Zabezpečte svůj podnik s Managed Detection and Response od DELL Technologies

Detekce, vyšetřování a reakce na pokročilé hrozby v prostředí IT

Plně spravovaná, end-to-end, 24/7 služba, která kombinuje bezpečnostní dovednosti a hluboké znalosti IT od Dell Technologies s vaší volbou vybraných platforem pro analýzu bezpečnosti XDR od průmyslových lídrů.

Jak bezpečný je váš podnik?

IT týmy čelí rostoucí výzvě zvládat stále větší počet a složitost bezpečnostních hrozeb. V roce 2022 bylo na celém světě 5,5 miliardy útoků malware, o 100 milionů více než v roce 2021.

K efektivní ochraně vaší organizace je třeba rychle detekovat a reagovat na nové hrozby v celém prostředí. To je obtížné kvůli produktům a nástrojům, které omezují viditelnost, obtížím při hledání a udržování kvalifikovaných bezpečnostních profesionálů a IT týmům, které jsou již zaneprázdněny kritickými požadavky a každodenními operacemi.

Managed Threat Detection and Response

je kompletní služba, která sleduje, detekuje, vyšetřuje a reaguje na hrozby v celém IT prostředí, pomáhá organizacím s 50 nebo více koncovými body významně a rychle zlepšit jejich bezpečnostní pozici při ulehčení zátěže na IT.

Služba se spoléhá na dvě klíčové schopnosti:

• Odbornost analytiků bezpečnosti Dell Technologies, kteří mají roky zkušeností s pomocí organizacím po celém světě zlepšit jejich bezpečnost

• Špičkové platformy pro rozšířenou detekci a reakci (XDR) na bezpečnost, které využívají analýzy umožněné AI telemetrií a událostí z více útočných vektorů.

Detekujte, vyšetřujte a reagujte na pokročilé hrozby v celém vašem IT prostředí.

Klíčové benefity:

• Jednotná detekce a reakce napříč celým IT ekosystémem

• Neustále aktualizovaná databáze hrozeb udržuje ochranu aktuální

• Dokáže detekovat i nejutajenější taktiky útočníků

• Komplexní pohled na celou aktivitu útočníka

• Tým profesionálů v oblasti bezpečnosti Dell Technologies, jejichž odbornost zahrnuje bezpečnost, pokročilou infrastrukturu, cloud a další

• Odborná pomoc při nastavení nativního SaaS XDR

• Rychlé zahájení reakce na kybernetické incidenty, když dojde k narušení

• Nejvyšší úroveň dodržování bezpečnostních předpisů pro poskytovatele služeb

Kompletní řešení služby

Analytici bezpečnosti Dell Technologies pomáhají s počátečním nastavením, sledováním, detekcí, nápravou a reakcí - vše za jednu předvídatelnou cenu. Úzce spolupracují s vaším IT týmem, aby porozuměli prostředí, poradili s vylepšeními bezpečnostní pozice a pomohli nasadit softwarového agenta XDR na koncové body.
Upozornění jsou sledována a přezkoumávána 24/7. Pokud si upozornění zaslouží šetření, analytici určí a provedou příslušnou reakci. Pokud je hrozba škodlivá nebo vyžaduje vaši akci, jste informováni a pokud je to nutné, jsou vám poskytnuty podrobné instrukce krok za krokem.

V případě bezpečnostního incidentu vám Dell Technologies pomáhá zahájit proces, aby se váš podnik znovu rozjel.

Vyberte si svou platformu XDR

Vaše bezpečnostní a technologické potřeby a preference jsou jedinečné. Dáváme vám flexibilitu vybrat si z tří průmyslově vedoucích možností: **Secureworks® Taegis™ XDR, CrowdStrike Falcon® XDR nebo Microsoft Defender XDR[2], abyste mohli získat platformu XDR**, která vyhovuje vašim potřebám.

Klíčové funkce

Důvěryhodná podpora

- Úzce s vámi spolupracujeme na pochopení vašeho prostředí, poradenství ohledně vylepšení bezpečnostní pozice
- 24/7 sledování s vaší volbou vybraných platform XDR, které využívají analýzy umožněné AI telemetrií a událostí z více útočných vektorů
- Odborné rady pro nasazení a konfiguraci platformy XDR

Reakce na hrozby a konfigurace bezpečnosti

- Využitím schopností XDR tým Dell SOC automatizuje nápravu nebo spolupracuje s vámi na řešení hrozeb odhalených během sledování
- Poskytuje podrobné, snadno srozumitelné instrukce k obsažení hrozby i v komplexních situacích
- Až 40 hodin konfigurace je zahrnuto v této službě jednou za ¼ roku

24/7 detekce a vyšetřování

- Procesy a upozornění přizpůsobené bezpečnostnímu prostředí vaší organizace a automatizované pro efektivní každodenní operace
- Proaktivní hledání hrozeb specifických pro každé prostředí zákazníka k objevení nových hrozeb nebo variací známých hrozeb, které se vyhýbají bezpečnostním systémům
- Denní souhrn méně kritických upozornění umožňuje týmu Dell SOC soustředit pozornost na kritická upozornění
- Čtvrtletní zprávy o vyšetřování, analýzách trendů upozornění a pokyny pro bezpečnostní pozici

Zahájení reakce na kybernetické incidenty

- 40 hodin roční vzdálené pomoci při reakci na incidenty umožňuje rychle zahájit vyšetřovací aktivity
- Poradenství od Dell certifikovaných bezpečnostních expertů, kteří pomohli organizacím všech velikostí zvládnout vážné bezpečnostní události

Začněte zabezpečovat své prostředí se společností Dell ještě dnes

1. Statistikaa, Roční počet útoků malwaru ve světě v letech 2015 až 2022
2. Pro použití Microsoft Defender XDR je vyžadováno minimálně 500 koncových bodů