Microsoft Security

3 důvody pro přechod na integrovanou ochranu před hrozbami

Obsah

Úvodem

Průměrný podnik dnes používá více než 30 různých bezpečnostních nástrojů, často nesourodých a „přilepených“.

Zabezpečení se nachází ve zlomovém bodě. Kybernetické útoky jsou stále sofistikovanější, protože organizace se potýkají s různými problémy, od nedostatku talentů a vyrovnávání nákladů až po zvládání požadavků hybridní práce.

Současně je trh se zabezpečením roztříštěnější a složitější než kdykoli předtím. Průměrný podnik nyní používá více než 30 různých nástrojů zabezpečení, které jsou často nesourodé a „přilepené“. Poskytují bezpečnostním operačním centrům (SOC) omezenou viditelnost a nedostatečné přehledy.

Vedoucí pracovníci v oblasti zabezpečení a dodržování předpisů chtějí lépe porozumět nejnovějším rizikům a hrozbám, ale také potřebují vědět, co funguje, co ne a kde existují nedostatky.

Přestože se rozsah dnešních výzev v oblasti zabezpečení může zdát nepřekonatelný, pro CISO existuje důvod k optimismu, pokud chtějí zlepšit účinnost a efektivitu operací zabezpečení. Řešení spočívá v integrovaném, komplexním přístupu k ochraně před kybernetickými hrozbami, který pomůže organizacím v následujících oblastech:

Důvod č. 1: Lepší výsledky efektivněji

Konsolidace bodových řešení a snížení režie bezpečnostních operací (SecOps).

Důvod č. 2: Posílení schopnosti SecOps soustředit se na úkoly s vysokou hodnotou

Používání nástrojů, které zvyšují efektivitu a umožňují i junior analytikům pracovat lépe než kdykoli předtím.

Důvod č. 3: Zvyšování produktivity zaměstnanců

Ochrana organizace způsobem, který vašim pracovníkům umožní bez obav tvořit a inovovat.

Tento přístup je umožněn integrací řešení rozšířené detekce a reakce (XDR) s nativně cloudovou správou akcí a informací o zabezpečení (SIEM), která využívá umělou inteligenci (AI) a možnosti automatizace. Integrované řešení může pomoci SOC stát se prediktivnějším, proaktivnějším a preventivnějším vůči útokům v celém podniku.

Důvod č. 1

Lepší výsledky efektivněji

Díky konsolidaci nástrojů s integrovaným řešením Microsoftu můžete také ušetřit tím, že budete platit pouze za to, co používáte.

Mnoho organizací přistupuje k nástrojům zabezpečení tak, že se zaměřuje na nejlepší bodová řešení. Bohužel tento přístup může odborníkům na zabezpečení ztížit rychlou identifikaci hrozeb a reakci na ně. Může to mít také negativní dopad na výdaje na IT a produktivitu koncových uživatelů.

Vzhledem k tomu, že se organizace snaží zvládnout více s menšími náklady, může jim pomoci integrovaný přístup, jako je SIEM a XDR od Microsoftu. Konsolidace jednotlivých nástrojů může snížit složitost. Vzhledem k tomu, že se jedná o cloudové řešení, může integrované řešení také zlepšit výkon a škálování.

Díky konsolidaci nástrojů s integrovaným řešením Microsoftu můžete také ušetřit tím, že budete platit pouze za to, co používáte. Zvýšením automatizace a integrace můžete také snížit režijní náklady SecOps potřebné ke správě řešení.

> Zahájení procesu zavádění nových nástrojů zabezpečení je snadné, protože očekáváte, že nedostatky budou velké. Brzy zjistíte, že nástroje od různých dodavatelů se mohou potenciálně překrývat. Takové překrytí by mohlo být žádoucí z hlediska kontroly a rovnováhy, **ale mohlo by být spojeno s vysokými finančními náklady.**“
>
> **Jonathan Cassar**
> Chief Technology Officer, MITA

1,6 mil. USD

ušetřeno ročně díky konsolidaci dodavatelů

Společnost Microsoft pověřila společnost Forrester Consulting vypracováním studie TEI (Total Economic Impact™) a prozkoumáním potenciální návratnosti investic (ROI), které mohou podniky dosáhnout nasazením řešení SIEM a XDR od Microsoftu. Jednalo se o některá z klíčových zjištění pro hypotetickou složenou organizaci s celkovým počtem 8 000 zaměstnanců a 10 odborníků na zabezpečení:

- **Úspora téměř 1,6 milionu USD ročně díky konsolidaci dodavatelů.** Investice do řešení SIEM a XDR od Microsoftu umožňuje kompozitnímu řešení snížit náklady na předchozí SIEM (560 000 USD), související lokální infrastrukturu (přes 360 000 USD), tři bodová řešení XDR (192 000 USD) a průběžné náklady na práci při jejich správě (480 000 USD).
- **Snížení rizika závažného porušení o 60 %.** Díky efektivnějším pracovním postupům bezpečnostního vyšetřování a reakce, lepší automatizaci bezpečnostních reakcí a větší schopnosti chránit všechna počítačová prostředí, včetně ochrany multicloudových prostředí, snižuje kompozitní organizace riziko narušení a zároveň může uspořit 1,6 milionu USD ročně.
- **Návratnost investice ve výši 207 %.** Z reprezentativních rozhovorů a finanční analýzy vyplynulo, že organizace, která využívá kompozitní řešení, dosáhne během tří let zisků ve výši 17,68 milionu USD oproti nákladům ve výši 5,76 milionu USD, což dává dohromady čistou současnou hodnotu (NPV) ve výši 11,92 milionu USD.

Důvod č. 2

Posílení schopnosti SecOps soustředit se na úkoly s vysokou hodnotou

Je důležité integrovat SIEM a XDR, aby bylo možné korelovat výstrahy, stanovit priority největších hrozeb a koordinovat opatření v rámci celého podniku.

Týmy SecOps jsou zahlceny množstvím signálů, které musí analyzovat, včetně řady signálů s nízkou věrohodností, které je obtížné, nebo dokonce nemožné manuálně detekovat a zmírnit. Kvůli nárůstu hrozeb je pro přetížené SOC těžké udržet krok, zejména pokud se snaží analyzovat data z více bodových řešení. Vyčlenění dalších zdrojů na zaplnění mezer není řešením, protože trvalým problémem zůstává nedostatek kvalifikovaných odborníků v oblasti zabezpečení.

Proto je velmi důležité integrovat řešení SIEM a XDR, aby bylo možné korelovat výstrahy, určovat priority největších hrozeb a koordinovat opatření napříč podnikem. Pokročilá umělá inteligence a automatizace zajišťuje proaktivní detekci a nápravu hrozeb.

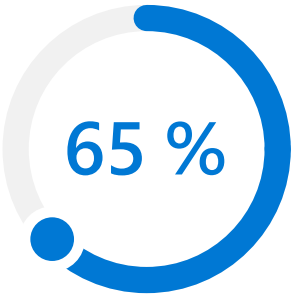
Vezměme například v úvahu, že tradiční systém SIEM nemusí věnovat velkou pozornost jedinému signálu nízké úrovně. Pomocí umělé inteligence by však cloudový SIEM mohl automaticky porovnávat tento signál se signály z jiných zdrojů v rámci celé organizace, korelovat napříč různými soubory dat a najít vícestupňové útoky.

Integrovaná řešení SIEM a XDR uvolňují zdroje SecOps a zároveň přináší více možností a jistoty i junior analytikům.

Systém normalizuje, analyzuje a koreluje data a zároveň poskytuje kontext o tom, jak se kybernetický útok dostal do infrastruktury, a obsahuje časovou osu jeho šíření. To umožňuje týmům SOC vizualizovat narušení – z jediné konzole – a efektivně ho řešit.

> Mnoho CISO si neuvědomuje, **jakou režii způsobuje svým týmům 20 různých skleněných tabulí** nebo bodových řešení a s tím spojené roční náklady… My jsme odstranili únavu z velkého počtu nástrojů prostřednictvím jediného dodavatele.“
>
> **Terence Jackson**
> Chief Information Security and Privacy Officer, Thycotic

Organizace by neměla potřebovat hluboké odborné znalosti, aby využila přínos bezpečnostního řešení. Integrovaná řešení SIEM a XDR uvolňují zdroje SecOps a zároveň přináší více možností a jistoty i junior analytikům.



Integrovaný přístup řešení SIEM a XDR od Microsoftu zkrátil dobu vyšetřování hrozeb o 65 %.

Studie Forrester Total Economic Impact™ (TEI), kterou si nechala vypracovat společnost Microsoft, ukázala tento druh efektivity SecOps v kompozitní organizaci:

- **Zkrácení doby vyšetřování hrozeb o 65 % a zkrácení doby reakce na hrozby o 88 %.** Integrovaný přístup řešení SIEM a XDR od Microsoftu k vyšetřování bezpečnostních rizik a reakci na ně zefektivňuje tyto pracovní postupy pro odborníky na zabezpečení kompozitní organizace. K identifikaci hrozeb již nemusí používat více nástrojů a funkce automatizace zabezpečení dále zlepšují pracovní postupy reakce.
- **Zkrácení času potřebného k vytvoření nového sešitu o 90 % a zkrácení času potřebného k nástupu nových odborníků na zabezpečení o 91 %.** Integrovaný přístup řešení SIEM a XDR od Microsoftu zefektivňuje i další pracovní postupy odborníků na zabezpečení. Vzhledem k tomu, že protokoly SIEM jsou integrovány do celé sady řešení, je tvorba sešitů téměř automatizovaná. Jediné přihlášení tak umožňuje novým odborníkům na zabezpečení nastoupit téměř o 16 týdnů rychleji.

Důvod č. 3

Zvyšování produktivity zaměstnanců

Integrované řešení SIEM a XDR může vaší organizaci pomoci zvýšit produktivitu koncových uživatelů.

Integrované řešení SIEM a XDR umožňuje zvládnout více s menšími náklady a zvýšit efektivitu SecOps. Navíc může vaší organizaci pomoci zvýšit produktivitu koncových uživatelů.

Jak týmy SecOps moc dobře vědí, když ztížíte zabezpečení, lidé ho obejdou. Pokud tedy prostředí pro koncové uživatele spíše snižuje produktivitu zaměstnanců, než aby ji zvyšovalo, může to organizaci vystavit větším rizikům v oblasti zabezpečení a vyšším nákladům. Slabá nebo ztracená hesla, nezabezpečený přístup přes osobní zařízení nebo neomezené sdílení citlivých dat představují jen některé z problémů.

> Dříve jsme používali hrubé nástroje, když měl někdo podezření na problém. Zavírali jsme služby a uzavírali přístup, což mělo negativní dopad na naše podnikání. A všem to bylo jasné, protože služby dočasně přestaly fungovat. Microsoft Sentinel představuje skalpel, kterým můžeme chirurgicky reagovat na to, co se děje. **Podnik obvykle ani neví, kdy na hrozbu reagujeme**, a to je opravdu důležité měřítko našeho úspěchu."
>
> **Rick Gehringer**
> Chief Information Officer, Wedgewood

Téměř

68 000

Řešení SIEM a XDR od Microsoftu zvýšila produktivitu ostatních zaměstnanců o téměř 68 000 hodin ročně.

Integrovaný přístup SIEM a XDR vám pomůže zajistit bezproblémové uživatelské prostředí, které udrží vaše pracovníky produktivní a zabezpečené ve všech aspektech jejich každodenní práce. Může snížit negativní dopady na produktivitu, jako je nutnost vypínat služby nebo izolovat a následně obnovovat počítače. Integrovaná řešení SIEM a XDR však mohou také vytvořit nové příležitosti pro zvýšení produktivity koncových uživatelů, například díky větší samoobslužné podpoře zabezpečení, lepším řídicím panelům a hlášením či větší odezvě a rychlejšímu spouštění díky menšímu počtu agentů zabezpečení.

Ve studii Forrester Total Economic Impact™ (TEI), kterou si nechala vypracovat společnost Microsoft, vykázala hypotetická kompozitní organizace s celkem 8 000 zaměstnanci zvýšení produktivity zaměstnanců díky nasazení řešení SIEM a XDR od Microsoftu:

- **Zvýšení produktivity ostatních zaměstnanců o téměř 68 000 hodin ročně.** Řešení SIEM a XDR od Microsoftu zabraňují negativním dopadům neefektivních procesů zabezpečení na ostatní zaměstnance. Například díky nové možnosti samoobsluhy pro IT profesionály, která zahrnuje aktualizace a doporučení v oblasti zabezpečení, ušetří kompozitní organizace 4 000 hodin ročně. Umožňuje také vzdálené řešení bezpečnostních problémů na počítačích zaměstnanců a snižuje počet agentů zabezpečení, kteří na nich běží. Tím se ročně ušetří téměř 64 000 hodin produktivity koncových uživatelů.

Zabezpečení se stalo základním předpokladem úspěchu v oblasti technologií. Proto organizace potřebují bezpečnostní opatření, která zajistí co největší odolnost proti moderním útokům, aby ochránily a umožnily produktivitu a inovace, které jsou hnací silou růstu.

Integrovaná ochrana před kybernetickými hrozbami pomocí SIEM a XDR

Tato integrace špičkových produktů poskytuje prevenci, detekci a reakci na kybernetické hrozby v jediném komplexním řešení.

Společnost Microsoft nabízí první a jediné integrované řešení SIEM a XDR, které poskytuje komplexní viditelnost napříč všemi cloudy a platformami. Tato integrace špičkových produktů poskytuje prevenci, detekci a reakci na kybernetické hrozby v jediném komplexním řešení.

Microsoft SIEM a XDR využívají sílu umělé inteligence a automatizace, stejně jako hluboké a trvalé investice do detekce a analýzy kybernetických hrozeb – s odbornými přehledy a viditelností 43 bilionů signálů každý den. Díky integraci těchto produktů mají týmy SOC k dispozici více souvislostí, aby mohly rychleji vyhledávat a řešit kritické kybernetické hrozby:

Microsoft Sentinel

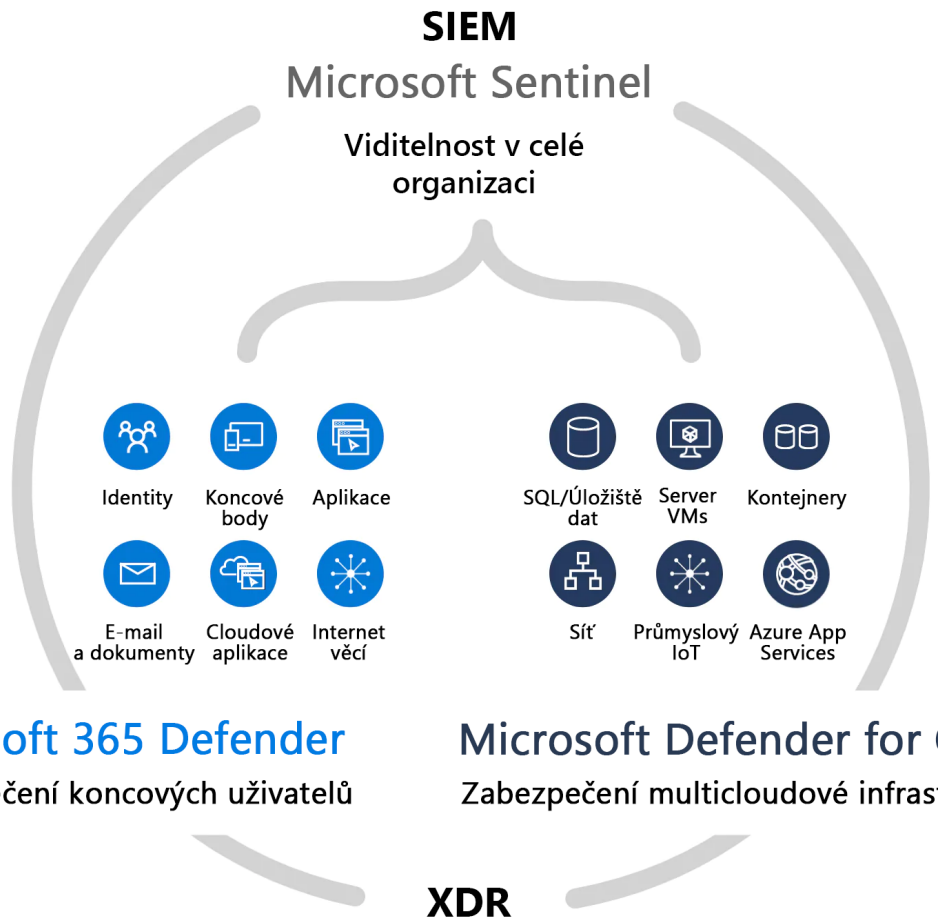
Prostřednictvím cloudového řešení SIEM od Microsoftu získáte přehled o celém podniku z ptačí perspektivy. Díky integrované orchestraci a automatizaci můžete agregovat data o zabezpečení z prakticky libovolného zdroje a použít umělou inteligenci k oddělení šumu od legitimních událostí, korelovat upozornění napříč komplexními řetězci útoků a urychlit reakci na kybernetické hrozby.

Microsoft Defender XDR

Pomocí funkcí XDR můžete předcházet kybernetickým útokům a odhalovat je napříč identitami, koncovými body, aplikacemi, e-maily, daty a cloudovými aplikacemi. Prostřednictvím připravené ochrany, která je nejlepší ve své třídě, můžete vyšetřovat kybernetické útoky a reagovat na ně. Z jediného řídicího panelu můžete vyhledávat hrozby a snadno koordinovat reakci.

Microsoft Defender for Cloud

Integrované funkce XDR chrání multicloudové a hybridní cloudové úlohy. Zabezpečte své servery, úložiště, databáze, kontejnery a další. Zaměřte se na to, co je nejdůležitější, díky výstrahám s prioritou.



Nepřilepujte zabezpečení. Integrujte ho.

Dejte správné nástroje a informace do rukou správným lidem. Chraňte se před moderními útoky pomocí komplexního cloudového a integrovaného řešení.

Další informace o integrované ochraně proti kybernetickým hrozbám pomocí řešení SIEM a XDR od Microsoftu >

Microsoft Security