Výzvy kybersecurity dneška a možnosti jejich pokrytí

EDR, XDR,
MDR, MXDR

Ochrana koncových zařízení a prostředí organizací a firem před malwarem a dalšími hrozbami/aktivitami kyber útočníků.

Ochrana vlastního prostředí a služby zákazníkům

javora@tisp.cz
www.antihacker.cz
www.linkedin.com/in/josefjavora/

bit.ly/EdrHeimdal

Ochrana koncových bodů proti malwaru a aktivitám hackerů

- Je součástí řady norem (ISO 27000, GDPR, NIS-2, ...)
- Mylně si ji spojujeme s antivirovou ochranou
- Normy nezmiňují způsob, ale nutnost ochrany
- Pokud antiviry nejsou efektivní, je třeba hledat jinde
- Skutečnost, že antiviry nefungují efektivně potvrzují statistiky:
  - Vysoká penetrace AV v IT prostředí jednotlivců i firem (99%)
  - Rostoucí úspěšnost hackerských útoků i výše škod

Kdy systémy EDR vznikly?

- Definice v roce 2013 (Anton Chuvakin / Gartner)
- Rozvoj od roku 2014
- Reakce na hackery, kteří získali schopnost obcházet AV ochranu

Jak útočníci obcházejí AV ochranu?

- Více způsoby:
  - jednoduchou kompilací malwaru v zakoupené sadě (změna zdrojového kódu, aby se malware odlišil od verze, kterou má AV v databázi)
  - extrémně jednoduchou funkcionalitou: cílem malwaru je navázat s útočníkem komunikaci (Teamviewer z příkazového řádku)
  - nepoužitím malware: vstup přes zranitelnost, e-mail nebo vzdálený přístup a pracuje ručně (SSH)
  - nejde o nic sofistikovaného- dnes postačí naučit se pár příkazů, které si osvojí denní praxí…

Jak na to reagují dodavatelé antivirů?

- Dovybavením AV dodatečnými nástroji ochrany
  - proti šifrování
  - IDS, IPS
  - Ochrana před škodlivými URL
- Většina nástrojů je založena na znalosti existující (známé) hrozby
- Reaktivní ochrana

Jak na to reagují dodavatelé antivirů?

- Dovybavením AV dodatečnými nástroji ochrany
  - proti šifrování
  - IDS, IPS
  - Ochrana před škodlivými URL
- Většina nástrojů je založena na znalosti existující (známé) hrozby
- Reaktivní ochrana
- NEJŠKODLIVĚJŠÍ HACKERSKÉ ÚTOKY MAJÍ NA SVĚDOMÍ NEZNÁMÉ HROZBY

Co je systém EDR?

- Endpoint Detection and Response- systém pro detekci hrozeb na úrovni koncového bodu a schopnost reakce na incident:
  - Kódový skener: Next-Gen antivirus hledá známé hrozby), které existují i dnes
  - Automatizovaná správa zranitelností pro pokrytí nejběžnějších vektorů útoku mimo viry/malware
  - Vrstva pro detekci aktivit útočníka na koncovém bodě pro jeho odhalení při překonání NGAV a správu zranitelností
  - Správa privilegovaných účtů- proti zneužití administrátorských oprávnění (a ovládnutí zařízení)
- Vše v komplexním balíku se společnou správou a propojenou reakcí s možností zapojení dohledu a přidání dalších vrstev ochrany.

Co je systém EDR? – PROAKTIVNÍ ochrana

- Endpoint Detection and Response - systém pro detekci hrozeb na úrovni koncového bodu a schopnost reakce na incident:
  - Kódový skener: Next-Gen antivirus hledá známé hrozby), které existují i dnes
  - Automatizovaná správa zranitelností pro pokrytí nejběžnějších vektorů útoku mimo viry/malware
  - Vrstva pro detekci aktivit útočníka na koncovém bodě pro jeho odhalení při překonání NGAV a správu zranitelností
  - Správa privilegovaných účtů - proti zneužití administrátorských oprávnění (a ovládnutí zařízení)
- Vše v komplexním balíku se společnou správou a propojenou reakcí s možností zapojení dohledu a přidání dalších vrstev ochrany.

Antivirus vs EDR systém

Antiviry jsou nadále schopny chránit proti tzv. známým hrozbám (databáze)

Dnešní nejškodlivější hrozby (nevyjímaje kryptoviry / ransomware) působí jako tzv. neznámé hrozby. Na ty už je antivirus krátký.

To platí i pro Next-Gen AV nebo AV s přídavnými vrstvami ochrany.

EDR systémy mají za úkol chránit uživatele a organizace proti neznámým i známým hrozbám.

Antivirus vs EDR systém

Pokud ale antiviry v tomto selhávají:

Proč nejsou EDR systémy nasazeny všude?

IT správci vědí o neefektivitě AV
...a že EDR situaci řeší. Mají ale za to, že:

- jde o drahý…
- a komplikovaný způsob ochrany…
- náročný na nasazení a správu…,
- který pro účinné využití potřebuje odborný SoC.

Často uváděný důvod vysvětlení, proč se daná organizace adekvátně nechrání

IT správci vědí o neefektivitě AV
…a že EDR situaci řeší. Mají ale za to, že:

- jde o drahý… pořizovací náklady
- a komplikovaný způsob ochrany… provozní náklady
- náročný na nasazení a správu…, náklady na správu
- který pro účinné využití potřebuje odborný SoC náklady na dohled

Skokový rozdíl v celkových nákladech na vlastnictví oproti antivirové ochraně

Často uváděný důvod vysvětlení, proč se daná organizace adekvátně nechrání

Jak to řeší Heimdal?

- Rozsáhle využívá AI a ML => eliminace překážek
  - Jednoduché a rychlé nasazení (zvládne každý správce IT nebo pokročilejší uživatel)
  - automaticky hlásí a blokuje drtivou většinu hrozeb
  - při minimálním počtu falešně pozitivních záchytů.
  - Nemá-li chráněný subjekt potřebu dohledu, není nezbytný
- Výsledek: útočník svoje aktivity zaměří na snadnější cíl

Antivirus Next-Gen AV EDR systém

Stavba ochrany endpointu
AV-EDR-XDR-MXDR

<– D-10 let

antivirus

Stavba ochrany endpointu
AV-EDR-XDR-MXDR

–> D-10 let –> současnost

antivirus

Stavba ochrany endpointu
AV-**EDR**-XDR-MXDR

–> D-10 let –> současnost

kódový skener

Patch&Asset Management

DNS Security

Stavba ochrany endpointu
AV-**EDR**-XDR-MXDR

+ aset management

+ logování událostí

+ řízení GPO

–> D-10 let –> současnost

+ windows systémy
+ 210 aplikací třetích stran

+ správa firewallu

+ ochrana proti brute-force attack

kódový skener

Patch&Asset Management

DNS Security

+ Blokuje na HTTP, HTTPS, DoH

+ Intrusion Detection

+ sleduje procesy

Stavba ochrany endpointu
AV-**EDR**-XDR-MXDR

–> současnost –>

+ odstraní lokální adminy

+ umožní elevaci oprávnění těm, kterým to povolíme

kódový skener

Patch&Asset Management

DNS Security

Privilege Access Mngmt

Stavba ochrany endpointu
AV-**EDR**-XDR-MXDR

–> současnost –>

EDR

Stavba ochrany endpointu
AV-EDR-**XDR**-MXDR

–> současnost –> +

EDR

Application Control

DNS Security Network

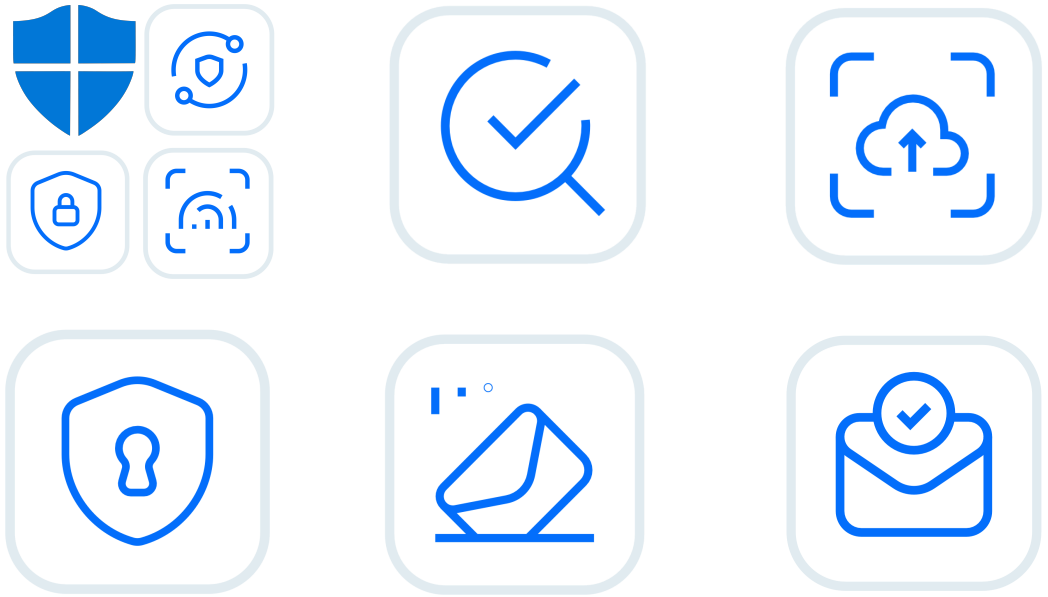
Ransomware Enc. Protection

Email Protection

Email Fraud Prevention

Stavba ochrany endpointu
AV-EDR-**XDR**-MXDR

–> současnost –> +

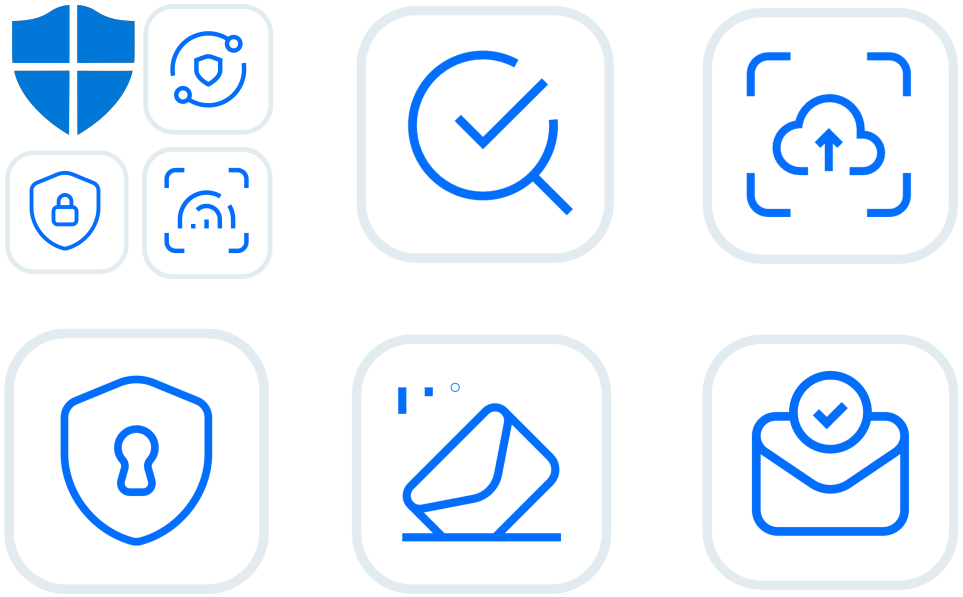


XDR

Stavba ochrany endpointu
AV-EDR-XDR-**MXDR**

–> současnost –> +++

Managed
Service



MXDR

- Vlastní dohled
- Služba SoC
- MDR Heimdal

Stavba ochrany endpointu
AV-EDR-**XDR**-MXDR

–> současnost –> +

EDR

Application Control

DNS Security Network

Ransomware Enc. Protection

Email Protection

Email Fraud Prevention

Ochrana perimetru

DNS
Security Network

- Vrstva pokročilé detekce komunikujících hrozeb
- Hybrid DNS technologie (HTTP, HTTPS, DoH)
- Výhodné pro ochranu OT/IoT zařízení,
  která se chrání obtížně
  - antiviry na pro operační systémy OT/IoT neexistují
  - systémy řízení zranitelností neexistují (v lepším případě se hlídají změny)
  - moderní hrozby (komunikující) se nevyhnou komunikaci DNS
  - levný a účinný nástroj pro ochranu OT/IoT
  - chrání veškerá zařízení v perimetru bez ohledu na OS (např. hostovská zařízení a mobily)

Rozšiřitelnost (další vrstvy ochrany)

- Důležitý požadavek pro řízení informační bezpečnosti a schopnosti reakce na novou situaci
- Heimdal nabízí celkem 11 vrstev ochrany spravovatelné v jediném dashboardu s jednou podporou *(výhodnější než skládání nezávislých řešení)*
  - Integrace jednotlivých vrstev od různých výrobců do 1 systému je náročná
  - Zvyšuje to nároky pro nasazení, provoz i dohled
- Rozšířením o ochranu perimetru vznikne XDR nebo se servisem MXDR

Limity ochrany systémem EDR

- Každá ochrana má svoje limity
  - Cílené útoky
  - Dobře motivovaní útočníci
  - Útočník najde vnitřního nepřítele (EDR pomůže i tak...)
  - Nejde o běžné útoky, ale špičku ledovce
- Systémem EDR se chrání i prvky kritické infrastruktury (dovybavují se dalšími systémy)

Možnost vyzkoušení formou POC

- Proof of Concept
- Nasazení do plného provozu na 30 dní
- Ověření při provozu v plné funkcionalitě (a ochraně) od prvního dne
- Ověří se kompatibilita i komfort a se nároky na provoz

Ocenění

- Četná ocenění v zahraničí (web heimdalsecurity.com)
- V ČR:
  - BusinessIT
  - „Pozoruhodný produkt pro rok 2024“
  - v kategorii Řešení pro bezpečnost

Jak se systém nasadí

- Zajistíme přístup do Dashboardu (rozhraní k cloudu Heimdal)
- z Dashboardu si stáhneme instalační balíček
- licenční klíč zkušební (po zakoupení komerční)
- Instalací balíčku a zadáním klíče se endpoint přiřadí a zobrazí v systému
- V něm se pak definují skupinové politiky a nastaví parametry ochrany
- ...a probíhá správa, detekce incidentů, nastavení reportů apod.

Jak vypadá provoz

- V dashboardu vidíte incidenty a získáte schopnost je řešit
  - vlastními silami nebo přes podporu Heimdal
- Vidíte veškeré endpointy, jejich parametry, řadu detailů a stav bezpečnosti
- Spravujete nastavení, vč. nastavení automatických aktualizací a jejich kontroly

Možnost využití Remote Access

- Pro pomoc nebo kompletní správu IT
- Remote Access od Heimdal používá stejný dahsboard pro správu a MFA
- Výhodné licencování pro servis

Děkuji za pozornost!

Na pokročilou hrozbu
použijeme
pokročilou ochranu

Vyzkoušejte adekvátní zbraně
odpovídající zbraním útočníků!

javora@tisp.cz
Josef Javora / TIS partners, s.r.o.
www.linkedin.com/in/josefjavora/

bit.ly/EdrHeimdal