

DFLabs IncMan SOAR wychodzi naprzeciw wymogom unijnego Rozporządzenia o Ochronie Danych Osobowych (RODO).

Niniejsze opracowanie przedstawia korzyści jakie mogą
odnieść z zastosowania platformy IncMan SOAR organizacje
zobowiązane do przestrzegania RODO.

DFLABS.COM

Automate.
Orchestrate.
Measure.

Orion
Instruments Polska

DFLABS
CYBER INCIDENTS UNDER CONTROL

Podmiot przetwarzający musi wdrożyć wewnętrzne procedury powiadamiania o naruszeniach.

DFLabs IncMan SOAR, pionierska platforma w zakresie technologii Security Orchestration, Automation and Response (SOAR) 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), umożliwia organizacjom, które muszą zachować

zgodność z RODO, przestrzeganie wymogów powiadamiania o naruszeniach poprzez automatyzację powiązanych procesów, priorytetyzację procesów reagowania na incydenty oraz zarządzanie dystrybucją powiadomień i późniejszą dokumentację każdego incydentu.

Niniejsze opracowanie przedstawia korzyści jakie mogą odnieść z zastosowania platformy IncMan SOAR organizacje zobowiązane do przestrzegania RODO.

Streszczenie.

Rozporządzenie Parlamentu Europejskiego i Rady Unii Europejskiej w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO) zostało przyjęte w kwietniu 2016 r. i zaczęło obowiązywać 25 maja 2018 r. Rozporządzenie kładzie nacisk na przejrzystość, bezpieczeństwo i rozliczalność procesów przetwarzania danych. RODO wprowadza obowiązek oceny skutków przetwarzania dla ochrony danych (DPIA – Data Protection Impact Assessment) w odniesieniu do organizacji, dla których przetwarzanie wiąże się z wysokim ryzykiem np. w przypadku wdrażania nowych technologii, jeśli wykorzystywane jest profilowanie, które może istotnie wpływać na osoby fizyczne jak też w przypadku systematycznego monitorowania na dużą skalę miejsc publicznie dostępnych.

DPIA jest procesem oceny skutków planowanych operacji przetwarzania danych osobowych, umożliwiającym administratorom zidentyfikowanie potencjalnych problemów związanych z prywatnością jeszcze przed ich wystąpieniem i znalezienie sposobu na ich złagodzenie.

Podmioty przetwarzające dane osobowe muszą wdrożyć wewnętrzny proces powiadamiania o naruszeniach i mają obowiązek zgłosić je organowi nadzorcemu nie później niż w ciągu 72 godzin, jak również bezzwłocznie poinformować o naruszeniu ochrony danych osobę, której dane dotyczą. Uchybienie powyższym obowiązkom zagrożone jest karą w wysokości do 20 000 EUR lub 4% całkowitego rocznego światowego obrotu przedsiębiorstwa z poprzedniego roku obrotowego.

Wymagania RODO.

Podmiot przetwarzający dane (procesor) musi:

- Ustanowić sformalizowane procedury reagowania na incydenty
- Wdrożyć wewnętrzne procesy powiadamiania o naruszeniach
- Bezzwłocznie informować osobę, której dane dotyczą, o naruszeniu jej danych osobowych
- Powiadomić organ nadzoru (Prezesa Urzędu Ochrony Danych Osobowych) w ciągu 72 godzin
- Zapewnić zgodność z regulacjami pod karą administracyjną w wysokości do 20 000 EUR lub do 4% rocznego obrotu

Główne wnioski.

1. Platforma DFLabs IncMan do orkiestracji i automatyzacji zadań z dziedziny bezpieczeństwa (SOA) zapewnia automatyzację i priorytetyzację odpowiedzi na incydenty oraz realizuje związane z nimi zadania wzbogacania danych i kontekstów oraz powstrzymywania zagrożeń, rozpowszechniania odpowiednich powiadomień i wdrażania planu reagowania na incydenty (IRP) w przypadku potencjalnego naruszenia danych.
2. IncMan obsługuje różne etapy procesu obsługi incydentów i powiadomień o naruszeniu bezpieczeństwa, w tym zapewnia zaawansowane funkcje raportowania z odpowiednimi wskaźnikami, a także umożliwia gromadzenia wiedzy o zagrożeniach i dzielenie się nią ze stronami trzecimi.

Jak IncMan zapewnia odpowiedź na incydent związany z RODO.

Ponieważ liczba naruszeń stale wzrasta, a cyberataki stają się coraz bardziej wyszukane, władze dostrzegły potrzebę zwiększenia poziomu regulacji w zakresie ochrony danych osobowych. Wzrosła również liczba równoczesnych procesów wymaganych w typowej analizie kryminalistycznej lub scenariuszu odpowiedzi na incydent.

Procesy te muszą obejmować szeroki zakres technologii i przypadków użycia, muszą być ustandaryzowane i powinny realizować jasno określone, w pełni udokumentowane działania oparte na wymogach regulacyjnych, międzynarodowych standardach i ustalonych najlepszych praktykach.

Dodatkowo, funkcje wzbogacania kontekstu i analizy zagrożeń powinny być zintegrowane, aby ułatwić i zautomatyzować raportowanie i powiadamianie o naruszeniach danych w ramach czasowych określonych przez RODO.

Na koniec należy utworzyć dostosowane schematy działania (playbooks), które umożliwią szybką reakcję na określone typy incydentów, a także zapewnią pomoc w priorytetyzacji zadań, przydzielaniu ich poszczególnym interesariuszom oraz sformalizowaniu, egzekwowaniu i mierzeniu określonych przepływów pracy.

Organizacje potrzebują nie tylko planu reagowania na incydenty, ale muszą również mieć powtarzalne i skalowalne procesy, ponieważ jest to jeden z kroków w kierunku uzyskania zgodności z wprowadzoną przez RODO zasadą rozliczalności, wymagającą od administratora danych wykazania, w jaki sposób zapewnia on przestrzeganie zasad ochrony danych podczas prowadzenia działalności biznesowej. Firmy muszą też być w stanie zapewnić spełnienie wymogu powiadomienia o naruszeniu w ciągu 72 godzin lub staną w obliczu surowej kary.

Organizacje powinny ustanowić ramy rozliczalności, a także kulturę monitorowania, przeglądu i oceny procedur przetwarzania danych w celu wykrywania, raportowania i prowadzenia postępowań we wszelkich przypadkach naruszenia ochrony danych osobowych.

Kluczowe jest więc posiadanie platformy służącej sformalizowaniu i wsparciu powyższych wymagań. DFLabs IncMan wyposażony jest we wszystkie niezbędne funkcje, aby to ułatwić.

DFLabs IncMan SOAR i spełnienie wymogów RODO:

• Wykazanie zgodności

- Zintegrowane schematy działania (playbooks) do odpowiedzi na incydent RODO i powiadamiania o nim
- Sformalizowane, powtarzalne i egzekwowalne przepływy pracy w ramach odpowiedzi na incydent związany z RODO

• Zapewnienie powiadomienia regulatora o naruszeniu w ciągu 72 godzin oraz powiadomienie stron trzecich

- Funkcje wzbogacania kontekstu oraz analizy zagrożeń
- Pozyskiwanie wiedzy o zagrożeniach z różnych źródeł i bezpieczne dzielenie się informacją z podmiotami trzecimi
- Zintegrowane raporty i wskaźniki KPI (Key Performance Indicators)

IncMan SOAR implementuje szczegółowe i dostosowane do konkretnych przypadków procedury reagowania na incydenty gwarantując segregację danych i spełniając wymogi kontroli krytycznych aspektów bezpieczeństwa. Dla zapewnienia właściwej odpowiedzi na incydenty i powiadamiania o naruszeniach w złożonych organizacjach z wieloma oddziałami, IncMan może być wdrożony jako rozwiązanie wieloinstancyjne ze zdefiniowanymi prawami dostępu opartymi na rolach.

W celu zaoszczędzenia cennego czasu i zasobów oraz zmniejszenia okna czasowego od wykrycia incydentu do powstrzymania zagrożenia niezbędne są zautomatyzowane reakcje. Organizacje mogą z łatwością przygotowywać zaawansowane raporty na podstawie danych automatycznie zbieranych

z incydentów i analiz śledczych. Mogą także dystrybuować powiadomienia w oparciu o szczegółowe zasady zgłaszania naruszeń i informowania klientów, których naruszenia te dotyczą, jeśli jest to wymagane do zapewnienia zgodności z RODO i uniknięcia kary finansowej.

Wreszcie, możliwość gromadzenia i udostępniania, pochodzącej z różnych źródeł, wiedzy o zagrożeniach przy zastosowaniu anonimizacji danych pozwala na bezpieczne udostępnianie informacji stronom trzecim, a tym samym zapewnia ochronę danych bez konieczności powstrzymywania dochodzenia. IncMan wyposażony jest w zintegrowany moduł bazy wiedzy do dokumentowania schematów działania, oceny zagrożeń, świadomości sytuacyjnej i najlepszych praktyk, które można udostępniać i przekazywać w obrębie całej organizacji.

Porozmawiaj z nami, aby dowiedzieć się więcej.

Organizacje muszą określić kryteria rozliczalności, jak również zasady monitorowania, analizowania i oceny.

O DFLabs.

DFLabs jest wielokrotnie nagradzanym i rozpoznawalnym światowym liderem w dziedzinie technologii Security Orchestration, Automation and Response (SOAR).

Jego nowatorska platforma IncMan SOAR została specjalnie zaprojektowana do zarządzania, pomiaru i orkiestracji zadań z dziedziny cyberbezpieczeństwa, w tym kwalifikacji, segregacji i eskalacji incydentów, wychwytywania i badania zagrożeń oraz podejmowania działań naprawczych.

IncMan SOAR wykorzystuje możliwości uczenia maszynowego i automatyzacji do zwiększenia możliwości analityków oraz maksymalizacji skuteczności i efektywności operacyjnych zespołów bezpieczeństwa, skracając czas od

wykrycia naruszenia do rozwiązania problemu przy jednoczesnym zwiększeniu zwrotu z inwestycji w istniejące technologie bezpieczeństwa.

Flagowy produkt DFLabs – IncMan SOAR jest używany na całym świecie przez organizacje z list Fortune 500 i Global 2000.

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.

DFLabs prowadzi działalność w Europie, Ameryce Północnej i regionie EMEA.

Więcej informacji na stronie:

www.dflabs.com.

KONTAKT DO NAS

IT – +39 037 382 416

UK – +44 203 286 4193

US – +1 201 579 0893

Email – sales@dflabs.com

O Orion Instruments Polska.

Orion Instruments Polska działa od roku 1990 i koncentruje się na rozwiązaniach klasy SIEM, monitoringu baz danych i aplikacji oraz wdrażaniu systemów zarządzania, pomiaru i orkiestracji zadań z dziedziny bezpieczeństwa (SOA) w tym kwalifikacji incydentów bezpieczeństwa, ich segregacji i eskalacji, wychwytywania i badania zagrożeń oraz podejmowania działań naprawczych.

Firma zapewnia ekspercką ofertę o wysokiej wartości dodanej, a oferowane rozwiązania są implementowane przez doświadczonych i certyfikowanych

architektów systemowych z dopuszczeniem do informacji niejawnej.

Od roku 2005 Orion Instruments posiada certyfikat ISO 9001 w zakresie dostawy sprzętu, oprogramowania i usług serwisowych w zakresie infrastruktury informatycznej, usług i doradztwa związanego z prawidłowym funkcjonowaniem systemów informatycznych.

Więcej informacji na stronie:

www.orion.pl.

KONTAKT DO NAS

Tel. – +48 22 638 31 45

Email – orion@orion.pl

**Automate.
Orchestrate.
Measure.**

Orion
Instruments Polska

DFLABS
CYBER INCIDENTS UNDER CONTROL