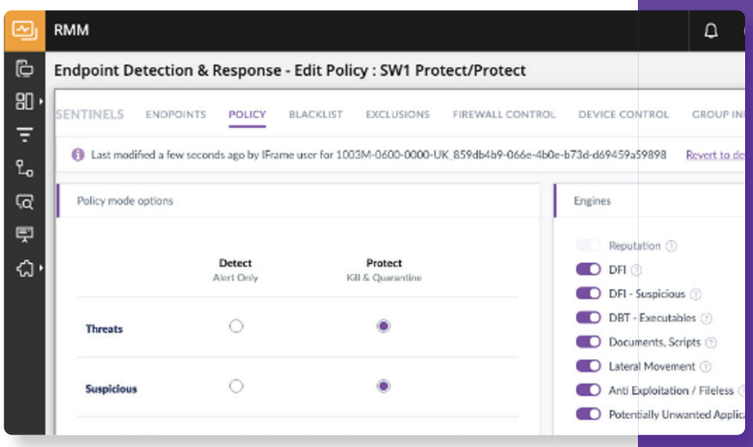
Endpoint Detection and Response

Integrovaná funkce dostupná u řešení N-able N-sight



N-able™ Endpoint Detection and Response (EDR) je integrovanou funkcí v řešení N-able N-sight, která IT týmům pomáhá zabraňovat neustále se měnícím hrozbám, detekovat je a reagovat na ně – a provádět rychlou obnovu, pokud zaútočí ransomware nebo jiný program, který zneužívá oslabení zabezpečení. Odstranění problému a obnova pomáhají napravit dopady útoku a obnovit koncové body do dobrého stavu před útokem s cílem omezit odstávky. Získejte kompletní možnost monitorování a správy zabezpečení koncových bodů – vše z jediného řídicího panelu.

Zabránění kyberútokům

- Pomáhá chránit před nejnovějšími hrozbami, aniž byste museli čekat na opakující se skenování nebo aktualizace definic.
- Prakticky okamžitě reaguje na hrozby pro koncové body.
- Umožňuje povolit/blokovat provoz na USB a koncových bodech (přizpůsobené pro váš podnik) s cílem určit vhodnou reakci.

Efektivní reagování prostřednictvím automatizace

- Zajišťuje automatizované reakce k rychlému řešení hrozeb.
- Pomáhá při zotavení po útocích pomocí nápravy negativních dopadů.

Využití technologie SentinelOne

- Funkce N-able EDR odpovídá platformě SentinelOne® Control.
- Zahrnuje možnosti řízení zařízení, řízení brány firewall koncového bodu a vzdálené spouštění jádra.
- Poskytuje integrované sestavy licencí.

Rychlé vrácení změn po útocích

- Umožňuje nahradit poškozené soubory jejich verzemi v dobrém stavu před útokem (pouze v operačním systému Microsoft® Windows®).
- Zajišťuje získání přehledu o ochraně koncového bodu díky přístupu k nativním výkazům vzdáleného monitorování a správy (RMM).
- Umožňuje spouštění kontrol služeb platformy.
- Umožňuje využít RMM pro snadné nasazení a správu agentů.

Detekce hrozeb pomocí behaviorální umělé inteligence

- Přehledné widgety na řídicím panelů poskytují podrobné nebo souhrnné informace o stavu všech zařízení.
- Výstrahy u nakažených zařízení a poruch služeb přímo v řídicím panelu N-sight
- Umožňuje snadno určit, kde a jak útok začal.
- Středisko hrozeb s vylepšeným stavovým panelem omezuje množství výstrah a umožňuje zmírnit dopady, aniž by bylo potřeba opouštět stránku.

ZEBRA SYSTEMS

ZEBRA SYSTEMS s.r.o.
Třída SNP 402
500 03 Hradec Králové

Tel.: +420 491 615 380
n-able@zebra.cz
www.zebra.cz