Najlepsza platforma SOAR.

DFLABS.COM

Wyzwanie.

Stale rosnąca liczba i stopień wyrafinowania cyberataków powodują, że incydenty cybernetyczne są nieuniknione, a organizacje muszą inwestować w rozwiązania umożliwiające minimalizowanie skutków tych incydentów poprzez ich skuteczniejsze identyfikowanie, zarządzanie i ograniczanie.

Zakres wyzwań wpływających na skuteczność i wydajność operacyjną programu bezpieczeństwa może być ogromny. Problemy te obejmują szczególnie: rosnącą liczbę alertów, zwiększone obciążenie analityków, konieczność wykonywania rutynowych zadań, rywalizację o wysokokwalifikowanych analityków, brak transferu wiedzy, a także potencjalne ograniczenia budżetowe.

„ Pojawiła się potrzeba podejścia nakierowanego na pełną automatyzację i orkiestrację, a DFLabs okazał się jedynym na dzień dzisiejszy dostawcą, który mógł zrealizować obie te funkcjonalności."

Jon Oltsik, Senior Principal Analyst, ESG.

Rozwiązanie.

Technologia Security Orchestration, Automation and Response (SOAR) działa jak multiplikator, umożliwiając operacyjnym zespołom bezpieczeństwa wykonywanie większej ilości zadań przy mniejszych nakładach. Realizacja operacji bezpieczeństwa przy pomocy SOAR prowadzi do skrócenia czasu wykrywania i rozwiązywania incydentów, ograniczenia związanego z nimi ryzyka oraz zwiększenia zwrotu z inwestycji (ROI) z wykorzystywanych technologii bezpieczeństwa, przy jednoczesnym zapewnieniu zgodności z przepisami i regulacjami prawnymi.

DFLabs IncMan SOAR jest wielokrotnie nagradzaną, pionierską platformą zaprojektowaną dla centrów bezpieczeństwa (SOC – Security Operations Center), zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT – Computer Security Incident Response Team) i dostawców zarządzalnych usług z dziedziny bezpieczeństwa (MSSP – Managed Security Service Provider). Zapewnia ona automatyzację, orkiestrację i pomiar operacji bezpieczeństwa oraz zarządzanie całym cyklem życia odpowiedzi na incydent. IncMan pozwala na bardziej wydajne i skuteczne kwalifikowanie i segregowanie incydentów, prowadzenie śledztw, eskalację i powstrzymywanie, a także proaktywne wychwytywanie zagrożeń i zaawansowaną analitykę.

Skraca czas odpowiedzi na incydent o 90%

Zwiększa efektywność analityków o 80%

Zwiększa ilość ilość obsługiwanych incydentów o 300%

Automatyzacja.

Zwiększenie możliwości analityków poprzez automatyzację typowych, powtarzalnych i żmudnych zadań.

- **Podręczniki Szybkiego Reagowania (R^3 Rapid Response Runbooks)** – konfigurowalne dynamiczne schematy działania obejmujące złożone, statyczne i warunkowe decyzje logiczne oraz ponad 100 zautomatyzowanych akcji dostępnych natychmiast po uruchomieniu.
- **Rekomendowane automatyczne reakcje** – Baza Wiedzy o Automatycznej Reakcji na Incydent (ARK – Automated Responder Knowledge) stosuje technologię uczenia maszynowego do historycznych odpowiedzi na zagrożenia i na tej podstawie rekomenduje odpowiednie scenariusze: dynamiczne (R^3 Runbooks) lub statyczne (Playbooks), co pozwala skuteczniej reagować na przyszłe incydenty.
- **Pełna automatyzacja cyklu życia incydentu** – automatyczne segregowanie, wzbogacanie, badanie i powstrzymywanie incydentów.
- **Akcje przeprowadzane w dwóch trybach** – połączenie manualnych, półautomatycznych i automatycznych działań zapewnia administratorom bezpieczeństwa możliwość określenia stopnia automatyzacji na każdym etapie procesu odpowiedzi na incydent.

DFLABS
CYBER INCIDENTS UNDER CONTROL

Orkiestracja.

Powtarzalne, egzekwowalne, mierzalne i skuteczne przepływy pracy w procesie reakcji na incydent; ciągły proces odpowiedzi na zagrożenia dzięki zastosowaniu orkiestracji różnych rozwiązań bezpieczeństwa.

- **Agregacja, korelacja, analiza** – orkiestracja setek rozwiązań firm trzecich przez Syslog, CEF, email, połączenia do baz danych oraz dwukierunkowe konektory do systemów SIEM i innych popularnych produktów z zakresu bezpieczeństwa; obsługa niestandardowych skryptów i dwukierunkowego API.
- **Statyczne (playbooki) i dynamiczne (runbooki R³) warunkowe scenariusze działania** – użytkownicy mogą w sposób elastyczny dobierać metody orkiestracji w nawet najbardziej złożonych procedurach bezpieczeństwa.
- **Zintegrowana baza wiedzy** – udostępnia informacje o zagrożeniach, szczegółowe procesy i procedury oraz najlepsze praktyki, co ułatwia transfer wiedzy i zachowanie jej spójności; artykuły zgromadzone w bibliotece wiedzy DFLabs obejmują RODO, ISO, NIST oraz szereg innych regulacji.
- **Wydajne zarządzanie incydentam** – zintegrowane funkcje informatyki śledczej, kompleksowe zarządzanie cyklem życia incydentu, śledzenie zadań i dowodów oraz zaawansowane narzędzia do współpracy sprawiają, że zarządzanie najbardziej nawet złożonymi incydentami jest łatwiejsze niż kiedykolwiek.

Pomiar.

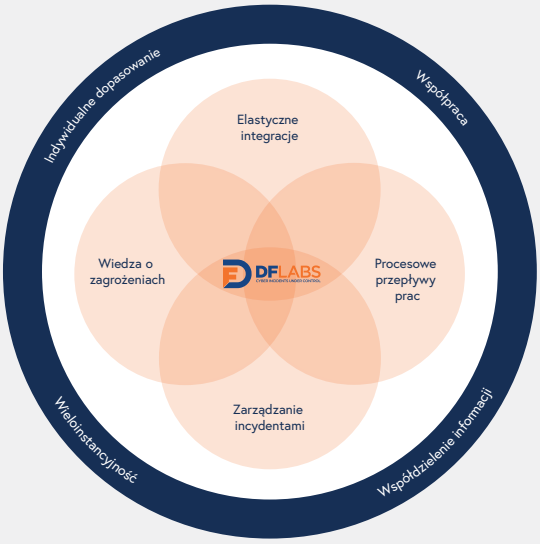
Mierzenie, porównywanie i optymalizacja operacji bezpieczeństwa oraz monitorowanie i ocena odpowiedzi na incydent.

- **Konfigurowalny pulpit nawigacyjny i konfigurowalne widżety** – możliwość obrazowania różnorodnych wskaźników np. KPI (Key Performance Indicators) m. in. w postaci schematów, wykresów, tabel i mierników.
- **Zintegrowany mechanizm raportowania i szablony** – ponad 140 konfigurowalnych wzorców raportów i wskaźników KPI m. in. dotyczących wydajności operacyjnej, incydentów, zagrożeń i zgodności z regulacjami.
- **Kompleksowe metryki incydentów** – pomiar każdej fazy procesu odpowiedzi na incydent w celu optymalizacji, porównania i określenia SLA.
- **Wizualizacja i analiza danych o zagrożeniach i incydentach** – wizualizacja danych o zagrożeniach i incydentach umożliwia wychwytywanie zagrożeń i zaawansowaną analizę danych.

„Platforma IncMan firmy DFLabs odzwierciedla głębię technicznego i procesowego zaawansowania producenta w dziedzinie automatyzacji odpowiedzi na incydent, analizy kryminalistycznej, współpracy i zarządzania sprawami."

Dan Cummins, Senior Analyst 451 Research.

Kompletne i kompleksowe rozwiązanie klasy SOAR.



O DFLabs.

DFLabs jest wielokrotnie nagradzanym i rozpoznawalnym światowym liderem w dziedzinie technologii Security Orchestration, Automation and Response (SOAR). Zespół zarządzający firmy wniósł ogromny wkład w rozwój branży bezpieczeństwa cybernetycznego m. in. uczestnicząc w opracowaniu wielu standardów przemysłowych takich jak ISO 27043 i ISO 30121. Flagowy produkt DFLabs – IncMan SOAR jest używany na całym świecie przez organizacje z list Fortune 500 i Global 2000. DFLabs prowadzi działalność w Europie, Ameryce Północnej i regionie EMEA. Więcej informacji na stronie: www.dflabs.com.

Zmień swoje operacje bezpieczeństwa dzięki technologii SOAR.
Poproś już dziś o wersję demo rozwiązania IncMan SOAR.

Orion Instruments Polska

Partner DFLabs w Polsce:
Orion Instruments Polska Sp. z o. o.
tel. 22 638 31 45, e-mail orion@orion.pl
więcej informacji: www.orion.pl/incident-response

DFLABS CYBER INCIDENTS UNDER CONTROL