Zabezpeční koncových zařízení

SentinelOne je sofistikované bezpečnostní řešení určené k ochraně koncových zařízení před různými druhy kybernetických hrozeb. Technologie SentinelOne využívá pokročilé techniky umělé inteligence, konkrétně strojové učení a behaviorální analýzu, k automatické detekci a neutralizaci potenciálních hrozeb. Tyto metody umožňují systému identifikovat anomální a podezřelé aktivity v reálném čase, čímž výrazně snižují riziko úspěšných kybernetických útoků. Klíčové funkce zahrnují ochranu v reálném čase, schopnost detekovat známé i neznámé hrozby, izolaci kompromitovaných zařízení od zbytku sítě a automatickou obnovu systémových změn způsobených malwarem. SentinelOne je zvláště efektivní v prevenci ransomware útoků, phishingu, zneužití bezpečnostních zranitelností a tzv. zero-day útoků. Podle nezávislých testů vykazuje SentinelOne účinnost prevence až 99,8 %.

SentinelOne poskytuje komplexní podporu pro Windows, macOS, Linux a mobilní operační systémy Android a iOS. Administrátoři mají přístup k intuitivnímu ovládacímu panelu, který nabízí přehled o aktuálním stavu zařízení, možnost analyzovat bezpečnostní incidenty, spravovat politiky ochrany a provádět operace na dálku, jako jsou izolace infikovaných zařízení nebo odstranění škodlivého softwaru.

V případě podezření na kybernetický útok by uživatelé měli být obezřetní vůči typickým příznakům, jako jsou náhlé zpomalení systému, neočekávaná vyskakovací okna, neobvyklé chování aplikací či náhlá ztráta přístupu k souborům. Pokud k těmto jevům dojde, uživatel by měl okamžitě zastavit práci, odpojit počítač od sítě (například fyzickým odpojením síťového kabelu nebo deaktivací bezdrátového připojení) a neprodleně kontaktovat IT správce. SentinelOne automaticky shromažďuje data o podezřelých aktivitách, poskytuje detailní hlášení incidentů a důležité informace pro jejich vyšetření. Je klíčové, aby uživatel neprováděl vlastní zásahy do systému, jako je mazání souborů nebo pokusy o nápravu, bez souhlasu odborníků, aby nedošlo ke zničení důkazů nutných pro analýzu incidentu.

Pokud potřebujete pomoc nebo radu, pak se **obraťte se na správce sítě**.

From:
https://navody.asuch.cas.cz/ -

Permanent link:
https://navody.asuch.cas.cz/doku.php/antivirova_ochrana

Last update: **2025/03/07 09:56**