

SMARTDEFENCE FIRMY CHECK POINT

Rozwiązanie typu Aktywna Ochrona™

Nasze rozwiązanie

Nasze rozwiązanie SmartDefense™ firmy Check Point wprowadza nową kategorię produktów przeznaczonych do zabezpieczania Internetu rozwiązania Aktywna Ochrona™. Produkt ten, używając inteligentnej technologii bezpieczeństwa, aktywnie chroni organizacje przed wszelkimi znanymi i nieznanymi zagrożeniami z sieci. Blokuję ataki identyfikując ich typ i klasę z użyciem sprawdzonej, opatentowanej przez Check Point technologii Stateful Inspection. Jednocześnie z poziomu pojedynczej, zunifikowanej konsoli administratora dostarcza na bieżąco informacje na temat wykrywania, blokowania, występowania i nadzorowania ataków oraz innych nadużyć bezpieczeństwa.

Twoje wyzwanie

Organizacje rozwijając swoje sieci i systemy, informatyczne są narażone na coraz większe ryzyko ataków z Internetu. Rosnąca liczba incydentów oraz skala zagrożeń wymagają ponownego skupienia się na tym problemie tak, aby aktywnie i inteligentnie mu przeciwdziałać.

Solidne i wiarygodne rozwiązania bezpieczeństwa muszą nie tylko skutecznie blokować ataki, lecz także umożliwiać oficerowi bezpieczeństwa dogłębne zrozumienie istoty tych zagrożeń. Użyteczna, dokładna informacja w połączeniu z aktualizacją zabezpieczeń w czasie rzeczywistym dostarczają lepszej ochrony i skutecznie zabezpieczają korporacje przed lawinowo pojawiającymi się w Internecie zagrożeniami.

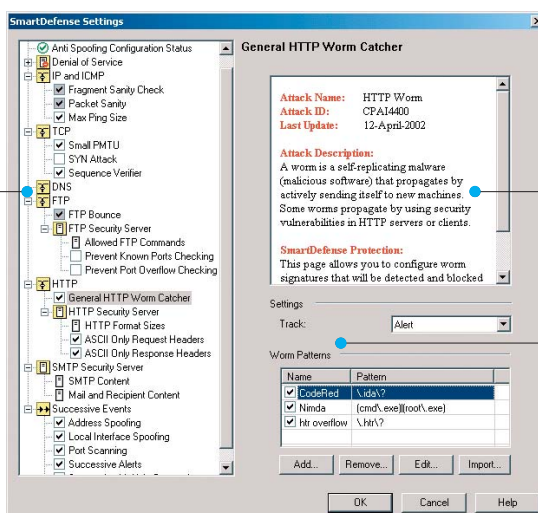
DATA SHEET

Centralny punkt kontroli wszystkich ataków

Aktywna ochrona przed zagrożeniami

Precyzyjny opis ataków w czasie rzeczywistym

Konfiguracja reakcji, alarmów i śledzenia zdarzeń w sieci



The screenshot shows the 'localhost - Check Point Log Viewer - fw.log' window. It displays a table of log entries with columns: No., Date, Time, Product, Attack Name, Source, Destination, and Info. Two entries are visible:

No.	Date	Time	Product	Attack Name	Source	Destination	Info.
618	31 Aug 2002	0:21:16	SmartDefense	Port Scanning	10.1.2.150	10.1.2.122	
621	31 Aug 2002	0:21:25	SmartDefense	URL worm	10.1.2.150	216.200.241.66	URL filter pattern detected /.ida?

At the bottom of the window, it shows 'For Help, press F1', the user 'logasm.fwi*', the host 'localhost', and 'Total records: 622'.

Graficzna konsola SmartDefence

Scentralizowane zarządzanie zabezpieczeń sieci przed atakami.



Scentralizowana kontrola zagrożeń

SmartDefence dostarcza oficerom bezpieczeństwa pojedynczy, scentralizowany punkt kontroli zagrożeń. Radzi sobie z szerokim wachlarzem typów zagrożeń takich jak ataki destrukcyjne i destabilizujące (DoS), ataki poprzez protokół IP, penetracje sieci, włamania wykorzystujące aplikacje podatne na błędy ochrony. Skonfigurowane centralnie alarmy, śledzenie i audyty gwarantują kompletne i skuteczne panowanie nad pojawiającymi się atakami.

Zwalczane zagrożenia sieciowe

Atak typu "odmowa dostępu" (DoS)

typu SYN Flood

typu Land

Ataki poprzez protokół IP

falszowanie IP

fragmentacja IP

nielegalne i zniekształcone pakiety

Słabe punkty aplikacji i sieci Web

ataki na DNS

niezgodności z protokołami

słabe punkty specyficzne dla aplikacji

konie trojańskie

ataki metodą "tylnych drzwi" oraz "zdalnej administracji"

mobilny kod (Java, JavaScript, ActiveX)

ukryte rozszerzenia plików

Przeszukiwanie sieci

skanowanie portów

skanowanie usług

Cechy produktu

- Kompletna integracja z FireWall-1
- Blokowanie ataków wg typów i klas
- Aktualizacja on-line Szczegółowa informacja na temat zagrożeń w czasie rzeczywistym
- Zwalczane zagrożenia sieciowe

Zalety produktu

- Zwiększa bezpieczeństwo sieci
- Wykrywa i chroni przed wszelkimi znanymi atakami z sieci
- Gwarantuje odpowiednią i spójną obronę w całym chronionym środowisku
- Zwiększa zrozumienie i kontrolę nad zagrożeniami.

użytkowników SmartDefence. Aktualizacje on-line rozszerzają możliwości produktu, gwarantując odpowiedni poziom reakcji i elastyczności, którego nie oferują sprzętowe i oparte na technologii ASIC zapory ogniowe. Informacja o atakach w czasie rzeczywistym.

Informacja o atakach w czasie rzeczywistym

Interfejs użytkownika SmartDefence podaje dodatkowe szczegóły na temat wykrywanych zagrożeń oraz odnośniki do obszerniejszej informacji dotyczącej natury i specyfiki ataków.

Wartościowe i szczegółowe informacje SmartDefence zapewnione są dzięki bogatym dziennikom systemowym oraz rozproszonej infrastrukturze zabezpieczeń Check Point, rejestrujących zdarzenia w sieci.

Dane te dostarczają oficerom bezpieczeństwa wiedzę o naturze zagrożeń i ich potencjalnych skutkach, zapewniając większe zrozumienie i kontrolę nad atakami z sieci.

Aktualizacje on-line

Ponieważ kluczowym elementem dla bezpieczeństwa jest aktualność informacji, SmartDefence działa w połączeniu z usługą subskrypcji gwarantującej, że najświeższe informacje dotyczące nowych i pojawiających się zagrożeń będą dostępne dla

SmartDefence firmy Check Point wprowadza nowy paradygmat do technologii zabezpieczeń. Po raz pierwszy oficerowie bezpieczeństwa, mając do dyspozycji scentralizowane punkty ochrony i kontroli nad atakami, informacje o zagrożeniach w czasie rzeczywistym oraz aktualizacje on-line, mogą naprawdę aktywnie chronić systemy informatyczne przed znanymi i nieznanymi atakami.

Architektura Secure Virtual Network

Wszystkie produkty Check Point są budowane na bazie architektury SVN (Secure Virtual Network) w celu zapewnienia bezpiecznego i bezproblemowego łączenia użytkowników, sieci, systemów oraz aplikacji poprzez środowiska Internet, intranet i ekstranet. W celu uzyskania dalszych informacji prosimy o kontakt z lokalnym partnerem lub zapoznaniem się z zawartością serwisu <http://www.checkpoint.pl>

Dystrybucja w Polsce:



CLICO Sp. z o.o.
30-063 Kraków, Al. 3-go Maja 7
tel. (12) 632-51-66
tel. (12) 292-75-22 ... 25
fax (12) 632-36-98
e-mail: checkpoint@clico.pl
www.clico.pl

CLICO Oddział Katowice
40-555 Katowice, ul. Rolna 43
tel. (32) 203-92-35
tel. (32) 609-80-50
tel. (32) 609-80-51
fax (32) 203-92-24

© 2002 Check Point Software Technologies Ltd. Wszelkie prawa zastrzeżone. Check Point, logo Check Point, FireWall-1, FireWall-1 SecureServer, FloodGate-1, INSPECT, IQ Engine, Meta IP, Open Security Extension, OPSEC, Provider-1, Reporting Module, User-to-Address Mapping, VPN-1, VPN-1 Accelerator Card, VPN-1 Appliance, VPN-1 Certificate Manager, VPN-1 Gateway, VPN-1 SecuRemote, VPN-1 SecureServer i ConnectControl są znakami firmowymi lub zarejestrowanymi znakami firmowymi (towarowymi) Check Point Software Technologies Ltd. albo jej jednostek stowarzyszonych. Wszystkie inne wymienione tu nazwy wyrobów są znakami firmowymi (towarowymi) lub zarejestrowanymi znakami firmowymi (towarowymi) ich odpowiednich właścicieli. Produkty opisane w niniejszym dokumencie są chronione przez U.S. Patent No. 5,606,668 oraz 5,835,726 i mogą być chronione innymi patentami USA, patentami zagranicznymi lub zgłoszeniami w toku.

© 2002 CLICO Sp. z o.o. (polska wersja językowa). CLICO i CLICO logo są zarejestrowanymi znakami towarowymi CLICO Sp. z o.o.