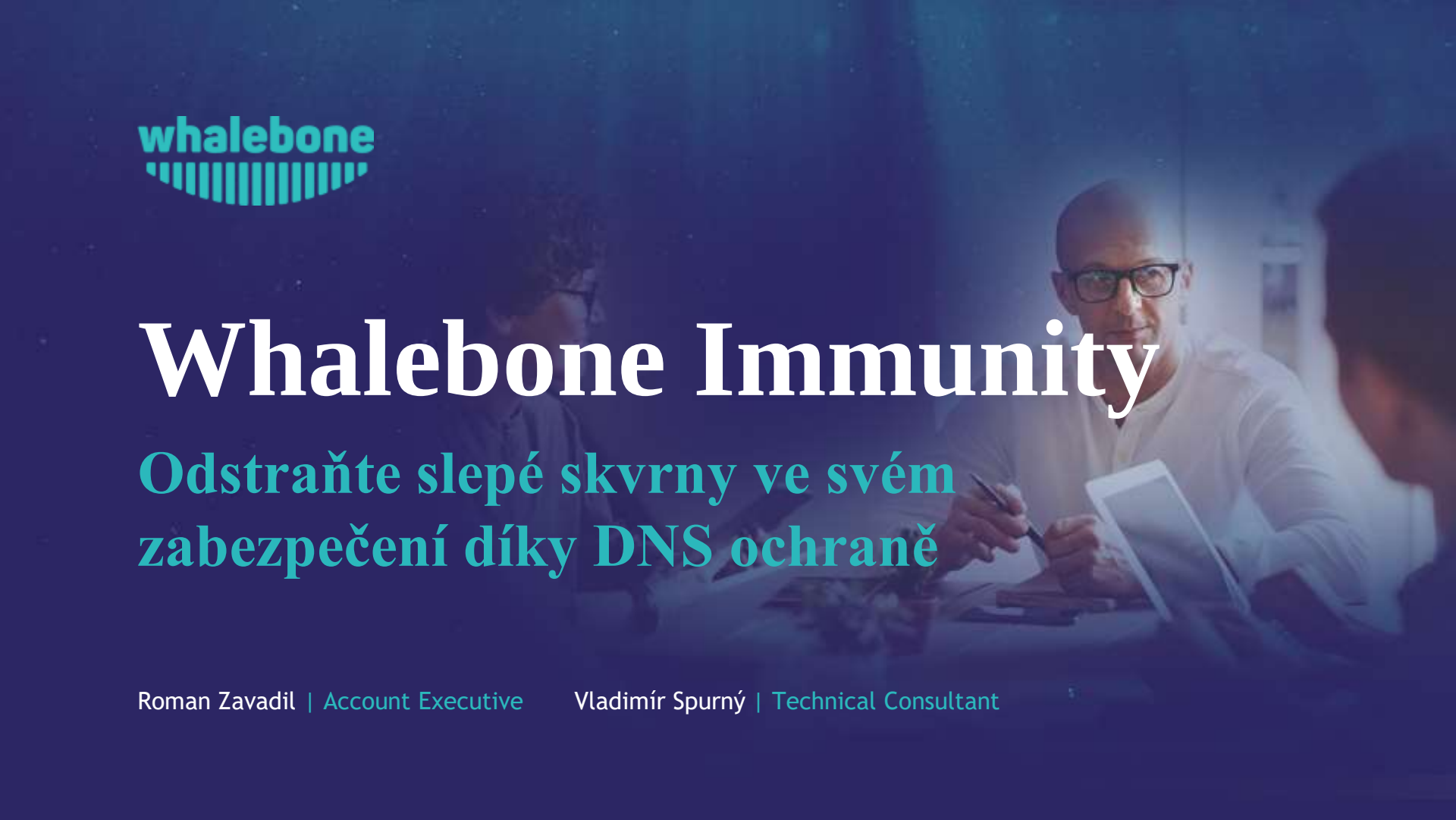


Whalebone Immunity

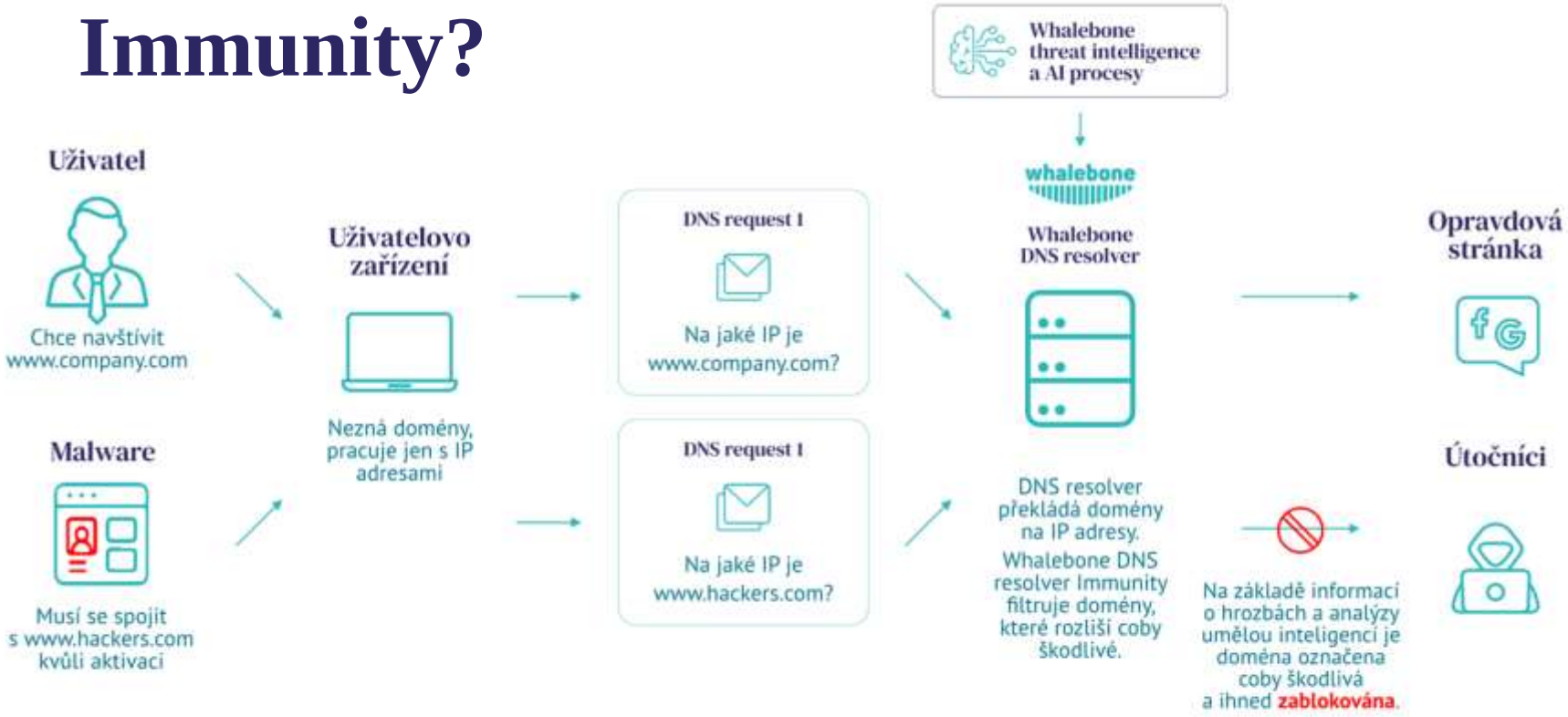
Odstraňte slepé skvrny ve svém zabezpečení díky DNS ochraně

Roman Zavadil | Account Executive

Vladimír Spurný | Technical Consultant

Co je DNS resolver?

Co je Whalebone Immunity?



Proč je DNS vrstva účinná?

DNS resolver

— Dostaňte pod kontrolu zásadní část infrastruktury

90%+ útoků využívá DNS

— Pokud nezastavíte útok při prvním kontaktu, lze ho odchytit během procesu

100%

…ochranu vám žádný produkt nezajistí, ale vrstvená ochrana vás může přiblížit

Typicky zneužívaná slepá místa

DNS tunneling a DGA	Používaný k obejití firewallů, umožní útočníkům dostat malware do sítě a ovládat ho
Zaměstnanci mimo síť	Když nejsou pod ochranou síťových prvků, jsou zranitelnější
Homografické útoky	Používaný k vylákání informací z uživatelů nebo k rozšíření malware
Uniklá hesla & citlivá data	Leaklé databáze třetích stran jsou nejjednodušší způsob, jak získat hesla
Supply chain, IoT, phishing, 0-day attacks	Cokoli, co se dostane za vaši ochranu, je vektor pro malware

DNS tunneling and DGA

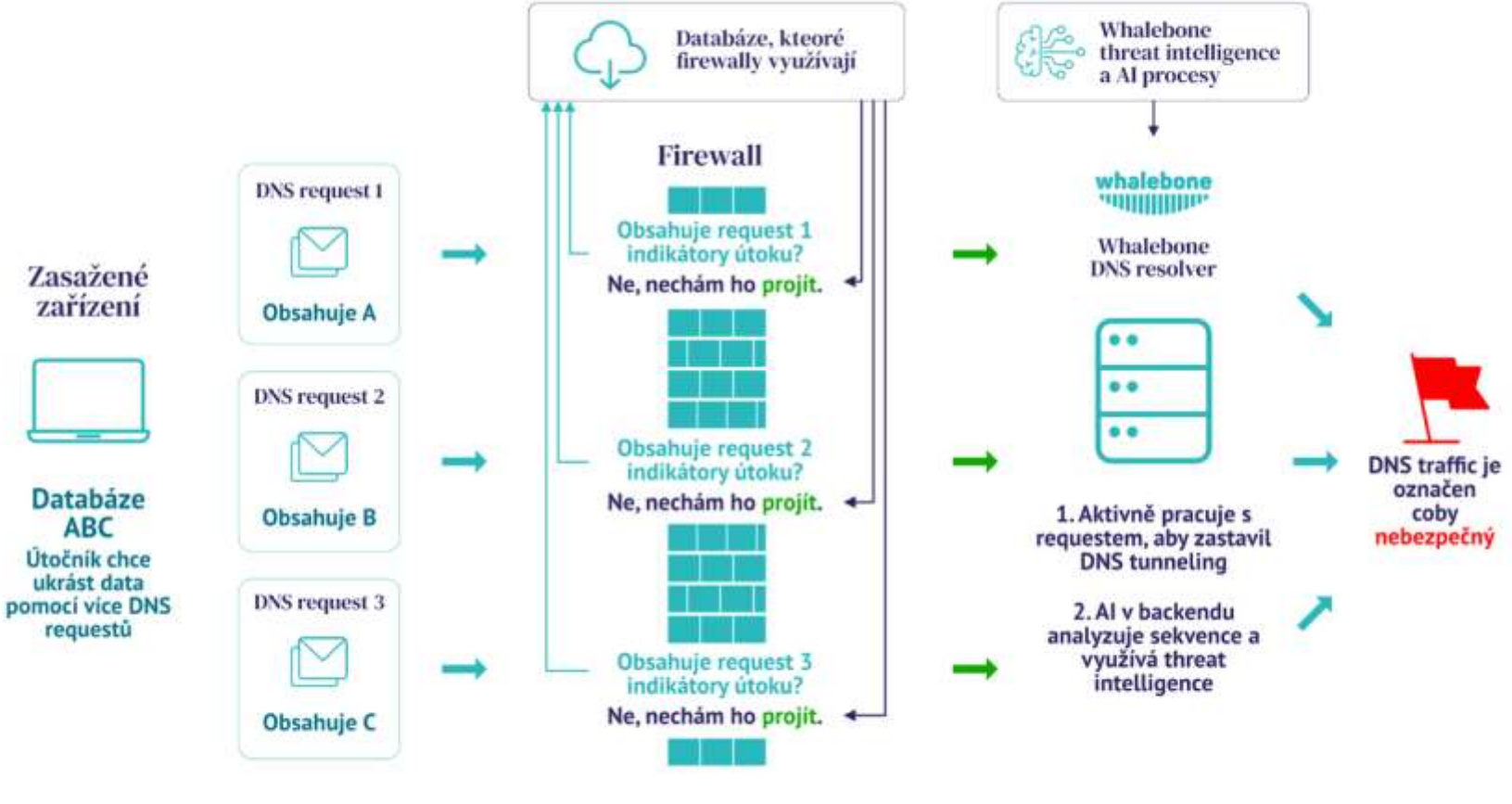
- Využívá DNS queries k **pašování dat** do nebo z vaší sítě
- Použité při SolarWinds útoku, touto technikou byla ukradena data z **18,000 sítí** včetně Microsoftu, Cisca nebo Pentagonu

- Domain generating algorithms vytváří nové domény, které malware může využít, jelikož **nejsou součástí žádné databáze**

Tyto typy hrozeb lze rozumně odhalit pouze díky **analýze série queries** — firewally pouze rozeznají již identifikované hrozby v jednotlivém query

Viz další slide →

Jak DNS tunneling funguje



Útoky na zaměstnance mimo síť

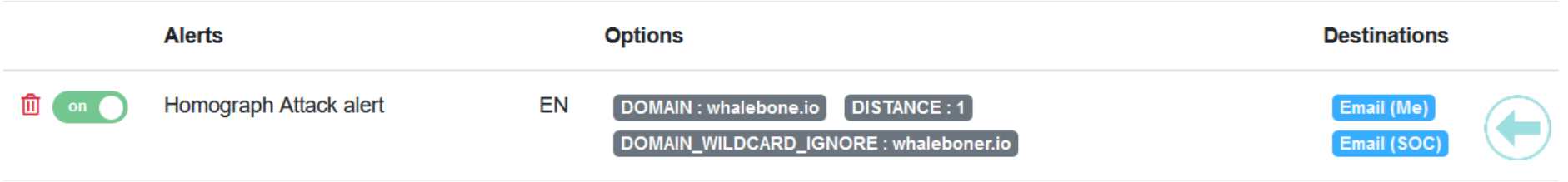
- Zaměstnance mimo síť nechrání zabezpečení ve vaší síti
- Nebezpečí na služebních cestách — nechráněné wi-fi v hotelích, na letištích nebo v kavárnách jsou zranitelné pro DNS spoofing
- Ochrana nesmí zaměstnance štvát (typické pro VPNky, pomalé spojení, nestabilita, atd.)

Řešení je jednoduchá appka, která funguje na jakémkoli OS — prostě přesměruje DNS requesty na Whalebone DNS resolver a zaměstnanec získá stejnou ochranu, jakou by měli ve firemní síti

Homografické útoky

- Použití podobných symbolů k napodobování domén (často v rámci phishingu):
  - www.google.com — standardní link
  - www.google.com
    — neplatný link s “o” z Cyrilice (zkuste ctrl+c)
- Využíváno pro nalákání uživatele na stránky, které se tváří jako legitimní, případně na phishing e-maily
- Phishingové kampaně typicky vrcholí během jednoho dne, než si toho všimnou databáze

Řešení je nastavit upozornění na homografické hrozby a vyrobit blacklisty.

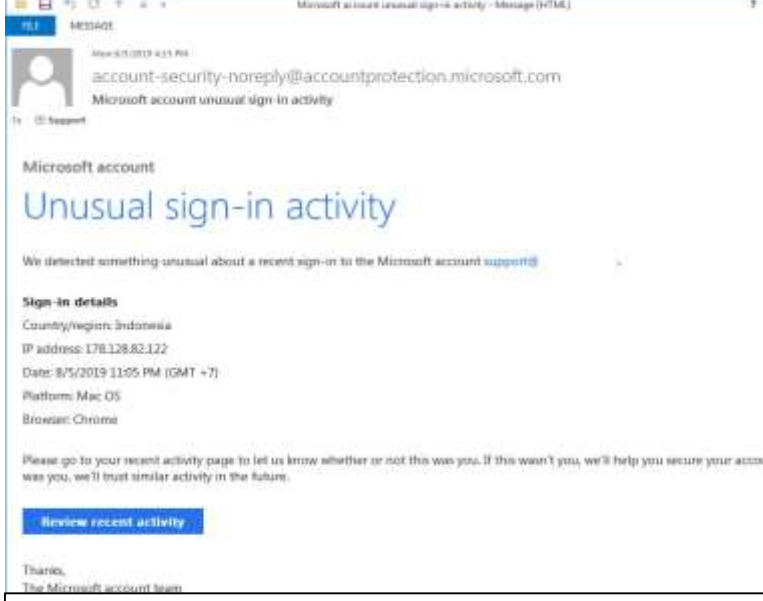


Phishing – Lidé jsou nejslabší článek

- 98% útoků používá nějakou formu social engineeringu
- Kvůli užívání AI je těžké phishing rozlišit

Když uživatel klikne na závadný link, musí být zastaven ještě než se stránka načte.

Security školení jsou sice nutná, nicméně problém nemohou vyřešit.



Krádež identity

- Průzkum Google: více než 65% lidí používá stejné heslo na více služeb — a hesla jsou mimo kontrolu IT týmu
- LinkedIn, Adobe, Canva, Yahoo, ebay, atd. byly prolomeny
- Seznamy jsou běžně k prodeji za pár euro na dark webu
- Pokud někdo použil firemní e-mail, může být zneužitý — stejné heslo může zajistit přístup do firemního e-mailu, intranetu, účetnictví, databází, odkud lze ukrást data nebo napodobovat oběť

Je zásadní staré úniky vyřešit a co nejdříve identifikovat jakékoli nové. V 50 % případů u našich zákazníků najdeme potenciálně nebezpečné úniky.

Entity	Year	Records
Yahoo	2013	3,000,000,000
Verifications.io (total leaks)	2019	2,000,000,000
First American Corporation	2019	885,000,000
India Government Aadhar data breach	2023	810,000,000+
Verifications.io (first leak)	2019	809,000,000
Collection No. 1	2019	773,000,000
Facebook	2019	540,000,000
Marriott International	2018	500,000,000
Yahoo	2014	500,000,000
Friend Finder Networks	2016	412,214,295
Exactis	2018	340,000,000
Airtel	2019	320,000,000
Truecaller	2019	299,055,000
MongoDB	2019	275,000,000
Wattpad	2020	270,000,000
Facebook	2019	267,000,000
Microsoft	2019	250,000,000
MongoDB	2019	202,000,000
Unknown	2020	201,000,0
Instagram	2020	200,000,000

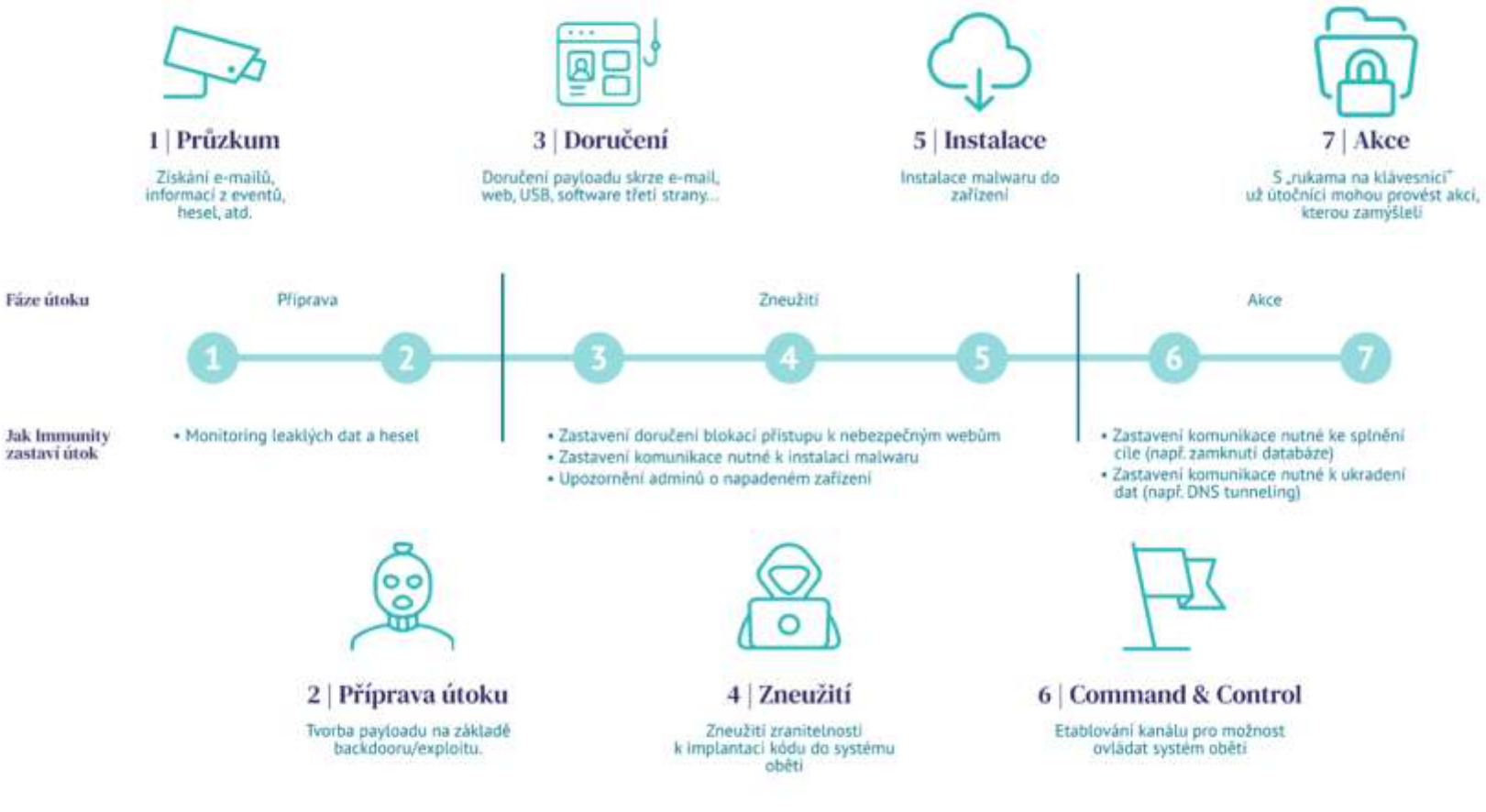
Supply chain, IoT, 0-day hrozby…

V podstatě cokoli, co se dostane za váš perimetr.

- žádná databáze není kompletní, IoT zařízení jsou zranitelná,
  software třetích stran má povolení, denně jsou odhalena nová zneužití bugů…
- **ALE** útok lze zastavit i jindy, než při prvním kontaktu

Viz další slide →

Životní cyklus kyberútoku

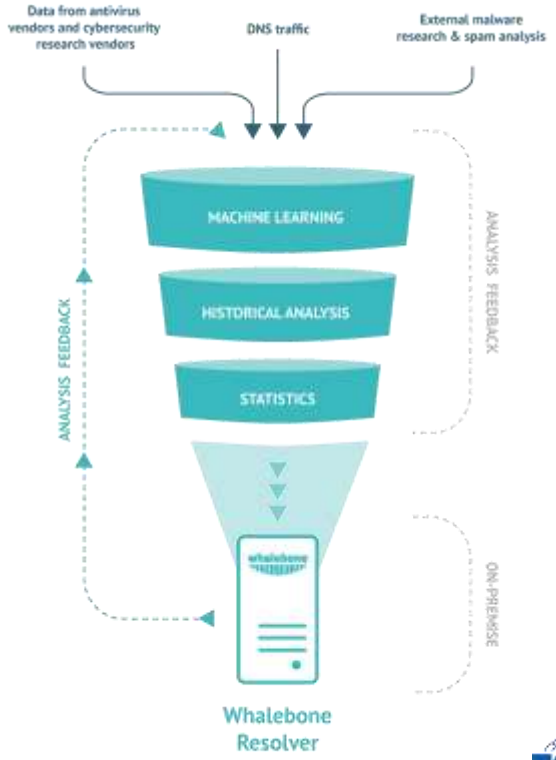


Co pohání Immunity

150,000+
domén je denně přidáno do databáze

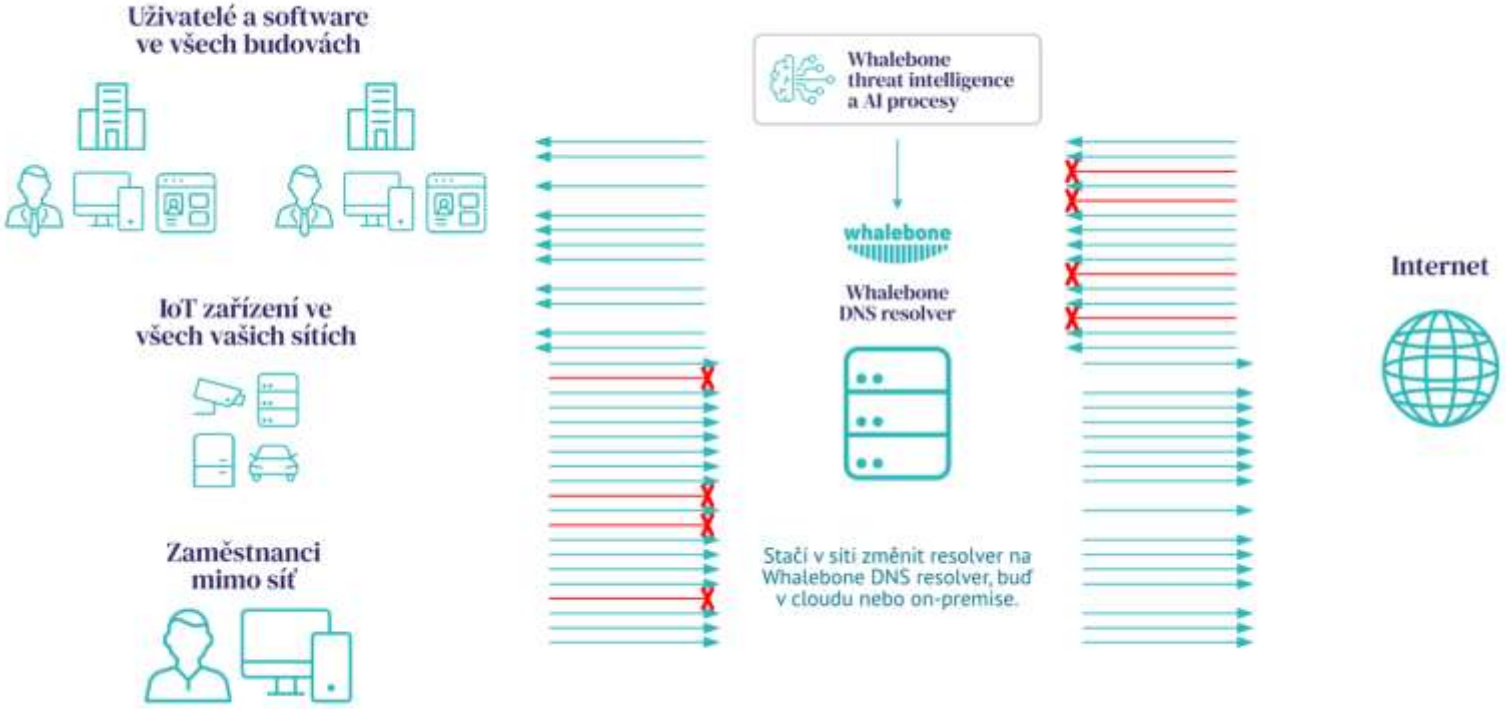
15,000,000+
aktivních domén v databázi

Včetně unikátních dat od CERTů a operátorů

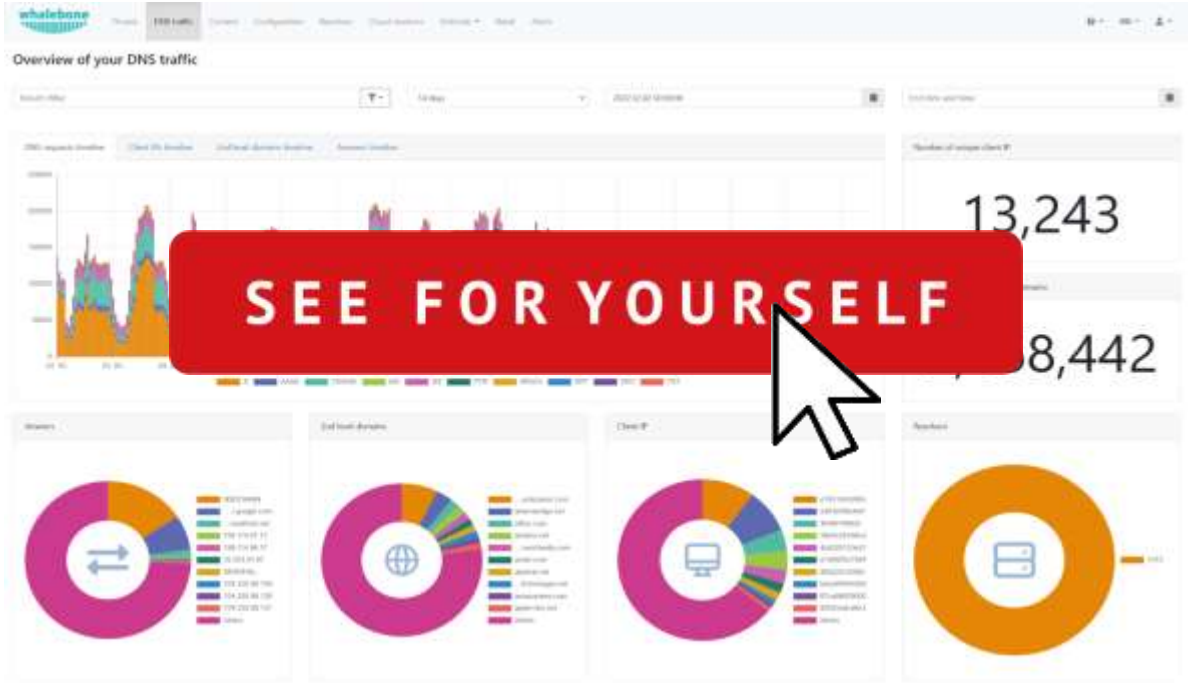


ISO 9001 27001 22301 27018

Jak získám DNS ochranu?



Live demo Whalebone Immunity



Jednoduché zavedení bez jakéhokoli vlivu na činnost firmy

Tak rychlou a bezproblémovou integraci zabezpečení do celé sítě jsem za svou kariéru ještě nezažil.

Miloš Vodička | ICT ředitel, AERO Vodochody

Viditelné a spočitatelné výsledky

Zavedení zabere 2–3 hodiny

Bez nutnosti instalace na zařízení nebo školení (pro Home Office security je třeba appka)

Testování

50+% najde důležitý security incident, 50% uniklé údaje

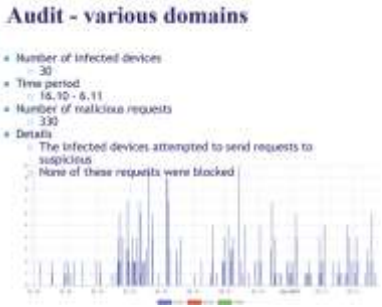
Reporty

Data a pravidelné reporty ukazují přínos Immunity

Report po zkušební době na vyžádání

Audit - various domains

- Number of infected devices
  - 30
- Time period
  - 16.10 - 6.11
- Number of malicious requests
  - 330
- Details
  - The infected devices attempted to send requests to suspicious
  - None of these requests were blocked

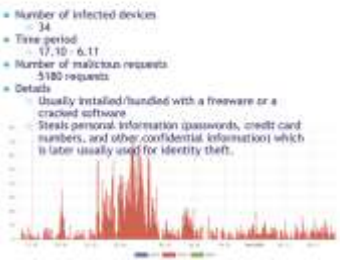


Identity Protection

- Number of incidents
  - 289
- Severity rating
  - High: 11
  - Medium: 274
  - Low: 4
- Recommended steps:
  - **Password change and forced 2FA**
  - **Regular trainings**
- Data found in leaks:
  - e-mails and passwords
  - Names
  - Telephone numbers
  - Sex
  - Date of birth
  - Physical addresses
  - IP addresses
  - Job titles
  - Social media profiles
- Potential threats:
  - Unauthorized account access
  - Impersonation of the company
  - Spear-phishing

Malware - Omnatuor

- Number of infected devices
  - 34
- Time period
  - 17.10 - 6.11
- Number of malicious requests
  - 5180 requests
- Details
  - Usually installed/bundled with a freeware or a cracked software
  - Steals personal information (passwords, credit card numbers, and other confidential information) which is later usually used for identity theft.



Phishing - friendshipmale.com

- Number of infected devices
  - 20
- Time period
  - 16.10 - 5.11
- Number of malicious requests
  - 441 requests
- Details
  - Fake streaming website
  - installs malicious plugins
  - Still uses adobe

Neural network and DGA

- No DGA domains were detected during the testing period.
- DGA (shortcut for Domain Generation Algorithm) is a means by which a malware is trying to connect to its C&C server. Using DGA analysis we are able to detect 0-day threats.

DNSSEC validation

- During the testing period the DNSSEC module did not detect any anomalies in that would suggest a potential attack.
- Overall the occasions that we identified can be considered as usual noise. It is important to realize that DNSSEC validation failure does not always mean that an attack occured. It is often a result of misconfiguration on the domain proprietor side.

Integrace a další funkce

Integrace s DNS FW & network segmentation, SIEM/Log mngmt včetně log storage a analýzy, MS Azure, end-point, anomaly detection, DHCP, honeypot, SOC

DNSSEC — SMTP (e-mail) a HTTP/HTTPS (web)communication

Content filtering — gambling, násilí, cryptomining, torrenty, pornografie…

Hluboký vhled — dostaňte pod kontrolu DNS traffic a okamžitě identifikujte napadená zařízení

Věří nám 350+ firem po celém světě

whalebone

Poskytujeme user-centric kyberbezepčnost 350+ operátorům, poskytovatelům internetu, firmám a institucím ve více než 40 zemích

Deloitte. Technology Fast50

2016 — Založeno v Brně, městě kyberbezepčnosti

2017 — 100,000 domácností chráněných Whalebone

2019 — První velcí zákazníci z řad operátorů

O2

2020 — Výhra Deloitte Rising Star Award

2022 — Výhra v tendru Evropské komise na DNS4EU, oficiálního DNS resolveru pro EU

DNS4EU

2023 — #22 na Deloitte seznamu nejrychleji rostoucích firem ve střední evropě (růst o 1104 %)

2024 — Market leader v počtu consumer security zákazníků z řad operátorů

? — Našim cílem je chránit 1 miliardu lidí

Buďte součástí iniciativy Evropské komise pro bezpečnější evropský kyberprostor

Konsorcium 14 institucí vedené Whalebonem je **jediným tvůrcem a provozovatelem DNS4EU**, oficiálního DNS resolveru pro EU.

Immunity je součástí plánu na ochranu **100 milionů lidí** a institucí pomocí **privacy-compliant** DNS resolveru.

Díky spolupráci evropských CERTů tvoříme unikátní **real-time databázi regionální hrozeb**.

DNS4EU

Immunity na zkoušku zdarma

1–2 hodiny

Nastavit infrastrukturu

- Čistá Linux VM/HW instalace
- Vytvoření účtu Whalebone
- Push install script & stahování

1–2 hodiny

Settings & configuration

- Nastavení přístupu k síti (FW admin)
- Poskytnutí informací o interních doménách, domain controllers (AD)
- DHCP & DNS nastavení (AD, proxy)

Individuální

Trial run

- Možnost postupného zapojování částí či úseků sítě
- Ochrana celé sítě
- Obsahuje ochranu identity
- Poskytuje cenná data

2 hodiny

Evaluation

- Prezentace výstupů a výsledků zkušební doby (na vyžádání)
- Otázky a nápady
- Deal — změna na plný provoz

Pojd’me do toho společně

+420 777 110 310

roman.zavadil
@whalebone.io

Více než 20 let v cybersecurity

Roman Zavadil | Account Executive