DFLABS
CYBER INCIDENTS UNDER CONTROL

Orion
Instruments Polska

DFLabs IncMan i RODO

Dokument niniejszy wyjaśnia jakie korzyści w zakresie dostosowania się do wymogów RODO może odnieść organizacja wdrażając platformę IncMan

www.dflabs.com

www.orion.pl

DFLabs IncMan i RODO

DFLabs IncMan – platforma do orkiestracji i automatyzacji zadań z dziedziny bezpieczeństwa (SOA - Security Orchestration & Automation) umożliwia organizacjom, które zobowiązane są do zachowania zgodności z RODO, realizację obowiązku powiadamiania o naruszeniach poprzez automatyzację powiązanych procesów, nadawanie priorytetów odpowiedziom na incydenty, zarządzanie dystrybucją powiadomień i odpowiednie dokumentowanie każdego incydentu.

Niniejszy dokument prezentuje korzyści jakie wynikają z wdrożenia rozwiązania IncMan dla organizacji zobowiązanej do zgodności z 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 zacznie 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.

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

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 nadzorczemu nie później niż w 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.

Główne wnioski

- 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.

- 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.

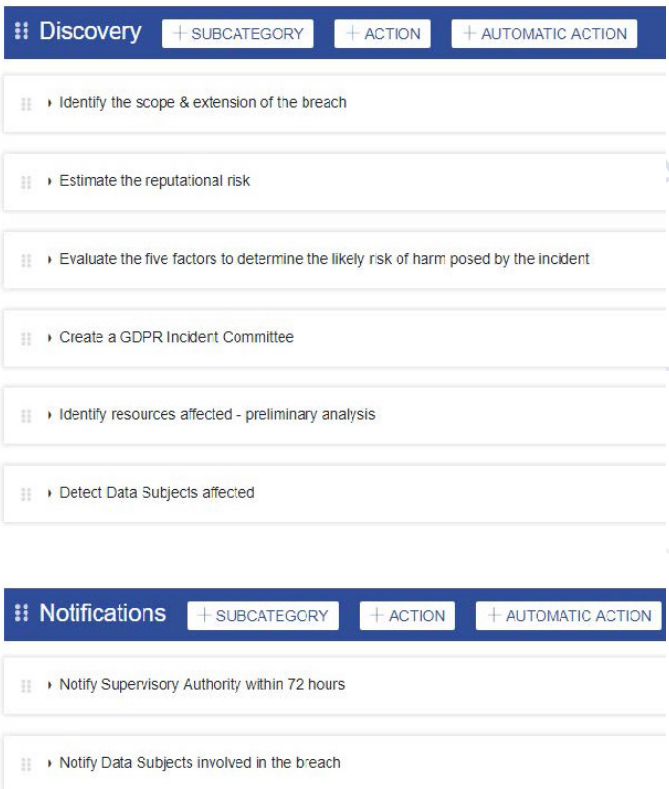
Na koniec należy utworzyć dostosowane schematy działania (playbooks), które umożliwią szybką reakcję na określone typy incydentów, a także zapewnią pomoc w priorytetyzacji zadań, przydzielaniu ich poszczególnym interesariuszom oraz sformalizowaniu, egzekwowaniu i mierzeniu określonych przepływów pracy.

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.

DFLabs IncMan 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 wzbogacanie 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)

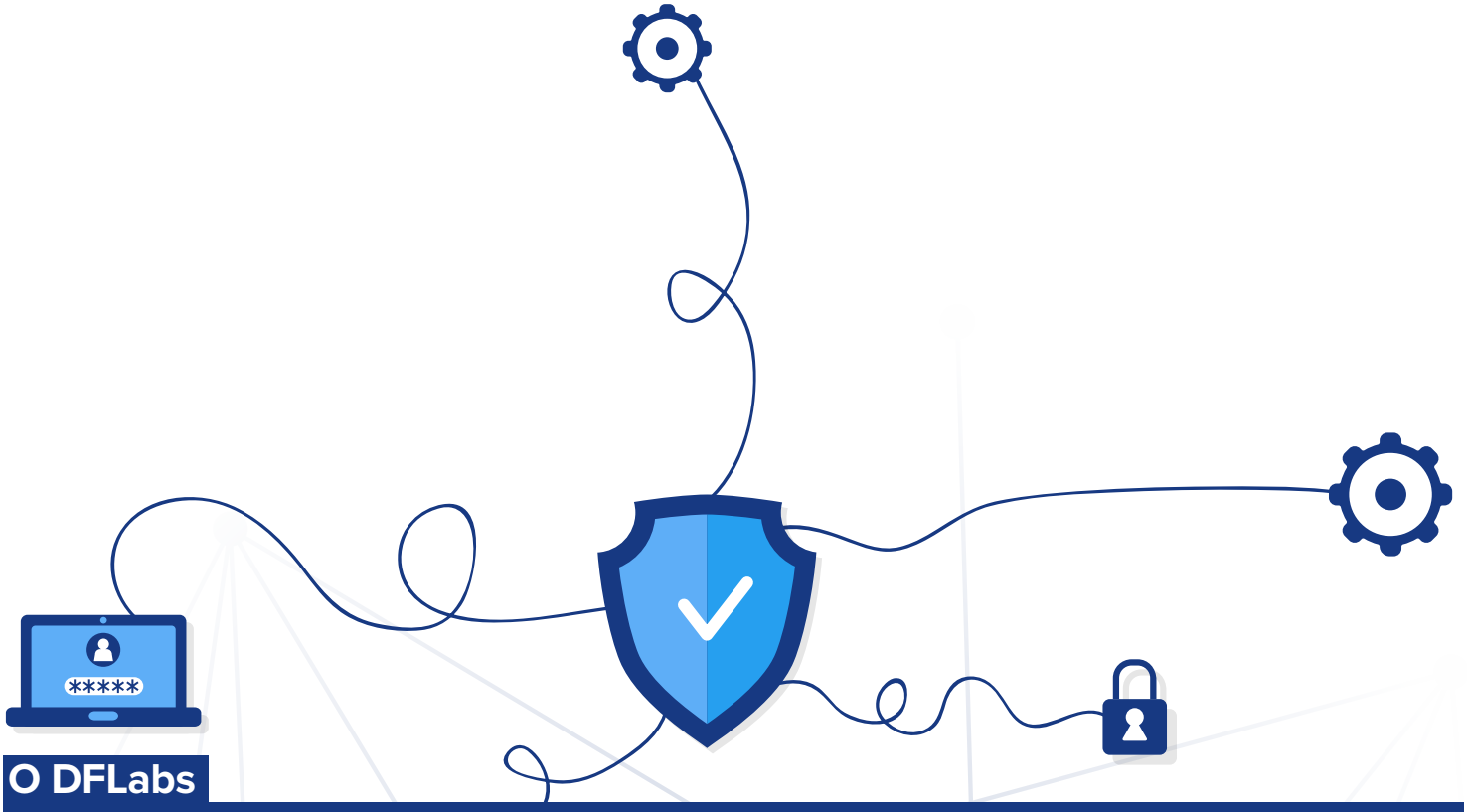


Kluczowe jest więc posiadanie platformy służącej sformalizowaniu i wsparciu powyższych wymagań. DFLabs IncMan wyposażony jest we wszystkie niezbędne funkcje, aby to ułatwić.

IncMan 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 udostępniania 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.



O DFLabs

DFLabs IncMan jest pionierską platforma technologiczną do zarządzania, pomiaru i orkiestracji zadań z dziedziny bezpieczeństwa w tym kwalifikacji incydentów bezpieczeństwa, ich segregacji i eskalacji, wychwytywania i badania zagrożeń oraz podejmowania działań naprawczych. IncMan wykorzystuje uczenie maszynowe i automatyzację do zwiększenia ludzkich możliwości w celu maksymalizacji efektywności i skuteczności zespołów operacji bezpieczeństwa. Redukuje również czas od momentu odkrycia włamania do rozwiązania problemu, co skutkuje zwiększeniem zwrotu z inwestycji wykorzystywanych technologii bezpieczeństwa. Osoby tworzące zespół zarządzający firmy DFLabs cieszą się bardzo wysokim uznaniem w branży ze względu na za wkład w powstanie i rozwój standardów takich jak ISO 27043 i ISO 30121.

www.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.

www.orion.pl

Partner DFLabs w Polsce:

Orion
Instruments Polska

Orion Instruments Polska Sp. z o. o.
05-082 Latchorzew, ul. Warszawska 164
tel. 22 638 31 45, e-mail orion@orion.pl
więcej informacji: www.orion.pl/incident-response