Hillstone I-Series

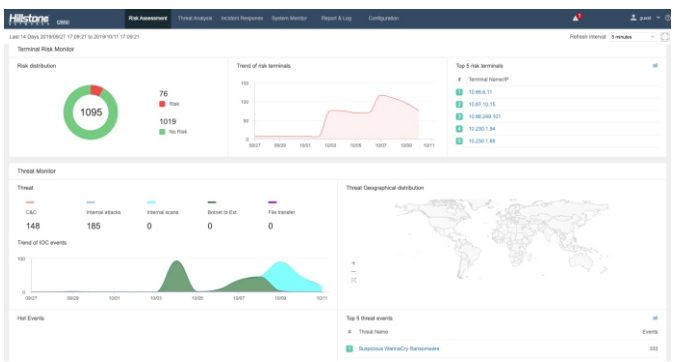
System sBDS (Server Breach Detection System)




Rozwiązanie Hillstone sBDS (Server Breach Detection System) służące do wykrywania zagrożeń sieciowych i reagowania (NDR - Network Detection and Response) wykorzystuje wiele technologii wykrywania zagrożeń, w tym tradycyjne metody oparte na sygnaturach, a także metody wykorzystujące reguły oraz wielkoskalowe modelowanie danych o zagrożeniach, a także analizy zachowań użytkowników przy pomocy uczenia maszynowego. System jest idealnym rozwiązaniem do wykrywania rozbudowanych zagrożeń, w tym ransomware czy crypto-mining, i zapewnia ochronę przed naruszeniami dla krytycznych serwerów i wrażliwych danych. Wraz ze szczegółowymi analitycznymi metodami wykrywania zagrożeń oraz rozbudowaną widocznością sieci, Hillstone sBDS zapewnia organizacjom skuteczne możliwości wykrywania zdarzeń IOC (Indicators of Compromise), lokalizowania obarczonych ryzykiem hostów i serwerów oraz odtwarzania łańcucha ataku. Co więcej, rozwiązanie umożliwia ograniczanie ataków i zagrożeń poprzez współpracę z firewallem NGFW oraz integrację z systemem XDR Hillstone iSource. Produkt Hillstone sBDS to skuteczne i kompleksowe rozwiązanie do wykrywania i reagowania na różnego rodzaju ataki sieciowe i zagrożenia w środowiskach korporacyjnych.

Najważniejsze cechy produktu

Kompleksowa analityka korelacji zagrożeń dla zaawansowanego wykrywania zagrożeń



Przeprowadzający cyber-ataki stają się coraz bardziej wyrafinowani w swoich metodach działania. Stosują nakierowane, ciągłe, niewidoczne i wieloetapowe ataki, które łatwo mogą pozostać niezauważone przez systemy bezpieczeństwa. Hillstone sBDS składa się z wielu mechanizmów wykrywania zagrożeń skoncentrowanych na różnych aspektach procesu po wystąpieniu naruszenia, w tym ATD (Advanced Malware Detection), ABD (Abnormal Behavior Detection), a także tradycyjnych mechanizmach wykrywania włamań i skanerach antywirusowych. Platforma do korelacji zagrożeń Hillstone analizuje szczegóły powiązań poszczególnych podejrzanych zdarzeń, a także inne kontekstowe informacje pochodzące z sieci, w celu zapewnienia dokładnego i skutecznego wykrywania złośliwego oprogramowania i ataków, z wysokim poziomem ufności.

Monitorowanie zagrożeń krytycznych serwerów i hostów w czasie rzeczywistym

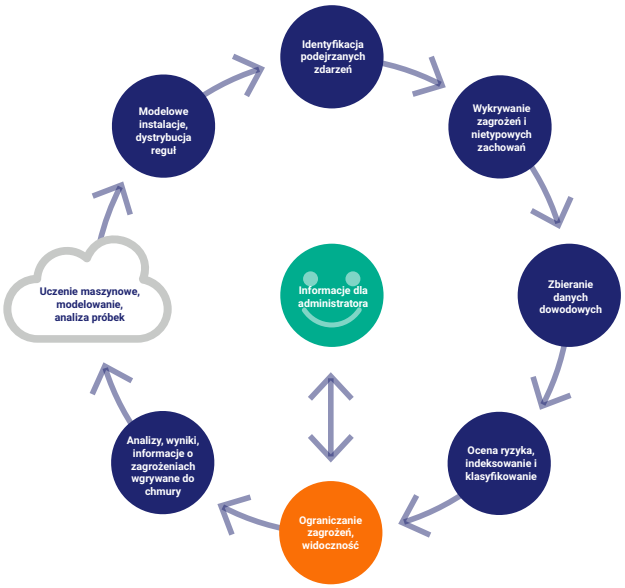
Platforma Hillstone sBDS skupia się na ochronie krytycznych serwerów intranetowych, wykrywając nieznane ataki (prawie zero-day) oraz rozpoznając anomalne aktywności na poziomie sieci i aplikacji dotyczące serwerów i hostów. W momencie wykrycia zagrożenia lub nietypowego zachowania, Hillstone sBDS przeprowadza analizę tej sytuacji oraz wykorzystuje oparte na topologii prezentacje graficzne, aby zapewnić większą widoczność szczegółów zagrożeń i anomalnych zachowań. W ten sposób administratorzy bezpieczeństwa mają lepszy obraz ataku, rozkładów ruchu w poszczególnych kierunkach, a także pozwala na ocenę ryzyka w całej sieci.

Pełny obraz zdarzeń IOC oraz łańcucha ataku

Zdarzenia IOC to zdarzenia związane z zagrożeniami, wykrywane podczas ataku następującego po zaistnieniu naruszenia. Są one identyfikowane spośród olbrzymiej liczby ataków w sieci, które są bezpośrednio powiązane z chronionym serwerem lub hostem. Zdarzenia IOC to zazwyczaj zagrożenia o większym stopniu ryzyka, cechujące się wysokim poziomem ufności detekcji naruszenia serwera lub hosta, przez co stanowią potencjalnie większe zagrożenie dla zasobów sieci korporacyjnej. Skuteczne wykrywanie IOC

oraz ich szczegółowa analiza, mają kluczowe znaczenie dla ograniczania ataków związanych z kradzieżą wrażliwych danych oraz zapobieganiem ich dalszego rozprzestrzeniania się w sieci. Rozwiązanie Hillstone sBDS przeprowadza bardzo szczegółowe analizy zdarzeń IOC, rekonstruuje łańcuch ataku w oparciu o te informacje, a także koreluje pozostałe zdarzenia bezpieczeństwa powiązane z tymi IOC w określonych ramach czasu i przestrzeni.

Bogate dane analityczne i działania zapobiegawcze



Platforma Hillstone sBDS realizuje działania ograniczające zagrożenia w połączeniu z urządzeniami NGFW Hillstone serii A, serii E oraz serii X, które instalowane są w ramach infrastruktury sieciowej. Po przeanalizowaniu i zweryfikowaniu powiadomień o zagrożeniach, administratorzy mogą dodać parametry zagrożenia takie jak adres IP, typ zagrożenia, itp. do czarnej listy lub polityki, a następnie przeprowadzić ich synchronizację z firewallami Hillstone. W ten sposób kolejne ataki tego samego typu lub rodziny zagrożeń będą odpowiednio wcześnie zablokowane w obszarze dostępowym sieci. Zapobiega to rozprzestrzenianiu się kolejnych ataków w sieci.

Cechy

Wykrywanie nietypowych zachowań
- Modelowanie zachowań w oparciu o ruch z warstw L3-L7, w celu wykrycia nietypowych zachowań sieci, np. skanowania HTTP, SPAM, Spider
- Wykrywanie ataków DDoS, w tym Flood, Sockstress, Zip of Death, Reflect, DNS Query, SSL oraz aplikacyjnych
- Kontrola szyfrowanego, tunelowanego ruchu w celu wykrycia nieznanych aplikacji
- Bieżące aktualizowanie bazy danych z modelami zachowań
- Wykrywanie ataków brute force RDP/VNC/SMB/SSH/FTP oraz podejrzanych żądań HTTP opartych na TOR

Zaawansowane wykrywanie zagrożeń
- Oparte na zachowania zaawansowane wykrywanie złośliwego oprogramowania
- Wykrywanie ponad 2000 znanych i nieznanych rodzin zagrożeń, w tym wirusów, robaków, trojanów, przepełnień bufora, itp.
- Wykrywanie oprogramowania ransomware i cryptomining

Analizy korelacji zagrożeń
- Korelacja nieznanych zagrożeń, nietypowych zachowań sieci i aplikacji w celu wykrycia potencjalnych ataków
- Wielowymiarowe reguły korelacji, aktualizowane codziennie w sposób automatyczny, z wykorzystaniem cloud

Wykrywanie zagrożeń związanych z oszustwami
- Lokalny mechanizm wykrywania, z regularnie aktualizowanymi modelami
- Ochrona serwerów web, dokumentacyjnych i bazodanowych, obsługa protokołów FTP, HTTP, MySQL, SSH i TELNET

Wykrywanie włamań
- Ponad 30 tys. sygnatur, wykrywanie anomalii w protokołach oraz na podstawie ruchu
- Własne sygnatury, ręczne lub automatyczne aktualizowanie sygnatur, wbudowana encyklopedia zagrożeń
- Ponad 20 typów anomalii w protokołach, w tym HTTP, SMTP, IMAP, POP3, VoIP, NETBIOS, VxLAN, MPLS, itp.
- Wykrywanie ataków związanych z przepełnieniem bufora, wstrzykiwaniem SQL oraz cross-site scripting
- Wykrywanie słabych haseł dla protokołów takich jak FTP, HTTP, SMTP, POP3, IMAP, TELNET

Skaner antywirusowy
- Baza danych z ponad 13 mln sygnaturami wirusów, aktualizowana na bieżąco
- Skanowanie skompresowanych plików

Anty-Spam
- Klasyfikacja i ochrona przed spamem w czasie rzeczywistym
- Potwierdzony spam, podejrzewany spam, spam masowy
- Ochrona niezależnie od języka, formatu czy treści wiadomości
- Obsługa protokołów SMTP i POP3
- Białe listy wiadomości od zaufanych domen/ nadawców

Cloud-Sandbox
- Wgrywanie złośliwych plików do chmury w celu analizy
- Obsługa protokołów HTTP, SMTP, POP3, IMAP4 i FTP
- Obsługa plików PE, APK, JAR, MsOffice, PDF, SWF, RAR, ZIP
- Pełny raport analizy zachowań dla złośliwych plików
- Globalna wymiana informacji o zagrożeniach, blokowanie zagrożeń w czasie rzeczywistym
- Wiele statycznych mechanizmów wykrywania dla szybkiego odfiltrowywania normalnych plików i znanych zagrożeń
- Wizualizacja nieznanych zagrożeń w oparciu o logi, raporty, informacje z monitorowania, raporty dotyczące zachowania plików

Wykrywanie Botnet C&C
- Odnajdywanie hostów botnet w sieci intranet poprzez monitorowanie połączeń C&C
- Wykrywanie adresu IP i nazwy domeny C&C w ruchu TCP, HTTP i DNS
- Automatyczne aktualizowanie biblioteki sygnatur C&C

Wykrywanie ataku
- Wykrywanie ataków na protokoły
- Wykrywanie ataków DoS/DDoS, w tym SYN Flood, DNS Query Flood
- Wykrywanie ataków na zasoby Web w oparciu o reguły WAF dotyczące protokołu HTTP
- Wykrywanie ataków ARP, DDoS, wstrzykiwania kodu, cross-site, opartych na specjalnych podatnościach, wycieków informacji, złośliwego oprogramowania, nielegalnego dostępu do zasobów
- Białe listy dla zachowań sieci Web

Identyfikacja aplikacji
- Ponad 4 tys. aplikacji, w tym komunikatory, P2P, transfer plików, poczta, gry online, streaming, itp.
- Wielowymiarowe statystyki dotyczące aplikacji, w oparciu o strefy, interfejs, lokalizację, użytkownika i adres IP
- Obsługa aplikacji mobilnych Android i IOS

Ograniczanie wpływu zagrożeń
- Możliwość zmiany statusu zdarzeń - otwarte, fałszywe alarmy, naprawione, ignorowane, potwierdzone
- Czyszczenie zagrożeń serwera/ komputera jednym kliknięciem i ponowna ocena bezpieczeństwa hosta
- Białe listy zdarzeń, w tym nazwa zagrożenia, źródłowy/ docelowy adres IP, liczba wystąpień, itp.
- Współpraca z firewallami Hillstone dla blokowania zagrożeń
- Integracja z usługą Sysmon urządzeń końcowych
- Wyszukiwanie zagrożeń w sieci

Wykrywanie ARP Spoofing
- Ochrona przed ARP spoofing przewiązanie IP-MAC i inspekcję pakietów ARP

Monitorowanie
- Dynamiczne, aktualizowane na bieżąco dashboardy oraz szczegółowe widgety
- Przewidywanie zagrożeń dla sieci intranet
- Przegląd ogólnego stanu zagrożenia sieci, w tym TOP5 zagrożeń, trendy, stan ryzyka krytycznych zasobów i hostów, typ i dotkliwość zagrożeń, geolokalizacja zewnętrznych ataków, itp.
- Wizualne informacje o stanie zagrożeń krytycznych zasobów i innych istotnych hostów, w tym poziom ryzyka, prawdopodobieństwo, geolokalizacja ataku, mapowanie łańcucha ataku i inne informacje statystyczne
- Wizualne informacje o zdarzeniach w sieci, w tym analiza zagrożeń, baza wiedzy, historia i topologia
- Wysyłanie powiadomień pocztą lub poprzez SMTP Trap
- Usługa push z informacjami o zagrożeniach oparta na technologii cloud

Logi i raportowanie
- 3 wbudowane raporty: Security, Flow i System
- Możliwość tworzenia raportów przez użytkownika
- Eksportowanie raportów do plików PDF, Word, HTML - przez email lub FTP
- Logi, w tym zdarzenia, sieci, zagrożenia i konfiguracyjne
- Możliwość eksportu logów przez Syslog lub email
- Agregacja logów AV i Botnet
- Ocena stopnia zagrożenia hosta

Administracja
- Monitorowanie hostów i serwerów w sieci wewnętrznej, identyfikacja nazwy, systemu operacyjnego, przeglądarki, typu i statystyk sieciowych
- Dostęp dla zarządzania: HTTP, HTTPS, SSH, telnet, konsola
- Powiadomienia o stanie urządzeń: wykorzystanie CPU, pamięci, dysku, nowe i jednoczesne sesje, pasmo, temperatura chassis i CPU
- Powiadomienia oparte na paśmie aplikacji i liczbie nowych połączeń
- Obsługa 3 typów alertów: email, wiadomość tekstowa, komunikat Trap
- Obsługiwany język: angielski

Scentralizowane zarządzanie
- Urządzenia zarejestrowane w HSM (Hillstone Security Management Platform)
- Monitorowanie stanu wielu urządzeń, ruchu i zagrożeń poprzez chmurę, z ciągłym dostępem (24/7) przez aplikację web lub mobilną (CloudView)
- Współpraca z systemami innych producentów w celu wykrywania złośliwych plików, adresów URL i IP

API RESTful
- Obsługa standardowych API RESTful w celu uzyskania dostępu do informacji o zdarzeniach dotyczących sprzętu, systemu, itp.
- Bezproblemowa integracja z innymi systemami zarządzania siecią

Specyfikacja techniczna

	I-1850	I-1870	I-2850	I-2860
				
Przepustowość wykrywania [1]	1 Gb/s	1 Gb/s	2 Gb/s	2 Gb/s
Nowe sesje [2]	20,700	32,000	75,000	75,000
Maks. jednoczesnych sesji [2]	750,000	750,000	1.5 mln	1.5 mln
Rozmiar obudowy	1 U	1 U	1 U	1 U
Przestrzeń dyskowa	1T HDD	1T SSD	1T HDD	1T SSD
Porty zarządzania	2 x USB, 1 x RJ45	2 x USB 1 x RJ45 1 x MGT	2 x USB, 1 x RJ45, 2 x MGT	2 x USB 1 x RJ45 2 x MGT
Wbudowane porty I/O	4 x GE	2 x SFP+ 8 x SFP 8 x GE	4 x GE	2 x SFP+ 8 x SFP 16 x GE
Dostępne gniazda na moduły rozszerzenia	1 x Generic	0	1 x Generic	1 x Generic
Moduły rozszerzenia (opcjonalne)	IOC-S-4SFP-L	N/A	IOC-S-4GE-B, IOC-S-4SFP, IOC-S-8SFP, IOC-S-4GE-4SFP, IOC-S-2SFP+, IOC-S-4SFP+	IOC-A-4SFP+
Zasilanie	AC 100-240V, 50/60Hz	AC 100-240V, 50/60Hz DC -36V~ -72V	AC 100-240V, 50/60Hz	AC 100-240V, 50/60Hz DC -36V~ -72V
Specyfikacja zasilania	60W, pojedynczy zasilacz AC	50W, pojedynczy zasilacz AC	250W, pojedynczy zasilacz AC	100W, podwójny redundantny AC
Wymiary (szer.×głęb.×wys., mm)	16.9 x 11.8 x 1.7 in (430 x 300 x 44mm)	17.2 x 12.6 x 1.7 in (436 x 320 x 44mm)	16.9 x 11.8 x 1.7 in (430 x 300 x 44mm)	17.2 x 17.2 x 1.7 in (436 x 437 x 44mm)
Waga	8.8lb (4 kg)	9 lb (4.1 kg)	15.4 lb (7 kg)	18.7 lb (8.5 kg)
Temperatura	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Wilgotność względna	5-85% (bez kondensacji)	10-95% (bez kondensacji)	5-85% (bez kondensacji)	10-95% (bez kondensacji)

	I-3850	I-3860	I-5850	I-5860
				
Przepustowość wykrywania [1]	5 Gb/s	5 Gb/s	10 Gb/s	10 Gb/s
Nowe sesje [2]	120,000	210,000	250,000	500,000
Maks. jednoczesnych sesji [2]	3 mln	3 mln	6 mln	6 mln
Rozmiar obudowy	2 U	1 U	2 U	1 U
Przestrzeń dyskowa	1T HDD	1T SSD	1T HDD	2T SSD
Porty zarządzania	2 x USB, 1 x RJ45, 2 x MGT	2 x USB 1 x RJ45 3 x MGT	2 x USB, 1 x RJ45, 2 x MGT	2 x USB 1 x RJ45 2 x MGT
Wbudowane porty I/O	6 x GE	6 x SFP+ 16 x SFP 8 x GE	N/A	2 x QSFP+ 16 x SFP+ 8 x GE
Dostępne gniazda na moduły rozszerzenia	2 x Generic	1 x Generic	4 x Generic	1 x Generic
Moduły rozszerzenia (opcjonalne)	IOC-S-4GE-B, IOC-S-4SFP, IOC-S-8SFP, IOC-S-4GE-4SFP, IOC-S-2SFP+, IOC-S-4SFP+	IOC-A-4SFP+	IOC-BDS-8GE-H, IOC-BDS-8SFP-H, IOC-BDS-4SFP+-H	IOC-A-4SFP+
Zasilanie	AC 100-240V, 50/60Hz	AC 100-240V, 50/60Hz DC -36V~ -72V	AC 100-240V, 50/60Hz	AC 100-240V, 50/60Hz DC -36V~ -72V
Specyfikacja zasilania	350W, podwójny redundantny AC	289W, podwójny redundantny AC	350W, podwójny redundantny AC	382W, podwójny redundantny AC
Wymiary (szer.×głęb.×wys., mm)	16.9 x 19.7 x 3.5 in (430 x 500 x 88mm)	17.2 x 17.2 x 1.7 in (436 x 437 x 44mm)	16.9 x 19.7 x 3.5 in (430 x 500 x 88mm)	17.2 x 17.2 x 1.7 in (436 x 437 x 44mm)
Waga	26.5 lb (12 kg)	22.5 lb (10.2 kg)	26.5 lb (12 kg)	22.5 lb (10.2 kg)
Temperatura	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Wilgotność względna	5-85% (bez kondensacji)	10-95% (bez kondensacji)	5-85% (bez kondensacji)	10-95% (bez kondensacji)

Opcjonalne moduły rozszerzeń

Moduł	IOC-S-4SFP-L	IOC-S-4GE-B	IOC-S-4SFP	IOC-S-8SFP	IOC-S-4GE-4SFP
Porty I/O	4 x SFP	4 x GE Bypass	4 x SFP	8 x SFP	4 x SFP
Wymiary	1U (zajmuje 1 gniazdo generic)	1U (zajmuje 1 gniazdo generic)	1U (zajmuje 1 gniazdo generic)	1U (zajmuje 1 gniazdo generic)	1U (zajmuje 1 gniazdo generic)
Waga	0.22 lb (0.1 kg)	0.33 lb (0.15 kg)	0.33 lb (0.15 kg)	0.55 lb (0.25 kg)	0.55 lb (0.25 kg)

Moduł	IOC-S-2SFP+	IOC-S-4SFP+	IOC-BDS-8GE-H	IOC-BDS-8SFP-H	IOC-BDS-4SFP+-H	IOC-A-4SFP+
Porty I/O	2 x SFP+	4 x SFP+	8 x GE	8 x SFP	4 x SFP+	4 x SFP+, moduł SFP+ nie jest w zestawie
Wymiary	1U (zajmuje 1 gniazdo generic)	1U (zajmuje 1 gniazdo generic)	1U (zajmuje 1 gniazdo generic)	1U (zajmuje 1 gniazdo generic)	1U (zajmuje 1 gniazdo generic)	1U
Waga	0.33 lb (0.15 kg)	0.44 lb (0.2 kg)	0.55 lb (0.25 kg)	0.55 lb (0.25 kg)	0.44 lb (0.2 kg)	2.09 lb (0.96 kg)

Zalecana konfiguracja Sysmon

Specyfikacja	Serwer Sysmon	Klient Sysmon
CPU	4 rdzeniowy	\
Pamięć	16G	1G
Przestrzeń dyskowa	1T HDD, możliwość rozbudowy	40G HDD
Pakiet instalacyjny	OVF Mirror	MSI Service Program
Wymagania systemowe	VMware ESXi	Windows 7 / Windows Server 2008 lub nowszy

UWAGI:
(1) Przepustowość wykrywania naruszeń obliczona z uwzględnieniem dwukierunkowego wykrywania ruchu HTTP, przy aktywnych wszystkich funkcjach wykrywania zagrożeń.
(2) Dane uzyskano przy wyłączonej funkcji wykrywania ataków Web. Wydajność może ulec zmianie po jej aktywowaniu.