CYBER RESILIENCE

24. februar, 2023 Sarajevo

O čemu razgovaramo danas?

Šta su danas realne cyber prijetnje?

Primjer jednog realnog cyber napada

Cyber resilience

Svijet se promijenio

Promijenila se priroda poslovanja i rada

Konvencionalni sigurnosni alati nisu zadržali korak

Troškovi rastu

Kontekstualno interesantni podaci i statistike

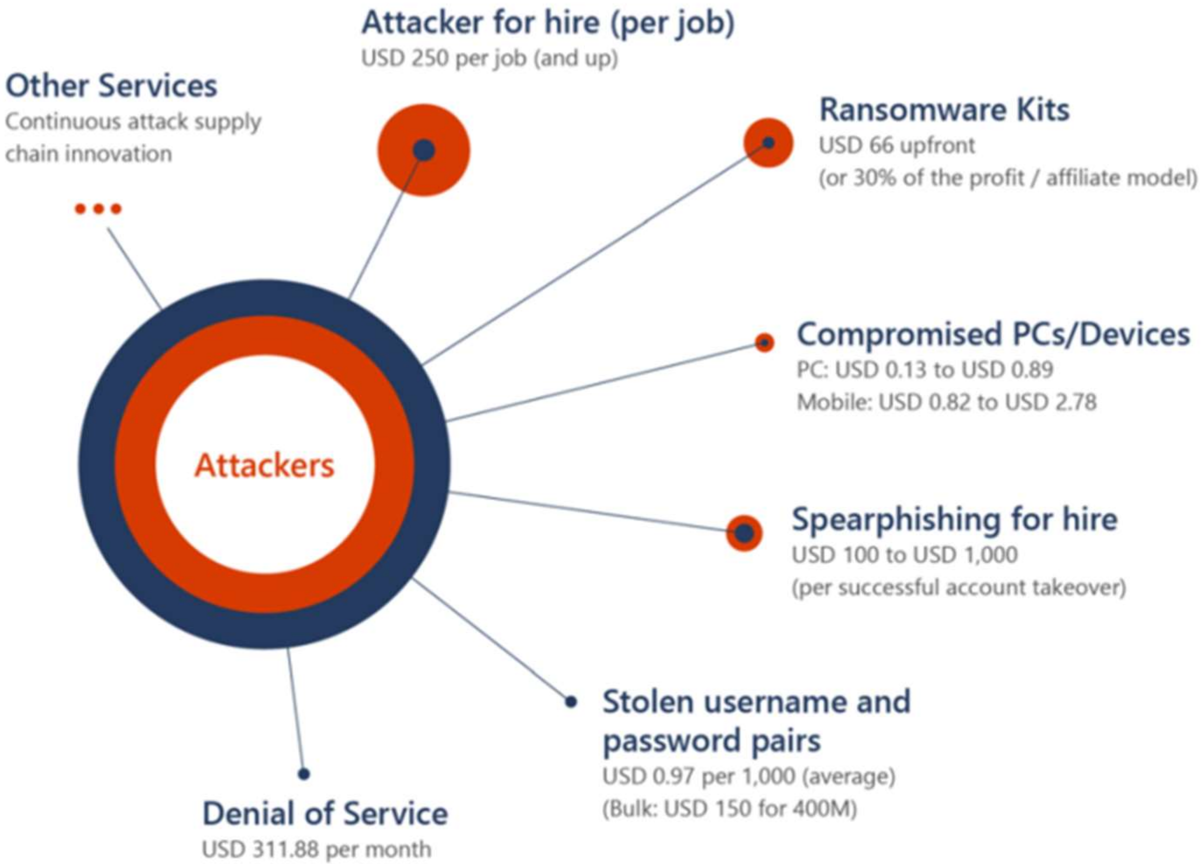
Prosječno vrijeme koje napadač provede „unutra“ prije egzekucije napada je 150-180 dana.

Najveći broj napada se realizuje ugrožavanjem digitalnog identiteta. U Q3 2022 je broj account breach incidenata porastao za 70% (izvor: Gobal data breach stats)

Čak ½ data breach incidenata u Q3 2022 se desila u Evropi. Prema zvaničnom FBI izvještaju, broj globalnih cyber napada povećan je za 300% u zadnje dvije godine i 1500% u zadnjih 5 godina.

Najčešći razlog uspješnog cyber napada – „negligent insiders“.

Prosječna cijena prodaje usluga cyber napada na dark marketu



Attacker for hire (per job)
USD 250 per job (and up)

Other Services
Continuous attack supply chain innovation

Ransomware Kits
USD 66 upfront
(or 30% of the profit / affiliate model)

Compromised PCs/Devices
PC: USD 0.13 to USD 0.89
Mobile: USD 0.82 to USD 2.78

Attackers

Spearphishing for hire
USD 100 to USD 1,000
(per successful account takeover)

Stolen username and password pairs
USD 0.97 per 1,000 (average)
(Bulk: USD 150 for 400M)

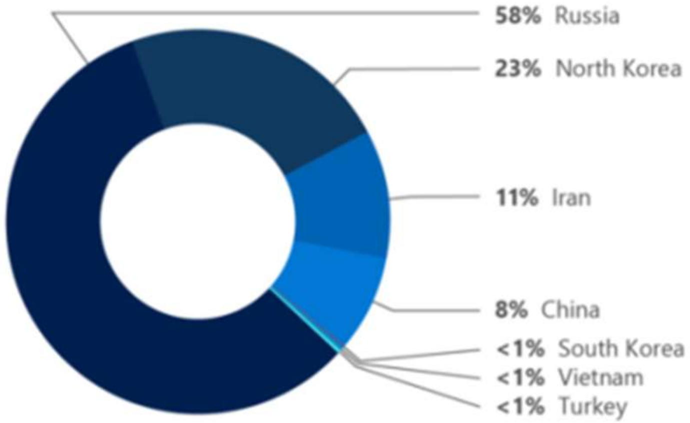
Denial of Service
USD 311.88 per month

Kompanije se sada susreću sa industrijalizacijskom napadačkom ekonomijom, koja trguje stručnim specijalizacijama i nedozvoljenim radnjama.

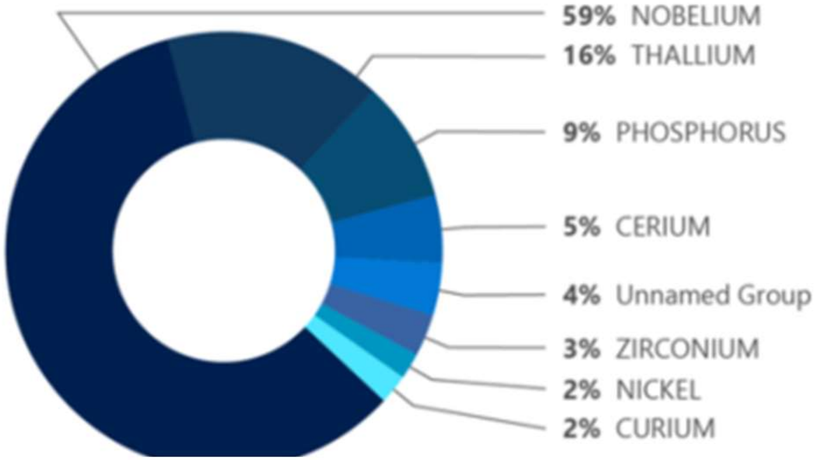
Mnoge cyber napade je moguće kupiti po vrlo niskim cijenama na dark marketu, čime je jeftinija dobavljivost i lakša izvodljivosti cyber napada, čime se direktno povećava količina napada.

Izvori cyber napada

Attacks by country of origin (July 2020-June 2021)



Most active nation state activity groups (July 2020-June 2021)

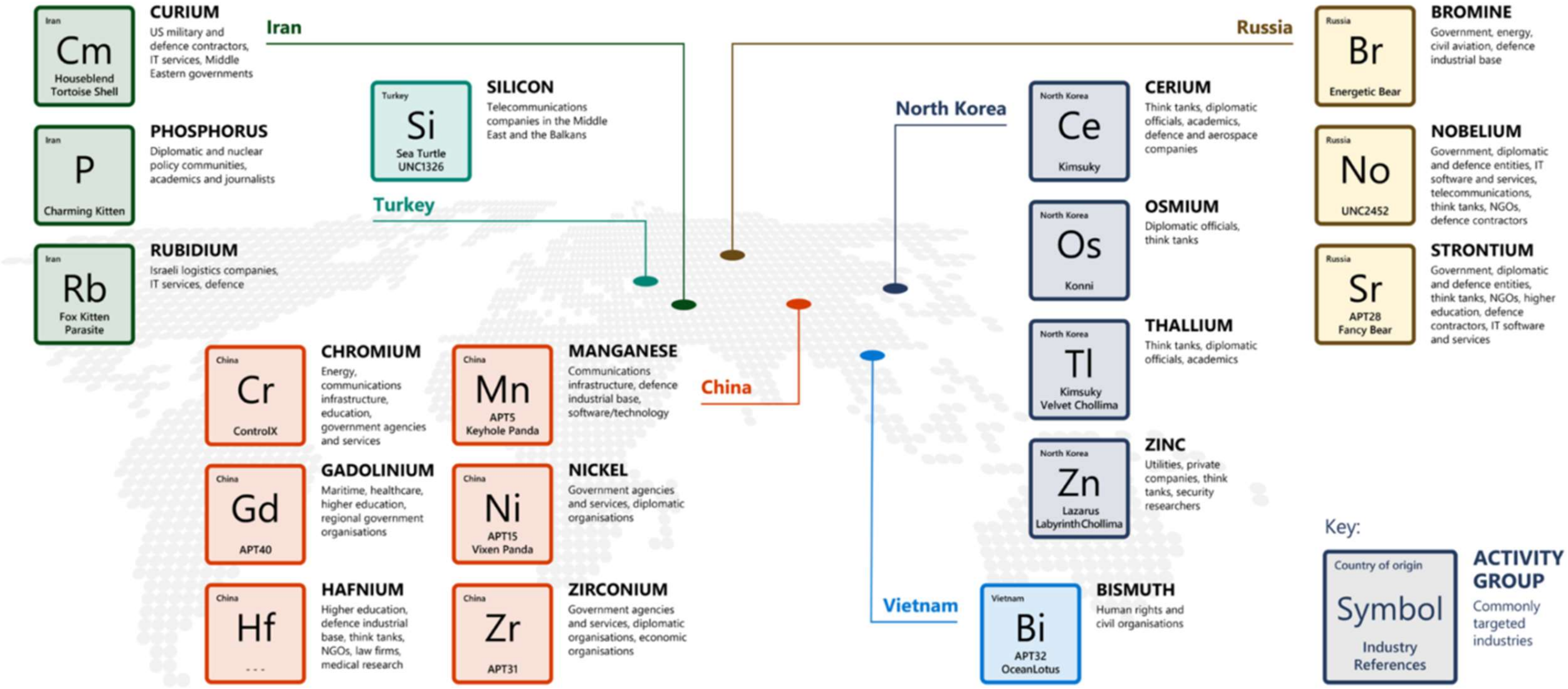


Attack vectors used by nation state malicious actors

PASSWORD SPRAY
SOCIAL ENGINEERING
PHISHING
IDENTITY SPOOFING
MALWARE
SUPPLY CHAIN INSERTION
MAN-IN-THE-MIDDLE
DENIAL OF SERVICE

Nation states are advanced enough to do reconnaissance on their victims and select the attack method that best suits each goal or intended outcome.

Uzorak aktera iz pojedinih država i njihove aktivnosti



Iran

Iran
Cm
Houseblend
Tortoise Shell

CURIUM
US military and defence contractors, IT services, Middle Eastern governments

Iran
P
Charming Kitten

PHOSPHORUS
Diplomatic and nuclear policy communities, academics and journalists

Iran
Rb
Fox Kitten
Parasite

RUBIDIUM
Israeli logistics companies, IT services, defence

Turkey

Turkey
Si
Sea Turtle
UNC1326

SILICON
Telecommunications companies in the Middle East and the Balkans

China

China
Cr
ControlX

CHROMIUM
Energy, communications infrastructure, education, government agencies and services

China
Mn
APT5
Keyhole Panda

MANGANESE
Communications infrastructure, defence industrial base, software/technology

China
Gd
APT40

GADOLINIUM
Maritime, healthcare, higher education, regional government organisations

China
Ni
APT15
Vixen Panda

NICKEL
Government agencies and services, diplomatic organisations

China
Hf
- - -

HAFNIUM
Higher education, defence industrial base, think tanks, NGOs, law firms, medical research

China
Zr
APT31

ZIRCONIUM
Government agencies and services, diplomatic organisations, economic organisations

North Korea

North Korea
Ce
Kimsuky

CERIUM
Think tanks, diplomatic officials, academics, defence and aerospace companies

North Korea
Os
Konni

OSMIUM
Diplomatic officials, think tanks

North Korea
Tl
Kimsuky
Velvet Chollima

THALLIUM
Think tanks, diplomatic officials, academics

North Korea
Zn
Lazarus
LabyrinthChollima

ZINC
Utilities, private companies, think tanks, security researchers

Vietnam

Vietnam
Bi
APT32
OceanLotus

BISMUTH
Human rights and civil organisations

Russia

Russia
Br
Energetic Bear

BROMINE
Government, energy, civil aviation, defence industrial base

Russia
No
UNC2452

NOBELIUM
Government, diplomatic and defence entities, IT software and services, telecommunications, think tanks, NGOs, defence contractors

Russia
Sr
APT28
Fancy Bear

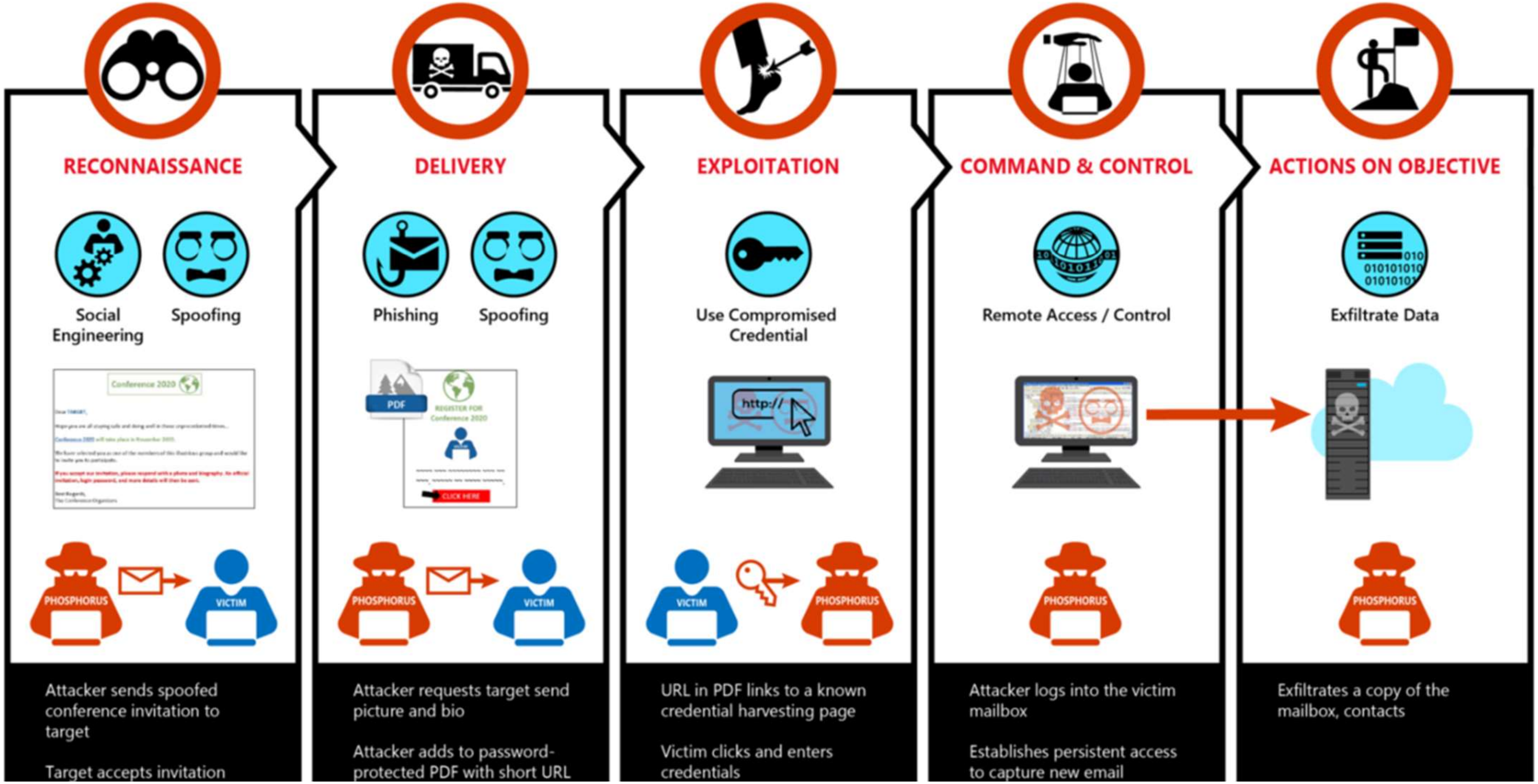
STRONTIUM
Government, diplomatic and defence entities, think tanks, NGOs, higher education, defence contractors, IT software and services

Key:

Country of origin
Symbol
Industry
References

ACTIVITY GROUP
Commonly targeted industries

Slijed tipičnog FOSFOR kompromitovanja iz ‚spear phishing' napada



RECONNAISSANCE
Social Engineering
Spoofing
Conference 2020
Dear TARGET,
Hope you are all staying safe and doing well in these unprecedented times...
Conference 2020 will take place in November 2020.
We have selected you as one of the members of this illustrious group and would like to invite you to participate.
If you accept our invitation, please respond with a photo and biography. An official invitation, login password, and more details will then be sent.
Best Regards,
The Conference Organizers
PHOSPHORUS
VICTIM
DELIVERY
Phishing
Spoofing
PDF
REGISTER FOR Conference 2020
CLICK HERE
PHOSPHORUS
VICTIM
EXPLOITATION
Use Compromised Credential
http://
VICTIM
PHOSPHORUS
COMMAND & CONTROL
Remote Access / Control
PHOSPHORUS
ACTIONS ON OBJECTIVE
Exfiltrate Data
010
010101010
01010101
PHOSPHORUS

Attacker sends spoofed conference invitation to target

Target accepts invitation

Attacker requests target send picture and bio

Attacker adds to password-protected PDF with short URL

URL in PDF links to a known credential harvesting page

Victim clicks and enters credentials

Attacker logs into the victim mailbox

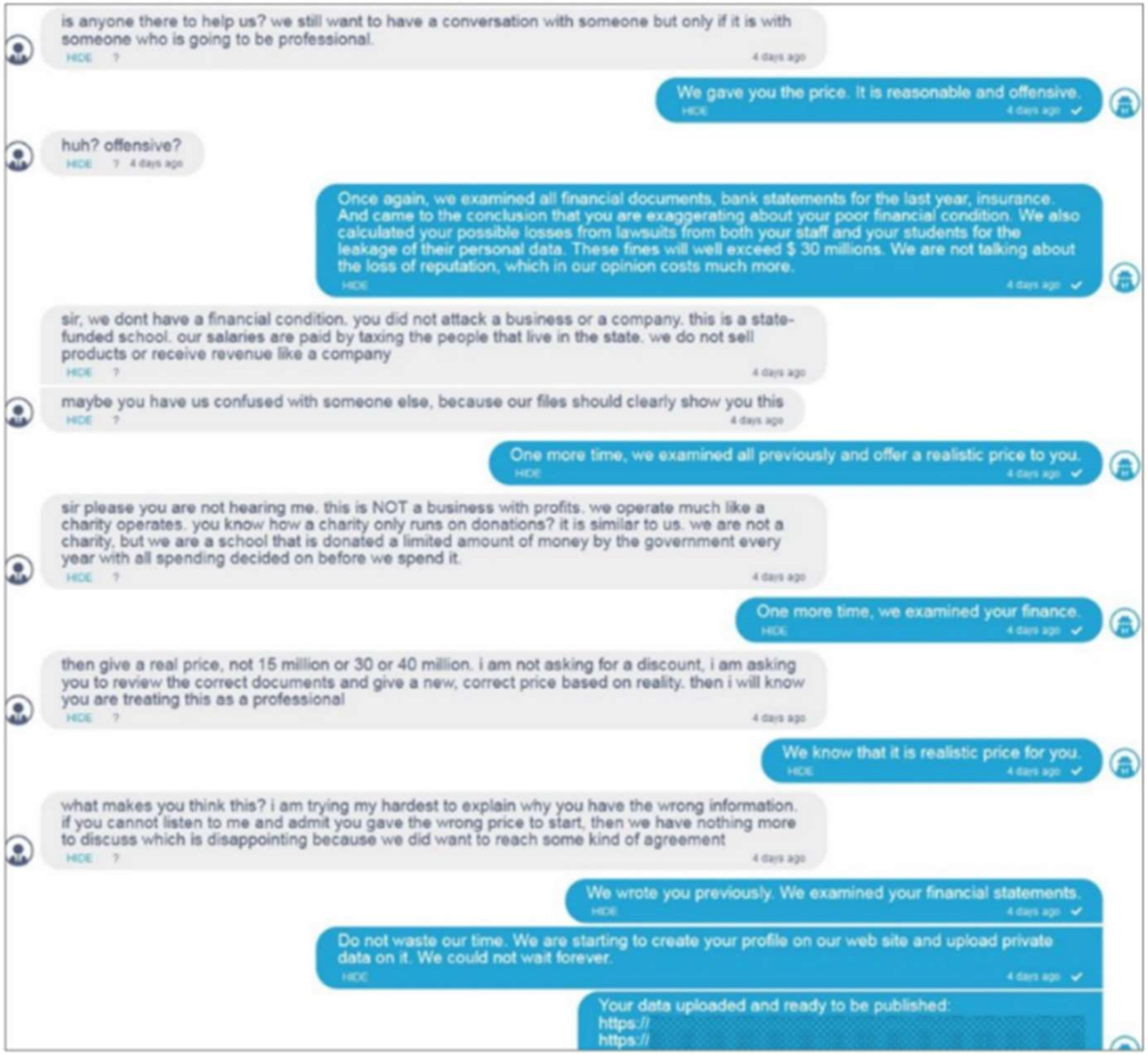
Establishes persistent access to capture new email

Exfiltrates a copy of the mailbox, contacts

Conferences, conventions and trade shows are widely known throughout industry and the US government as a hotbed of intelligence collection activities, both by domestic competitive intelligence and foreign adversaries. Individuals have been known to collect information thrown out in the trash, record presentations, attempt to steal products and solicit sensitive information from employees. Though these events were widely paused due to pandemic restrictions, major conventions are coming back to calendars.

LOGOSOFT

Ransomware negotiation chat



is anyone there to help us? we still want to have a conversation with someone but only if it is with someone who is going to be professional.
HIDE ? 4 days ago

We gave you the price. It is reasonable and offensive.
HIDE 4 days ago ✓

huh? offensive?
HIDE ? 4 days ago

Once again, we examined all financial documents, bank statements for the last year, insurance. And came to the conclusion that you are exaggerating about your poor financial condition. We also calculated your possible losses from lawsuits from both your staff and your students for the leakage of their personal data. These fines will well exceed $ 30 millions. We are not talking about the loss of reputation, which in our opinion costs much more.
HIDE 4 days ago ✓

sir, we dont have a financial condition. you did not attack a business or a company. this is a state-funded school. our salaries are paid by taxing the people that live in the state. we do not sell products or receive revenue like a company
HIDE ? 4 days ago

maybe you have us confused with someone else, because our files should clearly show you this
HIDE ? 4 days ago

One more time, we examined all previously and offer a realistic price to you.
HIDE 4 days ago ✓

sir please you are not hearing me. this is NOT a business with profits. we operate much like a charity operates. you know how a charity only runs on donations? it is similar to us. we are not a charity, but we are a school that is donated a limited amount of money by the government every year with all spending decided on before we spend it.
HIDE ? 4 days ago

One more time, we examined your finance.
HIDE 4 days ago ✓

then give a real price, not 15 million or 30 or 40 million. i am not asking for a discount, i am asking you to review the correct documents and give a new, correct price based on reality. then i will know you are treating this as a professional
HIDE ? 4 days ago

We know that it is realistic price for you.
HIDE 4 days ago ✓

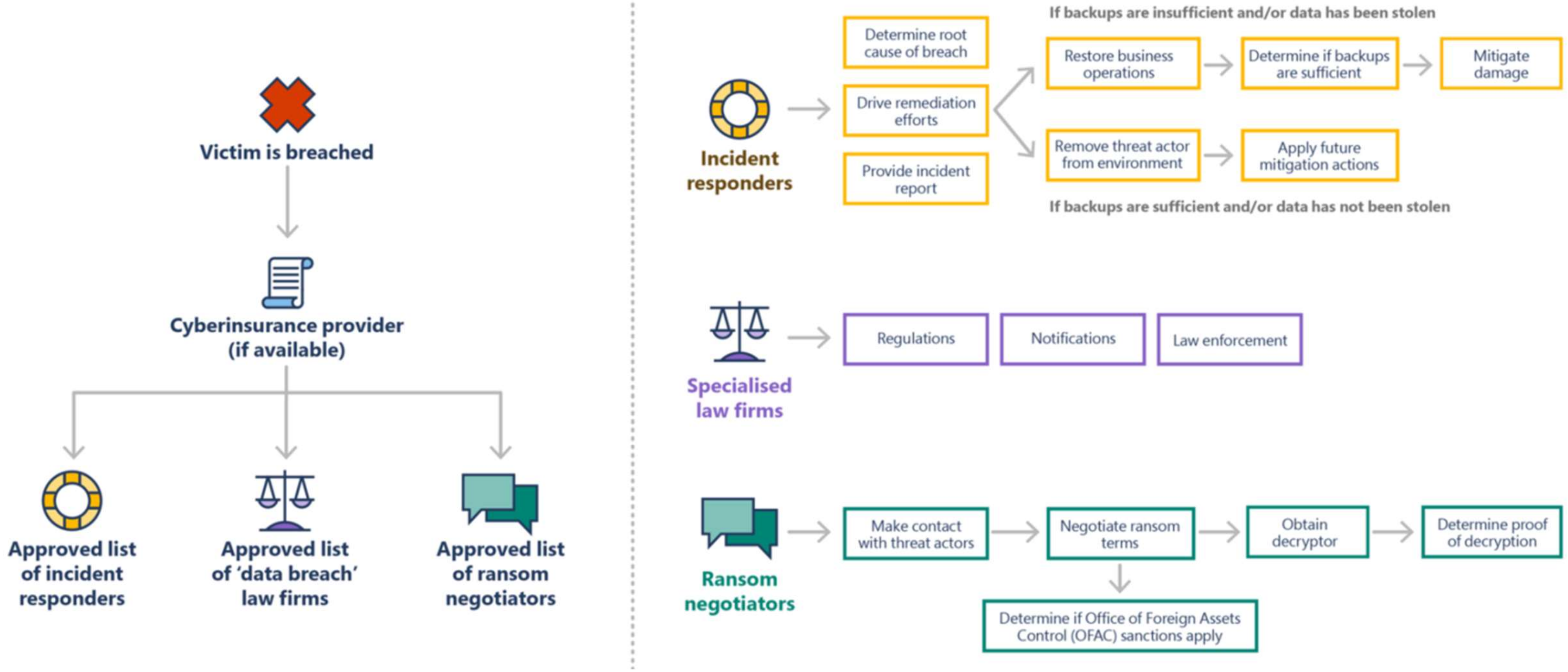
what makes you think this? i am trying my hardest to explain why you have the wrong information. if you cannot listen to me and admit you gave the wrong price to start, then we have nothing more to discuss which is disappointing because we did want to reach some kind of agreement
HIDE ? 4 days ago

We wrote you previously. We examined your financial statements.
HIDE 4 days ago ✓

Do not waste our time. We are starting to create your profile on our web site and upload private data on it. We could not wait forever.
HIDE 4 days ago ✓

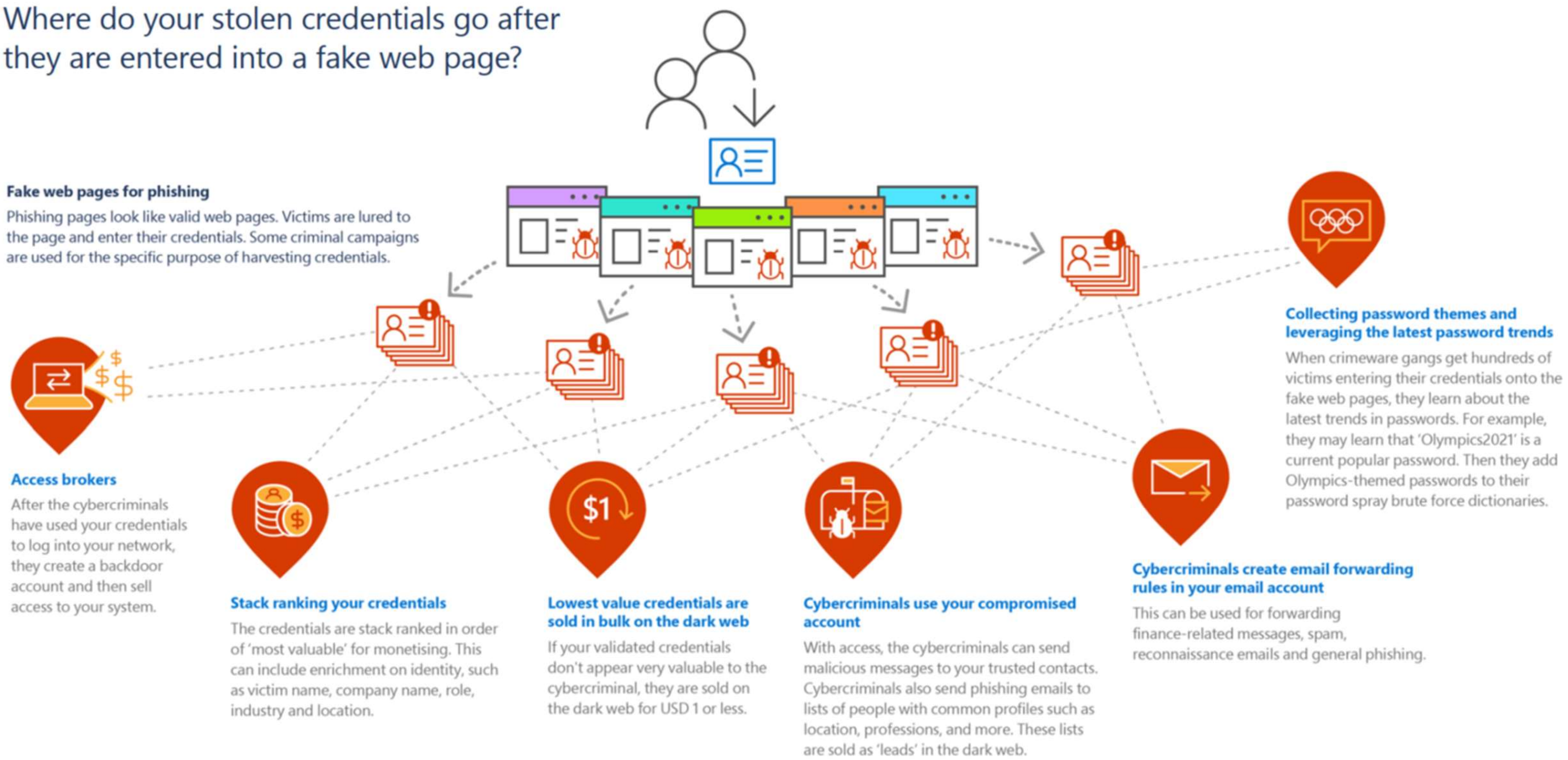
Your data uploaded and ready to be published:
https:// [redacted]
https://

Zainteresovane strane i uloge uključene u odgovor na cyber incident



Victim is breached
Cyberinsurance provider (if available)
Approved list of incident responders
Approved list of 'data breach' law firms
Approved list of ransom negotiators
Incident responders
Determine root cause of breach
Drive remediation efforts
Provide incident report
If backups are insufficient and/or data has been stolen
Restore business operations
Determine if backups are sufficient
Mitigate damage
Remove threat actor from environment
Apply future mitigation actions
If backups are sufficient and/or data has not been stolen
Specialised law firms
Regulations
Notifications
Law enforcement
Ransom negotiators
Make contact with threat actors
Negotiate ransom terms
Obtain decryptor
Determine proof of decryption
Determine if Office of Foreign Assets Control (OFAC) sanctions apply

Digitalni put ukradenih kredencijala



Where do your stolen credentials go after they are entered into a fake web page?

Fake web pages for phishing

Phishing pages look like valid web pages. Victims are lured to the page and enter their credentials. Some criminal campaigns are used for the specific purpose of harvesting credentials.

Access brokers

After the cybercriminals have used your credentials to log into your network, they create a backdoor account and then sell access to your system.

Stack ranking your credentials

The credentials are stack ranked in order of 'most valuable' for monetising. This can include enrichment on identity, such as victim name, company name, role, industry and location.

Lowest value credentials are sold in bulk on the dark web

If your validated credentials don't appear very valuable to the cybercriminal, they are sold on the dark web for USD 1 or less.

Cybercriminals use your compromised account

With access, the cybercriminals can send malicious messages to your trusted contacts. Cybercriminals also send phishing emails to lists of people with common profiles such as location, professions, and more. These lists are sold as 'leads' in the dark web.

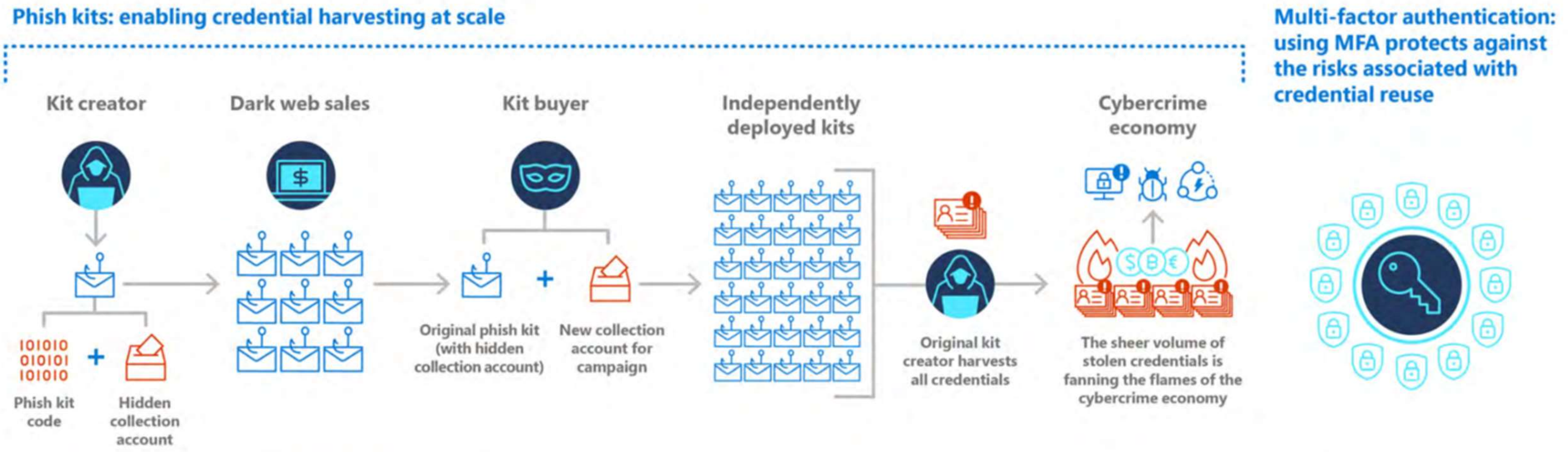
Cybercriminals create email forwarding rules in your email account

This can be used for forwarding finance-related messages, spam, reconnaissance emails and general phishing.

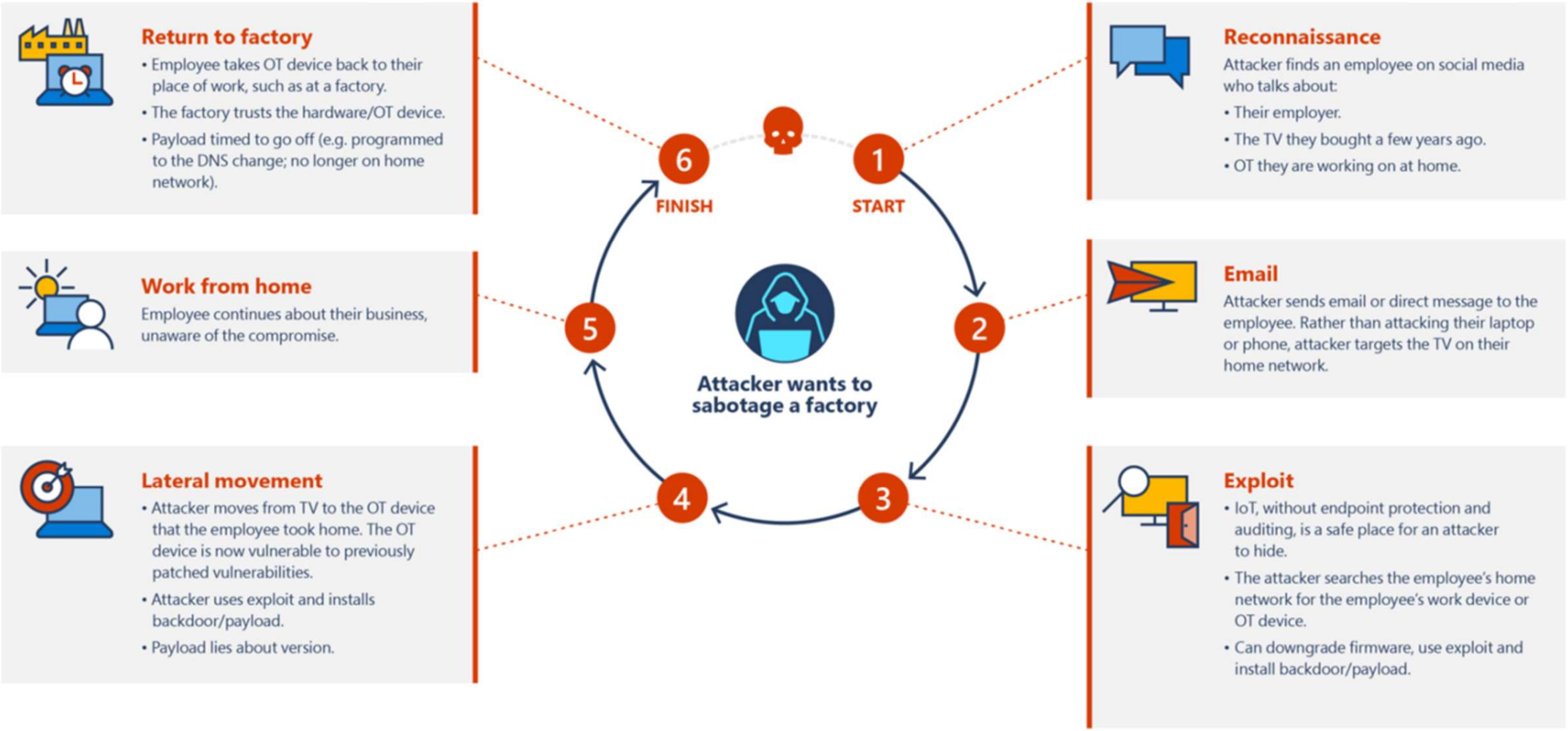
Collecting password themes and leveraging the latest password trends

When crimeware gangs get hundreds of victims entering their credentials onto the fake web pages, they learn about the latest trends in passwords. For example, they may learn that 'Olympics2021' is a current popular password. Then they add Olympics-themed passwords to their password spray brute force dictionaries.

Phishing kompleti i prikupljanje kredencijala


Phish kits: enabling credential harvesting at scale
Kit creator
Dark web sales
Kit buyer
Independently deployed kits
Cybercrime economy
101010
010101
101010
Phish kit code
Hidden collection account
Original phish kit (with hidden collection account)
New collection account for campaign
Original kit creator harvests all credentials
The sheer volume of stolen credentials is fanning the flames of the cybercrime economy
Multi-factor authentication: using MFA protects against the risks associated with credential reuse

Na koji način napadači ulaze u kompanije kroz IoT



Reconnaissance

Attacker finds an employee on social media who talks about:

- Their employer.
- The TV they bought a few years ago.
- OT they are working on at home.

Email

Attacker sends email or direct message to the employee. Rather than attacking their laptop or phone, attacker targets the TV on their home network.

Exploit

- IoT, without endpoint protection and auditing, is a safe place for an attacker to hide.
- The attacker searches the employee's home network for the employee's work device or OT device.
- Can downgrade firmware, use exploit and install backdoor/payload.

Lateral movement

- Attacker moves from TV to the OT device that the employee took home. The OT device is now vulnerable to previously patched vulnerabilities.
- Attacker uses exploit and installs backdoor/payload.
- Payload lies about version.

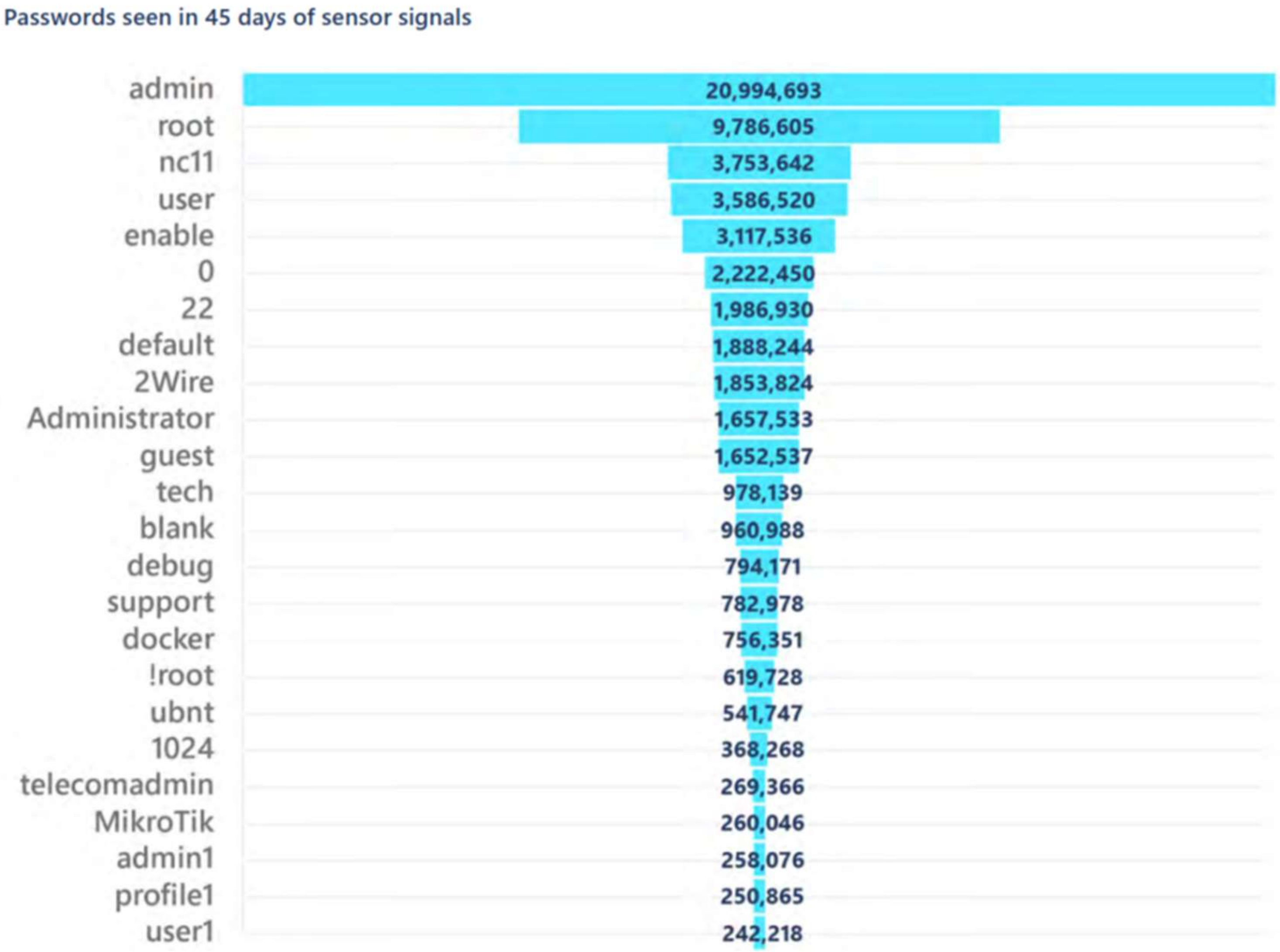
Work from home

Employee continues about their business, unaware of the compromise.

Return to factory

- Employee takes OT device back to their place of work, such as at a factory.
- The factory trusts the hardware/OT device.
- Payload timed to go off (e.g. programmed to the DNS change; no longer on home network).

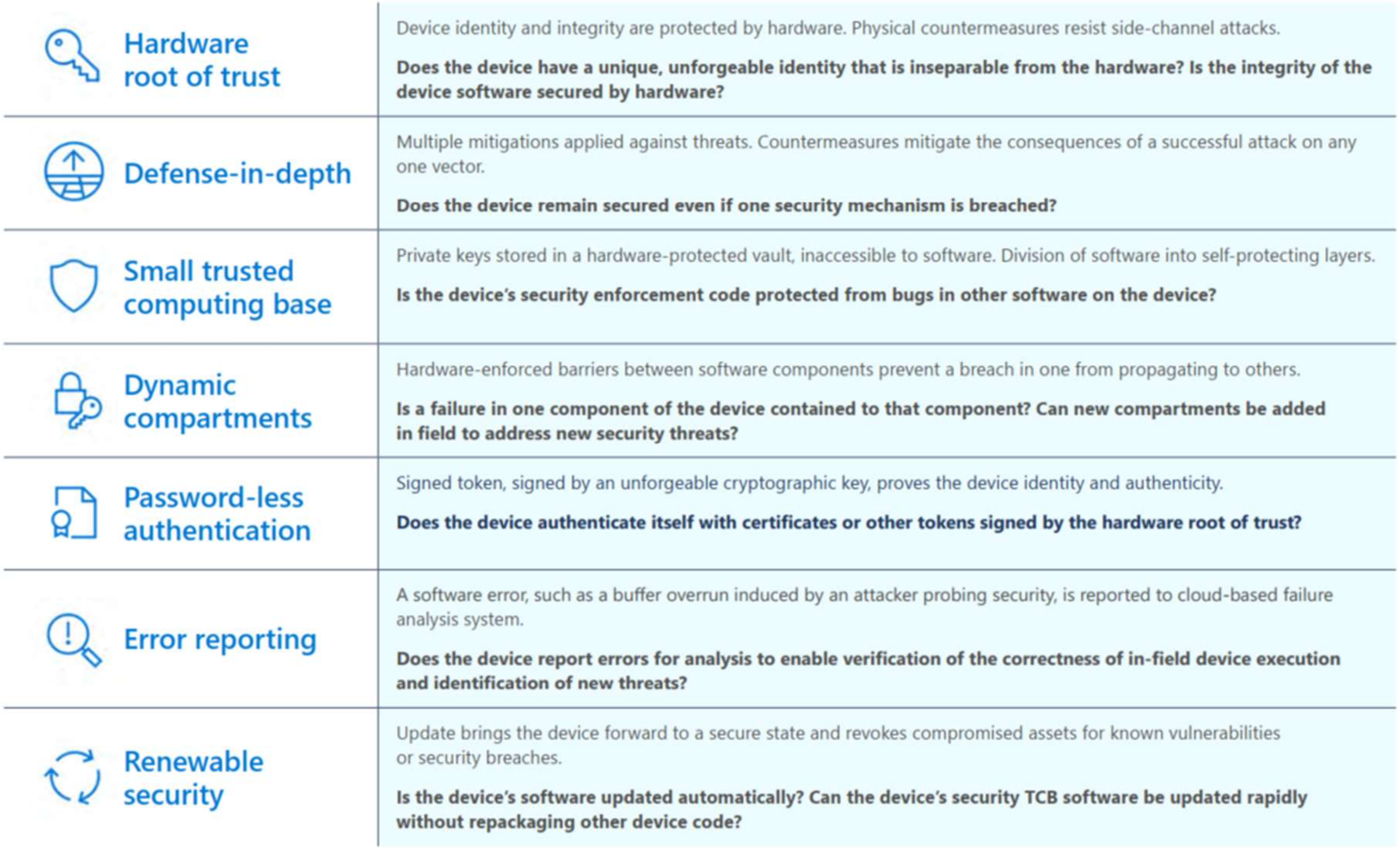
Passwordi IoT uređaja


Passwords seen in 45 days of sensor signals

The seven properties of highly secured devices

We suggest ensuring the hardware and operating system of both your and your suppliers' devices are designed and implemented securely, have high barriers to compromise and incorporate mechanisms and processes that continually monitor, alert and restore security when necessary.

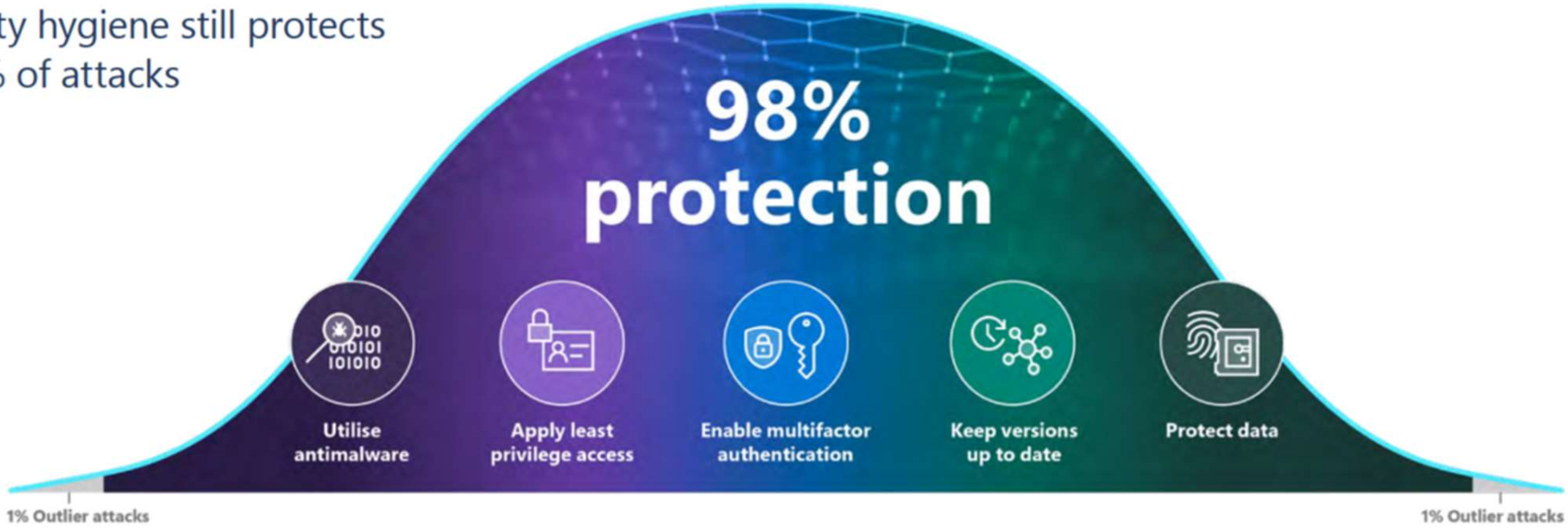
Through extensive research and testing, Microsoft identified the seven properties that are present in all standalone, internet-connected devices considered to be highly secured. In many cases, these highly secured devices apply additional security measures, but in all cases each of the seven properties is present. Collectively, these seven properties provide a baseline foundation of security throughout device silicon, software architecture and OS, cloud communications and cloud services. The complexity of maintaining all seven properties could be a barrier for some organisations, despite the exceptional cost that often results from a fallout of incomplete device security.



Hardware root of trust	Device identity and integrity are protected by hardware. Physical countermeasures resist side-channel attacks. **Does the device have a unique, unforgeable identity that is inseparable from the hardware? Is the integrity of the device software secured by hardware?**
Defense-in-depth	Multiple mitigations applied against threats. Countermeasures mitigate the consequences of a successful attack on any one vector. **Does the device remain secured even if one security mechanism is breached?**
Small trusted computing base	Private keys stored in a hardware-protected vault, inaccessible to software. Division of software into self-protecting layers. **Is the device's security enforcement code protected from bugs in other software on the device?**
Dynamic compartments	Hardware-enforced barriers between software components prevent a breach in one from propagating to others. **Is a failure in one component of the device contained to that component? Can new compartments be added in field to address new security threats?**
Password-less authentication	Signed token, signed by an unforgeable cryptographic key, proves the device identity and authenticity. **Does the device authenticate itself with certificates or other tokens signed by the hardware root of trust?**
Error reporting	A software error, such as a buffer overrun induced by an attacker probing security, is reported to cloud-based failure analysis system. **Does the device report errors for analysis to enable verification of the correctness of in-field device execution and identification of new threats?**
Renewable security	Update brings the device forward to a secure state and revokes compromised assets for known vulnerabilities or security breaches. **Is the device's software updated automatically? Can the device's security TCB software be updated rapidly without repackaging other device code?**

The cybersecurity bell curve:

Basic security hygiene still protects against 98% of attacks



Ključne korisničke bolne tačke

Zero day napadi

Zero days napadi nastavljaju biti glavna prijetnja

Mrežne granice

Perimetri erodiraju, potrebna su jedinstvena rješenja za zaštitu

Cross platforme

Heterogena okruženja su izazovna

U konačnici: Kompanije teško postižu da proaktivno prilagode svoj sigurnosni položaj

Ključne korisničke bolne tačke

⚠ Rješenja koja ovise o redovnim ažuriranjima ne mogu zaštititi od čak 7 miliona jedinstvenih prijetnji, koje se pojavljuju tokom jednog sata

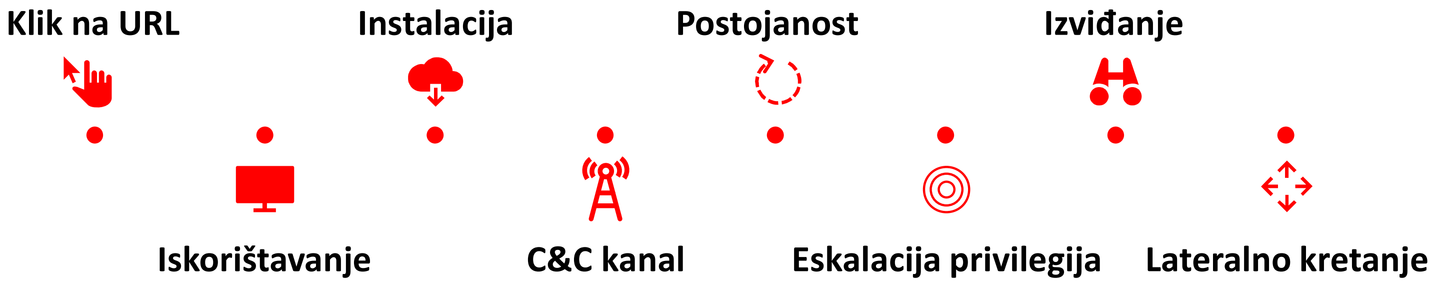
⚠ Igra je prešla s blokiranja prepoznatljivih izvršnih datoteka na zlonamjerni softver koji koristi sofisticirane tehnike iskorištavanja (npr.: fileless)

⚠ Dok Attack Surface Reduction može dramatično povećati vašu sigurnosnu poziciju, još uvijek je potrebna detekcija za preostale ključne tačke

⚠ Živimo u svijetu hiperpolimorfnih prijetnji s 5 milijardi jedinstvenih instanci mjesečno

Ključne korisničke bolne tačke

Kako napadi postaju složeniji i višefazni, sve je teže shvatiti prikrivene prijetnje



Klik na URL

Iskorištavanje

Instalacija

C&C kanal

Postojanost

Eskalacija privilegija

Izviđanje

Lateralno kretanje

46% kompromitiranih sistema nije imalo zlonamjerni softver na sebi

Praćenje naprednog napada preko mreže i različitih senzora može biti teško

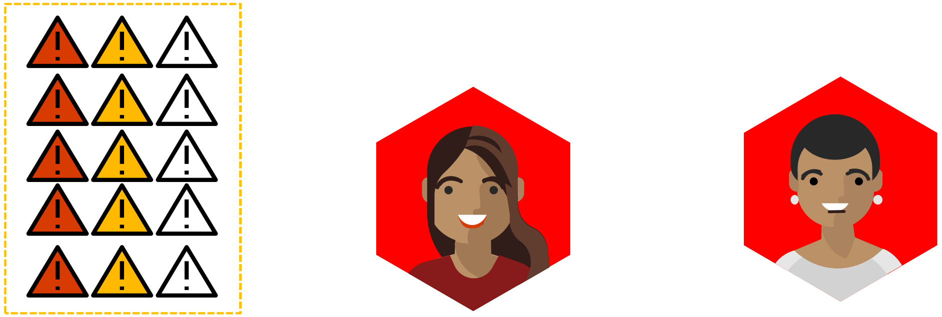
Prikupljanje dokaza i upozorenja, čak i s jednog zaraženog uređaja, može biti dugotrajan proces

Living off the land - Napadači koriste tehnike izbjegavanja

Ključne korisničke bolne tačke

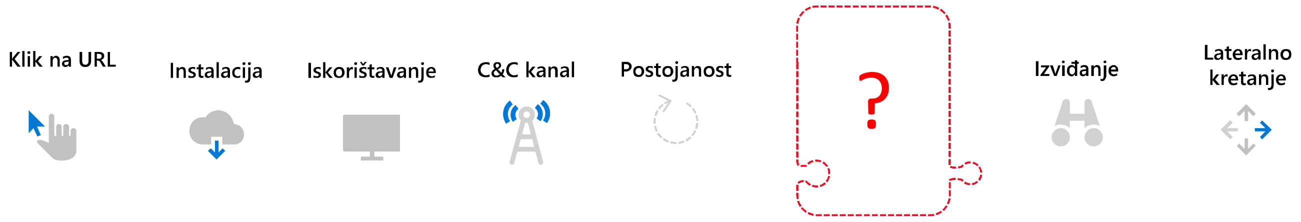
- Više prijetnji, više upozorenja dovodi do zamora analitičara
- Istraga upozorenja je dugotrajna
- Vještačenje je skupo
- Ručna sanacija je dugotrajna (80+ dana)
- Nedostatak eksperata u cyber sigurnosti

Analitičari su preopterećeni ručnom istragom upozorenja i sanacijom istih


Red čekanja upozorenja

Ključne korisničke bolne tačke

Budući da prijetnje postaju složene, potreban je dodatni kontekst i smjernice o upravljanju upozorenjima



Klik na URL

Instalacija

Iskorištavanje

C&C kanal

Postojanost

?

Izviđanje

Lateralno kretanje

- ⚠ Potreba za dodatnim kontekstom prijetnje
- ⚠ Nedostaju smjernice o upravljanju upozorenjima
- ⚠ Važna upozorenja se lako propuste
- ⚠ Teško se odvaja bitno od nebitnog

Statički i dinamički pristup zaštiti

Static signatures:
focus on a file

Hashes

Strings

Emulators

⊘

Ineffective

Dynamic heuristics:
focus on *run-time behaviors*

Behavior monitoring

Memory scanning

AMSI

Command-line scanning

✓

Effective

Istorijske IT uloge i nesuglasice

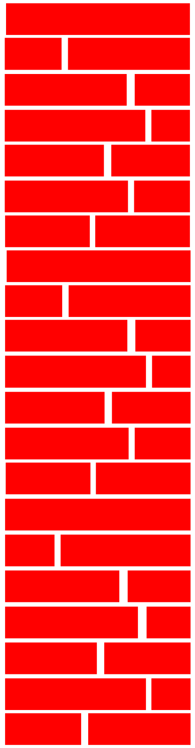
Sigurnosni tim

→ Odgovoran za nadzor sigurnosti i smanjenje rizika

→ Analizira prijetnje, sigurnosne incidente, izloženost i identificira načine ublažavanja prijetnji

→ Definira sigurnosne politike

→ Prioritet je brzo saniranje zahvaćenih uređaja/korisnika



IT tim

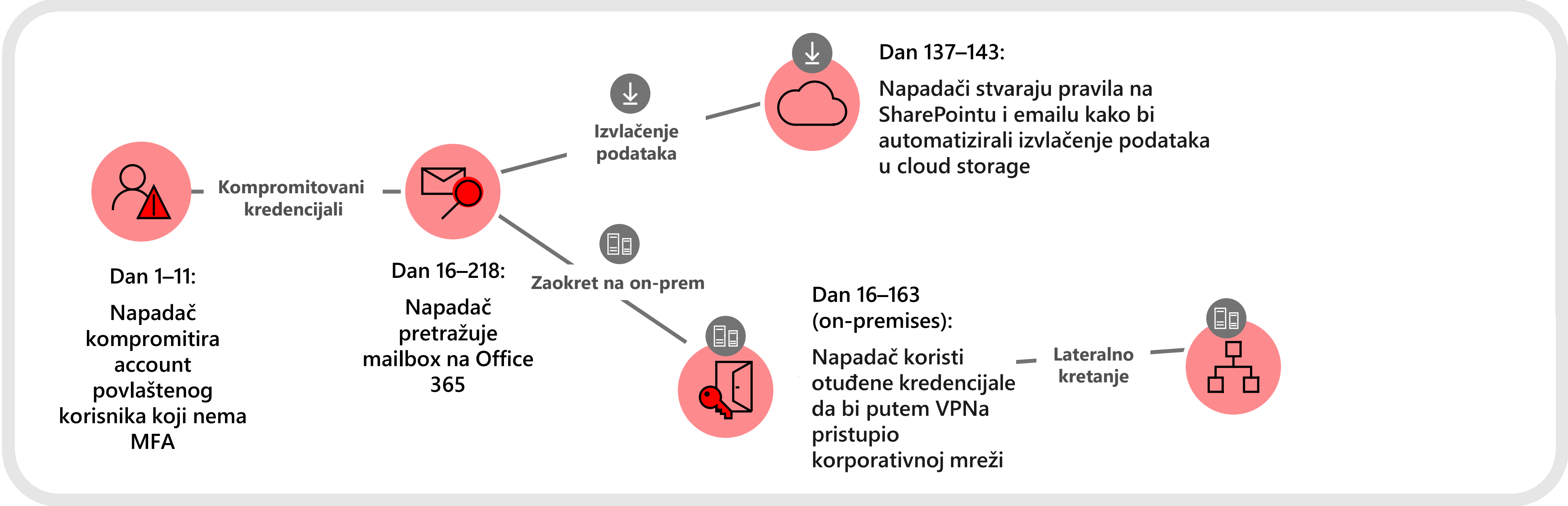
→ Odgovoran za konfiguraciju pravila uključujući sigurnosna pravila

→ Analizira utjecaj promjena i postupno uvodi globalne politike

→ Prioritet je stabilno IT okruženje i niski troškovi

Okruženje i proces izvršenja napada

Primjer kako dolazi do napada i kompromitiranja cijele kompanije



Kompromitovani kredencijali

Dan 1–11:

Napadač kompromitira account povlaštenog korisnika koji nema MFA

Dan 16–218:

Napadač pretražuje mailbox na Office 365

Izvlačenje podataka

Dan 137–143:

Napadači stvaraju pravila na SharePointu i emailu kako bi automatizirali izvlačenje podataka u cloud storage

Zaokret na on-prem

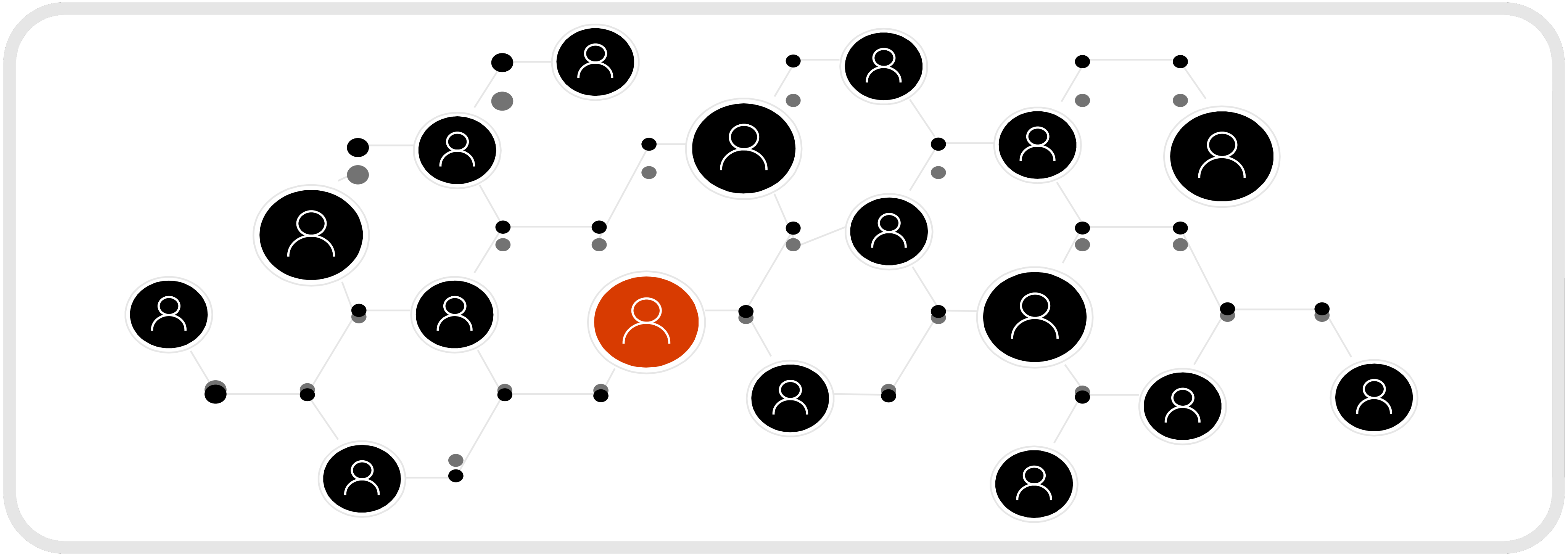
Dan 16–163 (on-premises):

Napadač koristi otuđene kredencijale da bi putem VPNa pristupio korporativnoj mreži

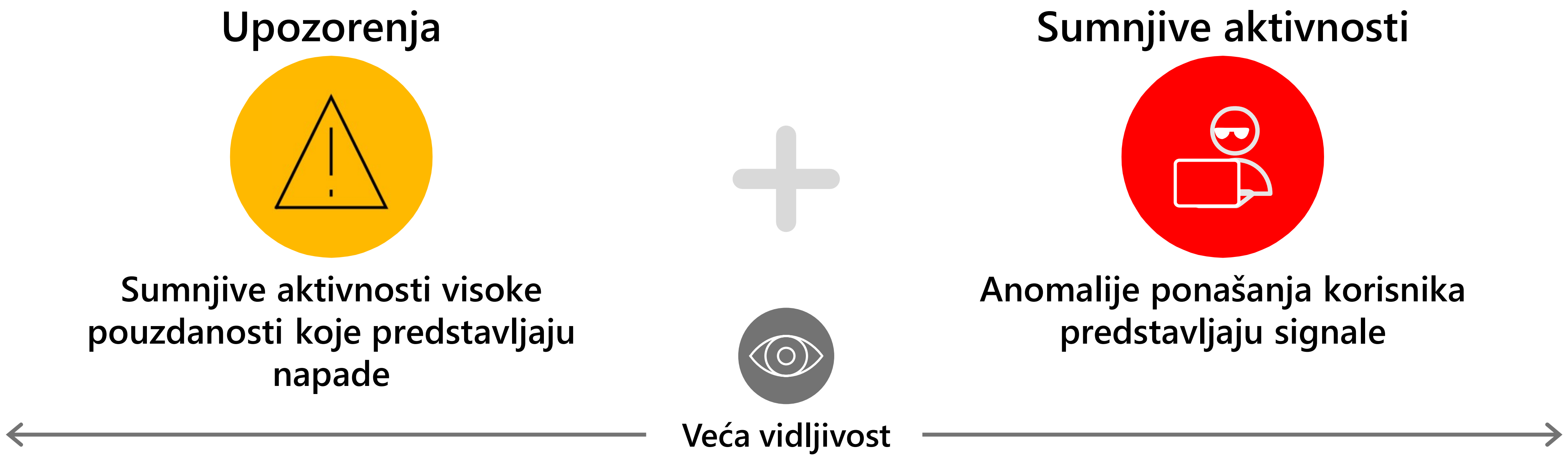
Lateralno kretanje

Novi sigurnosni perimeter-korisnički identitet

Korisnici su novi perimetar, a jedan kompromitovani korisnik može dovesti do totalnog kolapsa sistema



Opseg otkrivanja: sumnjive aktivnosti i analiza ponašanja



Upozorenja

Sumnjive aktivnosti visoke pouzdanosti koje predstavljaju napade

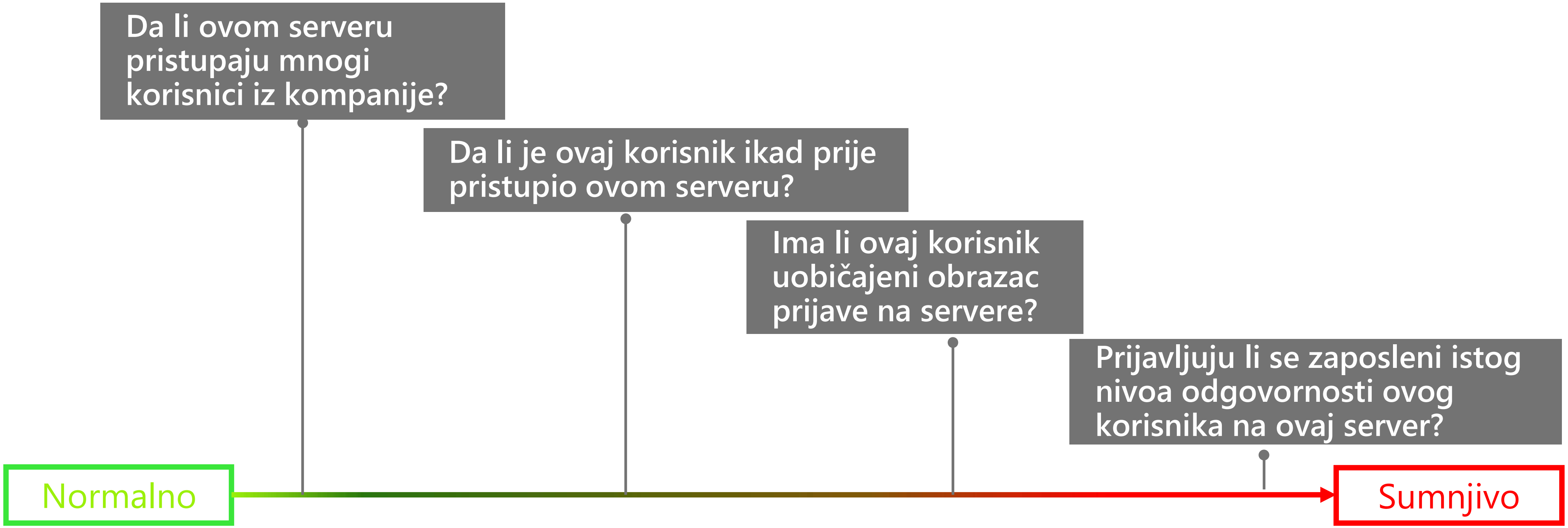
Sumnjive aktivnosti

Anomalije ponašanja korisnika predstavljaju signale

Veća vidljivost

Proces analize sumnjivih aktivosti

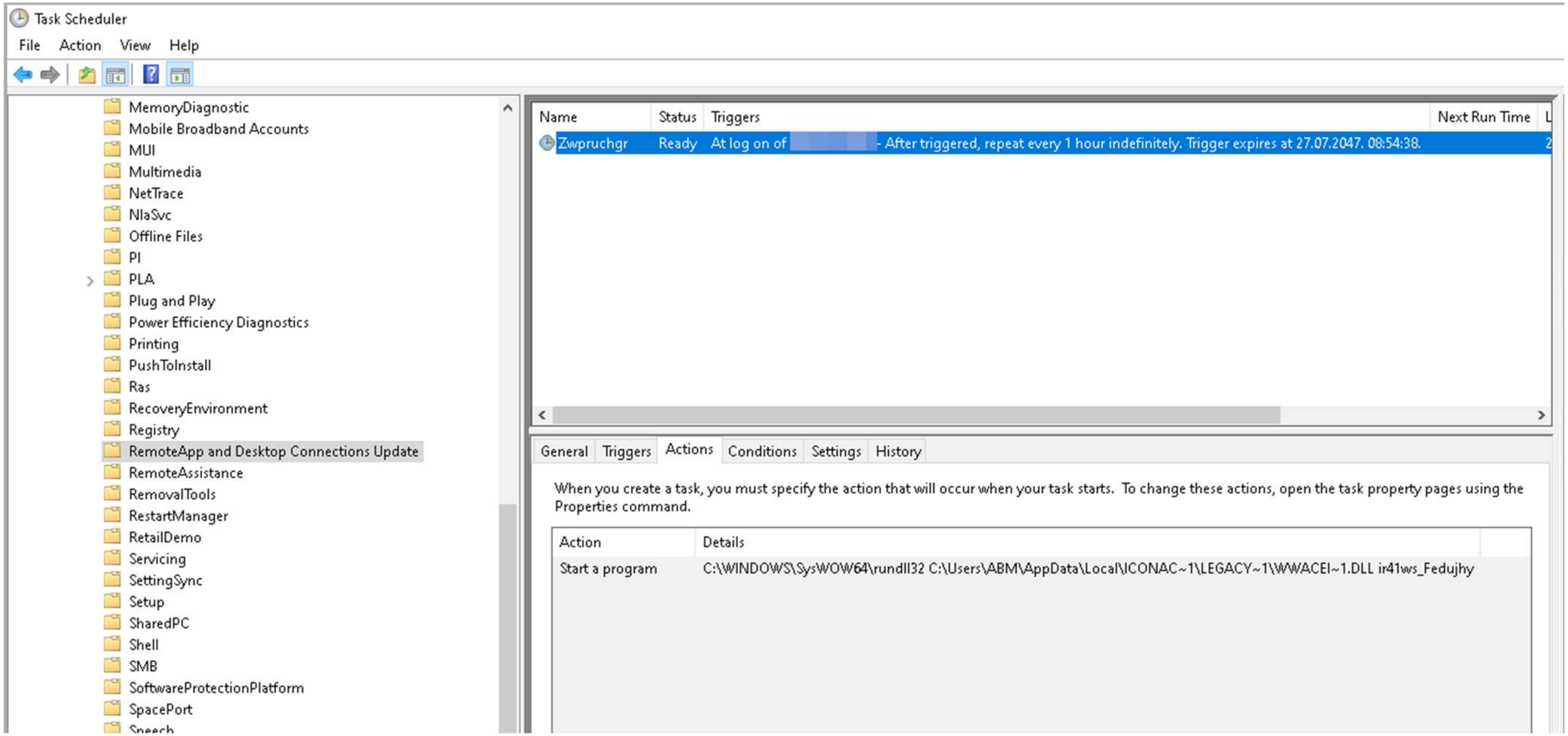
Primjer: Korisnik pristupa serveru sa sigurnosno kritičnim podacima



Da li ovom serveru pristupaju mnogi korisnici iz kompanije?
Da li je ovaj korisnik ikad prije pristupio ovom serveru?
Ima li ovaj korisnik uobičajeni obrazac prijave na servere?
Prijavljuju li se zaposleni istog nivoa odgovornosti ovog korisnika na ovaj server?
Normalno
Sumnjivo

Primjer forenzike jednog realnog cyber napada

Task Scheduler – vrlo dobro mjesto za skrivanje

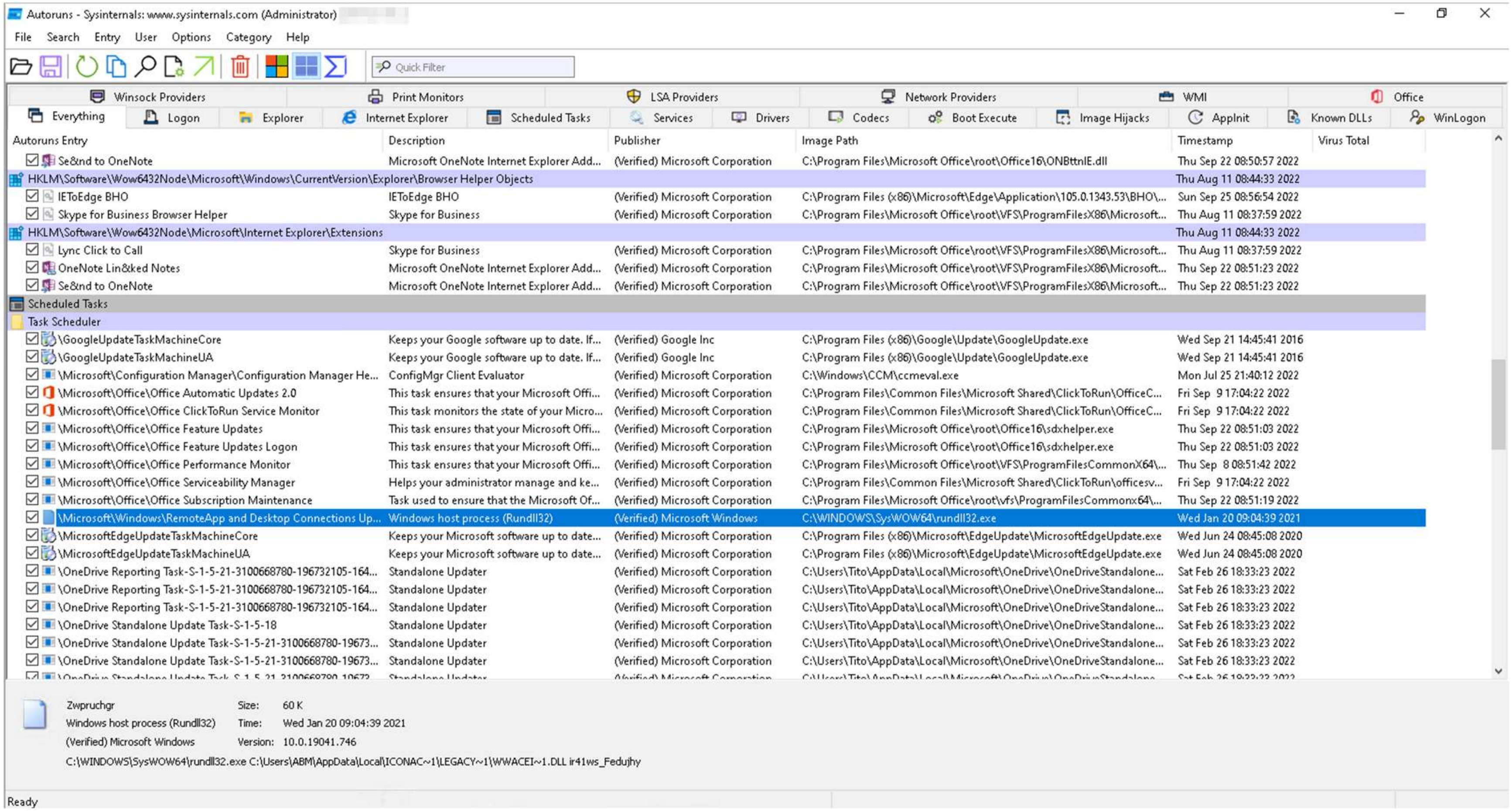


Name	Status	Triggers	Next Run Time	L
Zwpruchgr	Ready	At log on of [redacted] - After triggered, repeat every 1 hour indefinitely. Trigger expires at 27.07.2047. 08:54:38.		2

When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties command.

Action	Details
Start a program	C:\WINDOWS\SysWOW64\rundll32 C:\Users\ABM\AppData\Local\ICONAC~1\LEGACY~1\WWACEI~1.DLL ir41ws_Fedujhy

Sysinternals – vaš najbolji prijatelj

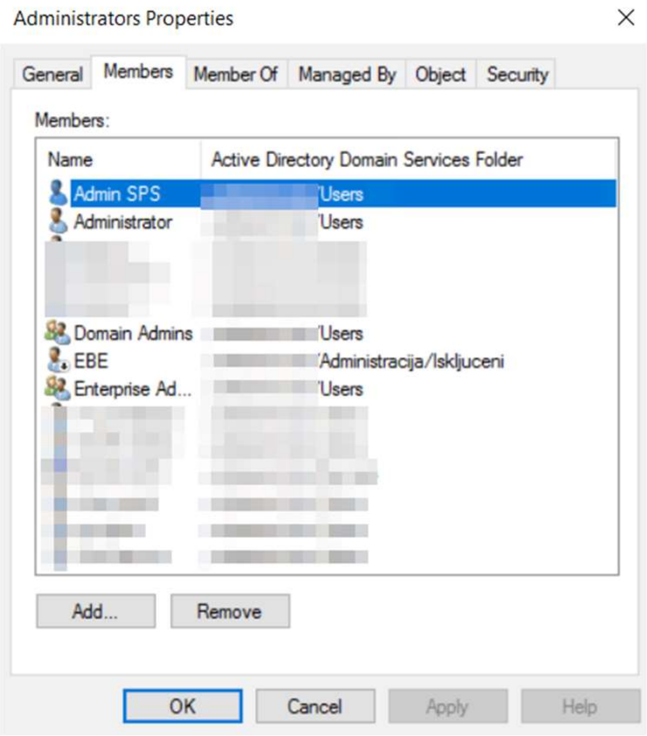


Autoruns Entry	Description	Publisher	Image Path	Timestamp	Virus Total
☑ Se&nd to OneNote	Microsoft OneNote Internet Explorer Add...	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\Office16\ONBttnIE.dll	Thu Sep 22 08:50:57 2022	
HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects				Thu Aug 11 08:44:33 2022	
☑ IEToEdge BHO	IEToEdge BHO	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\105.0.1343.53\BHO\...	Sun Sep 25 08:56:54 2022	
☑ Skype for Business Browser Helper	Skype for Business	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\VFS\ProgramFilesX86\Microsoft...	Thu Aug 11 08:37:59 2022	
HKLM\Software\Wow6432Node\Microsoft\Internet Explorer\Extensions				Thu Aug 11 08:44:33 2022	
☑ Lync Click to Call	Skype for Business	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\VFS\ProgramFilesX86\Microsoft...	Thu Aug 11 08:37:59 2022	
☑ OneNote Lin&ked Notes	Microsoft OneNote Internet Explorer Add...	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\VFS\ProgramFilesX86\Microsoft...	Thu Sep 22 08:51:23 2022	
☑ Se&nd to OneNote	Microsoft OneNote Internet Explorer Add...	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\VFS\ProgramFilesX86\Microsoft...	Thu Sep 22 08:51:23 2022	
Scheduled Tasks					
Task Scheduler					
☑ \GoogleUpdateTaskMachineCore	Keeps your Google software up to date. If...	(Verified) Google Inc	C:\Program Files (x86)\Google\Update\GoogleUpdate.exe	Wed Sep 21 14:45:41 2016	
☑ \GoogleUpdateTaskMachineUA	Keeps your Google software up to date. If...	(Verified) Google Inc	C:\Program Files (x86)\Google\Update\GoogleUpdate.exe	Wed Sep 21 14:45:41 2016	
☑ \Microsoft\Configuration Manager\Configuration Manager He...	ConfigMgr Client Evaluator	(Verified) Microsoft Corporation	C:\Windows\CCM\ccmeval.exe	Mon Jul 25 21:40:12 2022	
☑ \Microsoft\Office\Office Automatic Updates 2.0	This task ensures that your Microsoft Offi...	(Verified) Microsoft Corporation	C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeC...	Fri Sep 9 17:04:22 2022	
☑ \Microsoft\Office\Office ClickToRun Service Monitor	This task monitors the state of your Micro...	(Verified) Microsoft Corporation	C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeC...	Fri Sep 9 17:04:22 2022	
☑ \Microsoft\Office\Office Feature Updates	This task ensures that your Microsoft Offi...	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\Office16\sdxhelper.exe	Thu Sep 22 08:51:03 2022	
☑ \Microsoft\Office\Office Feature Updates Logon	This task ensures that your Microsoft Offi...	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\Office16\sdxhelper.exe	Thu Sep 22 08:51:03 2022	
☑ \Microsoft\Office\Office Performance Monitor	This task ensures that your Microsoft Offi...	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\VFS\ProgramFilesCommonX64\...	Thu Sep 8 08:51:42 2022	
☑ \Microsoft\Office\Office Serviceability Manager	Helps your administrator manage and ke...	(Verified) Microsoft Corporation	C:\Program Files\Common Files\Microsoft Shared\ClickToRun\officesv...	Fri Sep 9 17:04:22 2022	
☑ \Microsoft\Office\Office Subscription Maintenance	Task used to ensure that the Microsoft Of...	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\vfs\ProgramFilesCommonx64\...	Thu Sep 22 08:51:19 2022	
☑ \Microsoft\Windows\RemoteApp and Desktop Connections Up...	Windows host process (Rundll32)	(Verified) Microsoft Windows	C:\WINDOWS\SysWOW64\rundll32.exe	Wed Jan 20 09:04:39 2021	
☑ \MicrosoftEdgeUpdateTaskMachineCore	Keeps your Microsoft software up to date...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Wed Jun 24 08:45:08 2020	
☑ \MicrosoftEdgeUpdateTaskMachineUA	Keeps your Microsoft software up to date...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Wed Jun 24 08:45:08 2020	
☑ \OneDrive Reporting Task-S-1-5-21-3100668780-196732105-164...	Standalone Updater	(Verified) Microsoft Corporation	C:\Users\Tito\AppData\Local\Microsoft\OneDrive\OneDriveStandalone...	Sat Feb 26 18:33:23 2022	
☑ \OneDrive Reporting Task-S-1-5-21-3100668780-196732105-164...	Standalone Updater	(Verified) Microsoft Corporation	C:\Users\Tito\AppData\Local\Microsoft\OneDrive\OneDriveStandalone...	Sat Feb 26 18:33:23 2022	
☑ \OneDrive Reporting Task-S-1-5-21-3100668780-196732105-164...	Standalone Updater	(Verified) Microsoft Corporation	C:\Users\Tito\AppData\Local\Microsoft\OneDrive\OneDriveStandalone...	Sat Feb 26 18:33:23 2022	
☑ \OneDrive Standalone Update Task-S-1-5-18	Standalone Updater	(Verified) Microsoft Corporation	C:\Users\Tito\AppData\Local\Microsoft\OneDrive\OneDriveStandalone...	Sat Feb 26 18:33:23 2022	
☑ \OneDrive Standalone Update Task-S-1-5-21-3100668780-19673...	Standalone Updater	(Verified) Microsoft Corporation	C:\Users\Tito\AppData\Local\Microsoft\OneDrive\OneDriveStandalone...	Sat Feb 26 18:33:23 2022	
☑ \OneDrive Standalone Update Task-S-1-5-21-3100668780-19673...	Standalone Updater	(Verified) Microsoft Corporation	C:\Users\Tito\AppData\Local\Microsoft\OneDrive\OneDriveStandalone...	Sat Feb 26 18:33:23 2022	
☑ \OneDrive Standalone Update Task-S-1-5-21-3100668780-19673...	Standalone Updater	(Verified) Microsoft Corporation	C:\Users\Tito\AppData\Local\Microsoft\OneDrive\OneDriveStandalone...	Sat Feb 26 18:33:23 2022	

Zwpruchgr Size: 60 K
Windows host process (Rundll32) Time: Wed Jan 20 09:04:39 2021
(Verified) Microsoft Windows Version: 10.0.19041.746
C:\WINDOWS\SysWOW64\rundll32.exe C:\Users\ABM\AppData\Local\ICONAC~1\LEGACY~1\WWACEI~1.DLL ir41ws_Fedujhy

Ready

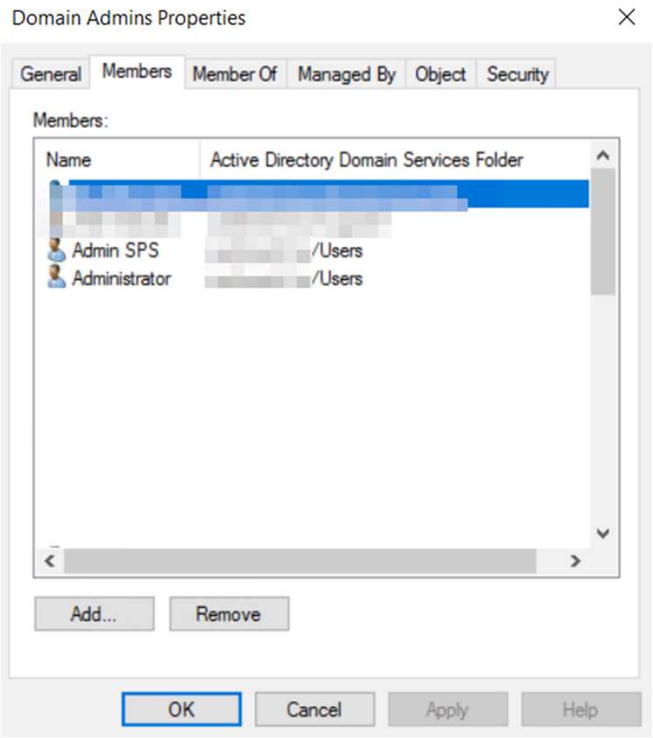
Dodatni admin account



Administrators Properties

Members:

Name	Active Directory Domain Services Folder
Admin SPS	[redacted]/Users
Administrator	[redacted]/Users
[redacted]	[redacted]
Domain Admins	[redacted]/Users
EBE	[redacted]/Administracija/Iskljuceni
Enterprise Ad...	[redacted]/Users
[redacted]	[redacted]

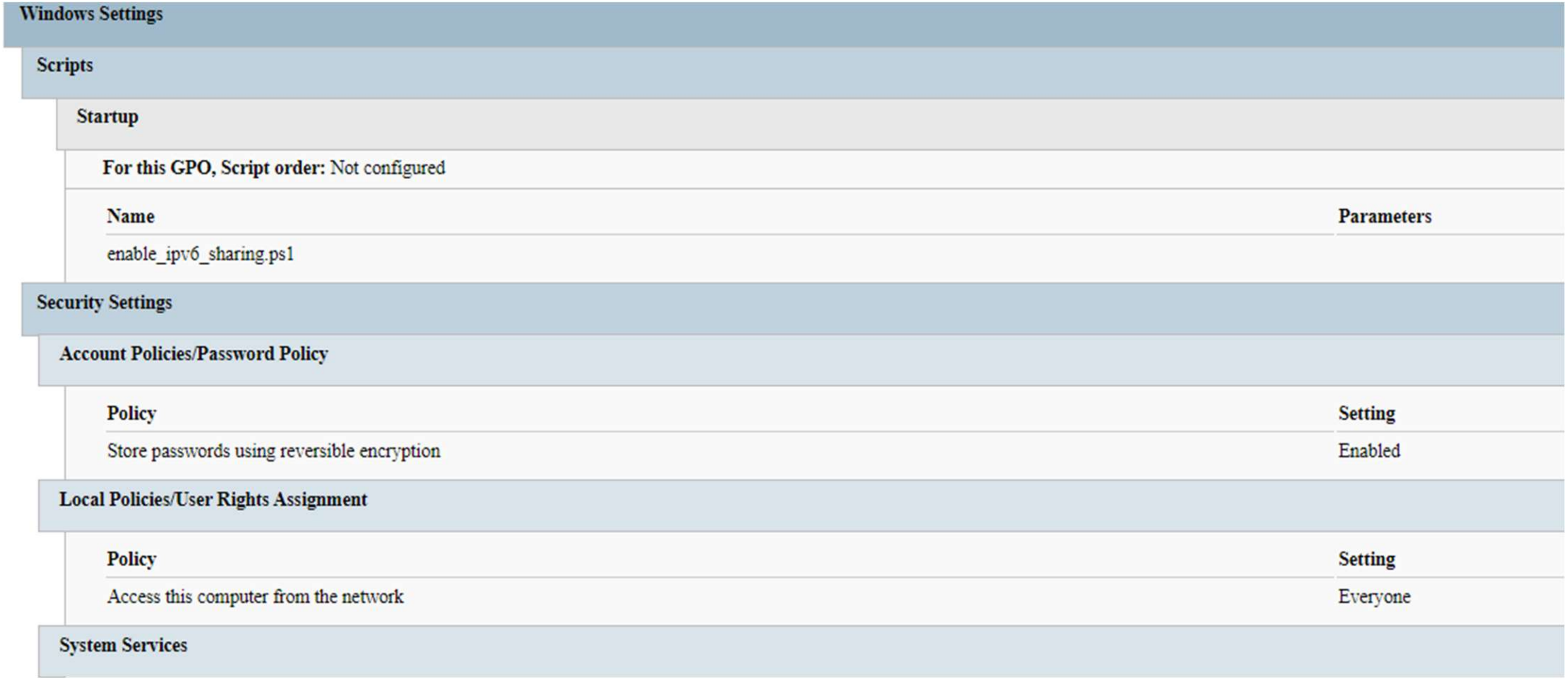


Domain Admins Properties

Members:

Name	Active Directory Domain Services Folder
[redacted]	[redacted]
Admin SPS	[redacted]/Users
Administrator	[redacted]/Users

Group Policy – priprema mjesta egzekucije



Windows Settings

Scripts

Startup

For this GPO, Script order: Not configured

Name	Parameters
enable_ipv6_sharing.ps1	

Security Settings

Account Policies/Password Policy

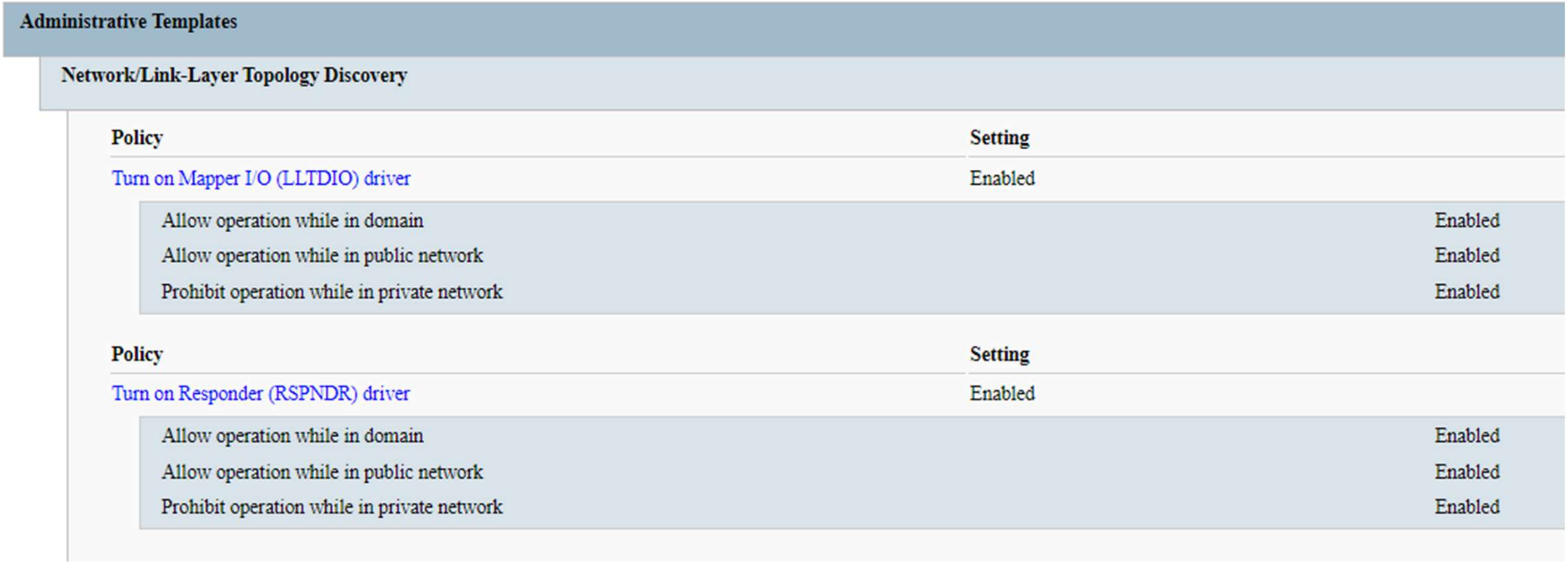
Policy	Setting
Store passwords using reversible encryption	Enabled

Local Policies/User Rights Assignment

Policy	Setting
Access this computer from the network	Everyone

System Services

Group Policy – priprema mjesta egzekucije



Administrative Templates

Network/Link-Layer Topology Discovery

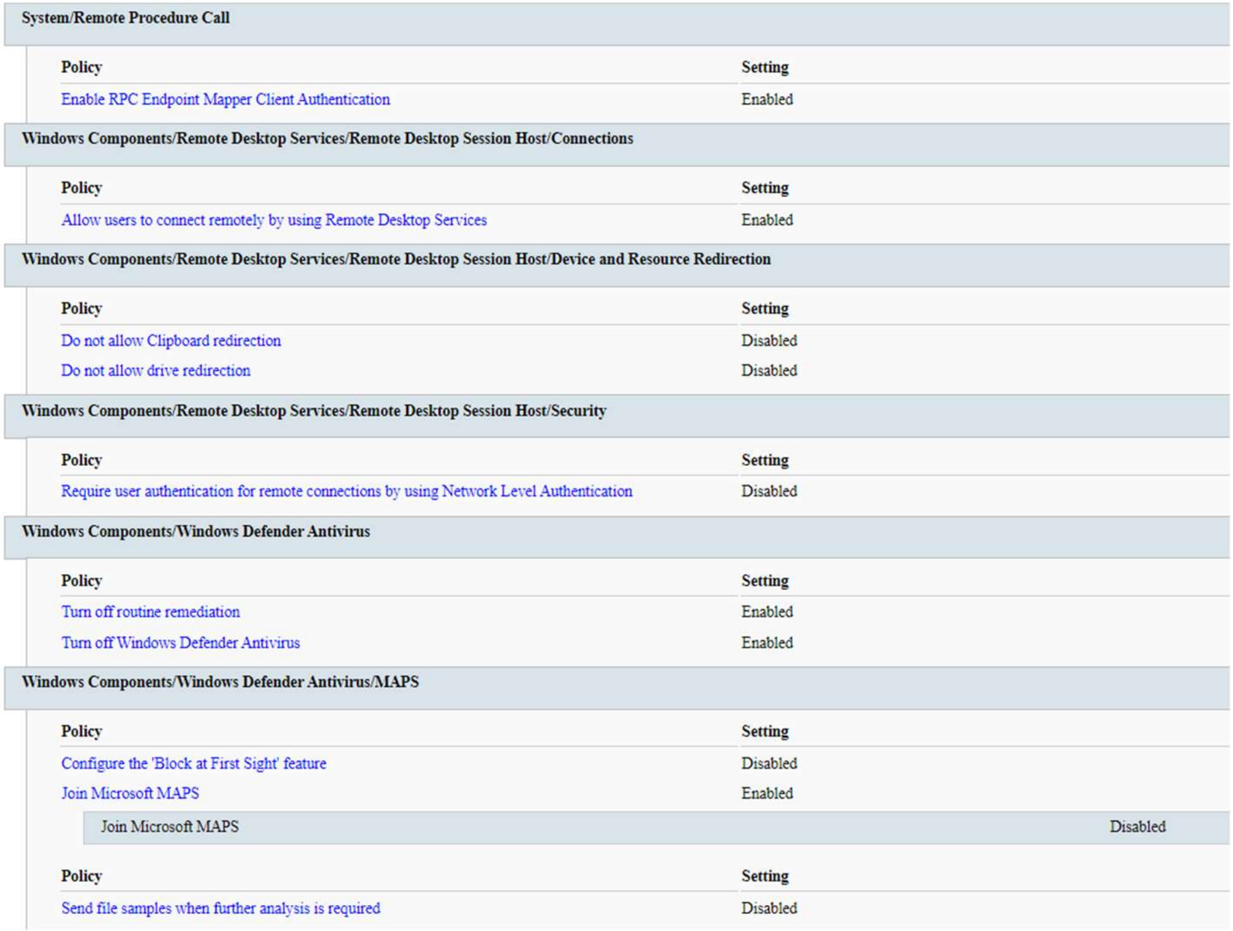
Policy	Setting
Turn on Mapper I/O (LLTDIO) driver	Enabled

Allow operation while in domain	Enabled
Allow operation while in public network	Enabled
Prohibit operation while in private network	Enabled

Policy	Setting
Turn on Responder (RSPNDR) driver	Enabled

Allow operation while in domain	Enabled
Allow operation while in public network	Enabled
Prohibit operation while in private network	Enabled

Group Policy – priprema mjesta egzekucije



System/Remote Procedure Call

Policy	Setting
Enable RPC Endpoint Mapper Client Authentication	Enabled

Windows Components/Remote Desktop Services/Remote Desktop Session Host/Connections

Policy	Setting
Allow users to connect remotely by using Remote Desktop Services	Enabled

Windows Components/Remote Desktop Services/Remote Desktop Session Host/Device and Resource Redirection

Policy	Setting
Do not allow Clipboard redirection	Disabled
Do not allow drive redirection	Disabled

Windows Components/Remote Desktop Services/Remote Desktop Session Host/Security

Policy	Setting
Require user authentication for remote connections by using Network Level Authentication	Disabled

Windows Components/Windows Defender Antivirus

Policy	Setting
Turn off routine remediation	Enabled
Turn off Windows Defender Antivirus	Enabled

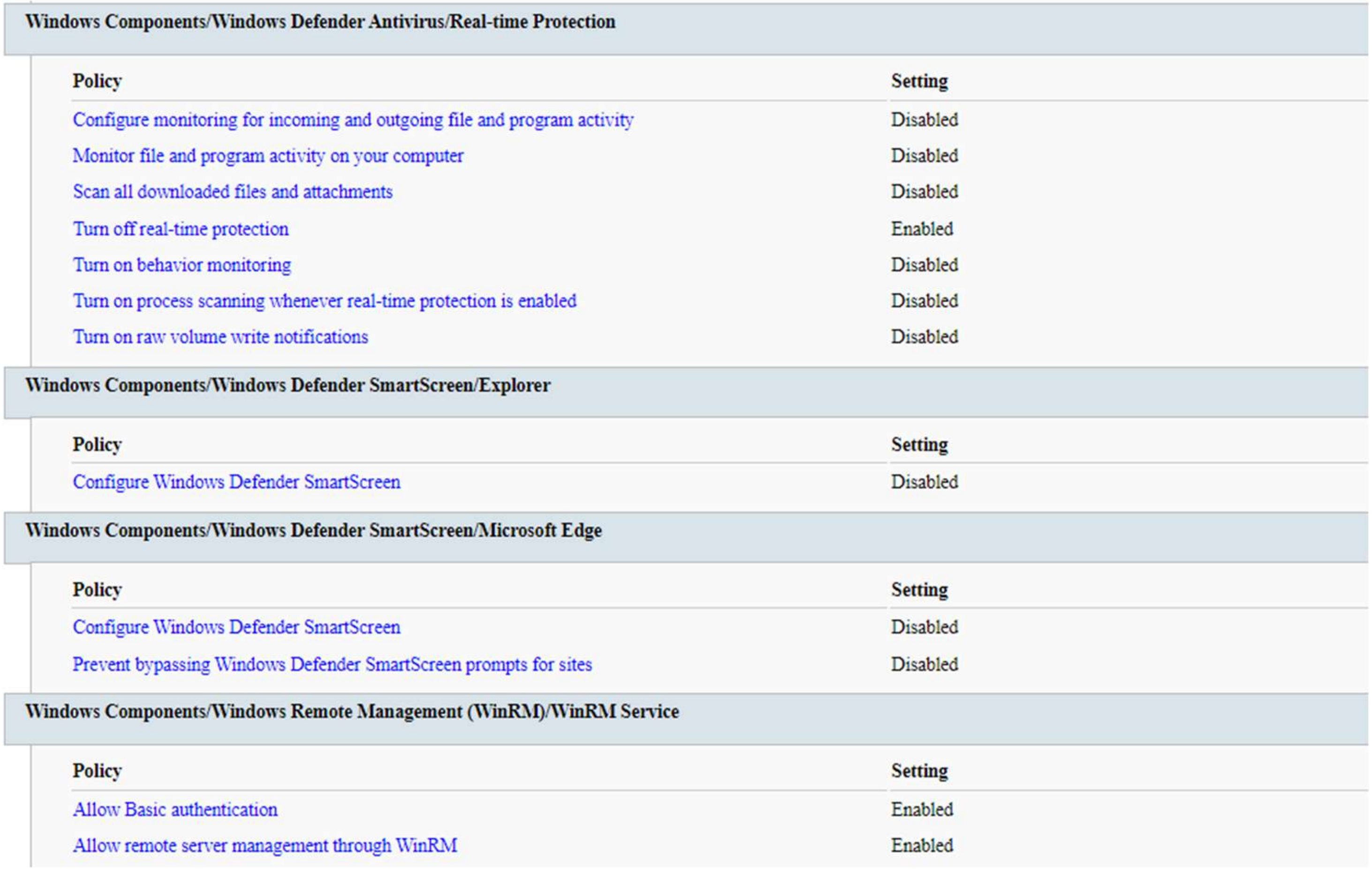
Windows Components/Windows Defender Antivirus/MAPS

Policy	Setting
Configure the 'Block at First Sight' feature	Disabled
Join Microsoft MAPS	Enabled

Join Microsoft MAPS Disabled

Policy	Setting
Send file samples when further analysis is required	Disabled

Group Policy – priprema mjesta egzekucije



Windows Components/Windows Defender Antivirus/Real-time Protection

Policy	Setting
Configure monitoring for incoming and outgoing file and program activity	Disabled
Monitor file and program activity on your computer	Disabled
Scan all downloaded files and attachments	Disabled
Turn off real-time protection	Enabled
Turn on behavior monitoring	Disabled
Turn on process scanning whenever real-time protection is enabled	Disabled
Turn on raw volume write notifications	Disabled

Windows Components/Windows Defender SmartScreen/Explorer

Policy	Setting
Configure Windows Defender SmartScreen	Disabled

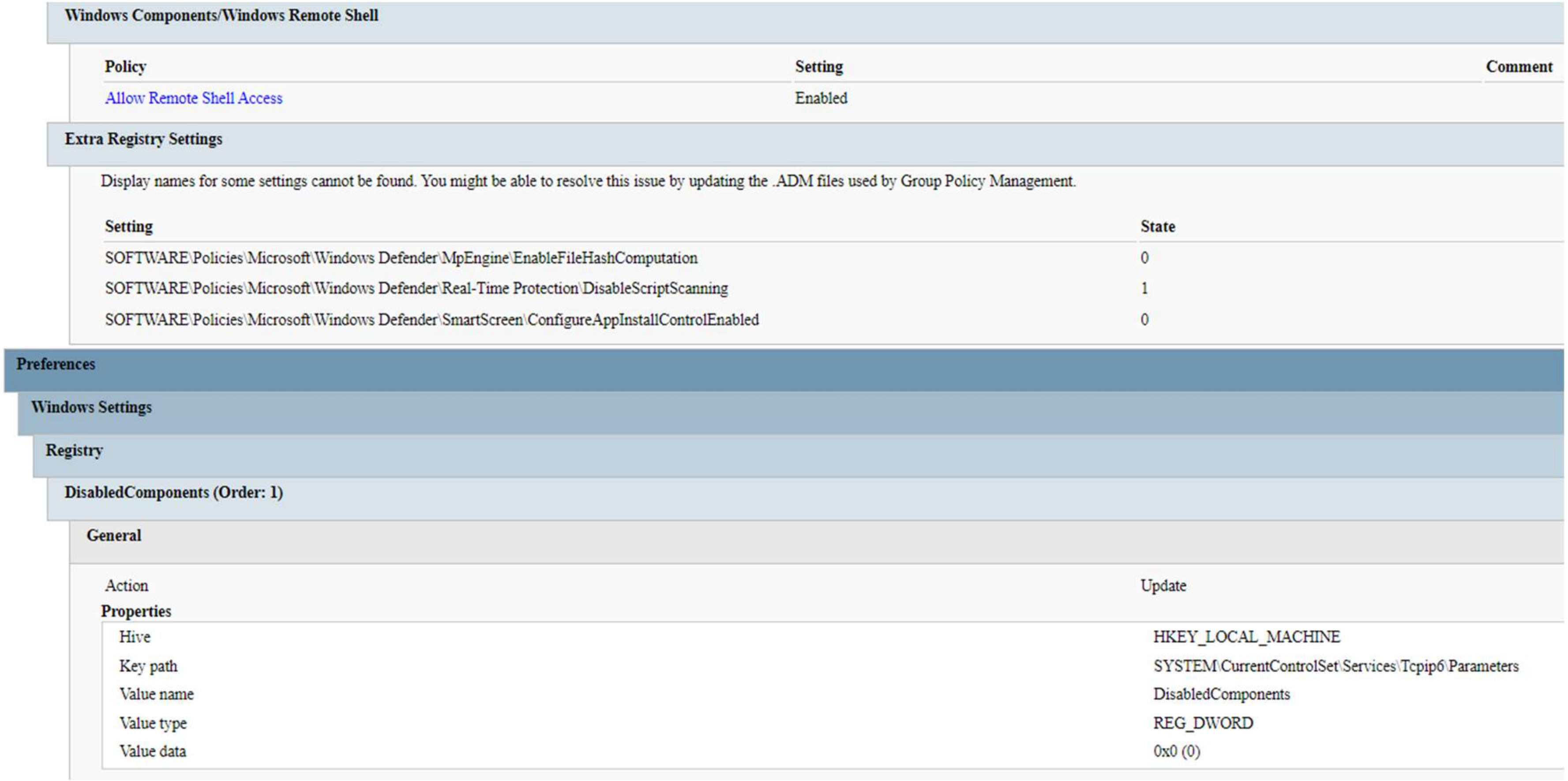
Windows Components/Windows Defender SmartScreen/Microsoft Edge

Policy	Setting
Configure Windows Defender SmartScreen	Disabled
Prevent bypassing Windows Defender SmartScreen prompts for sites	Disabled

Windows Components/Windows Remote Management (WinRM)/WinRM Service

Policy	Setting
Allow Basic authentication	Enabled
Allow remote server management through WinRM	Enabled

Group Policy – priprema mjesta egzekucije



Windows Components/Windows Remote Shell

Policy	Setting	Comment
Allow Remote Shell Access	Enabled	

Extra Registry Settings

Display names for some settings cannot be found. You might be able to resolve this issue by updating the .ADM files used by Group Policy Management.

Setting	State
SOFTWARE\Policies\Microsoft\Windows Defender\MpEngine\EnableFileHashComputation	0
SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableScriptScanning	1
SOFTWARE\Policies\Microsoft\Windows Defender\SmartScreen\ConfigureAppInstallControlEnabled	0

Preferences

Windows Settings

Registry

DisabledComponents (Order: 1)

General

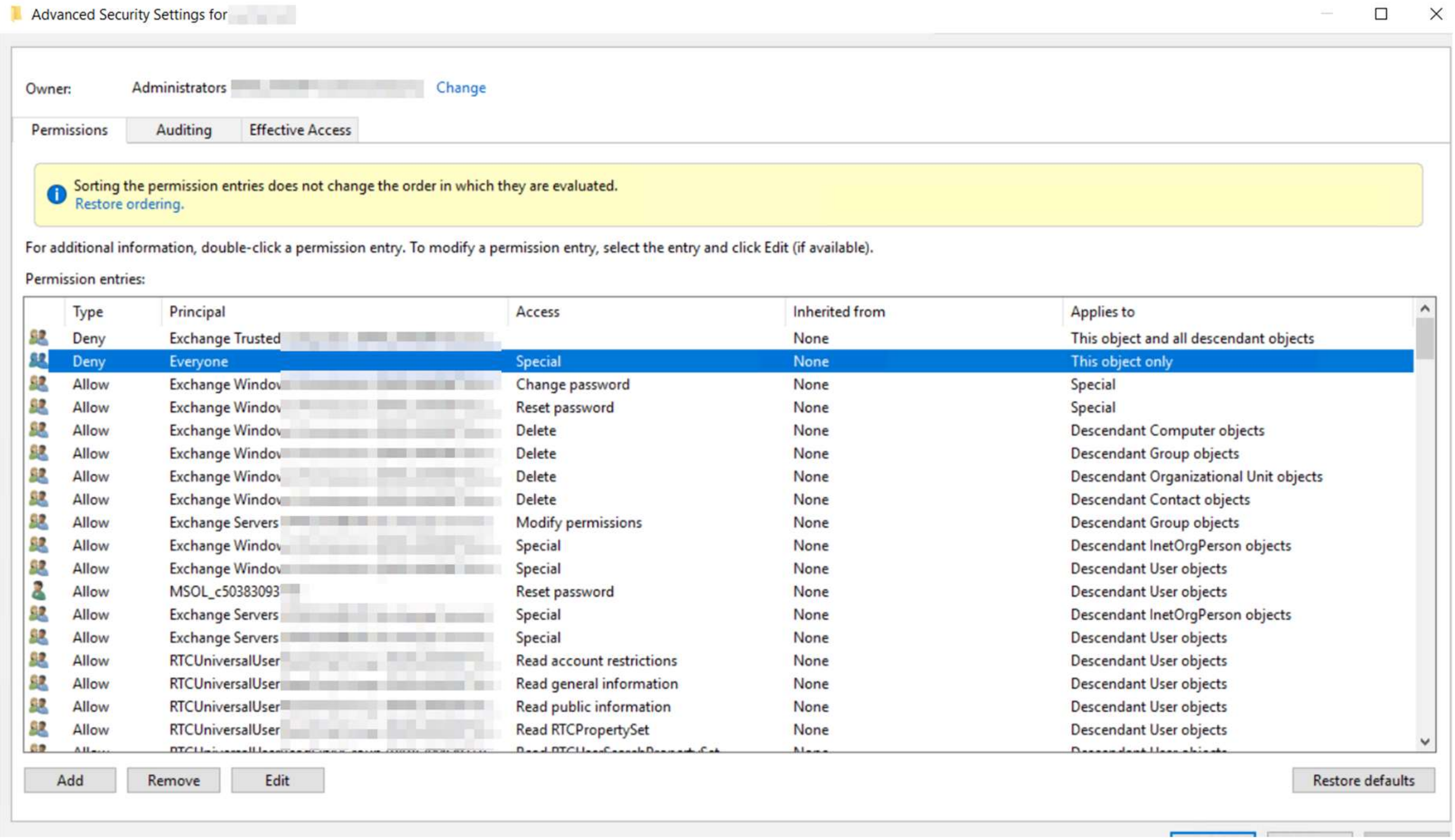
Action	Update

Properties

Hive	HKEY_LOCAL_MACHINE
Key path	SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
Value name	DisabledComponents
Value type	REG_DWORD
Value data	0x0 (0)

LOGOSOFT

Prevencija brzog otklanjanja problema



Advanced Security Settings for [redacted]

Owner: Administrators [redacted] Change

Sorting the permission entries does not change the order in which they are evaluated.
Restore ordering.

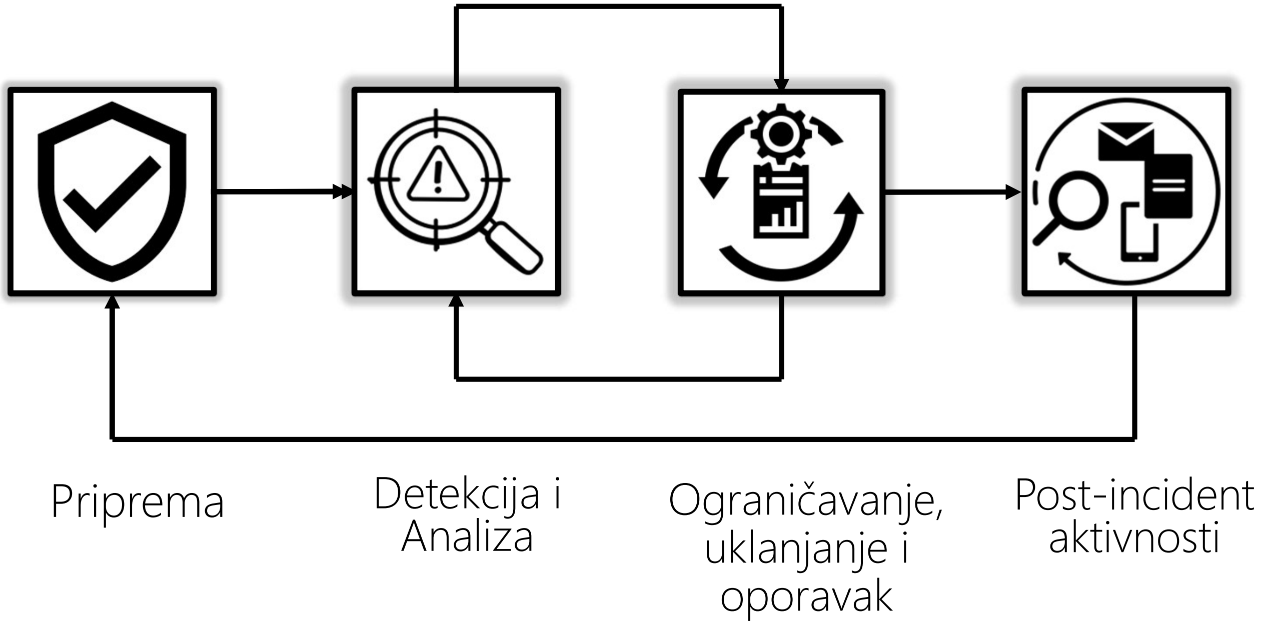
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Deny	Exchange Trusted [redacted]		None	This object and all descendant objects
Deny	Everyone	Special	None	This object only
Allow	Exchange Windov [redacted]	Change password	None	Special
Allow	Exchange Windov [redacted]	Reset password	None	Special
Allow	Exchange Windov [redacted]	Delete	None	Descendant Computer objects
Allow	Exchange Windov [redacted]	Delete	None	Descendant Group objects
Allow	Exchange Windov [redacted]	Delete	None	Descendant Organizational Unit objects
Allow	Exchange Windov [redacted]	Delete	None	Descendant Contact objects
Allow	Exchange Servers [redacted]	Modify permissions	None	Descendant Group objects
Allow	Exchange Windov [redacted]	Special	None	Descendant InetOrgPerson objects
Allow	Exchange Windov [redacted]	Special	None	Descendant User objects
Allow	MSOL_c50383093 [redacted]	Reset password	None	Descendant User objects
Allow	Exchange Servers [redacted]	Special	None	Descendant InetOrgPerson objects
Allow	Exchange Servers [redacted]	Special	None	Descendant User objects
Allow	RTCUniversalUser [redacted]	Read account restrictions	None	Descendant User objects
Allow	RTCUniversalUser [redacted]	Read general information	None	Descendant User objects
Allow	RTCUniversalUser [redacted]	Read public information	None	Descendant User objects
Allow	RTCUniversalUser [redacted]	Read RTCPropertySet	None	Descendant User objects
Allow	RTCUniversalUser [redacted]	Read RTCUserSearchPropertySet	None	Descendant User objects

Cyber resilience

Kako prevenirati cyber napad – životni ciklus ‘odgovora na cyber incident‘



Priprema

Framework ili standard + odgovornost menadžmenta

Politika upravljanja cyber incidentima

Procedura upravljanja cyber incidentima

Upravljanje informacionim resursima

BIA

Procjena rizika

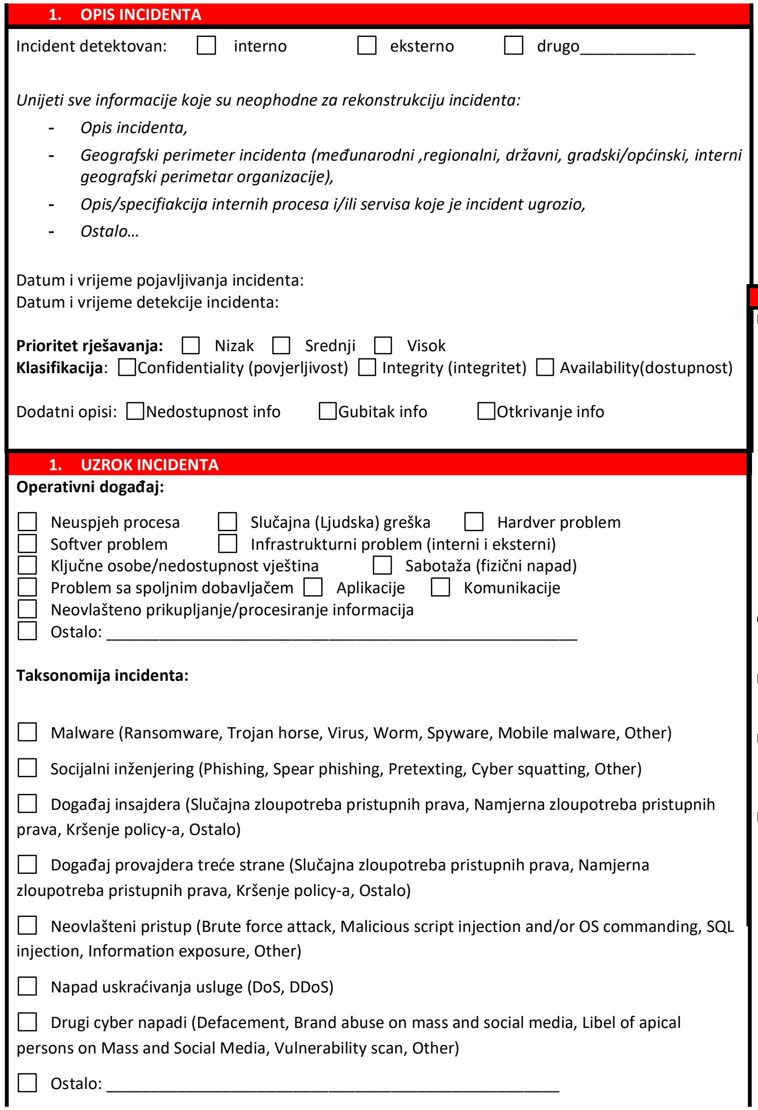
Potrebna infrastruktura

Tehnička rješenja

Priprema

Procedura upravljanja cyber incidentima

- Odgovornosti i definicija timova
- Postupak prijavljivanja incidenta
- Interno i eksterno obavještavanje
- Upravljanje incidentom
  - detekcija
  - opis
  - prioritet
  - klasifikacija
  - uzrok i root cause analiza
  - rješavanje i oporavak



1. OPIS INCIDENTA

Incident detektovan: □ interno □ eksterno □ drugo____________

Unijeti sve informacije koje su neophodne za rekonstrukciju incidenta:

- *Opis incidenta,*
- *Geografski perimeter incidenta (međunarodni ,regionalni, državni, gradski/općinski, interni geografski perimetar organizacije),*
- *Opis/specifiakcija internih procesa i/ili servisa koje je incident ugrozio,*
- *Ostalo…*

Datum i vrijeme pojavljivanja incidenta:
Datum i vrijeme detekcije incidenta:

Prioritet rješavanja: □ Nizak □ Srednji □ Visok
Klasifikacija: □Confidentiality (povjerljivost) □ Integrity (integritet) □ Availability(dostupnost)

Dodatni opisi: □Nedostupnost info □Gubitak info □Otkrivanje info

1. UZROK INCIDENTA

Operativni događaj:

□ Neuspjeh procesa □ Slučajna (Ljudska) greška □ Hardver problem
□ Softver problem □ Infrastrukturni problem (interni i eksterni)
□ Ključne osobe/nedostupnost vještina □ Sabotaža (fizični napad)
□ Problem sa spoljnim dobavljačem □ Aplikacije □ Komunikacije
□ Neovlašteno prikupljanje/procesiranje informacija
□ Ostalo: ____

Taksonomija incidenta:

□ Malware (Ransomware, Trojan horse, Virus, Worm, Spyware, Mobile malware, Other)

□ Socijalni inženjering (Phishing, Spear phishing, Pretexting, Cyber squatting, Other)

□ Događaj insajdera (Slučajna zloupotreba pristupnih prava, Namjerna zloupotreba pristupnih prava, Kršenje policy-a, Ostalo)

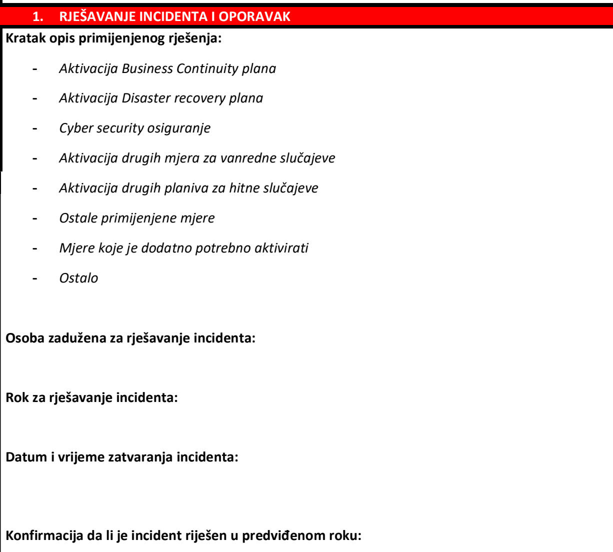
□ Događaj provajdera treće strane (Slučajna zloupotreba pristupnih prava, Namjerna zloupotreba pristupnih prava, Kršenje policy-a, Ostalo)

□ Neovlašteni pristup (Brute force attack, Malicious script injection and/or OS commanding, SQL injection, Information exposure, Other)

□ Napad uskraćivanja usluge (DoS, DDoS)

□ Drugi cyber napadi (Defacement, Brand abuse on mass and social media, Libel of apical persons on Mass and Social Media, Vulnerability scan, Other)

□ Ostalo: ____



1. RJEŠAVANJE INCIDENTA I OPORAVAK

Kratak opis primijenjenog rješenja:

- *Aktivacija Business Continuity plana*
- *Aktivacija Disaster recovery plana*
- *Cyber security osiguranje*
- *Aktivacija drugih mjera za vanredne slučajeve*
- *Aktivacija drugih planiva za hitne slučajeve*
- *Ostale primijenjene mjere*
- *Mjere koje je dodatno potrebno aktivirati*
- *Ostalo*

Osoba zadužena za rješavanje incidenta:

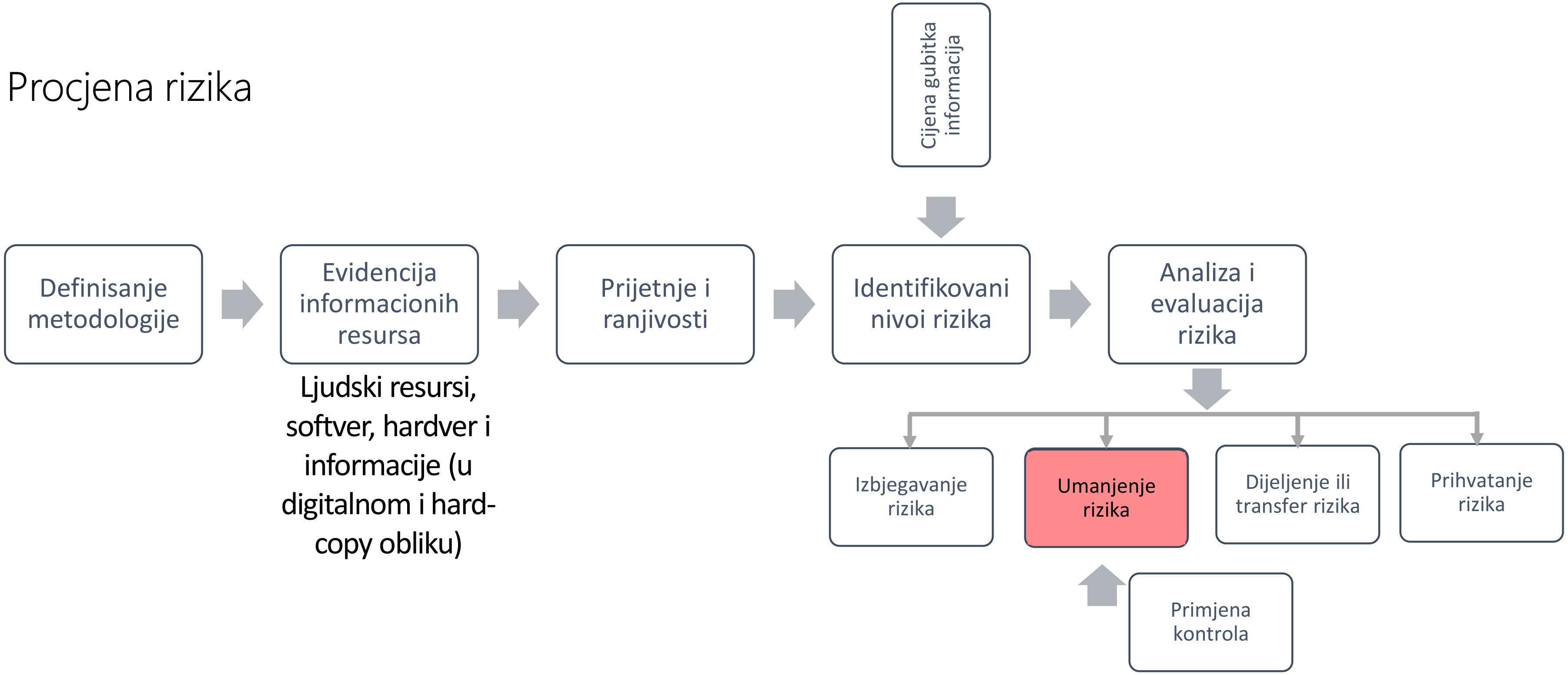
Rok za rješavanje incidenta:

Datum i vrijeme zatvaranja incidenta:

Konfirmacija da li je incident riješen u predviđenom roku:

Priprema

Procjena rizika



Cijena gubitka informacija

Definisanje metodologije

Evidencija informacionih resursa

Prijetnje i ranjivosti

Identifikovani nivoi rizika

Analiza i evaluacija rizika

Izbjegavanje rizika

Umanjenje rizika

Dijeljenje ili transfer rizika

Prihvatanje rizika

Primjena kontrola

Ljudski resursi, softver, hardver i informacije (u digitalnom i hard-copy obliku)

Priprema

Primjer procjene cyber sigurnosnog rizika

Grupa resursa	Operativni sistemi - Windows
Kategorija	OS
Vlasnik rizika	IT director
Prijetnja	Maskiranje identiteta korisnika (lažno predstavljanje)
Ranjivost	Loše upravljanje lozinkama
Vjerovatnoća (1-5)	4
Uticaj (1-5)	5
Rizik	20
Tretman	Umanjenje rizika
Odabrana mjera	Passwordless autentikacija
Odgovornost	Senior IT Admin
Prioritet	Visok
Rok	20.09.2023.

			Uticaj		
Vjerovatnoća	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Priprema

Kontrole za zaštitu od cyber napada – ISO 27001: 2022

Themes:

Organizational Controls	**(37)**
People Controls	**(8)**
Physical Controls	**(14)**
Technological Controls	**(34)**
Total number of Controls	**93**

Control type options	**Information security properties affected**	**Cybersecurity concepts***	**Operational capabilities**	**Security domains**
• Preventative • Detective • Corrective	• Confidentiality • Integrity • Availability	• Identify • Protect • Detect • Respond • Recover	• Governance • Asset management • Information protection • Human resource security • Physical security • System and network security • Application security • Secure configuration • Identity and access management • Threat and vulnerability management • Continuity • Supplier relationships security • Legal and compliance • Information security event management • Information security assurance	• Governance and ecosystem • Protection • Defence • Resilience

ISO 27001 and ISO 27002. Information security controls, 2022

5. Organizational controls

5.1. Policies for information security
5.2. Information security roles and responsibilities
5.3. Segregation of duties
5.4. Management responsibilities
5.5. Contact with authorities
5.6. Contact with special interest groups
5.7. Threat intelligence
5.8. Information security in project management
5.9. Inventory of information and other associated assets
5.10. Acceptable use of information and other associated assets
5.11. Return of assets
5.12. Classification of information
5.13. Labelling of information
5.14. Information transfer
5.15. Access control
5.16. Identity management
5.17. Authentication information
5.18. Access rights
5.19. Information security in supplier relationships
5.20. Addressing information security within supplier agreements
5.21. Managing information security in the ICT supply chain
5.22. Monitoring, review and change management of supplier services
5.23. Information security for use of cloud services
5.24. Information security incident management planning and preparation
5.25. Assessment and decision on information security events
5.26. Response to information security incidents
5.27. Learning from information security incidents
5.28. Collection of evidence
5.29. Information security during disruption
5.30. ICT readiness for business continuity
5.31. Legal, statutory, regulatory and contractual requirements
5.32. Intellectual property rights
5.33. Protection of records
5.34. Privacy and protection of PII
5.35. Independent review of information security
5.36. Compliance with policies, rules and standards for information security
5.37. Documented operating procedures

6. People controls

6.1. Screening
6.2. Terms and conditions of employment
6.3. Information security awareness, education and training
6.4. Disciplinary process
6.5. Responsibilities after termination or change of employment
6.6. Confidentiality or non-disclosure agreements
6.7. Remote working
6.8. Information security event reporting

7. Physical controls

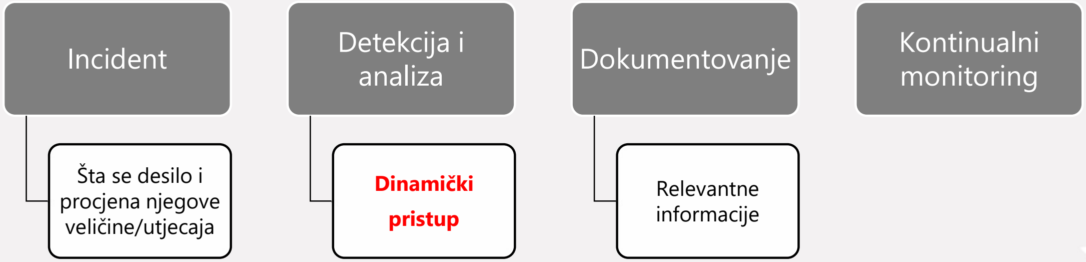
7.1. Physical security perimeter
7.2. Physical entry
7.3. Securing offices, rooms and facilities
7.4. Physical security monitoring
7.5. Protecting against physical and environmental threats
7.6. Working in secure areas
7.7. Clear desk and clear screen
7.8. Equipment siting and protection
7.9. Security of assets off-premises
7.10. Storage media
7.11. Supporting utilities
7.12. Cabling security
7.13. Equipment maintenance
7.14. Secure disposal or re-use of equipment

8. Technological controls

8.1. User endpoint devices
8.2. Privileged access rights
8.3. Information access restriction
8.4. Access to source code
8.5. Secure authentication
8.6. Capacity management
8.7. Protection against malware
8.8. Management of technical vulnerabilities
8.9. Configuration management
8.10. Information deletion
8.11. Data masking
8.12. Data leakage prevention
8.13. Information backup
8.14. Redundancy of information processing facilities
8.15. Logging
8.16. Monitoring activities
8.17. Clock synchronization
8.18. Use of privileged utility programs
8.19. Installation of software on operational systems
8.20. Network security
8.21. Security of network services
8.22. Segregation of networks
8.23. Web filtering
8.24. Use of cryptography
8.25. Secure development life cycle
8.26. Application security requirements
8.27. Secure system architecture and engineering principles
8.28. Secure coding
8.29. Security testing in development and acceptance
8.30. Outsourced development
8.31. Separation of development, test and production environments
8.32. Change management
8.33. Test information
8.34. Protection of information systems during audit testing

*New control, 2022

Detekcija i analiza



Incident

Šta se desilo i procjena njegove veličine/utjecaja

Detekcija i analiza

Dinamički pristup

Dokumentovanje

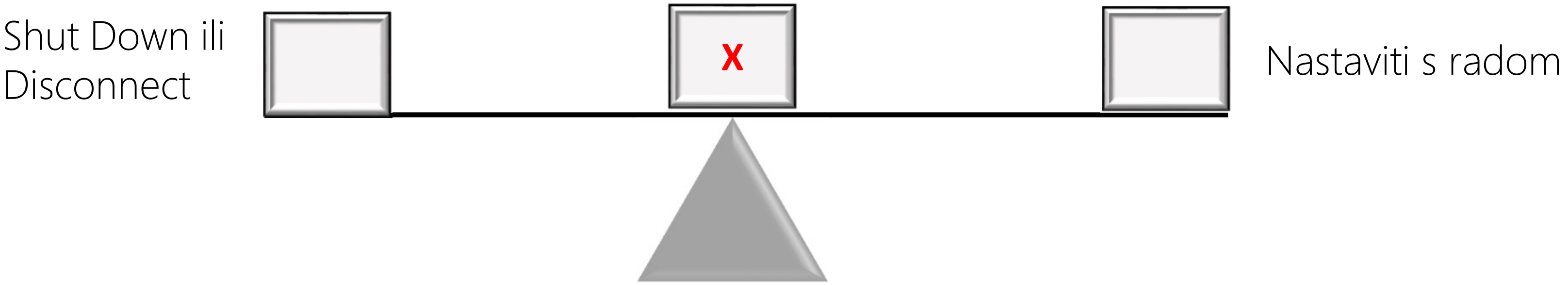
Relevantne informacije

Kontinualni monitoring

Ograničavanje

Odluke i ciljevi

- Ograničiti širenje incidenta
- Dinamički pristup
- Tradicionalni pristup: gašenje, isključenje s mreže, monitoring, izbjegavanje, isključenje feature-a, isključenje accounta itd.



Uklanjanje – ključni koraci

Ukloniti uzrok incidenta

Sačuvati dokaze

Software za eradikaciju

Clean/reformat diskova

Potvrda da su back-upi ‘čisti’

Dokumentovanje

Zakonska regulativa

Komunikacija

Oporavak – nastavak poslovanja

Povratak sistema/mreže u aktivni status

Tehničke procedure

‚All clear' poruka

Restore podataka

Go Passwordless

Dokumentovanje

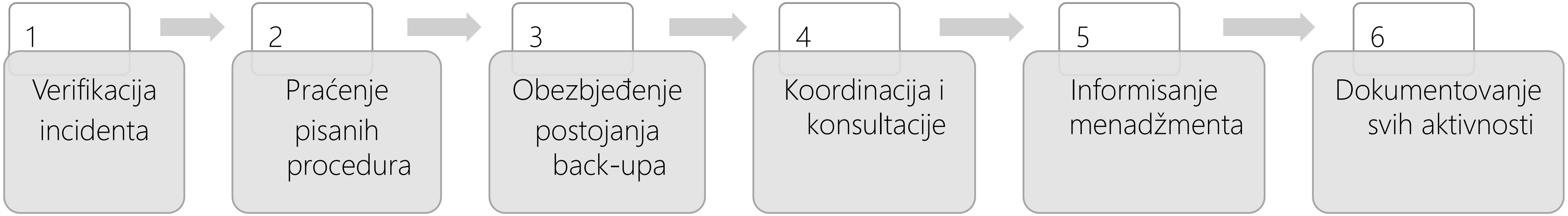
Provjera integriteta podataka

Komunikacija

Post-incident aktivnosti - unapređenje

- Pregled i integracija saznanja
- Postmortem analiza incidenta
- ‚Naučene lekcije'
- Reevaluacija/ modifikacija procedura
- Procjena novčanih troškova
- Dokumentovanje
- Priprema izvještaja
- Aktivnosti tužilaštva

Hints Moving Forward – upravljanje incidentima



1 Verifikacija incidenta

2 Praćenje pisanih procedura

3 Obezbjeđenje postojanja back-upa

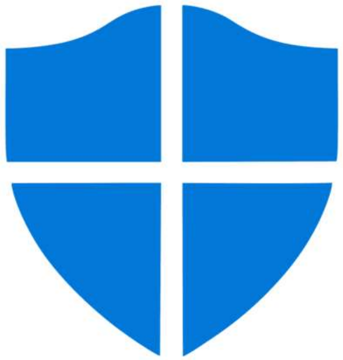
4 Koordinacija i konsultacije

5 Informisanje menadžmenta

6 Dokumentovanje svih aktivnosti

Cyber security rješenja

Detekcija, prevencija i istraživanje/analiza

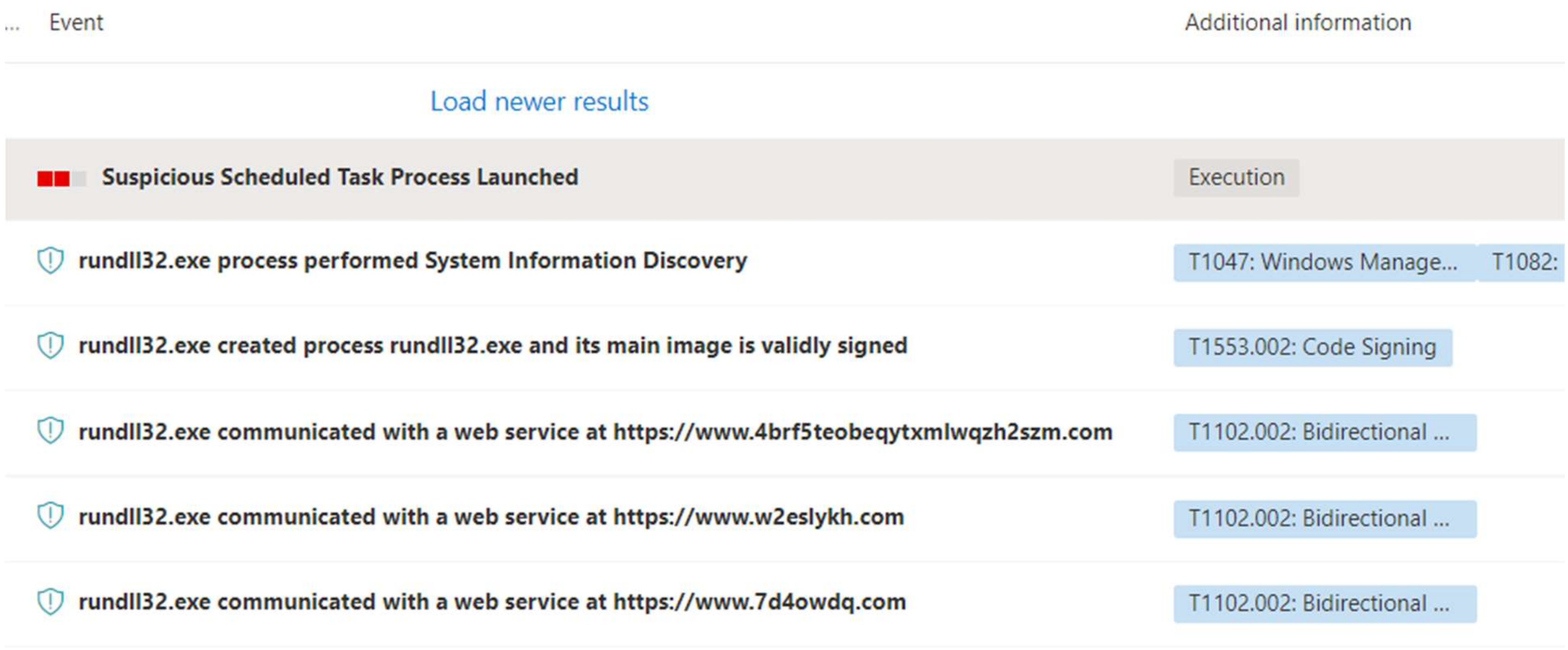


Microsoft Defender

YubiKey

Kako prevenirati cyber napad?

Primjer detekcije sumnjive radnje



...	Event	Additional information
	Load newer results	
🟥🟥	**Suspicious Scheduled Task Process Launched**	Execution
	rundll32.exe process performed System Information Discovery	T1047: Windows Manage... T1082:
	rundll32.exe created process rundll32.exe and its main image is validly signed	T1553.002: Code Signing
	rundll32.exe communicated with a web service at https://www.4brf5teobeqytxmlwqzh2szm.com	T1102.002: Bidirectional ...
	rundll32.exe communicated with a web service at https://www.w2eslykh.com	T1102.002: Bidirectional ...
	rundll32.exe communicated with a web service at https://www.7d4owdq.com	T1102.002: Bidirectional ...

Speed IT up

Microsoft Defender – multiplatformski pristup

Windows macOS

Endpoints and servers

iOS

Mobile device OS

Windows 365

Azure Virtual Desktop

Virtual desktops

Cisco

Juniper Networks

HP Enterprise

Palo Alto Networks

Network devices

An industry leader in endpoint security

Gartner names Microsoft a Leader in 2021 Endpoint Protection Platforms Magic Quadrant.

Forrester names Microsoft a Leader in 2021 Endpoint Security Software as a Service Wave.

Forrester names Microsoft a Leader in 2020 Enterprise Detection and Response Wave.

Our antimalware capabilities consistently achieve high scores in independent tests.

Microsoft leads in real-world detection in MITRE ATT&CK evaluation.

Microsoft Defender for Endpoint awarded a perfect 5-star rating by SC Media in 2020 Endpoint Security Review

Microsoft won six security awards with Cyber Defense Magazine at RSAC 2021:

- ✓ Best Product Hardware Security
- ✓ Market Leader Endpoint Security
- ✓ Editor's Choice Extended Detection and Response (XDR)
- ✓ Most Innovative Malware Detection
- ✓ Cutting Edge Email Security

Microsoft Defender for Endpoint Auto IR

✓

Security automation is…
mimicking the *ideal steps* a human would take *to investigate and remediate* a cyber threat

✗

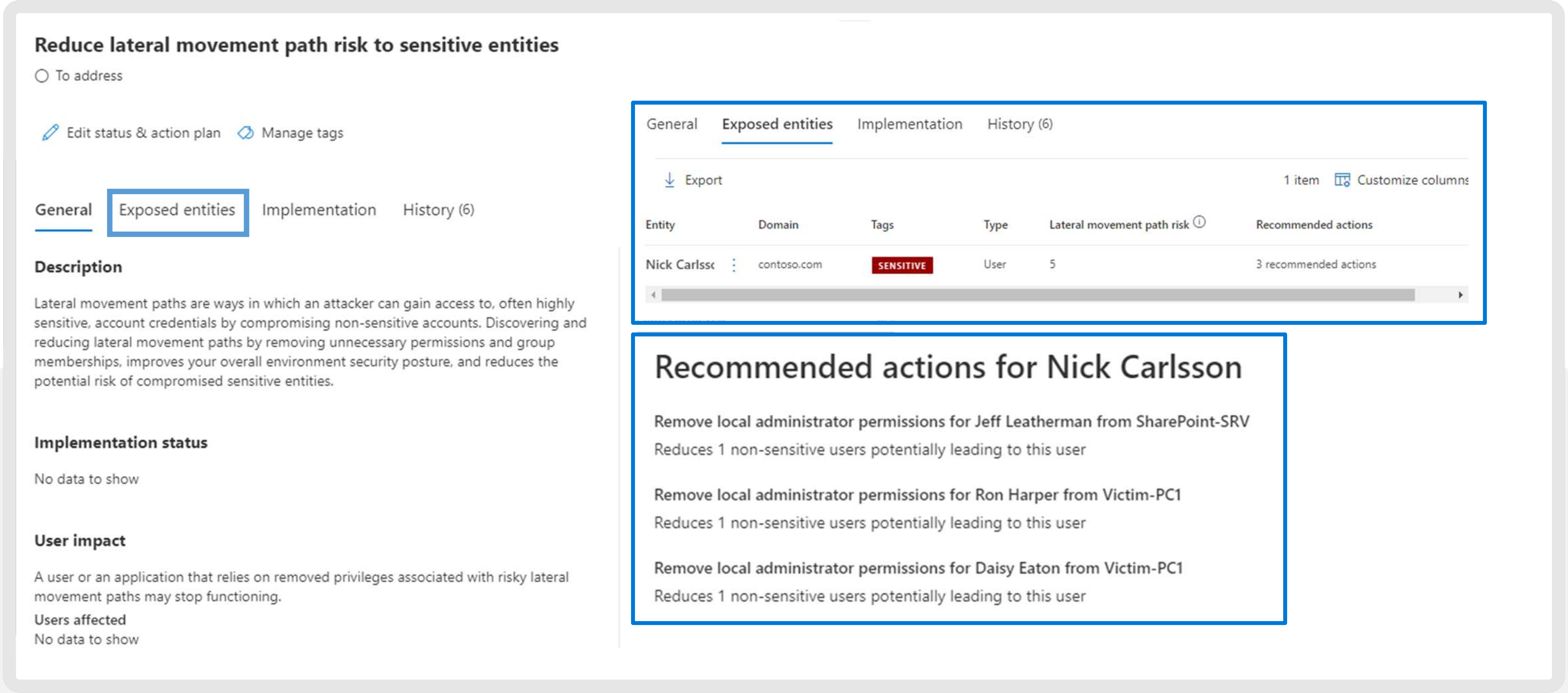
Security automation is not…
if machine has alert → auto-isolate

When we look at the steps an analyst is taking as when investigating and remediating threats we can identify the following high-level steps:

1. Determining whether the threat requires action
2. Performing necessary remediation actions
3. Deciding what additional investigations should be next
4. Repeating this as many times as necessary for every alert ☺

Risky lateral movement paths

View top sensitive accounts that carry lateral movement risk



Reduce lateral movement path risk to sensitive entities

○ To address

Description

Lateral movement paths are ways in which an attacker can gain access to, often highly sensitive, account credentials by compromising non-sensitive accounts. Discovering and reducing lateral movement paths by removing unnecessary permissions and group memberships, improves your overall environment security posture, and reduces the potential risk of compromised sensitive entities.

Implementation status

No data to show

User impact

A user or an application that relies on removed privileges associated with risky lateral movement paths may stop functioning.

Users affected

No data to show

Entity	Domain	Tags	Type	Lateral movement path risk ⓘ	Recommended actions
Nick Carlssc	contoso.com	SENSITIVE	User	5	3 recommended actions

Recommended actions for Nick Carlsson

Remove local administrator permissions for Jeff Leatherman from SharePoint-SRV

Reduces 1 non-sensitive users potentially leading to this user

Remove local administrator permissions for Ron Harper from Victim-PC1

Reduces 1 non-sensitive users potentially leading to this user

Remove local administrator permissions for Daisy Eaton from Victim-PC1

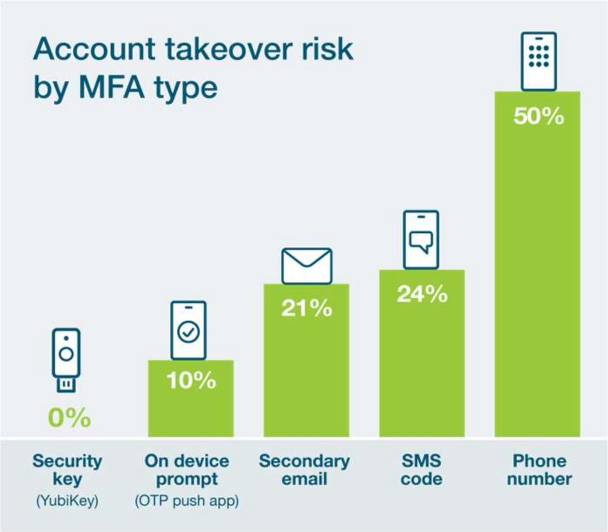
Reduces 1 non-sensitive users potentially leading to this user

yubico

YubiKeys

- Zero Trust strategija- phishing-resistantni MFA
- Legacy pristupi poput SMS, One-time passwords i mobile push apps nisu efikasni
- Koristite Strong 2FA, MFA i passwordless autentikaciju za zaštitu vašeg sistema

Touch or tap your key to authenticate



Fast IDentity Online 2.0

Standards-based, interoperable authentication

Works with the same devices people use every day

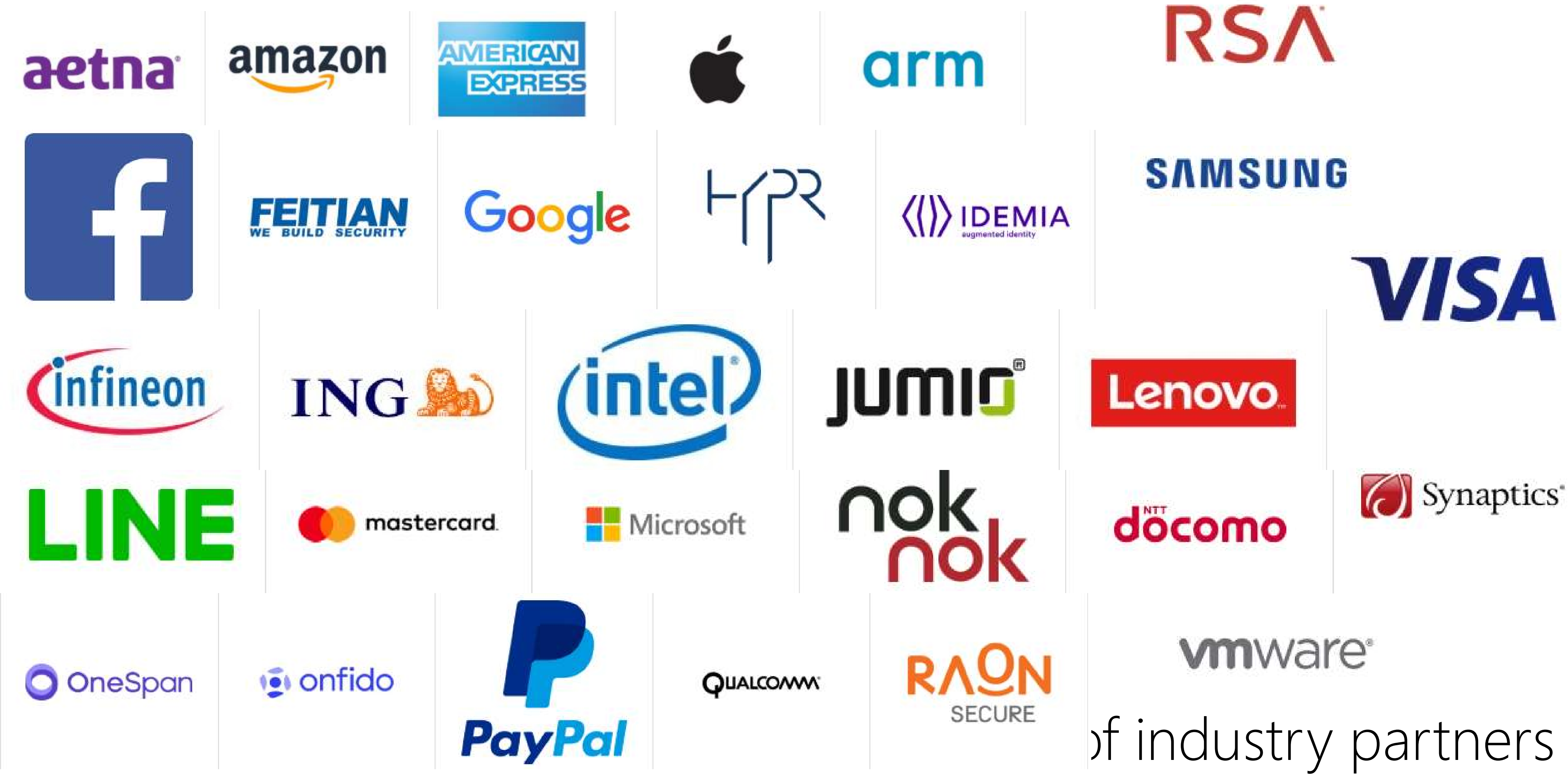
Based on public key cryptography

Biometrics and keys never leave the device

Protects against phishing, man-in-the-middle and replay attacks

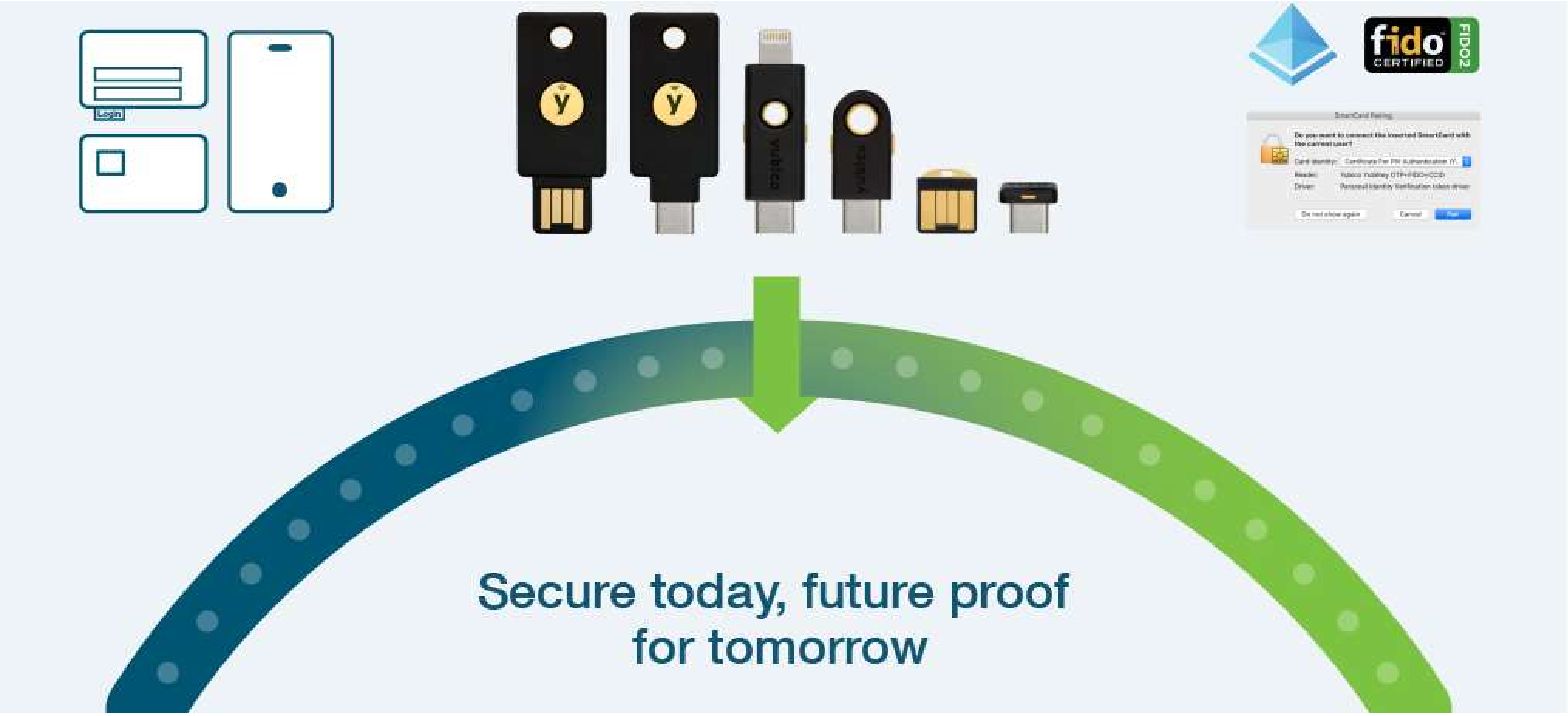
fido™ alliance 2.0

FIDO Alliance board members



of industry partners

Omogućava tranziciju i prelazak na passwordless autentikaciju



Do you want to connect the inserted SmartCard with the current user?

Card identity: Certificate For PIV Authentication (Y...

Reader: Yubico YubiKey OTP+FIDO+CCID

Driver: Personal Identity Verification token driver

Secure today, future proof for tomorrow

YubiKey 5 Series

YubiKey 5 FIPS Series

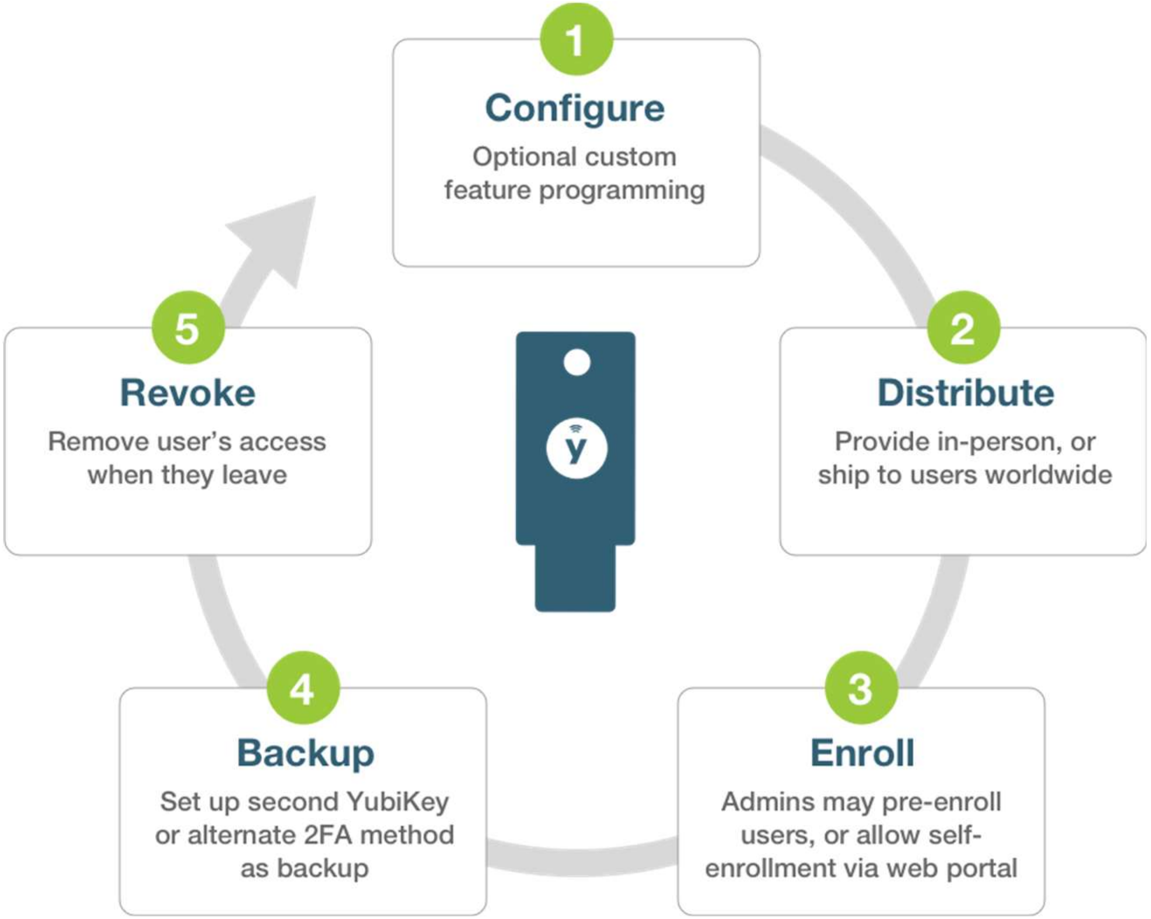
YubiKey Bio Series

Security Key Series

YubiKey 5 CSPN Series

YubiHSM 2 & YubiHSM 2 FIPS

Jednostavna implementacija i upravljanje



1 **Configure**
Optional custom feature programming

2 **Distribute**
Provide in-person, or ship to users worldwide

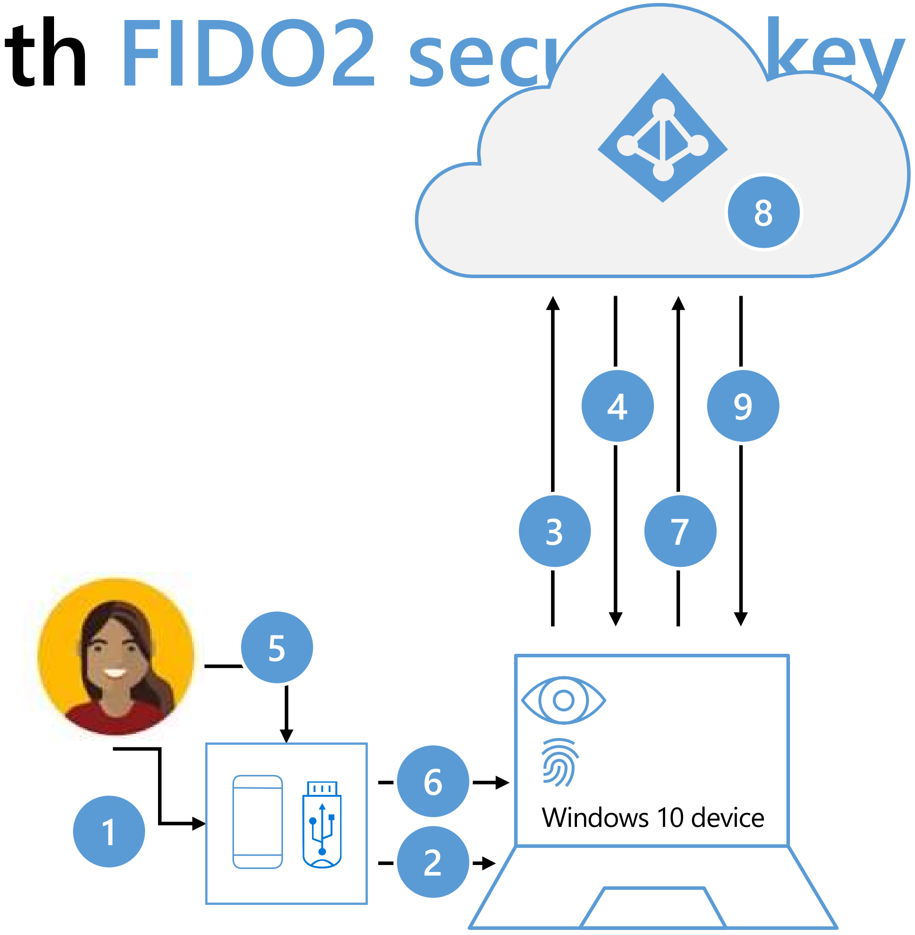
3 **Enroll**
Admins may pre-enroll users, or allow self-enrollment via web portal

4 **Backup**
Set up second YubiKey or alternate 2FA method as backup

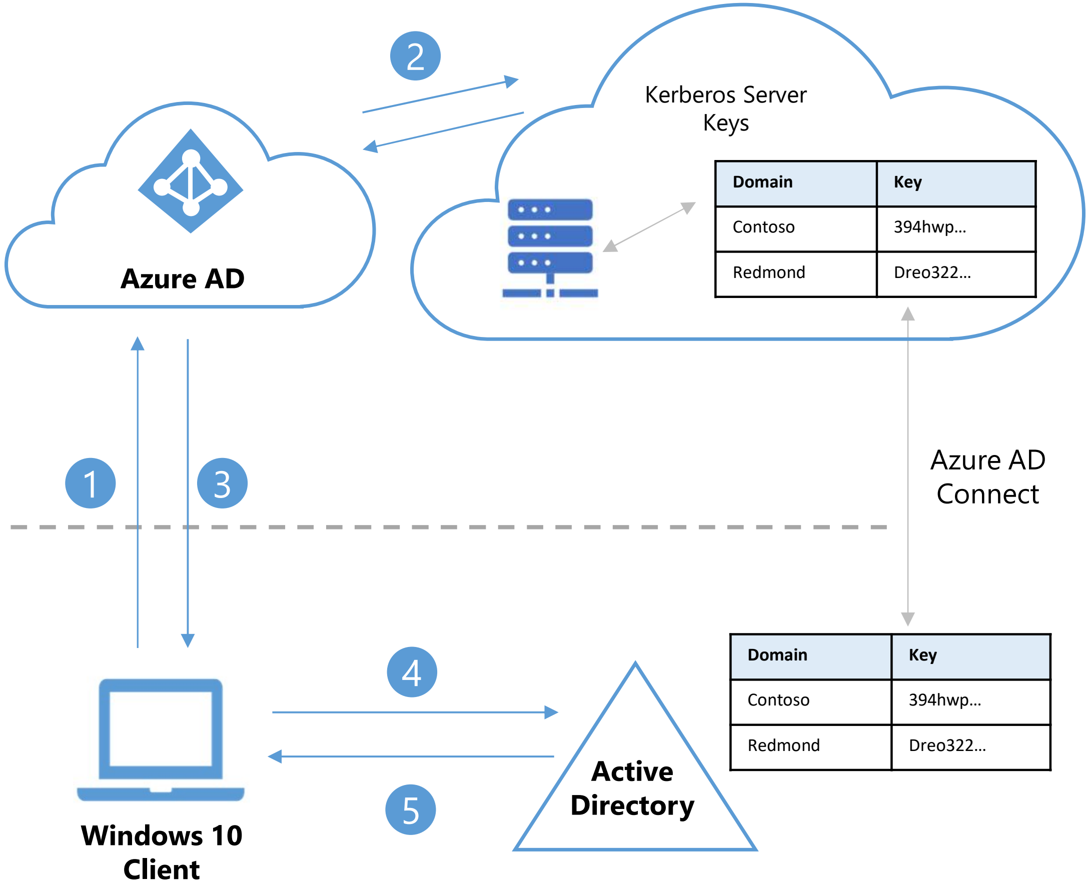
5 **Revoke**
Remove user's access when they leave

Strong Authentication with FIDO2 security key

1. User plugs FIDO2 security key into computer
2. Windows detects FIDO2 security key
3. Windows device sends auth request
4. Azure AD sends back nonce
5. User completes gesture to unlock private key stored in security key's secure enclave
6. FIDO2 security key signs nonce with private key
7. Primary Refresh Token (PRT) request with signed nonce is sent to Azure AD
8. Azure AD verifies FIDO key signature
9. Azure AD returns PRT to enable access to cloud resources



Authentication in hybrid



Domain	Key
Contoso	394hwp...
Redmond	Dreo322...

Domain	Key
Contoso	394hwp...
Redmond	Dreo322...

1. User authenticates to Azure AD with a FIDO2 security key.
2. Azure AD checks the tenant for a Kerberos server key matching the user's on-premises AD Domain.
   - Azure AD Generates a partial Kerberos Ticket Granting Ticket (TGT) for the users on-premises AD Domain. The TGT contains only the user SID. No authorization data (groups) are included in the TGT.
3. The partial TGT is returned to the Windows along with Azure AD Primary Refresh Token (PRT).
4. Windows contacts on-premises AD Domain Controller and trades the partial TGT for a full TGT.
5. Windows now has Azure AD PRT and a full Active Directory TGT.

LOGOSOFT

www.logosoft.ba
prodaja.biz@logosoft.ba
+387 33 931 987

Q&A

Smart Home rješenja

https://www.youtube.com/watch?v=O93NMq4lt2A

Kako učinkovito plasirati marketinšku poruku?

m:tel kao medij

powered by m:tel

Kome se obraćate?

Naša targetirana komunikacija sa korisnicima je vaša prilika da učinkovito plasirate sopstvene promotivne poruke i to za sljedeće grupe korisnika:

- Muškarci/žene
- 18-65 godina starosti
- Žive na teritoriji BiH

- Srednje i više platežne moći
- Srednjeg i višeg obrazovanja
- Tehnološki osviješteni

Kontakt mejl na koji možete poslati upit za ponudu: marketing.dir@mtel.ba

Sve cijene navedene u prezentaciji su bez uključenog PDVa.

m:tel kao medij

Prodaja oglasnog prostora

Kako?

IPTV platforma

TV oglašavanje

m:agazin

Oglas u online magazinu

m:blog

web oglašavanje

Mondo portal

na mondo.ba

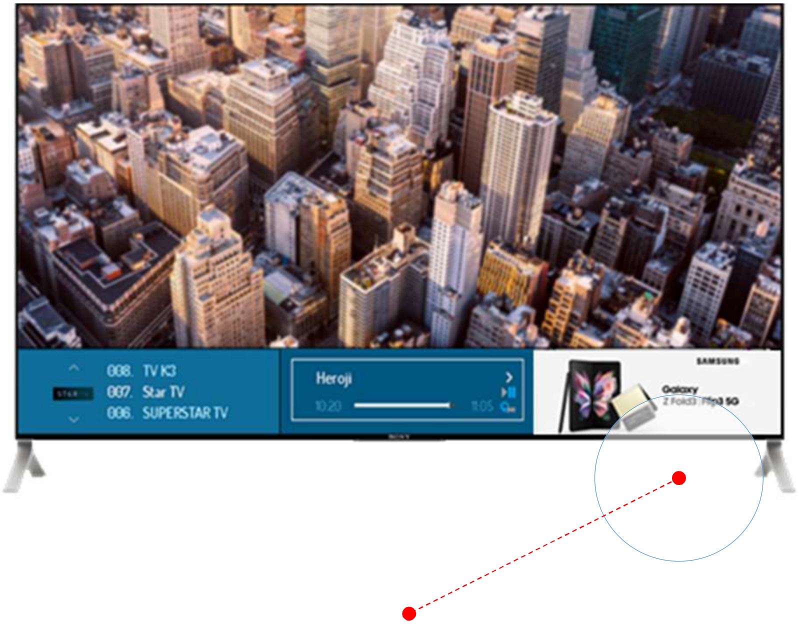
Baneri

m:GO mobilna aplikacija

powered by

m:tel kao medij

Prodaja oglasnog prostora
(TV oglašavanje/IPTV platforma)



Statički baner na program status liniji (PS baner)

Baner sa ikonom i ispisom na ekranu pri prebacivanju kanala

- U udobnosti svog doma i opuštenoj atmosferi, korisnik prebacivanja dolazi u kontakt sa promotivnom porukom prilikom mijenjanja TV kanala.
- Klikom na baner, ulazi u dodatni „prozor“ na TV ekranu u kome može pročitati više informacija o proizvodu/usluzi koja se reklamira.

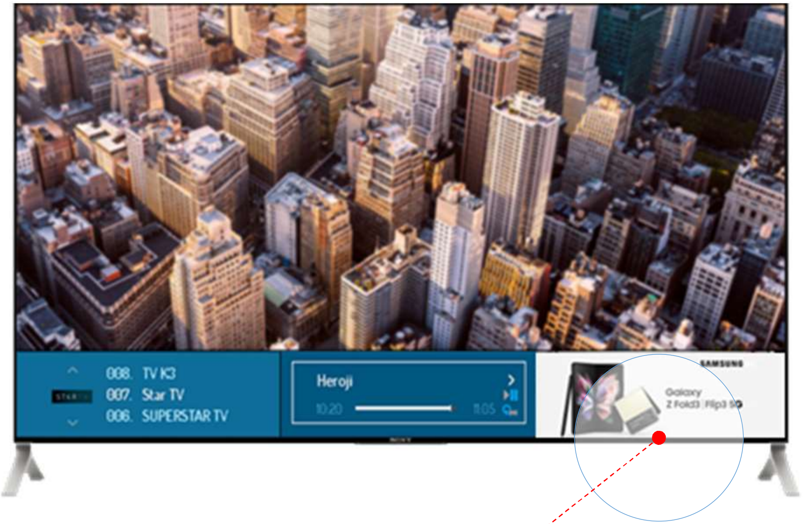
- Cijena po danu; CPD 100 KM
- Kapacitet: maksimalno 5 klijenata
- Izbor određenog seta kanala povećava cijenu za 30%
- Slobodne pozicije i vremenski period slobodnih pozicija, na zahtjev dostavlja m:tel

powered by m:tel

m:tel kao medij

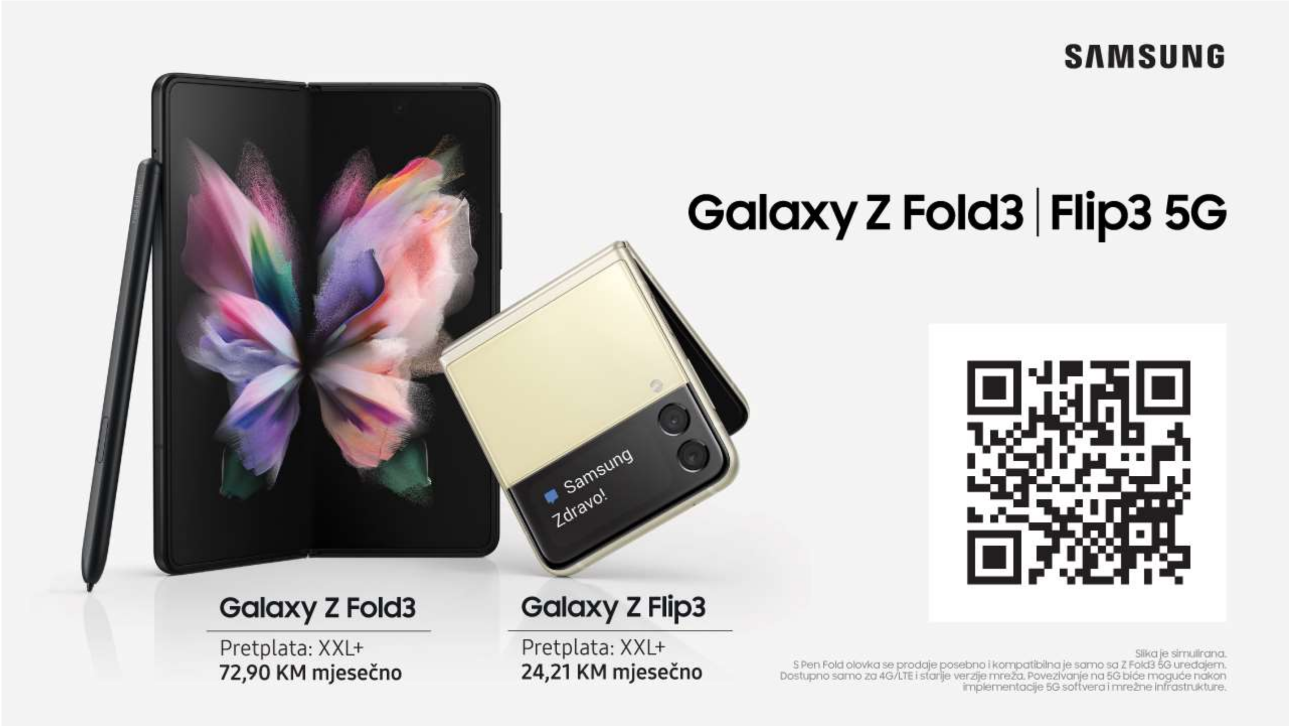
Prodaja oglasnog prostora
(TV oglašavanje/IPTV platforma)

Kako funkcioniše?



1. Prilikom mijenjanja TV kanala, baner sa Vašim vizualom i natpisom pojavljuje se na TV ekranu na našoj program status liniji.

2. Klikom na baner, na televizoru se otvara novi prozor u kojem je prezentovana vaša ponuda koju želite da prezentujete svojim kupcima.



Galaxy Z Fold3
Pretplata: XXL+
72,90 KM mjesečno

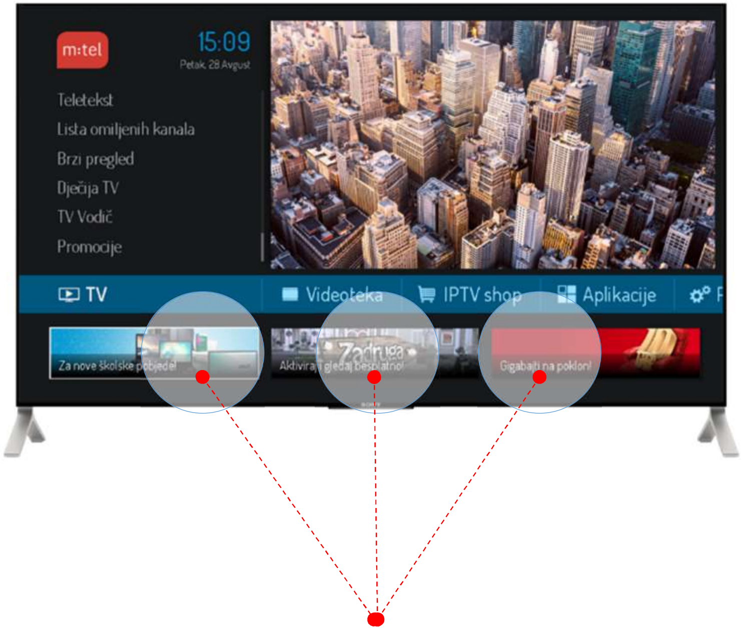
Galaxy Z Flip3
Pretplata: XXL+
24,21 KM mjesečno

Slika je simulirana.
S Pen Fold olovka se prodaje posebno i kompatibilna je samo sa Z Fold3 5G uređajem.
Dostupno samo za 4G/LTE i starije verzije mreža. Povezivanje na 5G biće moguće nakon implementacije 5G softvera i mrežne infrastrukture.

powered by
m:tel

m:tel kao medij

Prodaja oglasnog prostora
(TV oglašavanje/IPTV platforma)



Statički baner unutar glavnog menija (GM baner)

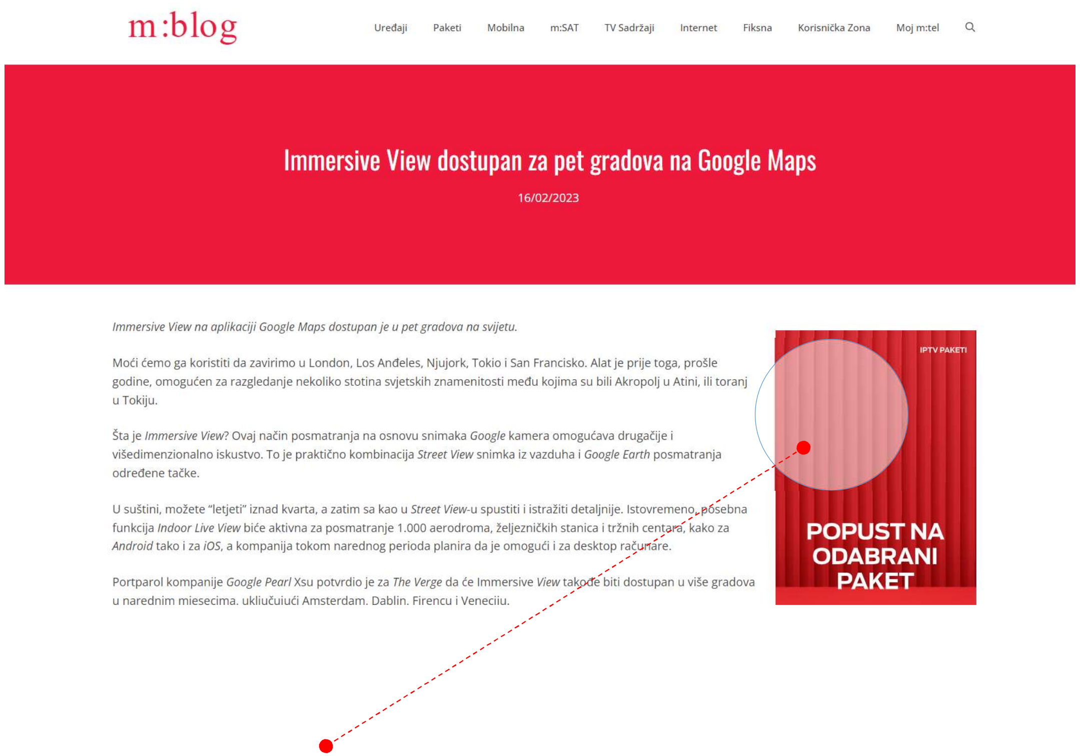
Baneri sa ikonom i ispisom u glavnom meniju IPTV platforme

- Ulaskom u glavni meni na IPTV platformi, korisnik traži dodatne usluge (videoteka, TV raspored, dodatne funkcionalnosti). Tom prilikom u donjem dijelu ekrana pojavljuju se statički baneri sa promotivnim porukama. Ukoliko korisnik želi više informacija, jednostavnim klikom na baner ulazi u novi „prozor“ na TV ekranu i čita plasirane informacije o proizvodu/usluzi.

- Cijena po kliku; CPC 0,10
- Kapacitet: maksimalno klijenta
- Prosječan broj „otvaranja“ banera u glavnom meniju za mjesec dana iznosi cca 40 000
- Slobodne pozicije i vremenski period slobodnih pozicija, na zahtjev dostavlja m:tel

m:tel kao medij

Prodaja oglasnog prostora (m:BLOG ads)



Immersive View dostupan za pet gradova na Google Maps

16/02/2023

Immersive View na aplikaciji Google Maps dostupan je u pet gradova na svijetu.

Moći ćemo ga koristiti da zavirimo u London, Los Anđeles, Njujork, Tokio i San Francisko. Alat je prije toga, prošle godine, omogućen za razgledanje nekoliko stotina svjetskih znamenitosti među kojima su bili Akropolj u Atini, ili toranj u Tokiju.

Šta je *Immersive View*? Ovaj način posmatranja na osnovu snimaka *Google* kamera omogućava drugačije i višedimenzionalno iskustvo. To je praktično kombinacija *Street View* snimka iz vazduha i *Google Earth* posmatranja određene tačke.

U suštini, možete "letjeti" iznad kvarta, a zatim sa kao u *Street View*-u spustiti i istražiti detaljnije. Istovremeno, posebna funkcija *Indoor Live View* biće aktivna za posmatranje 1.000 aerodroma, željezničkih stanica i tržnih centara, kako za *Android* tako i za *iOS*, a kompanija tokom narednog perioda planira da je omogući i za desktop računare.

Portparol kompanije *Google Pearl* Xsu potvrdio je za *The Verge* da će Immersive *View* takođe biti dostupan u više gradova u narednim miesecima. ukliučuiući Amsterdam. Dablin. Firencu i Veneciiu.

STATIČKI ili ANIMIRANI BANER

Vertikalni wallscape baneri na blog.mtel.ba

- Blog kompanije m:tel je web kutak za sve ljubitelje tehnologije i nauke. Na opušten, jednostavan i zabavan način, čitaoci mogu saznati sve o velikim idejama koje mijenjaju svijet, velikim prijateljstvima koja ga obogaćuju i malim inovacijama koje ga čine još zabavnijim.

- Cijena za 1000 prikaza; CPM 30 KM
- Prosječan broj jedinstvenih pregleda stranice za jedan mjesec je cca 100 000
- Kapacitet: maksimalno 4 klijenta

m:tel kao medij

Prodaja oglasnog prostora (m:agazin ads)

OGLAS u online magazinu

Cijela strana, puni kolor, 210x270mm

- Kvartalni online magazin
- Plasira se na preko 3000 adresa
- Ko čita m:agazin? Ključni poslovni korisnici, ali i ambasade, kulturne ustanove, sportski kolektivi
- Sadržaj: tehnologija budućnosti, ponuda, sport, kultura, intervjui, događaji

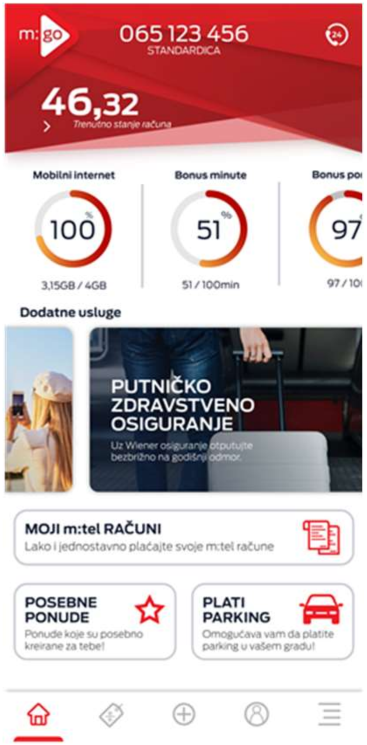
---

- Cijena 1/1 FC oglasa 800 KM
- Broj klijenata: 5
- Kapacitet: 5
- Maksimalan broj klijenata po jednom broju: 3

powered by m:tel

m:tel kao medij

Prodaja oglasnog prostora (m:GO aplikacija)



m:go 065 123 456
STANDARDICA

46,32
Trenutno stanje računa

Mobilni internet 100 % 3,15GB / 4GB

Bonus minute 51 % 51 / 100min

Bonus po 97 97 / 10

Dodatne usluge

PUTNIČKO ZDRAVSTVENO OSIGURANJE
Uz Wiener osiguranje otputujte bezbrižno na godišnji odmor.

MOJI m:tel RAČUNI
Lako i jednostavno plaćajte svoje m:tel račune

POSEBNE PONUDE
Ponude koje su posebno kreirane za tebe!

PLATI PARKING
Omogućava vam da platite parking u vašem gradu!

m:GO aplikacija
Reklamni baneri vidljivi odmah po pristupu aplikaciji

- Plasiranje promotivnog/reklamnog sadržaja u okviru m:GO aplikacije, koja je aplikacija br.1 po broju aktivnih korisnika u BiH.
- Prilikom svakog otvaranja/pristupanja m:GO aplikaciji promotivni/reklamni baner biće vidljiv korisniku aplikacije
- Kanal komunikacije koji je idealan za kupovinu usluga/proizvoda jer je naša m:GO aplikacija osmišljena sa svrhom što lakše i kraće kupovine servisa koji svakodnevni život čine lakšim

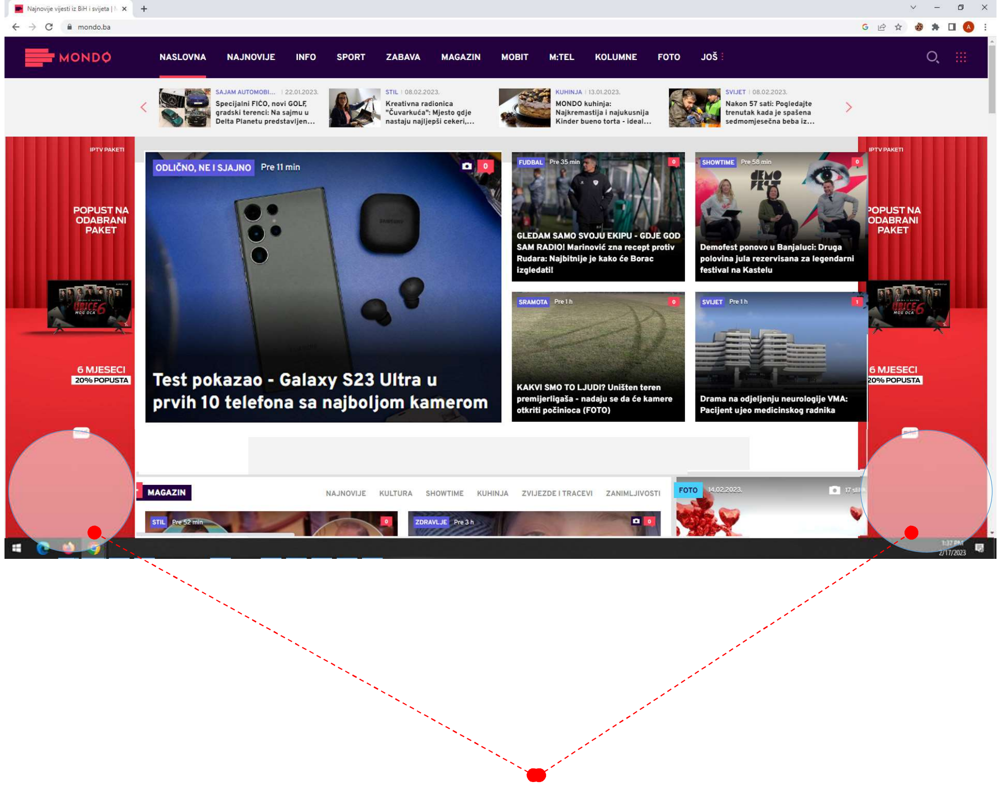
---

- Cijena 1500 KM/mjesečno/flat

powered by m:tel

m:tel kao medij

Prodaja oglasnog prostora (Mondo portal)



SAJAM AUTOMOBI... | 22.01.2023. Specijalni FIĆO, novi GOLF, gradski terenci: Na sajmu u Delta Planetu predstavljen...

STIL | 08.02.2023. Kreativna radionica "Čuvarkuća": Mjesto gdje nastaju najljepši cekeri,...

KUHINJA | 13.01.2023. MONDO kuhinja: Najkremastija i najukusnija Kinder bueno torta - ideal...

SVIJET | 08.02.2023. Nakon 57 sati: Pogledajte trenutak kada je spašena sedmomjesečna beba iz...

ODLIČNO, NE I SJAJNO Pre 11 min — Test pokazao - Galaxy S23 Ultra u prvih 10 telefona sa najboljom kamerom

FUDBAL Pre 35 min — GLEDAM SAMO SVOJU EKIPU - GDJE GOD SAM RADIO! Marinović zna recept protiv Rudara: Najbitnije je kako će Borac izgledati!

SHOWTIME Pre 58 min — Demofest ponovo u Banjaluci: Druga polovina jula rezervisana za legendarni festival na Kastelu

SRAMOTA Pre 1 h — KAKVI SMO TO LJUDI? Uništen teren premijerligaša - nadaju se da će kamere otkriti počinioca (FOTO)

SVIJET Pre 1 h — Drama na odjeljenju neurologije VMA: Pacijent ujeo medicinskog radnika

STATIČKI ili ANIMIRANI BANERI

Vertikalni wallscape baneri na www.mondo.ba

- Mondo je jedan od najčitanijih informativnih portala u regiji (mondo.ba)
- Bilježe više od 4 miliona otvaranja stranice na mjesečnom nivou

- Saradnja i uslovi zakupa dogovaraju se direktno sa Mondo portalom

powered by
m:tel

Hvala na pažnji!

Kontakt: marketing.dir@mtel.ba

LOGOSOFT

Hvala Vam!

www.logosoft.ba
prodaja.biz@logosoft.ba
+387 33 931 987