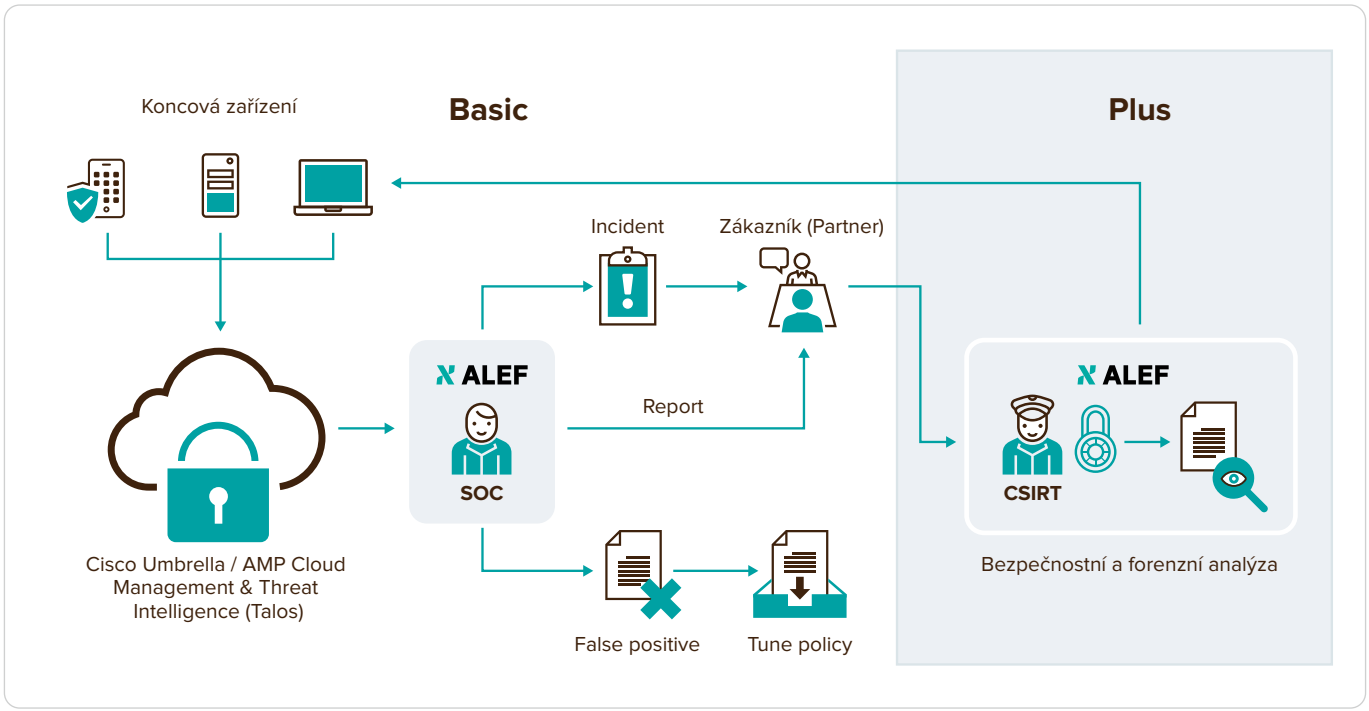
ALEF

ALEF OctoShield

Basic & Plus

Hlavním účelem služby ALEF OctoShield je zajistit vyšší standard zabezpečení koncových zařízení, která jsou připojená do vaší sítě nebo se připojují odkudkoliv do internetu. S naší službou budete chráněni před naprostou většinou škodlivého softwaru, který používají útočníci pro kybernetické útoky.

Využíváme kombinaci cloudových produktů společnosti Cisco Systems – Advanced Malware Protection (AMP) a Umbrella, jejichž funkce přesahují běžné antivirové programy. Společně s bezpečnostním monitoringem společnosti ALEF pak zajišťujeme zákazníkům velice silnou a nepřetržitou obranu před bezpečnostními incidenty.



Trust the Strong

ALEF Distribution CZ, s.r.o. | Pernerova 691/42, 186 00 Praha 8, Česká republika | Phone: +420 225 090 240
cz-sales@alef.com | www.alef.com

ACCREDITED BY TRUSTED INTRODUCER

cisco Partner
Distribution Partner

ALEF

Co služba obsahuje

- Nepřetržitou ochranu koncových uživatelských zařízení pomocí moderních cloudových produktů společnosti Cisco Systems — Antimalware Protection for Endpoints (dále AMP4E) a Umbrella.
- Rychlé a velice účinné zastavení kybernetického útoku na koncová zařízení, ať jsou připojená do internetu přes vaši síť nebo mimo ni.
- Důkladné objasnění kybernetických útoků na koncová zařízení a doporučení, jak útokům příště předcházet.
- Spolupráci našich odborníků při realizaci preventivních opatření proti dalším útokům.

BEZPEČNOSTNÍ MONITORING NABÍZÍME VE DVOU VARIANTÁCH – BASIC A PLUS

ALEF OctoShield Basic

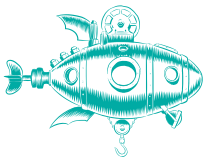
Součástí varianty Basic je:

- Prvotní aktivace AMP4E a Umbrella, kdy náš profesionální tým provede analýzu současného stavu zabezpečení vaší sítě a koncových zařízení, navrhne nejlepší možný scénář implementace těchto dvou cloudových produktů a vyladí je na míru.
- Nepřetržitá a automatická ochrana koncových zařízení před bezpečnostními útoky. Ochrana funguje i v případě, že uživatel pracuje mimo firmu např. při home-office.
- Průběžné monitorování a hodnocení vzniku bezpečnostních událostí, které zaznamená AMP4E a Umbrella na vašich koncových zařízeních bezpečnostním týmem ALEF Security Operations Center (SOC) v režimu 8×5.
- Základní analýza zaznamenaných bezpečnostních událostí na koncových zařízeních, zejména typu malware, command and control callbacks, cryptomining.
- Posílání pravidelných týdenních reportů s přehledem bezpečnostních událostí zjištěných na vašich koncových zařízeních.
- Předání informace o vzniku, dopadu a bezpečnostním riziku potvrzeného bezpečnostního incidentu i s návrhy, jak dál konkrétní situaci řešit.

ALEF OctoShield Plus

Tato varianta osahuje službu ALEF Incident Response:

- Řešení bezpečnostních incidentů včetně implementace nápravných opatření bezpečnostním týmem ALEF CSIRT, který je registrovaným členem mezinárodní organizace Trusted Introducer, zaměřené na kybernetickou bezpečnost.
- Hloubkovou analýzu škodlivého kódu odhaleného ve vaší síti týmem ALEF CSIRT.
- Security Scan tj. pravidelné preventivní denní nebo měsíční bezpečnostní skenování vaší komunikační a systémové infrastruktury specializovaným nástrojem, kdy vám dodáme přehled zranitelností vaší sítě a hodnocení jejich kritičnosti.



Trust the Strong

ALEF Distribution CZ, s.r.o. | Pernerova 691/42, 186 00 Praha 8,
Česká republika | Phone: +420 225 090 240
cz-sales@alef.com | www.alef.com

ACCREDITED BY TI TRUSTED INTRODUCER

CISCO Partner
Distribution Partner

ALEF

Cisco Umbrella

Technologie Cisco Umbrella je nenahraditelná jako první linie obrany vaší sítě proti internetovým hrozbám. Využívá k tomu základní stavební kameny internetu – DNS a IP vrstvu. Zabezpečením těchto dvou komponent pomocí tzv. reputace dokáže Umbrella zablokovat požadavky na závadné, či nežádoucí datové zdroje ještě před tím, než se spojení s nimi vůbec sestaví.

Umbrella je vhodná zejména pro koncové stanice pohybující se mimo firemní síť, která běžně poskytuje uživatelům centrální ochranu (tzv. roaming computers). Funguje jako bezpečná internetová brána, která využívá přesměrování DNS provozu na cloudové servery Cisco Systems, které díky pokročilé analytice a strojovému učení dokážou vyhodnotit, zda je dotazovaná doména bezpečná, závadná nebo podezřelá. Podezřelé domény navíc mohou být přesměrovány do cloudové proxy pro hloubkovou inspekci, jestli je i přenášený datový obsah (soubory, skripty atp.) bezpečný.

Celosvětová infrastruktura Umbrelly vyhodnocuje každý den více než 125 miliard DNS dotazů, což umožnuje unikátní trasování vztahů mezi doménami, IP adresami, sítěmi a malwarem v celém internetu. Podobně jako systémy firmy Amazon dokáží vytvářet vzorce nakupování zákazníků a předpovídat jejich další nákupy, Umbrella se učí z internetové aktivity uživatelů a vytváří vzorce k automatickému rozkrytí infrastruktury útočníka. Je tak připravená na další útoky a prediktivní blokaci všech jí známých datových zdrojů.

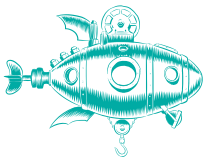
VLASTNOSTI CISCO UMBRELLA

- Redukuje infekce malwarem až o 98 %
- Umožňuje filtrovat až 60 různých kategorií domén
- Detekuje použití cloudových aplikací a zobrazí report jejich použití
- Brání únikům dat z vaší sítě a zařízení
- Chrání uživatele jak ve firemní síti, tak i mimo ni
- Pro vysoké zabezpečení koncových zařízení není zapotřebí jejich VPN připojení do firemní sítě

Cisco Advanced Malware Protection for Endpoints (AMP4E)

V rychle se rozvíjejícím světě malwaru jsou hrozby stále sofistikovanější a je čím dál těžší je odhalit. Nejpokročilejší 1% z těchto hrozeb by nakonec mohlo vstoupit do vaší sítě a zůstat tam nedetekováno. AMP4E však poskytuje komplexní ochranu i proti tomuto 1% hrozeb. Tento bezpečnostní software zabraňuje narušení zařízení, blokuje malware na vstupu a nepřetržitě sleduje a analyzuje aktivity souborů a procesů tak, aby dokázal rapidně detekovat a napravoval hrozby, které se mohou vyhnout obraně v první linii.

Jeho největší výhodou oproti tradičním antivirovým řešením je okamžitá reakce na hrozby (nestahují se žádné signatury) a blokování všech souborů, které jsou součástí malware kampaně, i když samy o sobě nevykazují žádnou špatnou aktivitu. AMP4E umožňuje tzv. **„Threat Hunting“**, což je nejmodernější způsob hledání příznaků kybernetického nebezpečí či probíhajícího útoku ve velkém množství dat z koncových zařízení.



Trust the Strong

ALEF Distribution CZ, s.r.o. | Pernerova 691/42, 186 00 Praha 8, Česká republika | Phone: +420 225 090 240
cz-sales@alef.com | www.alef.com

ACCREDITED BY TRUSTED INTRODUCER

cisco Partner
Distribution Partner

AMP4E Prevence

Reputace souborů – AMP Cloud obsahuje komplexní databázi každého souboru, který byl kdy prověřen, a jemu odpovídající dobrou nebo špatnou reputaci. Výsledkem je, že známý malware je rychle a snadno umístěn do karantény v místě vstupu do vaší sítě bez jakéhokoli skenování náročného na procesor.

Antivirus – AMP4E obsahuje též tradiční a neustále aktualizované antivirové signatury pro různé platformy (Windows, Mac nebo Linux). Antivirová databáze je umístěna lokálně v každém koncovém bodě, což znamená, že se při provozu nespoléhá na cloudové připojení. Tím je zajištěno, že vaše koncová zařízení jsou chráněná online i offline.

Detekce polymorfního malwaru – Tvůrci malwaru často tvoří různé varianty stejného malwaru, aby se vyhnuli běžným technikám detekce. AMP4E dokáže detekovat tyto varianty nebo polymorfní malware pomocí tzv. digitálních otisků (loose fingerprinting). Každý digitální otisk podezřelého souboru bude dále porovnán s digitálními otisky známých rodin malwarů a pokud dojde k nalezení podstatné shody, je soubor ihned zablokován.

Analýza strojového učení – AMP4E je pomocí algoritmů trénován tak, aby se „naučil“ identifikovat škodlivé soubory a aktivitu na základě atributů známého malwaru. Funkce strojového učení v AMP4E jsou synchronizovány s komplexní databází Cisco Talos ™, která zajišťuje lepší a přesnější model analýzy. Společně může strojové učení v AMP4E pomoci detekovat dosud nezjištěný malware v okamžiku prvotního vstupu do vaší sítě.

Prevence proti zneužití exploitů (Exploit Prevention) – Stále častější jsou útoky typu „fileless attack“, kdy malware utočí na místo v paměti, kde je načtena aplikace. Tato funkce zabrání malwaru vložení instrukcí do paměti přes její zranitelnost.

Ochrana před skripty – AMP4E poskytuje lepší viditelnost spouštění skriptů nad koncovými zařízeními a pomáhá tak chránit před útoky založenými na skriptech, které jsou hojně používány malwarem. Kontrola nad spouštěním skriptů poskytuje další ochranu tím, že umožňuje modulu Exploit Prevention zabránit načítání určitých DLL knihoven na počítačích, jejíchž aplikace mají relevantní zranitelnost.

Behaviorální ochrana – Vylepšená analýza chování koncových bodů AMP4E nepřetržitě sleduje veškerou aktivitu uživatelů a koncových bodů a porovnává je v reálném čase se vzorky chování malware, které jsou dynamicky aktualizovány tak, jak se malware vyvíjí. Touto metodou je možné detekovat např. útoky typu „living-off-the-land“.

AMP4E Detekce

Ochrana před škodlivými aktivitami – AMP4E nepřetržitě sleduje veškerou aktivitu koncového bodu a poskytuje detekci za běhu a blokování abnormálního chování spuštěného programu v koncovém zařízení. Například když chování koncového zařízení indikuje ransomware, jsou detekované procesy ukončeny, což zabrání šifrování koncového bodu a zastaví útok.

Cloudové indikátory kompromitace – Talos je přední organizace zabývající se analýzou kybernetických hrozeb, která neustále analyzuje malware, aby objevila nové typy hrozeb a vytvořila behaviorální a forenzní profily pro vznikající hrozby, jinak známé jako Indicators of Compromise (IoC). Získaná forenzní data, jako jsou umístění souborů, jména procesů, nebo úpravy hodnot klíčů registru, mohou pomoci správcům nalézt systémy, u kterých již došlo ke kompromitaci systému.

Hostitelské IoC – Správci mohou psát své vlastní IoC pro použití v reakci na incidenty ke skenování indikátorů kompromitace v všech koncových stanic, na kterých je naistalován AMP4E. Vlastní IoC jsou psány v otevřeném standardním formátu (OpenIOC), což usnadňuje využití dat z jakýchkoli existujících informačních kanálů.

AMP4E Reakce

Vzhledem k neustále se zvyšujícímu počtu a rozmanitosti pokročilých hrozeb navržených tak, aby unikly preventivním opatřením, měl by být považován jakýkoliv pokus o narušení bezpečnosti za incident.

S tímto nastavením by měla být nasazena výkonná sada nástrojů, která pomůže snadno identifikovat infikovaná koncová zařízení a porozumět rozsahu útoku. Kromě více funkcí prevence a detekce nabízí AMP granulární viditelnost koncových zařízení a nástroje pro rychlou a efektivní reakci na bezpečnostní incidenty.

Endpoint forensics – Výkonné nástroje, jako je trajektorie souborů a trajektorie zařízení využívají schopnosti kontinuální analýzy AMP4E k zobrazení celého rozsahu útoku. AMP4E identifikuje všechny postižené aplikace, procesy a systémy k určení prvotní nákazy, stejně jako metodu útoku a místo nákazy. Tyto funkce vám pomohou rychle pochopit rozsah problému identifikováním všech cest (vektorů), které útočníci používají k získání přístupu do systému.

Dynamická analýza – AMP4E zahrnuje integrované vysoce bezpečné prostředí izolovaného prostoru, které využívá technologii Cisco Threat Grid a umožňuje analyzovat chování podezřelých souborů. Analýza souborů vytváří podrobné informace o souborech, včetně závažnosti chování, původního názvu souboru, snímků obrazovky při provádění malwaru a zachycení ukázkových paketů. Vyzbrojeni těmito informacemi budete lépe rozumět tomu, co je nezbytné pro zvládnutí ohniska a blokování budoucích útoků.

Viditelnost příkazového řádku – viditelnost do argumentů příkazového řádku pomáhá určit, zdali nejsou legitimní aplikace (včetně nástrojů systému Windows) zneužívány ke škodlivým účelům.

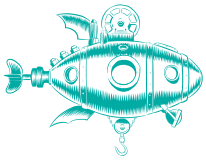
AMP4E může odhalit těžko detekovatelné chování, např.:

- použití vssadmin k odstranění stínových kopií
- deaktivaci bezpečného spouštění (safe boot)
- využívání PowerShellu,
- provádění eskalace privilegií
- úpravy seznamů řízení přístupu
- System enumeration.

Retrospektivní zabezpečení – AMP4E využívá patentovanou technologii, která automaticky odhaluje pokročilé hrozby, které se dostaly do vašeho prostředí. Díky nepřetržitému monitorování AMP for Endpoints koreluje nové informace o hrozbách s vaší minulou historií a automaticky ukládá soubory do karantény v okamžiku, kdy začnou vykazovat škodlivé chování. Tato automatizovaná reakce na nejnovější hrozby poskytuje rychlejší čas na detekci a výrazně snižuje šíření škodlivého softwaru.

Pokročilé vyhledávání – Pokročilé vyhledávání usnadňuje investigaci a hledání hrozeb tím, že poskytuje více než sto předem připravených dotazů, což umožňuje rychle spouštět složité dotazy na jakémkoliv (nebo všech) koncových zařízeních. To umožní získat hlubší přehled o tom, co se kdy stalo s jakým koncovým zařízením, díky pořízení snímku jeho aktuálního stavu. Ať už provádíte vyšetřování jako součást reakcí na incidenty, nebo hledání hrozeb, pokročilé vyhledávání vám rychle poskytne odpovědi, které potřebujete o svých koncových zařízeních vědět.

V případě dotazů nás neváhejte kontaktovat: cz-sales@alef.com



Trust the Strong

ALEF Distribution CZ, s.r.o. | Pernerova 691/42, 186 00 Praha 8,
Česká republika | Phone: +420 225 090 240
cz-sales@alef.com | www.alef.com

ACCREDITED BY TRUSTED INTRODUCER

cisco Partner
Distribution Partner