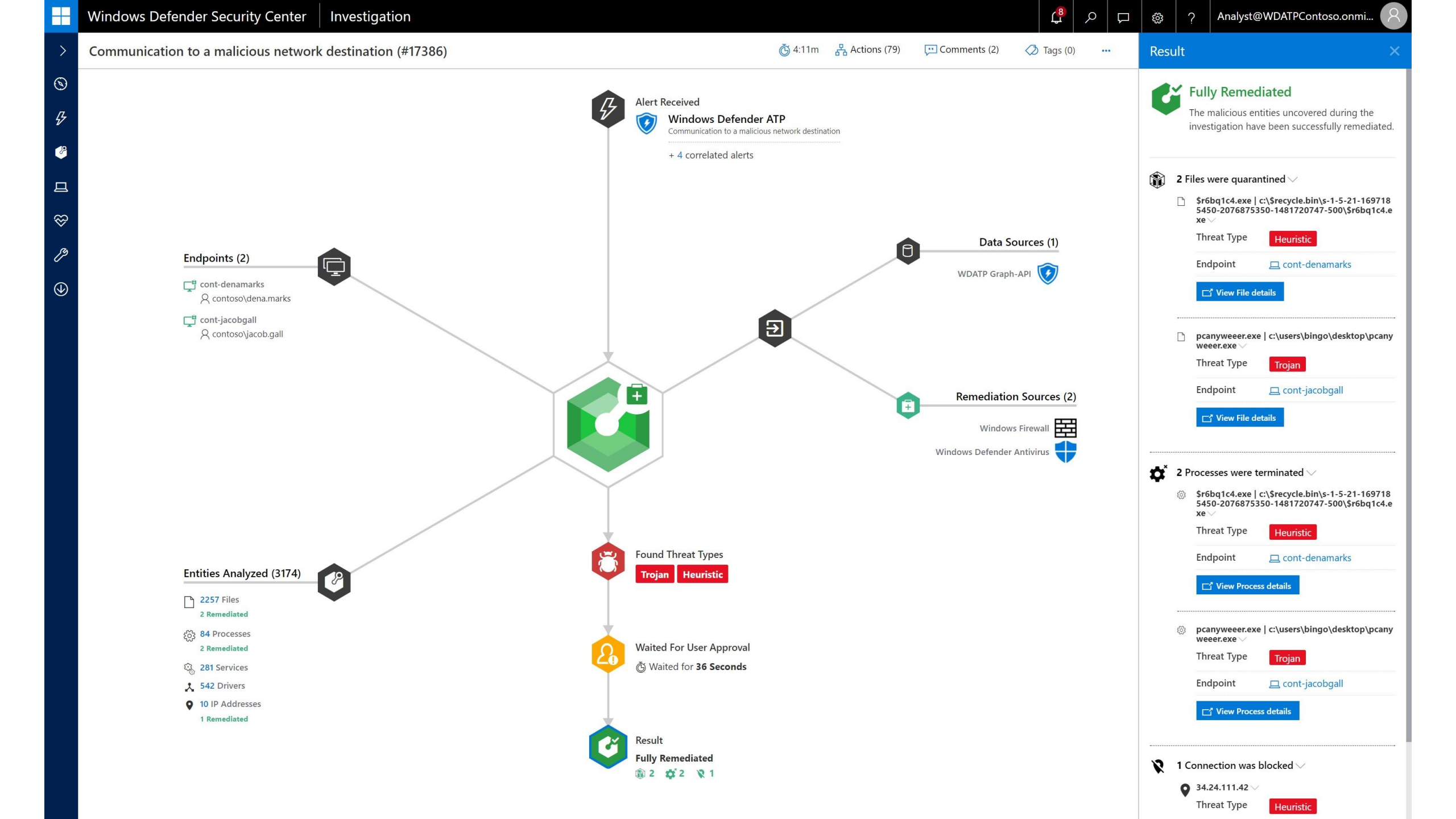
Proč AI v oblasti detekce?

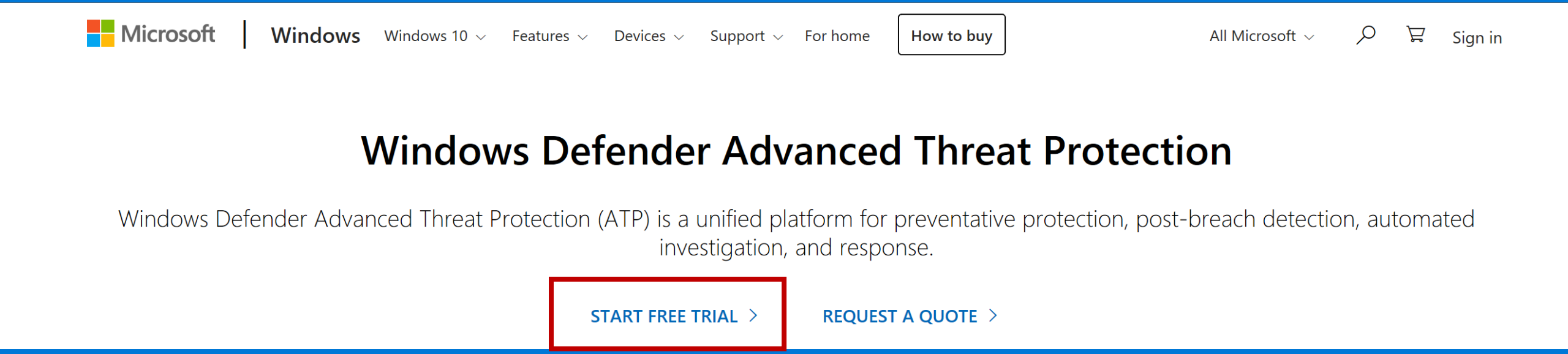
Co je WDATP Auto-IR?

- Auto-IR je:

  Napodobení ideálních kroků, které by člověk měl udělat **k vyšetření a nápravě** cyber hrozby

- Co takové kroky jsou:
  - Analýza informací z alertu a sběr dalších informací
  - Spuštění potřebných nápravných akcí
  - Určení rozsahu a analýza postranních hrozeb
  - Opakování výše uvedeného pro každý další alert


Windows Defender Security Center
Investigation
Analyst@WDATPContoso.onmi...
Communication to a malicious network destination (#17386)
4:11m
Actions (79)
Comments (2)
Tags (0)
Alert Received
Windows Defender ATP
Communication to a malicious network destination
+ 4 correlated alerts
Endpoints (2)
cont-denamarks
contoso\dena.marks
cont-jacobgall
contoso\jacob.gall
Data Sources (1)
WDATP Graph-API
Remediation Sources (2)
Windows Firewall
Windows Defender Antivirus
Entities Analyzed (3174)
2257 Files
2 Remediated
84 Processes
2 Remediated
281 Services
542 Drivers
10 IP Addresses
1 Remediated
Found Threat Types
Trojan
Heuristic
Waited For User Approval
Waited for 36 Seconds
Result
Fully Remediated
2 2 1
Result
Fully Remediated
The malicious entities uncovered during the investigation have been successfully remediated.
2 Files were quarantined
$r6bq1c4.exe | c:\$recycle.bin\s-1-5-21-1697185450-2076875350-1481720747-500\$r6bq1c4.exe
Threat Type
Heuristic
Endpoint
cont-denamarks
View File details
pcanyweeer.exe | c:\users\bingo\desktop\pcanyweeer.exe
Threat Type
Trojan
Endpoint
cont-jacobgall
View File details
2 Processes were terminated
$r6bq1c4.exe | c:\$recycle.bin\s-1-5-21-1697185450-2076875350-1481720747-500\$r6bq1c4.exe
Threat Type
Heuristic
Endpoint
cont-denamarks
View Process details
pcanyweeer.exe | c:\users\bingo\desktop\pcanyweeer.exe
Threat Type
Trojan
Endpoint
cont-jacobgall
View Process details
1 Connection was blocked
34.24.111.42
Threat Type
Heuristic



Vyzkoušejte i u vás a zdarma!

Aka.ms/wdatp

Jan.pilar@microsoft.com