Załącznik nr 6 – Opis równoważności

Dostawa systemu Hillstone Networks iSource (XDR).

Opis równoważności

Gromadzenie danych

Obsługuje gromadzenie danych o ruchu i danych dziennika z sensorów, terminali, urządzeń zabezpieczających (takich jak NGFW, IDPS, WAF itp.) i urządzeń sieciowych innych firm.

Obsługuje dane w formatach Syslog, sysmon, netflow, metadanych i linux.

Wydajność platformy

Obsługuje do 5 urządzeń w celu utworzenia klastra HA, aby osiągnąć elastyczną rozbudowę przestrzeni dyskowej i wydajności przetwarzania;

Obsługa dostępu do platformy poprzez adres typu IPv6 oraz IPv4

Podczas wdrażania platformy obsługiwane jest używanie adresów IPv6 do konfigurowania powiązanych adresów platformy

Wyświetlanie pełnoekranowe

Obsługa mapy rozkładu ataków, kompleksowych wyników, sytuacji podatności, sytuacji serwerów, sytuacji terminali, najnowszych zagrożeń

Możliwość przeglądania statystyk i wyświetlania podziału ataków zewnętrznych na poziomie zdarzeń, 5 najpopularniejszych źródłowych adresów IP ataków, 5 najpopularniejszych lokalizacji geograficznych źródeł ataków, rozkład etapów ataku, sytuację zdarzeń ataku oraz 5 najpopularniejszych zasobów/obszarów objętych atakiem.

Moduł wyświetlania pełnoekranowego, który obsługuje serwer, rozkład stanu bezpieczeństwa, TOP5 ryzykownych serwerów, TOP5 zagrożeń, tygodniowy trend ryzyka i ranking zagrożeń.

Moduł wyświetlania pełnoekranowego, który obsługuje terminale, dystrybucję statusu bezpieczeństwa, TOP5 ryzykownych serwerów, TOP5 zagrożeń, tygodniowy trend ryzyka i ranking zagrożeń

Moduł wyświetlania pełnoekranowego obsługujący zdarzenia, statystyki zagrożeń, najnowsze zagrożenia, najnowsze informacje o zagrożeniach, tygodniowy trend ryzyka i historyczny ranking zagrożeń

Moduł wyświetlania pełnoekranowego, który obsługuje podatności hostów, dystrybucję podatności na zagrożenia, trend podatności i ranking historycznych podatności

Obsługa obszarów ryzyka i wyświetlanie serwerów, punktów końcowych, zagrożeń i luk w zabezpieczeniach w ramach każdego obszaru ryzyka

Obsługa przeskakiwania z pełnoekranowego wyświetlacza kompleksowej sytuacji bezpieczeństwa do innych wyświetlaczy pełnoekranowych; manualna lub automatyczna

Obsługa kontroli filtrów czasowych, wybór wyświetlania informacji z dnia dzisiejszego, 7 dni i 30 dni

Monitorowanie sytuacji infrastruktury

Obsługuje powiadamianie o alarmach oraz o zagrożeniach, informacjach alarmowych o działaniu systemu i informacjach alarmowych o licencjach w systemie.

Obsługuje przegląd sytuacji bezpieczeństwa, w tym kompleksowy status ryzyka całej sieci, porównanie statusu ryzyka w tym samym okresie tygodnia, liczbę zadań i status wykonania zadania, zagrożenia i ich rozkład w tygodniu, status ryzyka i status naruszonych zasobów.

Obsługuje statystyki i wyświetlanie całkowitej liczby ryzykownych terminali, całkowitej liczby ryzykownych serwerów, całkowitej liczby zadań, ukończonych zadań i niedokończonych zadań

Obsługa niestandardowych ustawień w celu wyświetlania zagrożeń, którymi zainteresowany jest użytkownik, oraz wsparcie dla drill-down odpowiednich zdarzeń w celu przejścia do strony szczegółowej.

Obsługa ogólnej oceny stanu zagrożenia całej sieci i porównywanie stanu zagrożenia z jednego tygodnia w tym samym okresie czasu.

Obsługa statystyk i wyświetlanie 5 najważniejszych zdarzeń związanych z zagrożeniami w danym tygodniu

Obsługa statystyk zagrożeń i wyświetlania rozkładu na mapie

Obsługuje funkcję monitorowania ruchu i wykonuje statystyki, analizę i wyświetlanie informacji o danych NetFlow uzyskanych przez platformę z trendów ruchu, trendów nowych połączeń, aktywności źródłowych adresów IP i docelowych adresów IP.

Obsługa monitorowania całkowitego trendu ruchu i monitorowania ruchu źródłowego adresu IP / docelowego adresu IP, obsługa wyświetlania adresu IP, typu zasobu, nazwy zasobu, obszaru, ruchu uplink i downlink, nowego połączenia i innych informacji oraz obsługa rankingu TOP.

Obsługa zliczania liczby serwerów/terminali o różnych poziomach ryzyka zgodnie z poziomem ryzyka: krytycznym, wysokim, średnim i niskim oraz tygodniowy wykres trendu oraz TOP5

Obsługa statystyk trendów liczby serwerów/terminali o różnych poziomach ryzyka w ciągu tygodnia.

Obsługa wyświetlania statystyk TOP5 serwerów/terminali o najbardziej krytycznym ryzyku w ciągu tygodnia.

Obsługa rankingu TOP5 zagrożeń związanych z zasobami i obsługa statystyk ryzyka związanych z zasobami w ciągu tygodnia

Obsługa pulpitu monitorowania zasobów, zliczanie wszystkich zasobów/serwerów/terminali o różnych poziomach ryzyka, oraz wyświetlanie 5 najbardziej ryzykownych zasobów/serwerów/terminali.

Obsługa wyświetlania typu zasobu związanego z pojedynczym adresem IP, nazwy zasobu, zlokalizowanego regionu, liczby nowych połączeń, całkowitego ruchu, rozkładu ruchu i powiązanych z nim działań

Obsługa statystyk i wyświetlanie całkowitej liczby zasobów, całkowitej liczby serwerów/terminali/sprzętu sieciowego/sprzętu bezpieczeństwa/innego sprzętu, liczby zasobów w stanie naruszenia

Obsługa statystyk i wyświetlanie rozkładu typu zasobu, rozkładu źródła i systemu operacyjnego, rankingu TOP5 otwartych portów, rankingu TOP5 aplikacji oraz rankingu TOP5 dystrybucji zasobów.

Obsługa statystyk zagrożeń, tygodniowych statystyk zagrożeń

Obsługa konfigurowania danych zdarzeń, statystyk i wyświetlania rozkładu danych zagrożeń oraz informacji o zasobach dotkniętych danymi zagrożeniami

Obsługa statystyk luk w zabezpieczeniach, tygodniowego trendu luk w zabezpieczeniach i tygodniowej liczby luk w zabezpieczeniach

Obsługa statystyk obszaru ryzyka, tygodniowego trendu obszaru ryzyka i tygodniowej liczby statystyk obszaru ryzyka

Obsługa śledzenia źródła globalnie, obsługa śledzenia źródła poprzez IP/nazwę domeny/MD5 i musi obejmować informacje o zdarzeniach zagrożeń, analizie podatności, monitorowaniu ruchu, powiązanych danych wywiadowczych i innych powiązanych informacjach.

Obsługuje monitorowanie w czasie rzeczywistym użycia procesora, pamięci i dysku twardego

Obsługa statystyk stanu czujników, w tym całkowitej liczby czujników, liczby niedziałających czujników i liczby działających czujników,

Obsługa niestandardowej planszy tematycznej, wielowymiarowe wyświetlanie wykresów zasobów, zagrożeń i luk w zabezpieczeniach

Analiza zagrożeń

Obsługa statystyk statusu wszystkich zasobów - statusu serwera, statusu terminala, statusu usługi i zagrożenia.

Obsługa tygodniowych statystyk trendów zagrożeń, w tym ryzykownych serwerów, ryzykownych terminali i zagrożeń

Obsługa analizy statystycznej zagrożeń, w tym etapu ataku, typu, informacji o opisie, sugestii usunięcia, informacji o zagrożeniu, informacji o dowodach i informacji o procesie. Można dostosować elementy wyświetlane w nagłówku i sortować według pól nagłówka.

Obsługuje kompleksowe wyświetlanie sytuacji zagrożenia z perspektywy kompleksowej, zasobów i ataku

Obsługuje oznaczanie zagrożeń i powiązanych zagrożeń, w tym rozwiązanych lub fałszywie pozytywnych.

Obsługa zapytań o zagrożeniu z kombinacją wielu warunków, w tym nazwy, typu, poziomu, adresu IP, statusu itp.

Obsługa zagregowanego wyświetlania i statystyk zagregowanych szczegółów zagrożeń według nazwy zagrożenia

Obsługuje funkcję przechowywania pakietów informacji o dowodach i obsługuje pobieranie oryginalnego ruchu zebranego przez czujnik

Obsługa pobierania oryginalnego pakietu danych

Obsługa narzędzi dekodujących, informacje o zagrożeniach obsługują dekodowanie URL i Base64

Obsługa bezpośredniej obsługi zagrożeń na stronie zdarzeń. Poza normalną konfiguracją polityk, można wydawać polityki bezpieczeństwa hosta, w tym blokowanie IP, kontrolę dostępu, kontrolę procesu, izolowanie plików, ponowne uruchamianie terminala, kontrolę USB itp.

Obsługa analizy statystycznej serwerów/terminali zagrożeń, w tym etykiet zagrożeń, zagrożeń, poziomów ważności itp.

Obsługuje powiązanie użytkowników końcowych w celu wyświetlenia najnowszego adresu IP logowania, adresu MAC i czasu ostatniego zdarzenia

Obsługa uszkodzeń serwera/terminala, ocena aktualnego uszkodzenia hosta, wizualizacja zagrożeń na różnych etapach ataku i dostarczanie sugestii dotyczących usuwania zagrożeń.

Obsługa perspektywy zagrożenia, relacji zagrożenia, kierunku ataku i wizualizacji zakresu wpływu.

Obsługa widoku zasobu, który został podejrzany o naruszenie, oraz przeglądanie raportów dotyczących naruszeń, raportów ryzyka, powiązanych zagrożeń i informacji o lukach w zabezpieczeniach.

Obsługuje statystyki monitorowania usług zagrożeń, które mogą być statystycznie filtrowane według obszaru, czasu, nazwy, poziomu i etykiety ryzyka, a także mogą być sortowane według pola nagłówka.

Obsługuje szczegółowe statystyki zagrożeń, w tym serwery, obszary, opisy biznesowe, raporty o naruszeniach.

Obsługa odbierania, przechowywania i wyświetlania dzienników Syslog, w tym dzienników Syslog IPv6

Obsługa odbierania i przechowywania dzienników Netflow

Obsługa odbierania i przechowywania metadanych

Obsługa odbierania i przechowywania dziennika sysmon

Obsługa odbierania i przechowywania dzienników systemu Linux

Obsługa statystyk dziennika, w tym ogólnej liczby i statystyk typu dzienników Syslog, netflow, metadanych, sysmon i linux.

Obsługa analizowania i wyświetlania dzienników IPv6 Netflow.

Obsługa wyszukiwania zagrożeń, serwerów, usług i dzienników w języku naturalnym, języku SPL i kombinacji predefiniowanych warunków.

Obsługuje zdarzenia oznaczone jako false positive i zapewnia funkcję czyszczenia, którą można ręcznie usunąć pojedyncze zagrożenia lub usunąć zagrożenia partiami

Analiza podatności

Obsługa wyświetlania i przeglądania sytuacji podatności z perspektywy hosta, w tym: adres IP hosta, nazwa raportu podatności, czas skanowania, status podatności,

Obsługa wyświetlania i przeglądania sytuacji podatności z perspektywy podatności, w tym: nazwa podatności, typ podatności, poziom podatności, liczba ustaleń

Obsługa ręcznego importu raportów o podatnościach, minimum raportów w formacie .nessus z wersji 6.x i 8.x.

Obsługa instalacji dodatkowych skanerów podatności w celu uzyskania raportów o podatnościach, administratorzy mogą dodawać, przeglądać, modyfikować i usuwać skanery;

Obsługa wydawania zasad skanowania i konfiguracji skanowania do urządzeń skanujących podatności

Obsługa okresowego zarządzania zadaniami skanowania (codziennie, co tydzień, co miesiąc), dodawanie, usuwanie, modyfikowanie, otwieranie i zamykanie zadań skanowania

Zarządzanie ryzykiem

Wyświetlanie ogólnych informacji o ryzyku wszystkich zasobów/serwerów/usług w formie wykresów, w tym: liczba ryzykownych zasobów, liczba ważnych zagrożonych zasobów, rozkład ryzykownych serwerów, rozkład zagrożeń serwera / trend tygodniowy, rozkład podatności serwera / trend tygodniowy.

Obsługuje wyświetlanie listy ryzykownych zasobów/serwerów/usług i szczegółów poszczególnych ryzykownych zasobów. Szczegóły ryzykownych zasobów obejmują trzy wymiary: raport ryzyka, podatność serwera i same zagrożenia.

Obsługa eksportowania 10 000 najważniejszych zagrożeń/informacji o ryzykownych zasobach przechowywanych w systemie w formacie CSV

Obsługuje funkcję oceny awarii ryzykownych serwerów i ryzykownych terminali

Reagowanie na incydenty

Wspieranie wyznaczonej osoby odpowiedzialnej za przetwarzanie odpowiednich zagrożeń, podatności i obiektów ryzyka za pośrednictwem systemu zleceń pracy

Obsługa statystycznego wyświetlania wskaźnika realizacji zleceń, całkowitej liczby zleceń, oczekujących zleceń i innych informacji.

Obsługuje dodawanie powiązanych podmiotów do platformy XDR w celu scentralizowanego zarządzania, wykonywanie działań na powiązanych podmiotach,

Obsługa sieciowych urządzeń zabezpieczających NGFW, IPS, WAF tego samego producenta

Obsługa statystycznego wyświetlania całkowitej liczby playbooków, automatycznych playbooków i potwierdzonych playbooków oraz innych informacji.

Obsługuje konfigurację warunków wyzwalania, warunków oceny dla automatycznej reakcji i działań odpowiedzi (wydawanie polityk, blokowanie adresów IP lub tworzenie zleceń pracy),

Wbudowane 5 predefiniowanych playbooków, w tym miningu, wymuszeń i słabych haseł.

Podczas wydawania polityki obsługuje ustawianie czasu jej działania

Obsługuje dwa tryby: automatycznych playbooków i potwierdzonych playbooków, tryb potwierdzony obsługuje powiadomienia e-mail do administratora.

Playbook obsługuje dopasowywanie adresów IPv4 i IPv6 oraz segmentów adresów.

Gdy playbook wykonuje zadanie, które wymaga ręcznego potwierdzenia, zostanie ono zapisane na liście zadań, na które należy odpowiedzieć,

Obsługa polityk dostarczanych do firewalla za pośrednictwem playbooków, muszą być sprawdzane przez agregację polityk, aby uniknąć dużej liczby podobnych polityk pojawiających się na urządzeniu firewall i wpływających na wydajność firewalla.

Zarządzanie raportami

Centralne wyświetlanie wszystkich wygenerowanych raportów, obsługa przeglądania zawartości raportów online lub eksportowanie i wyświetlanie w formacie PDF; obsługa natychmiastowego ręcznego generowania raportów o określonych wymaganiach

Obsługa konfiguracji zadań raportowania i regularne generowanie odpowiednich raportów zgodnie z ustalonymi warunkami, w tym raportów dziennych, tygodniowych i miesięcznych, a także raportów krótkich i szczegółowych.

Obsługa uruchamiania/zatrzymywania zadań raportowania w dowolnym momencie

Wstępnie ustawione szablony dla ogólnych raportów ryzyka, raportów ryzyka terminali, raportów ryzyka serwerów i raportów reagowania na incydenty, a także obsługa niestandardowych szablonów raportów skonfigurowanych przez użytkownika

Obsługa logo raportu zdefiniowanego przez użytkownika

Wsparcie dla statystyk i archiwizacji dokumentów i raportów

Intelligence Center

Obsługuje odbieranie nowych informacji o zagrożeniach i obsługuje zapytania wywiadowcze na podstawie adresu IP/pliku/domeny/nazwy URL/nazwy/CVEID/etykiety zagrożenia z perspektywy poziomu zagrożenia i zakresu czasu.

Po otrzymaniu wypchniętych informacji CVE, wsparcie w celu zainicjowania powiązanych zadań skanowania podatności i wysyłania zleceń pracy

Obsługa wyświetlania informacji o rodzinie/grupie i obsługa powiązania z modułem śledzenia w celu generowania tagów

Obsługuje co najmniej 7 typów baz danych wywiadowczych, w tym bazę danych wywiadowczych DNS, bazę danych wywiadowczych złośliwego kodu, bazę danych wywiadowczą URL, bazę danych wywiadowczą IP, bazę danych wywiadowczą podatności, bazę danych wywiadowczą wykrywania włamań i bazę danych geolokalizacyjnych.

Obsługuje aktualizację offline i aktualizację online bazy danych wywiadowczych. Aktualizacja online obejmuje aktualizację ręczną i zaplanowaną.

Obsługa zdefiniowanej przez użytkownika białej listy nazw domen, skutecznej dla wszystkich reguł DNS;

Obsługa zdefiniowanej przez użytkownika białej listy plików, która obowiązuje dla wszystkich reguł klasy plików;

Obsługa zdefiniowanej przez użytkownika konfiguracji globalnej białej listy

Obsługa importu/eksportu białych list globalnych, klas DNS i klas plików jako plików CSV

Obsługa zdefiniowanej przez użytkownika czarnej listy DNS, złośliwego kodu i IP

Zarządzanie zasobami

Obsługa wsadowego importu/eksportu informacji o zasobach obszaru, usługi, serwera i terminala w postaci plików CSV.

Obsługa aktywnego wykrywania i ręcznego importowania w celu wykrywania i wyświetlania zasobów w sieci prywatnej, ale nie na liście zasobów, które mogą być klasyfikowane i aktualizowane przez użytkowników

Obsługa ekstrakcji odcisków palców zasobów, w tym informacji o systemie operacyjnym, otwartych portach, wdrożonych aplikacjach i wersjach, adresach MAC, producentach itp.

Obsługa zaawansowanej klasyfikacji zasobów, w tym etykiet klasyfikacji zasobów w 5 głównych kategoriach i 29 podkategoriach, takich jak terminale, serwery, sprzęt sieciowy, sprzęt bezpieczeństwa, sprzęt IOT i inny sprzęt.

Obsługa scentralizowanego zarządzania obszarami sieci, w tym zarządzanie konfiguracją ważności, lokalizacji i osób odpowiedzialnych.

Obsługa statystycznego wyświetlania liczby terminali i serwerów w obszarze sieci.

Obsługa scentralizowanego zarządzania serwerami i grupami serwerów, w tym zarządzanie konfiguracją adresu IP, obszaru, usługi, systemu operacyjnego, typu usługi itp., obsługa konfiguracji wielu segmentów sieci IP;

Obsługa scentralizowanego zarządzania terminalami i grupami terminali, w tym zarządzanie konfiguracją adresów IP, obszarów, systemów operacyjnych itp., obsługa konfiguracji wielu segmentów sieci IP;

Obsługa odbierania pakietów rozliczeniowych Radius wysyłanych przez zewnętrzne serwery uwierzytelniania, analizowanie bieżących informacji o użytkownikach i hostach online oraz wyświetlanie ich w "Statusie użytkownika".

Obsługa scentralizowanego zarządzania usługami i przeprowadzanie analizy zagrożeń z poziomu usługi poprzez dodawanie serwerów tego samego typu do tej samej usługi.

Obsługa pasywnej identyfikacji ruchu, wykrywanie i wyświetlanie zasobów sieci prywatnej, które nie znajdują się na liście konfiguracji zasobów, oraz oczekiwanie na potwierdzenie i klasyfikację przez użytkownika.

Obsługuje konfigurację zasobów serwerowych typu IPv6 i zasobów terminalowych oraz obsługuje identyfikację zasobów typu IPv6 za pomocą informacji Netflow.

Rules Engine

Obsługa wykrywania skanowań, w tym skanowanie SYN, skanowanie UDP, atak skanowania adresu IP, atak skanowania portów

Obsługa silnika plików, w tym wykrywanie podejrzanych plików PE (wykonywalnych), plików z niedopasowanym sufiksem i zawartością, podejrzanych plików z wieloma sufiksami, podejrzanych plików z wieloma sufiksami, plików z podejrzanym rozmiarem, plików z niedopasowanym sufiksem i zawartością oraz wrażliwych plików.

Obsługa mechanizmów wykrywania HTTP, w tym HTTP Header Contain Abnormal Keywords, HTTP Response Contain X-Sinkhole, Excessive HTTP Response Errors, Suspicious HTTP Request via Tor.

Obsługa mechanizmów wykrywania podejrzanych protokołów, w tym podejrzanej aktywności IRC, podejrzanej aktywności LDAP, podejrzanej aktywności NetBIOS, podejrzanej aktywności SMB i podejrzanej aktywności SSDP.

Obsługa mechanizmów brute force, w tym FTP Brute Force Attack, IMAP4 Brute Force Attack, LDAP Brute Force Attack, MYSQL Brute Force Attack, POP3 Brute Force Attack, SMTP Brute Force Attack, SSH Brute Force Attack, TELNET Brute Force Attack, Weak Password Cracking, RDP Brute Force Attack, VNC Brute Force Attack i SMB Brute Force Attack.

Obsługa silnika domen, w tym DNS Domain is Generated by DGA, Suspicious Amount of DNS NXDOMAIN Responses, Abnormal DNS Response, TTL in DNS Message is 0, IP Mapped Domain is in Blacklist, IP Mapped Domain is Generated by DGA, Suspicious DNS Tunnel Activity, DNS Protocol Abuse i Suspicious DNS Tunnel Data Transfer.

Obsługa silnika ransomware, analiza i wykrywanie zgodnie z zachowaniem ransomware

Obsługa miningu, inteligentne wykrywanie cech zachowania miningu

Obsługuje silnik klasy zachowania USB, taki jak zachowanie podczas podłączania i odłączania urządzeń USB.

Obsługuje blokowanie dostępu, w tym naruszenie dostępu, tworzenie złośliwych procesów Powershell, naruszenie uprawnień użytkownika do plików lub aplikacji, nieprawidłowe logowanie i naruszenie dostępu do aplikacji;

Obsługuje regułę "Naruszenie dostępu do aplikacji". Użytkownicy mogą określić czarną listę / białą listę dostępu do aplikacji, konfigurując obiekt ochrony w regule, wykrywać, czy ruch ma złośliwy dostęp do określonych zasobów usługi aplikacji i generować zdarzenia zagrożeń

Obsługuje wykrywanie słabych haseł dla 6 protokołów HTTP, TELNET, SMTP, POP3, IMAP i FTP, które przesyłają nazwę użytkownika i hasło w postaci zwykłego tekstu.

Obsługuje ustawienia personalizacji silnika w oparciu o zebrane dzienniki zagrożeń, ustawienia wstępne: Malware, Spam, Phishing, DoS, Atak sieciowy, Skanowanie, EternalBlue, Próba ataku WebShell, RDP Remote Windows Kernel Release Reuse Vulnerability

Obsługuje konfigurację analizy korelacji dzienników zagrożeń hostów

Obsługuje statystyki zagrożeń oparte na polu x-forward

Wsparcie dla korelacji wielu zagrożeń i konfiguracji silnika kill-chain w celu odkrywania nowych informacji o zagrożeniach i dokładnej identyfikacji zagrożeń.

Reguła analizy korelacji klas dzienników zagrożeń sieciowych obsługuje konfigurację adresu źródłowego/docelowego IPv6.

Reguły analizy asocjacji klas nietypowego ruchu obsługują konfigurację segmentów sieci IP typu IPv6,

Zarządzanie logami

Obsługa konfiguracji zaufanych źródeł logów w celu zarządzania i kontrolowania źródeł danych oraz zapewnienia bezpieczeństwa systemu.

Nie ma ograniczeń co do liczby dostępnych źródeł logów

Obsługuje zarządzanie i kontrolę źródeł dzienników Syslog/Netflow oraz ustawienia tworzenia kopii zapasowych i przeglądania dzienników.

Obsługuje analizowanie, prezentowanie i dalszą analizę dzienników Syslog urządzeń innych firm; zapewnia predefiniowane konfiguracje analizowania dzienników i szablony dla popularnych sieciowych urządzeń zabezpieczających innych firm; obsługuje również tworzenie niestandardowych dzienników w oparciu o format konfiguracji i szablonu analizowania dziennika informacji Syslog, reguły parsowania obejmują Grok, klucz-wartość, JSON

Obsługa niestandardowych pól mapowania dla dzienników innych firm

Obsługa wyświetlania miejsca na dysku oraz tworzenie kopii zapasowych

Obsługa przeglądania informacji o hoście, który wysyła dzienniki Sysmon

Obsługuje wysyłanie dzienników Syslog odebranych przez iSource i zagrożeń wykrytych przez platformę do innych serwerów ； Obsługuje konfigurację szyfrowanego protokołu TCP i obsługuje użycie szyfrowanego protokołu TCP do odbierania i przesyłania informacji dziennika.

System zarządzania

Obsługa wyświetlania podstawowych informacji o oprogramowaniu i sprzęcie systemu, takich jak: platforma sprzętowa, wersja oprogramowania, baza reguł, baza geograficzna, wersja bazy danych analizy zagrożeń itp.

Obsługa dodawania, modyfikowania i usuwania użytkowników systemu

Obsługa rozdziału uprawnień dla administratorów, operatorów i audytorów logów.

Obsługa konfiguracji zaufanych hostów i kontrola praw dostępu każdego hosta do systemu XDR

Obsługa konfiguracji i zarządzania wszystkimi kontaktami w systemie

Obsługa rejestrowania dziennika zdarzeń i dziennika operacji samego systemu oraz obsługa ustawiania maksymalnego czasu przechowywania dziennika systemu

Obsługa aktualizacji wersji offline

Obsługa przeglądania licencji systemowych

Obsługa serwera pocztowego, ustawień konta i odbiorcy

Bramka SMS, obsługuje konfigurację modułu SMS

Obsługuje ustawianie reguł alarmowych dla zagrożeń i systemów sprzętowych oraz wyzwala alarmy w postaci wiadomości e-mail, wiadomości tekstowych lub dźwięków;

obsługuje wyświetlanie informacji alarmowych o zagrożeniach, działaniu systemu i wygaśnięciu licencji w interfejsie

Obsługa ustawień systemowego adresu IP i serwera DNS

Obsługa edycji i usuwania podłączonych urządzeń typu Sensor

Obsługa monitorowania podstawowych informacji o podłączonych czujnikach, w tym adresu IP, numeru seryjnego i modelu sprzętu.

Obsługa monitorowania informacji o stanie podłączonych urządzeń Sensor, w tym stanu online, ruchu w czasie rzeczywistym, wykorzystania procesora i wykorzystania dysku.

Obsługa ustawień zabezpieczeń systemu, ustawień zasad logowania, ustawień zasad haseł

Obsługa ustawień serwera pocztowego, konta i odbiorcy

Obsługa funkcji ustawień zabezpieczeń:

W przypadku korzystania z domyślnego administratora systemu do logowania i hasła początkowego do urządzenia, system obsługuje funkcję wymuszania zmiany hasła początkowego;

Obsługuje konfigurację funkcji limitu czasu logowania. Po zalogowaniu się użytkownika do urządzenia, jeśli żadna operacja nie zostanie wykonana po upływie określonego limitu czasu, użytkownik musi ponownie zalogować się do urządzenia

Obsługa funkcji blokady użytkownika, jeśli użytkownik wprowadzi nieprawidłową nazwę użytkownika i hasło określoną liczbę razy. System zablokuje konto użytkownika lub adres IP zgodnie z określonym czasem blokady

Obsługuje konfigurację reguł haseł, z którymi muszą być zgodne hasła użytkowników;

Obsługa konfiguracji funkcji wymuszonej zmiany hasła dla nowych użytkowników.

Obsługa konfiguracji funkcji wymuszonej modyfikacji hasła. Jeśli hasło do konta użytkownika przekroczy określoną datę wygaśnięcia, system wymusi na użytkowniku użycie hasła przy ponownym logowaniu.

Obsługuje generowanie niezależnych reguł alarmowych dla zasobów/zdarzeń, aby spełnić zróżnicowane wymagania alarmów w różnych scenariuszach.

Obsługa przeglądania stanu każdego urządzenia w klastrze

Obsługa przywracania ustawień fabrycznych, z wyborem czy wyczyścić wszystkie informacje konfiguracyjne, przechowywane dane, licencję

Zarządzanie hierarchiczne

Obsługuje hierarchiczne wdrażanie zarządzania, wykorzystuje kanał kaskadowy oparty na transmisji TCP i dwukierunkowym uwierzytelnianiu SSL do realizacji połączenia między platformą wyższego poziomu a platformą niższego poziomu.

Platforma wyższego poziomu obsługuje pełnoekranowe zarządzanie hierarchiczne, prezentując sytuację ryzyka całej platformy.

Platforma wyższego poziomu obsługuje przełączanie do widoku innych platform, obsługuje przeglądanie ryzykownych aktywów, słabych punktów, zagrożeń i innych informacji

Proponowane rozwiązanie musi obsługiwać przepustowość 3 Gb/s

Proponowane rozwiązanie musi obsługiwać 5000 EPS

Licencja oprogramowania powinna być bezterminowa wraz ze wsparciem na okres 36 miesięcy

Wsparcie techniczne dystrybutora rozwiązań w języku polskim

Wdrożenie obejmuje:

- Konfiguracja systemu bezpieczeństwa;
- Integrację źródeł danych z posiadanych systemów bezpieczeństwa;
- Standaryzację danych w celu umożliwienia efektywnej analizy oraz identyfikowania wzorców wskazujących na potencjalne zagrożenia;
- Utworzenie reguł alarmowych i progów wykrywania anomalii;
- Implementacja mechanizmów umożliwiających odpowiedzi na wykryte zagrożenia;
- Automatyzacja procesów reagowania na incydenty bezpieczeństwa obejmujące pozostałe elementy systemu bezpieczeństwa;
- Przeprowadzenie testów w celu upewnienia się, że wszystkie systemy działają zgodnie z założeniami.
- Dostosowanie ustawień na podstawie wyników testów i bieżących potrzeb.
- Przeszkolenie zespołu IT w zakresie obsługi nowych narzędzi i procesów;