COMGUARD SOPHOS

Sophos Managed Detection and Response

Bezpečnost v režii expertů výrobce šetří Vaše zdroje i nervy

Rozvoj kybernetických hrozeb a s tím související rizika jsou neustále na vzestupu. Útoky jsou často sofistikovanější a mají jasný impact na firemní aktiva. O úspěšnosti nebo neúspěšnosti takovýchto útoků často rozhodují nejen technologie, ale také rychlost reakce. Sophos MDR (Managed Detection and Response) je plně spravovaná služba 24/7 poskytovaná odborníky z řad SOPHOS, kteří odhalují a reagují na kybernetické útoky zaměřené na vaše počítače, servery, sítě, cloudové úlohy, e-mailové účty a další.

Ransomware a služby typu Breach Prevention – Potřeba neustálého dohledu a kontinuálně probíhajících bezpečnostních operací se stává nezbytností. Složitost moderních operačních prostředí a rychlost útočníků v rámci kybernetických hrozeb však pro většinu organizací stále více ztěžují situaci, aby si samy úspěšně řešili a řídili detekci a reakci. Se Sophos MDR expertní tým výrobce dokáže zastavit pokročilé útoky vedené lidmi a podniká kroky k neutralizaci hrozeb dříve, než mohou narušit Vaše obchodní operace nebo ohrozit Vaše citlivá data. Sophos MDR je přizpůsobitelný s různými úrovněmi služeb, kdy se můžete buď plně svěřit do rukou výrobce, anebo být pouze upozorňováni na podezřelé aktivity. MDR může být dodáváno buď prostřednictvím Sophos proprietární technologie nebo s využitím Vašich stávajících technologií kybernetické bezpečnosti.

Kybernetická bezpečnost poskytovaná jako služba

Díky rozšířeným schopnostem detekce a reakce za pomocí XDR (eXtended Detection and Response), které poskytuje úplné zabezpečení všude tam, kde jsou vaše data uložena, Sophos MDR může:

- Odhalit více kybernetických hrozeb, než dokážou bezpečnostní nástroje samy identifikovat. Sophos nástroje automaticky blokují 99,98 % hrozeb, což analytikům výrobce umožňuje soustředit se na „lov" těch nejsofistikovanějších útočníků, které dokáže odhalit a zastavit pouze vysoce vyškolený specialista.
- Podniknout kroky ve Vašem zastoupení, aby zabránili hrozbám, jakkoliv narušovat fungování firmy. Analytici výrobce odhalují, vyšetřují a reagují na hrozby v řádu několika minut – ať už potřebujete komplexní reakci na incidenty nebo pomoc s přesným rozhodováním.
- Identifikovat hlavní příčinu hrozeb, aby se předešlo budoucím incidentům. Sophos proaktivně přijímá opatření a poskytuje doporučení, která snižují riziko nákazy či útoku na Vaši organizaci.

Kompatibilní s kyberbezpečnostními nástroji, které již vlastníte

V rámci zavedení bezpečnosti na úrovni MDR Vám můžeme poskytnout technologii Sophos, kterou potřebujete a případně ještě nemáte, nebo mohou analytici výrobce využít Vaše stávající technologie kybernetické bezpečnosti k detekci a reakci na hrozby. Sophos MDR je kompatibilní s bezpečnostní telemetrií od výrobců jako např. Microsoft, CrowdStrike, Palo Alto Networks, Fortinet, Check Point, Rapid7, Amazon Web Services (AWS), Google, Okta, Darktrace a mnoho dalších. Telemetrická data jsou automaticky konsolidována, korelována a prioritizována s pomocí přehledů v rámci Sophos Adaptive Cybersecurity Ekosystem (ACE) a Sophos X-Ops.

Klíčové výhody SOPHOS MDR

- Nepřetržitá ochrana 24x7x365
- Redukce interních zdrojů
- Zvýšená ochrana proti ransomware a dalším pokročilým kybernetickým hrozbám
- Zkušený tým odborníků s vysokou mírou znalostí a zdrojů
- Rychlost reakce
- Přímý kontakt na support + dedikovaný leader
- Proaktivní doporučení + Root Cause analýza
- Breach Warranty Protection
- Externí „SOC"
- Redukce nákladů na školení
- Celkové snížení nákladů na kyberbezpečnost

Sophos MDR integrace

Bezpečnostní data z následujících zdrojů lze integrovat pro použití operačním týmem Sophos MDR. Zdroje telemetrie se používají k rozšíření viditelnosti napříč Vaším prostředím, generování nových detekcí hrozeb a zlepšení spolehlivosti stávajících detekcí hrozeb, provádění vyhledávání hrozeb a umožnění dalších možností reakce.

V rámci SOPHOS ekosystému lze (bez dalších nákladů) integrovat:

- Sophos XDR / Sophos Firewall / Microsoft Graph Security / Sophos Endpoint / Sophos Email / MS Office 365 Management Activity / Sophos Cloud / 90denní retence dat / Endpoint ochrana třetích stran (Trellix, Microsoft, Crowdstrike, SentinelOne, Symantec, TrendMicro a další)

Integrace dat z dalších produktů a z produktů třetích stran – Integrační balíčky:

- Sophos Network Detection and Response / Firewall / Identity / Public Cloud / Email / Network / Roční retence dat

COMGUARD communication security

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel. +420 513 035 400
info@comguard.cz | www.comguard.cz

COMGUARD SOPHOS

Sophos Managed Detection and Response

Sophos MDR nabízí různé úrovně služby a možnosti reakce na hrozby. Umožněte operačnímu týmu Sophos MDR, aby v plném rozsahu reagoval na incidenty, spolupracoval s vámi na řízení kybernetických hrozeb nebo informoval Vaše interní bezpečnostní operační týmy, kdykoli jsou hrozby zjištěny nebo je zaznamenána podezřelá aktivita. S pomocí silného expertního týmu SOPHOS můžete i Vy těžit z jejich know-how, globálního přesahu, technologii a informací, které Vám jako celek skýtají možnosti bezprecedentní úrovně ochrany. Společně se Sophosem dokážete reagovat na hrozby v řádu několika minut.

	Sophos Threat Advisor	Sophos MDR	Sophos MDR Complete
24x7 monitoring hrozeb a reakce na hrozby vedené expertním týmem výrobce	✓	✓	✓
Kompatibilita s non-Sophos bezpečnostními řešeními	✓	✓	✓
Týdenní a měsíční reporting	✓	✓	✓
Briefing na měsíční bázi „Sophos MDR ThreatCast“	✓	✓	✓
Sophos Account Health Check (identifikace a adresace konfiguračních chyb)		✓	✓
Threat hunting vedený expertním týmem výrobce		✓	✓
Blokace hrozeb: útoky jsou blokovány, prevence šíření • Využívá Sophos XDR agenta nebo Sophos XDR Sensor		✓	✓
Přímý tel. kontakt na support v průběhu aktivního incidentu		✓	✓
Plnohodnotná reakce na incident – hrozby jsou plně eliminovány • Vyžaduje Sophos XDR agenta			✓
Root cause analýza			✓
Dedikovaný kontakt na expertní tým výrobce (Incident Respons Lead)			✓
Breach Protection Warranty • Krytí škod až do výše 1 milionu USD			✓

24 x 7 x 365 monitoring hrozeb a reakce na hrozby – Sophos detekuje hrozby a reaguje na ně dříve, než mohou ohrozit Vaše data nebo způsobit výpadky. Sophos MDR, podporovaný šesti globálními bezpečnostními operačními centry (SOC), poskytuje nepřetržité pokrytí

Kompatibilita s bezpečnostními nástroji třetích stran – Sophos MDR dokáže integrovat telemetrii z koncového bodu třetí strany, firewallu, identity, e-mailu a dalších bezpečnostních technologií jako součást Sophos ACE.

Reakce na incident v plném rozsahu – Když je identifikována aktivní hrozba, operační tým Sophos MDR může Vaším jménem provést rozsáhlou sadu reakcí, aby na dálku narušil aktivitu útočníka, zadržel jeho další postup a následně zcela eliminoval útočníkovi další akce.

Reporting na týdenní nebo měsíční bázi – Sophos Central je váš jediný dashboard panel pro aletry v reálném čase, reporting a management. Týdenní a měsíční zprávy poskytují přehled o bezpečnostních vyšetřováních, kybernetických hrozbách a Vašem celkovém stavu zabezpečení.

Sophos Adaptive Cybersecurity Ecosystem – Sophos ACE automaticky předchází a zabraňuje škodlivým aktivitám, a expertnímu týmu umožňuje hledat i ty nejmenší signály pro hrozby, které vyžadují lidský zásah, aby byly detekovány, vyšetřeny a eliminovány.

Threat Hunting vedený expertním týmem výrobce – Proaktivní vyhledávání hrozeb prováděné vysoce vyškolenými analytiky odhalí a rychle odstraní více hrozeb, než mohou bezpečnostní produkty samy detekovat. Operační tým Sophos MDR může také používat telemetrii od dodavatelů třetích stran při hledání hrozeb a identifikaci chování útočníků, které uniklo detekci z nasazených sad nástrojů.

Přímé volání na support (direct calls) – Váš tým má přímý „call-in“ přístup k Sophos Security Operations Center (SOC) pro kontrolu potenciálních hrozeb a aktivních incidentů. Operační týmy Sophos MDR jsou k dispozici 24/7/365 a jsou rozloženy na 26 místech po celém světě.

Dedikovaný kontakt pro řešení incidentů – výrobce Vám poskytuje dedikovaného specialistu, který funguje jako garant, průvodce a incident response leader v jedné osobě. Ten bez prodlení reaguje a spolupracuje s Vaším interním týmem a případně s externím týmem partnera (partnerů), a to až do úplného vyřešení incidentu.

Breach Protection Warranty

Společnost Sophos a jejich expertní MDR tým jsou si plně vědomi, že zodpovídají za Vaši kybernetickou Bezpečnost. Sophos Breach Protection Warranty je proto automaticky a bez dalších nákladů zahrnuto v ceně MDR ve verzi Complete a kryje škody způsobené útočníkem až do výše 1 milionu USD. Finanční krytí se vztahuje na endpointy, servery a ostatní zařízení běžící pod Windows a macOS.

COMGUARD communication security

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel. +420 513 035 400
info@comguard.cz | www.comguard.cz