S VYLEPŠENÝMI NÁSTROJI I PROTI POKROČILÝM HROZBÁM

ANTIVIR ANI BĚŽNÁ OCHRANA KONCOVÝCH BODŮ UŽ NESTAČÍ

Tradiční antivirové programy jsou schopny na koncových bodech vyhledávat a eliminovat škodlivé soubory a reaktivně tak poskytovat ochranu proti známým útokům. Jakýkoliv neznámý soubor je jimi ale považován za neškodný. Zároveň nedokáží reagovat na útoky zneužívající neznámé zranitelnosti, nebo útoky, které používají legitimní prostředky operačního systému napadeného zařízení k dosažení cíle útočníka.

Tradiční systémy ochrany koncových bodů (EDR) nabízejí oproti antiviru výrazně pokročilejší formy detekce a reakce. Jsou schopny detailně zmapovat a zaznamenat veškeré aktivity, ke kterým na koncových bodech dochází a na základě těchto dat detekovat bezpečnostní události. K dokonalé detekci jim ale stále chybí klíčová část, kterou je **kontext**. K datům ze samotných koncových bodů je nezbytné doplnit mj. informace ze síťového provozu, cloudu, autentizačních služeb a Threat Inteligence.

POTŘEBA CHRÁNIT MODERNÍ INFRASTRUKTURU

Dnešní doba přináší raketový nástup moderních technologií, které ovšem znamenají výrazné zvýšení plochy pro útok. Typickým příkladem je využití kontejnerů, jejichž zabezpečení je zpravidla opomíjeno. Bezpečnostní nástroje si musí poradit i s touto výzvou.

BEZPEČNOST NÁROČNÁ NA PROVOZ I ZNALOSTI

Potřeba sledovat velké množství zařízení v hybridním prostředí vede společnosti k investování do velkého množství stále robustnějších bezpečnostních nástrojů náročných na nasazení i následný provoz. Sledování mnoha různých konzolí a požadavky na znalosti a zkušenost operátorů vyžadují dlouhodobý trénink a jsou spojeny s vysokým stresem. To s sebou následně nese nebezpečí fluktuace zkušených specialistů a odliv těžce získávaného know-how.

SIEM – ROBUSTNÍ ALE I OBTÍŽNĚ UDRŽITELNÝ

SIEM a jeho schopnost integrovat data z dalších systémů jako NTA, UEBA, či EDR bývají stále ještě vnímány jako nejsilnější nástroje pro práci bezpečnostních týmů.

Používají ale velké množství nesourodých vstupních dat, která je třeba korelovat, což je náročné na zkušenosti a znalost prostředí. I přes veškerou snahu tyto systémy generují velká množství incidentů, často falešně pozitivních. Část z nich se z důvodu chybějících kapacit nepodaří vyhodnotit a druhá část postrádá detaily potřebné k plnému pochopení rozsahu události. Odhalit s jejich pomocí sofistikovaný útok kombinující několik technik a přístupů je tak velmi obtížné.

XDR POMŮŽE K LEPŠÍ DETEKCI A K MODERNIZACI ČINNOSTI SECURITY TÝMŮ

Moderní XDR systémy jsou novou generací prevenčních a dohledových nástrojů a přesahují možnosti jiných bezpečnostních řešení, protože dokáží centralizovat a korelovat data z více prostředí za účelem ověření známých i neznámých hrozeb, posílení viditelnosti a snížení falešných poplachů nebo výstrah. Za pomoci strojového učení a s využitím umělé inteligence umožňují nahradit složité nastavování korelačních pravidel rychlými automatizovanými reakcemi. To napomáhá k lepší detekci pokročilých útoků přetrvávajících v čase a kombinujících různé metody průniku. Zároveň to zvyšuje efektivitu a operabilitu bezpečnostních týmů a přispívá to k možnosti zapojení i juniorních operátorů do prvoúrovňového posuzování incidentů.

U 70% ZÁKAZNÍKŮ SE PO NASAZENÍ NOVÉHO MONITOROVACÍHO NÁSTROJE NAJDE NĚJAKÁ SKRYTÁ HROZBA JAKO NAPŘ. MALWARE, KTERÉ SE PODAŘILO OBEJÍT STÁVAJÍCÍ BEZPEČNOSTNÍ KONTROLY.

CO OD NÁS MŮŽETE OČEKÁVAT:

Zajistíme nasazení vylepšené ochrany pro koncové body, která je součástí **špičkové next-generation platformy pro detekci a zamezení bezpečnostním hrozbám** od předního světového poskytovatele řešení pro kybernetickou bezpečnost. Integruje kromě nejkomplexnější **ochrany koncových bodů** i **data ze síťového provozu, cloudu a třetích stran.**

Zprovoznění řešení je možno zajistit **v řádu několika dnů**, v případě krizové situace (např. v průběhu zjištěného probíhajícího útoku) **i během několika hodin**.

KLÍČOVÉ FUNKCE:

- **VYSPĚLEJŠÍ OCHRANA KONCOVÝCH BODŮ**
Lokální analytický engine založený na umělé inteligenci, behaviorální Threat Protection k blokování škodlivých akcí nebo kombinací chování, modul k ochraně proti ransomware nebo zcizení identifikačních údajů, USB device management
- **DETEKČNÍ A INVESTIGAČNÍ SCHOPNOSTI**
Automatizované propojení dat z koncových bodů, sítě, cloudu i identit, využití machine learning pro behaviorální a identity analýzy, analýzy časové osy výstrah, propojení Threat Inteligence s aktivním Threat Hunting
- **SCHOPNOST AUTOMATICKÉ ODEZVY**
Konzole pro vzdálený přístup ke koncovým bodům umožňující v případě napadení dynamický zásah s využitím funkcí jako izolace zařízení od části sítě, karantény pro soubory a funkce odstranění závadných souborů, ukončování procesů
- **FUNKCE PRO ŘÍZENÍ A VYKAZOVÁNÍ**
Intuitivní webový uživatelský portál, grafické reporty a nastavitelný dashboard, e-mail a slack notifikace, přeposílání systémových logů, auditní logy

MANAGED XDR

K dosažení maximálního efektu z nasazení XDR řešení je třeba zajistit **kontinuální vyhodnocování zjišťovaných událostí v nepřetržitém provozu**. Proto je vhodná kombinace se službami řízené bezpečnosti (MDR - Managed Detection and response service). Operátoři našeho **Security Operations Center (SOC)** jsou k dispozici pro spolupráci s Vaším bezpečnostním týmem ale i k „full managed“ službě pro zajištění nepřetržitého dohledu v režimu **24/7/365**.

24/7/365

Nepřetržitý provoz.

8.640 hodin práce operátorů centra měsíčně.

+60 %

Díky AI dokážeme zvýšit efektivitu provozu o 60 % oproti provozu pouze s lidskými operátory.

-85 %

Zkrátíme čas detekce bezpečnostních incidentů o 85 % oproti SOC spouze denním provozem (8x5).

VE VÝSLEDKU ZÍSKÁTE...

- ...**ochranu** i proti novým typům sofistikovaných cílených útoků s nasazením v řádu několika dnů i hodin
- ...**zjednodušení** bezpečnostní operativy a lepší vizibilitu napříč celým IT prostředím firmy včetně cloudu – sjednocení pod jeden nástroj s jednou konzolí od jednoho dodavatele
- ...**zapojení** a lepší využití i junior operátorů
- ...**s Managed XDR** i řízenou implementaci, precizní nastavení a **24/7/365 podporu** v podobě stálého dohledu

PROČ BYSTE SI MĚLI VYBRAT PRÁVĚ NAŠE ŘEŠENÍ.

Námi nabízená technologie se už čtvrtým rokem umisťuje na vrcholu žebříčku poskytovatelů v **MITRE ATT&CK Evaluation**.

Pro poskytování našeho řešení máme vysokou kvalifikaci. **Thein Security** je držitelem nejvyšší dodavatelské certifikace **Diamond Innovator** a zároveň je jediným **autorizovaným servisním centrem** pro ČR a SR.

Disponujeme týmem **expertů s dlouholetými zkušenostmi.** Od roku **2010** patříme k průkopníkům kybernetické bezpečnosti se zaměřením na **prevenci úniku citlivých dat**, obrany proti **sofistikovaným útokům**, detekce neznámého **malwaru** a aktivní ochrany proti **útokům DDoS**. Dodáváme služby a technologie do **hybridních prostředí** (on prem / cloud) a specializujeme se na **Zero Trust přístup.**

STANEME SE VAŠÍM PARTNEREM PRO OBLAST KYBERNETICKÉ BEZPEČNOSTI.

Pro více informací o ochraně serverů a koncových stanic a o službách řízené bezpečnosti kontaktujte naše obchodní zástupce na obchod.security@thein.eu nebo navštivte naše webové stránky.

Thein Security s.r.o., Pikrtova 1737/1a, 140 00 Praha 4 – Nusle, e-mail: info.security@thein.eu
Společnost vedená u Městského soudu v Praze oddíl C, značka 109813, IČO: 27415546, DIČ: CZ27415546

www.theinsecurity.eu