

Bez pořádku není bezpečnost

Tomáš Zloch

23.4.2025

ALTEPRO

Konec chaosu

- Bezpečnost je důležitá? ANO
- Co je základem bezpečnosti?

INVENTORY

DDI (DNS, DHCP a IPAM)

- Potřeba znalosti co je uvnitř sítě
- IP adresa, MAC adresa, DNS name, NETBIOS name, číslo portu, vlastník, uživatel, správce, lokalita, verze,...
- Kde máte tyto informace uložené? Kde je najdete?

- Takže máme incident s IP adresou (například z Flowmonu)

BARVA	START TIME - FIRST SEEN	TRVÁNÍ	IP ADRESA		TOKY
1	2021-03-15 23:50:32.593	9 min, 10.22 s	550.220	172.16.60.20	128 (1.4%)
2	2021-03-15 23:50:33.767	7 min, 12.607 s		172.16.60.108	4 (0.0%)
3	2021-03-15 23:50:32.593	8 min, 24.563 s		172.16.60.105	15 (0.2%)
4	2021-03-15 23:53:30.213	5 min, 50.65 s		10.100.100.54	273 (3.0%)

Co budu dělat?

- Zjistím DNS (microsoft, nebo to máme propojené s flowmonem)
- IP byla dynamická - logy DHCP serveru? Mám je?
- Kdo byl přihlášen? Logy na MS/XDR ?
- MAC adresa? Kde je? Logy na switchi? Port?
- Evidence zařízení - EXCEL tabulka (je aktuální??)



Co to zkusiť jinak?



Grid Manager

Disconnect NOW if you have not been expressly authorized to use this system.

Username

Password

Login

A kliknu hledat...

Search

Basic

Advanced

IP Address

equals

172.27.32.25

Search

Reset

☐ Include Network Insight Devices and Interfaces

→

☐	NAME	TYPE	MATCHED PROPE...	MATCHED VALUE	IP ADDRESS /
☐	default/172.27.32.10-172.27.35.100	IPv4 DHCP Range	Contained Addr...	172.27.32.25	
☐	Internal/25.32.27.172.in-addr.arpa	PTR Record	Address	172.27.32.25	172.27.32.25
☐	172.27.32.25	DHCP Lease	Network View/I...	172.27.32.25	172.27.32.25
☐	Internal/s4174167.ct.czech-tv.cz	A Record	Address	172.27.32.25	172.27.32.25
☐	172.27.32.25	DHCP Lease	Network View/I...	172.27.32.25	172.27.32.25
☐	default/172.27.32.25	IPAddress	IP Address	172.27.32.25	172.27.32.25
☐	default/172.27.32.0/22	IPv4 Network	Contained Addr...	172.27.32.25	

ALT E

PRO

172.27.32.25 IPv4 Address 

Type:	A Record, Lease, PTR Record, IPv4 DHCP Range	MAC Address:	00:23:24:8a:ef:04
Comment:		Name:	s4l74167.ct.czech-tv.cz, S4L74167.ct.czech-tv.cz
		DHCP Fingerprint:	

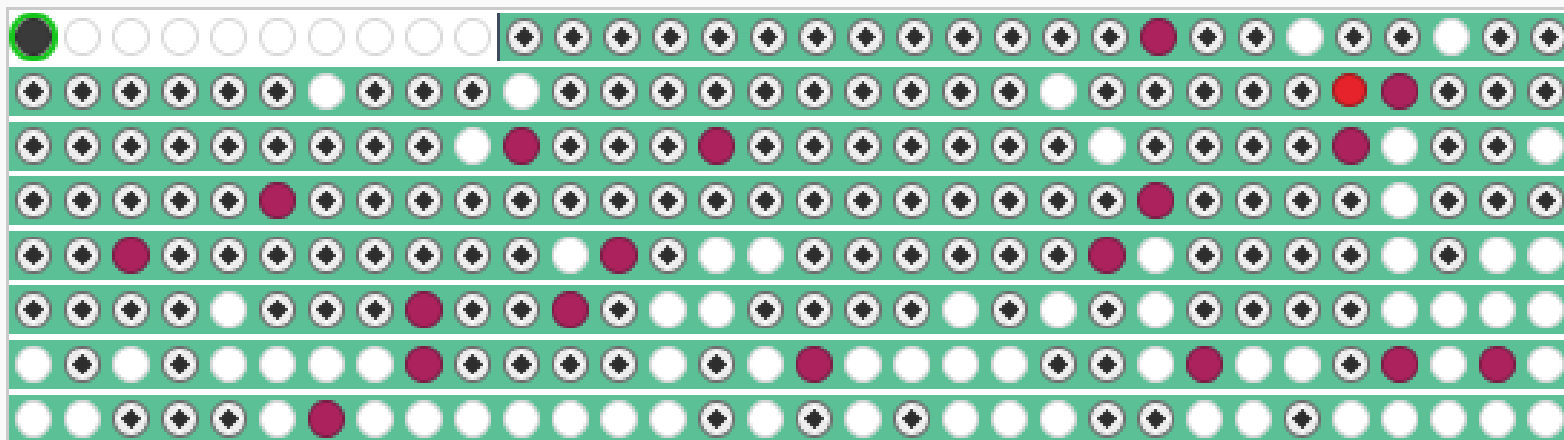
Discovered Data

NetBIOS Name:	OS: Microsoft Windows 7 (95%), Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2 (95%), Micros oft Windows 7 SP1 or Windows Server 2008 R2 (92%), Microsoft Windows Vista SP0 or SP1, Windows Serv er 2008 SP1, or Windows 7 (92%)
Discovered MAC Address: 00:23:24:8a:ef:04	Last Discovered: 2021-03-24 15:13:56 UTC
Task Name:	First Discovered: 2021-02-19 13:09:01 UTC
Discovered Name: unknown	Bridge Domain:
Tenant:	EPG:
Discoverer: Network Insight	Attached Device Address: 172.28.6.1
Attached Device Contact:	Attached Device Description: Cisco IOS Software, C2960S Software (C2960S-UNIVERSALK9-M), Version 15.2(2)E9, RELEASE SOFTWARE (fc4) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2018 by Cisco Systems, I nc. Compiled Sat 08-Sep-18 14:56 by prod_rel_team
Attached Device Location:	Attached Device Model: WS-C2960S-48TS-L
Attached Device Name: c2960s_	Attached Device Port Description: 802.1x
Attached Device Port Name: Gi1/0/41	Attached Device Port ID: 1766134930764336541
Attached Device Vendor: Cisco	Attached Device Port: 10141
Attached Device Type: Switch	BGP AS:
Device Contact:	Device Location:
Device Vendor:	Device Model:
Device Management IP: 172.27.32.25	Device Port Type:
Device Port Name:	Device Type(s): Windows
Port Duplex: Full	Port Link: Connected
Port Speed: 1G	Port Type: ethernet-csmacd
Port Status: Up	Open port(s): TCP:139 UDP:
VLAN Description:	VLAN Name: AD-TECH
VLAN ID: 222	VRF Name:

Jedno GUI

- DHCP server
- DNS server (nebo sync a integrace s MS)
- IPAM
 - Nahárda XLS tabulky
- API integrace s ***** (dosad'te si co potrebujete)
 - Service now, Extreme mngmt, Cisco ISE, CISCO catalyst center, Arista CloudVision, Huawei eSight,.....

IP Map [List](#)



172.27.32.0 - 172.27.32.255

Toggle Basic View

-  Unused
-  Conflict
-  Used
-  Pending
-  Unmanaged
-  Fixed Address / Reservation
-  DNS Object
-  Host Not In DNS/DHCP
-  Device
-  Active Lease
-  Selected IP Address
-  DHCP Range
-  DHCP Exclusion Range
-  Reserved Range

Takže pořádek...

- DHCP server
 - Přirazuje IP adresy a máme o všem záznam
- DNS server
 - Překlad mezi IP a DNS
- IPAM
 - Co je to za IP, kdo ji vlastní, kde je atd...
 - EXTENSIBLE ATTRIBUTE



Pořádek máme a můžeme řešit bezpečnost

DNS security

- Proč je DNS bezpečnost důležitá?
 - DNS client (PC)
 - DNS server (AD/MS/xxxx)
 - Firewall (něco hlídá)
 - Autoritativní DNS server (ten provede resolve)
- 80% malware používá DNS k aktivaci a komunikaci
- Lze je zarazit dříve než XDR

Příklady

- g63uar2ejiq5tlrkg3zez2fkemc6pi88tz.er.spotify.com
- 4rzjp8zy7i7vawluximoxrko1p2tn58gj0fjjj2g.p.03.s.sophosxl.net
- p2.a22a43lt5rwfg.ihg5ki5i6q3cfn3n.191742.i1.ds.ipv6-exp.l.google.com
- a1294.w20.akamai.net
- dnn506yrbagrg.cloudfront.net
- A98dc034c7781a941ebabac02262202668bbe918ea9fb5289cd2.r58.cf2.rackcdn.com

Report na klienta

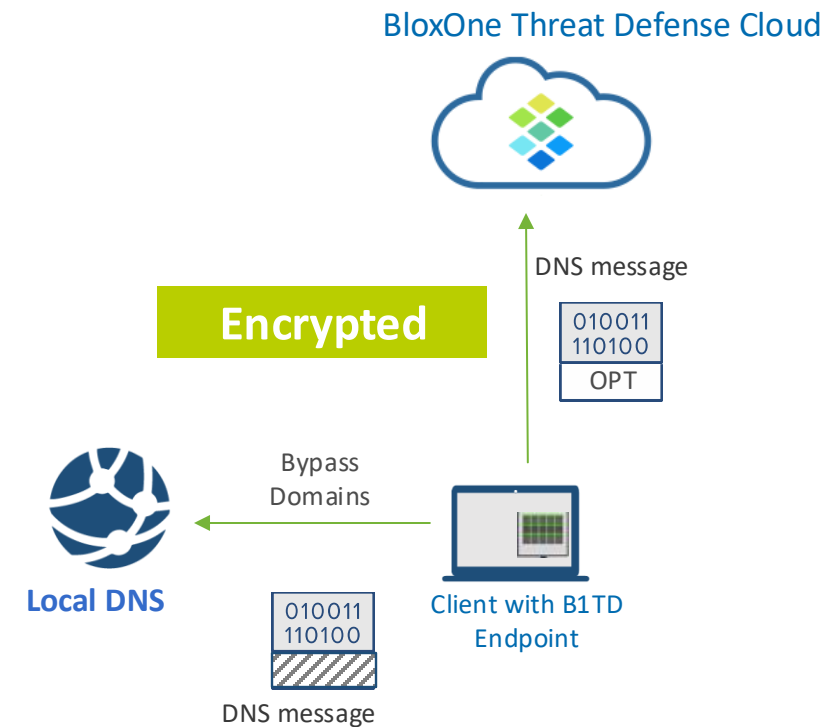
- Jak toto najdu v logách DNS na MS?

Malicious Activity by Client

	Client ID ↕	# Hits ↕	Domains ↕	Last Active ↕
1	172.16.10.51 / rs-czce-0001	290	cash-ldt.info chansouri-halist.com skypedataprdcoleus04.cloudapp.net	03/24/2021 16:00:00
2	10.10.14.84 / r1-czce-0084.	97	skypedataprdcoleus04.cloudapp.net	03/24/2021 14:40:00
3	10.10.14.59 / r1-czce-0059.	64	skypedataprdcoleus04.cloudapp.net	03/24/2021 16:00:00
4	10.10.14.18 / r1-czce-0018.	39	skypedataprdcoleus04.cloudapp.net	03/24/2021 16:10:00
5	10.10.14.44 / unknown	39	skypedataprdcoleus04.cloudapp.net	03/24/2021 16:00:00
6	10.10.14.90 / r1-czce-0090.	32	skypedataprdcoleus04.cloudapp.net	03/24/2021 16:10:00
7	10.10.14.185 / unknown	31	skypedataprdcoleus04.cloudapp.net	03/23/2021 15:10:00
8	10.10.14.65 / r1-czce-0065.	30	skypedataprdcoleus04.cloudapp.net	03/24/2021 15:40:00
9	10.10.14.95 / r1-czce-0095.	30	skypedataprdcoleus04.cloudapp.net	03/24/2021 12:30:00
10	10.10.14.159 / rw-czce-0009	29	chansouri-halist.com skypedataprdcoleus04.cloudapp.net	03/23/2021 15:00:00

Ochrana i mimo síť

- Uvnitř:
 - Vaše síť
 - Vaše pravidla
 - Váš firewall
 - Vaše DNS
- Mimo síť (HO/remote office)
 - Permanent VPN
 - Full Tunnel VPN
 - Nebo?



Scenario: Roaming device using B1TD Endpoint Agent (in hotel, at home etc.) without VPN

Thank you

www.altepro.cz

Tomas.zloch@altepro.cz



ALTEPRO solutions a.s.
Na Maninách 1092/20, Praha 7



+420 220 611 111
info@altepro.cz

