



Detect & Respond

I stedet for at sætte sin lid til heldet

sharp.dk

SHARP
Be Original.

Tjenesten, som håndterer hændelser før, under og efter et angreb

Det er vigtigt at beskytte din virksomhed. Du vil ikke blive bestjålet information eller få dine systemer nedlåst med lange nedetider eller mistede data som følge.

Trusselsbilledet omkring cyberkriminalitet er alvorlig. Kriminelle angriber alle brancher, mens fokus har flyttet sig fra store multinationale virksomheder til små og mellemstore virksomheder. Metoden er ikke at sigte ind på specifikke virksomheder, men derimod "fiske med net" og se, hvad fangsten bliver.

Detect & Respond understøttes af SOC (Security Operating Center) og giver dig slutpunktsovervågning og trusseldetektering. Tjenesten drives af SentinelOne, og den kan hurtigt identificere og stoppe selv de mest sofistikerede angreb, minimere skade og reducere risikoen for klientslutpunkter.

Detektering af malware

Identificerer hurtigt tusindvis af varianter af virus og malware.

Umiddelbar gendannelse

Hurtig reaktion på registrerede varianter af ransomware ved at udnytte journalføring for at gå tilbage til en acceptabel risikotilstand.

Fuldstændig gendannelsesevne

Ved eventuelle overskrevne systemer kan du anvende robuste gendannelsesfunktioner, der omfatter sporing af ændringer på slutpunktet.

Kriminalteknik til slutpunktsangreb

Identificere årsagerne til skadelig adfærd ved hurtigt at diagnosticere kildeprocesser og -programmer.

Komplette SOC-tjenester

Reducere falske positive indikationer og sikre omfattende beskyttelse gennem SOC-analyse af programmer og filer i karantæne.

Garanti mod ransomware

SentinelOne betaler op til 1.000 dollar af ransomware-beløbet pr. inficeret maskine. Dette gælder, hvis de ikke har kunne beskytte mod trussel eller ikke kan gendanne data efter et ransomware-angreb – op til 1 million dollar i alt for samtlige maskiner i angrebet.