iS Sec vs SIEM

Funkcjonalności i użyteczności

		SIEM	iS Sec
1	Korelacyjne reguły oparte na danych z różnych źródeł zdarzeń	🔒	🔒
2	Kategoryzacja techniczna potencjalnych incydentów	🔒	🔒
3	Zaawansowane parsowanie zdarzeń (regex, xml, json) w oparciu o podstawowe formaty pobierania zdarzeń m.in. Windows Event forwarding, syslog, konektory baz danych, e-mail oraz pliki płaskie	🔒	🔒
4	Rozszerzanie i standaryzacja zdarzeń	🔒	🔒
5	Proces uporządkowujący pracę osób odpowiedzialnych za zarządzanie incydentami	🔓	🔒
6	Korelacja wykrytych problemów i anomalii działania w infrastrukturze sieciowej z logami hostów/urządzeń	🔓	🔒
7	Informacja o priorytecie biznesowym oraz niebezpieczeństwie związanym z potencjalnym incydentem	🔓*	🔒
8	Wspomaganie szacowania ryzyka w odniesieniu do różnych typów zagrożeń	🔓	🔒
9	Prezentacja potencjalnych ścieżek ataków ułatwiająca operatorom ocenę rzeczywistego zagrożenia ich wystąpienia względem analizowanego zasobu z różnych obszarów sieci	🔓	🔒
10	Elementy SOAR działające na podstawie matrycy MITRE ATT & CK, umożliwiające automatyczną reakcję na różne techniki działania cyberprzestępców.	🔓	🔒
11	Agregacja i analiza niestandardowych logów pochodzących z systemów dziedzinowych	🔓	🔒
12	Integracja z systemami EDR wspomagająca szerszą analizę działania infrastruktury sieciowej z uwzględnieniem złośliwego oprogramowania	🔓	🔒
13	Integracja z systemami ticketowymi w celu zgłoszenia wykrytego problemu do specjalistycznego wsparcia IT.	🔓	🔒
14	Tworzenie raportów oraz zgłaszanie incydentów do CSIRT NASK	🔓	🔒

🔓* Systemy SIEM pozwalają tylko na budowanie list zasobów o określonej ważności dla organizacji

infoSoftware POLSKA

iS Sec

System klasy SIEM z elementami EDR oraz SOAR

Twoja tarcza do ochrony przed cyberatakami

- **iS Sec** daje możliwość wykrywania, reagowania i zarządzania incydentami oraz podatnościami
- Umożliwia pełny monitoring wraz z analizą logów, automatyzuje operacje związane z zarządzaniem bezpieczeństwa
- Dzięki **iS Sec** wszystkie dane na temat luk, incydentów i ryzyka są zebrane w jednym centralnym miejscu

Sprawdź co oferuje iS Sec →

Sprawdź co oferuje iS Sec

1 BEZPIECZEŃSTWO OPERACYJNE

System wspiera bezpieczne zarządzanie i eksploatację systemów informatycznych uwzględniając dyrektywę NIS2

2 BEZPIECZEŃSTWO SYSTEMÓW

iS Sec zabezpiecza infrastruktury sieciowe przed niepożądanym i nieprawidłowym działaniem urządzeń, systemów operacyjnych oraz oprogramowania.

3 BEZPIECZEŃSTWO STRATEGICZNE

iS Sec łączy zarządzanie informacjami o bezpieczeństwie i zarządzanie zdarzeniami bezpieczeństwa w jednym systemie.

4 BEZPIECZEŃSTWO KOMUNIKACJI

system integruje się z urządzeniami sieciowymi, daje to możliwość śledzenia bezpieczeństwa komunikacji wewnętrznej i zewnętrznej.

5 OCHRONA SIECI

nasz zintegrowany system wykrywa cyberataki i reaguje na różnego rodzaju zagrożenia z nich wynikające.

6 OCHRONA PRZED ZŁOŚLIWYM OPROGRAMOWANIEM

możliwość integracji z oprogramowaniem typu EDR.

BĄDŹ KROK PRZED ZAGROŻENIAMI

nasza baza danych o podatnościach informuje Cię o potencjalnych słabościach Twojego systemu.

ZROZUM ATAKUJĄCEGO

nasz framework analizy taktyk daje Ci wgląd w metody działania potencjalnych intruzów

ZARZĄDZAJ CIĄGŁOŚCIĄ DZIAŁAŃ

dzięki narzędziu do monitorowania zasobów IT, zawsze wiesz, kiedy coś jest nie tak. System śledzi działania poszczególnych urządzeń/hostów.

KONTROLUJ DOSTĘP

nasz system gwarantuje, że tylko uprawnione osoby mają dostęp do Twoich zasobów

MONITOROWANIE I RAPORTOWANIE

monitoruj urządzenia/hosty należące do Twojej infrastruktury sieciowej. System zbiera informacje dotyczące problemów, zdarzeń oraz incydentów.

Najważniejsze funkcje iS Sec

BEZPIECZEŃSTWO OPERACYJNE I SYSTEMOWE

- bezpieczne zarządzanie systemami informatycznymi
- wykrywanie i usuwanie zagrożeń/incydentów
- neutralizacja cyberataków
- automatyczna ochrona przed technikami cyberprzestępców (MITRE ATT & CK)

MONITORING , AGREGACJA I ANLIAZA LOGÓW

- wizualizacja wykresów w jednym widoku
- raporty i statystyki
- monitorowanie logów
- przegląd i analiza logów systemowych/ dziedzinowych oraz działań użytkowników
- śledzenie urządzeń i hostów

INWENTARYZACJA ZASOBÓW WRAZ Z ANALIZĄ PODATNOŚCI

- automatyczne / półautomatyczne dodawanie zinwentaryzowanych urządzeń i systemów
- alerty i powiadomienia o podatnościach na urządzeniach i systemach zinwentaryzowanych w obrębie jednostki

WYSOCE KONFIGUROWALNE ALARMOWANIE

- wysyłanie powiadomień, modyfikowane w zakresie harmonogramu eskalacji
- powiadomienia przygotowane i opracowane z użyciem zmiennych makr
- automatyzacja akcji, włącznie ze zdalnymi komendami

MAGAZYN DANYCH HISTORYCZNYCH

- dane przechowywane w bazie
- wbudowane procedury porządkowania
- konfigurowalna historia

WSPARCIE IT

- możliwość bezpośredniego zgłoszenia problemu do zespołu wsparcia IT

Moduły iS Sec

- Analiza podatności
- Monitoring zasobów
- Moduł analizy logów
- Wykrywanie i usuwanie zagrożeń EDR
- Moduł inwentaryzacji
- Zgłaszanie incydentów CSIRT NASK
- Wykrywanie zagrożeń
- Moduł raportów

www.infoSoftware.pl