Test: Safetica ONE, czyli ochrona przed wyciekiem informacji s. 48

Legalna dekompilacja s. 58

1
2022

Miesięcznik informatyków i menedżerów IT

www.it-professional.pl

IT professional

Nr 1 (122) styczeń 2022

PLANY CIĄGŁOŚCI DZIAŁANIA s. 8

Identyfikacja zagrożeń w IT, przedstawienie procesu zarządzania bezpieczeństwem i ciągłością działania organizacji

nftables s. 44

Nowe narzędzie w firewallu dla systemu Linux

Krótka historia ransomware'u s. 26

Opis przypadków cyberszantażu i ich konsekwencji na przestrzeni 30 lat

TheHive – reagowanie na incydenty s. 38

Omówienie platformy do analizy i reagowania na zagrożenia w cyberprzestrzeni

Cena 36,00 zł (w tym 8% VAT)
ISSN 2083-9588
9 772083 958004

Serwery ▪ Stacje robocze ▪ Bezpieczeństwo ▪ Infrastruktura i sieci ▪ Zarządzanie i prawo IT ▪ Technologie mobilne

Pojęcie ochrony danych jest dość szerokim zagadnieniem, ale bez wątpienia jest to temat, któremu warto poświęcić uwagę. Ochrona przed wyciekiem informacji w połączeniu z kontrolą użytkowników to dość nośne hasła, w związku z czym postanowiliśmy przetestować rozwiązanie wspomagające administratorów w tym zakresie.

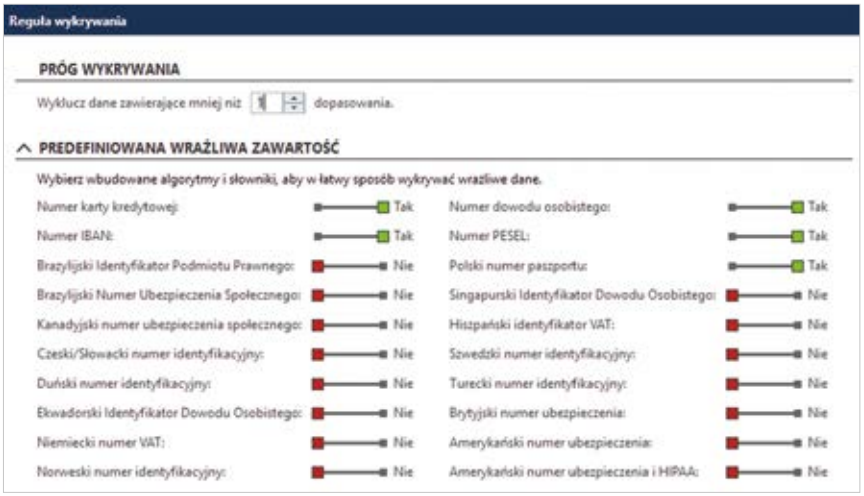
01/2022 REKOMENDACJA REDAKCJI IT professional

Bezpieczeństwo danych

Safetica ONE, czyli ochrona przed wyciekiem informacji

Marcin Jurczyk

Dotychczas testowaliśmy zróżnicowane rozwiązania, których głównym zadaniem była szeroko rozumiana ochrona zasobów informatycznych w przedsiębiorstwie. Wśród produktów, które przewinęły się przez redakcyjny stół testowy, znaleźć można zarówno sprzęt, jak i oprogramowanie, których głównym zadaniem była ochrona zasobów firmowych na wielu poziomach, począwszy od filtrowania ruchu sieciowego, poprzez produkty do monitoringu aktywności użytkowników, na szyfrowaniu danych kończąc. Tym razem mamy do czynienia z rozwiązaniem klasy DLP (Data Loss Prevention), a więc specjalizowanym produktem, którego głównym zadaniem jest zapobieganie utracie danych. Safetica ONE to propozycja od sąsiadów zza naszej południowej granicy. Czeska firma istnieje na rynku od 2007 r. i od samego początku skupia się na zabezpieczeniu danych przed wyciekiem. Własność intelektualna, zapisy kontraktowe, poufne analizy i raporty czy chociażby baza klientów to tylko wycinek większego obszaru, który należy chronić zarówno przed świadomym, jak i nieumyślnym upublicznieniem. Sprawdźmy zatem, w jaki sposób jesteśmy w stanie kontrolować dane z wykorzystaniem Safetiki.

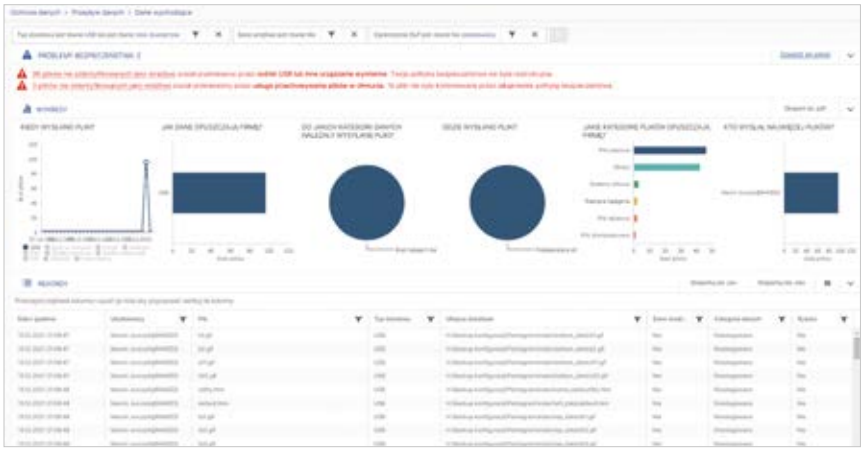


Klasyfikacja danych wrażliwych bazuje na wbudowanych wzorcach. Możliwe jest także zdefiniowanie własnych zasad kontroli danych.

> ARCHITEKTURA I MOŻLIWOŚCI

Podstawowym zadaniem rozwiązań klasy DLP jest ochrona przed zagrożeniami płynącymi z wewnątrz przedsiębiorstwa, mającymi źródło na urządzeniach końcowych obsługiwanych przez użytkowników. Safetica ONE ma za zadanie pomóc przy klasyfikacji danych wrażliwych znajdujących się w plikach oraz wiadomościach mailowych, aby następnie monitorować ich przetwarzanie na podstawie reguł dopasowanych do firmowej polityki ochrony informacji. Aplikacja działa w modelu klient–serwer, przez co konieczne jest zainstalowanie dedykowanego agenta oraz klienta na chronionych urządzeniach, za pośrednictwem których możliwa jest inwentaryzacja plików oraz monitoring wszelkich aktywności na stacjach roboczych. Aplikacja agenta pozwala na komunikację z serwerem. Klient z kolei wymagany jest do zarządzania politykami na chronionych urządzeniach. Z poziomu serwera z kolei wymuszane są zdefiniowane wcześniej polityki i reguły DLP. Wszelkie informacje na temat chronionego

środowiska przechowywane są w centralnej bazie danych. W przypadku Safetiki jest to Microsoft SQL, którego wersję Express wbudowano w program instalacyjny. W najprostszym scenariuszu wdrożeniowym jesteśmy w stanie zainstalować część serwerową wraz z bazą danych na pojedynczej maszynie. W bardziej złożonych implementacjach można odseparować część bazodanową od warstwy aplikacyjnej, a tam, gdzie możliwości darmowego silnika MS SQL nie wystarczą, skorzystać z wersji komercyjnej. Najnowsza oferta Safetiki składa się z trzech produktów oraz opcjonalnych modułów dodatkowych. Mowa tu o Safetica ONE Discovery, Protection oraz Enterprise, których funkcjonalność może być uzupełniona o moduły UEBA (User and Entity Behavior Analytics) oraz Mobile.



Safetica w prosty i przejrzysty sposób informuje o wszystkich operacjach wykonanych na plikach.

DISCOVERY

W przypadku modułu Discovery mamy do czynienia z warstwą budowania wiedzy na temat przechowywanych danych, ich inspekcji oraz kontroli przepływu informacji wraz z analizą ryzyka na bieżąco, uzupełnioną o raporty i alarmowanie. Administrator może w prosty sposób skonfigurować zakres audytu w odniesieniu do kategorii takich jak: aplikacje, urządzenia, strony internetowe, wydruki, ruch sieciowy, wiadomości e-mail oraz pliki. Funkcję ciągłego audytu dla wybranego elementu można po prostu włączyć lub wyłączyć. W zależności od istniejącej struktury organizacyjnej ustawienia te mogą być także dziedziczone. Safetica w pełni integruje się z Active Directory, tak więc łatwo wyobrazić sobie rozbudowany scenariusz z wieloma jednostkami organizacyjnymi czy też grupami dziedziczącymi główne ustawienia z poziomu organizacji, dopasowując wybrane opcje do charakterystyki konkretnej grupy pracowników czy wręcz pojedynczych użytkowników. Za sprawą modułu Discovery dostajemy szczegółowy podgląd aktywności użytkowników w kontekście wspomnianych wyżej kategorii, dzięki czemu łatwo przeanalizować chociażby wykorzystanie poszczególnych aplikacji wraz z czasem aktywnej pracy z podziałem na użytkowników. Dane wyświetlane są zarówno w formie tabelarycznej, jak również wykresów graficznych.

Możliwa jest także łatwa agregacja danych względem dowolnej kategorii, jak np. nazwa aplikacji, komputera, lokalizacja programu czy czas jej działania. Sytuacja wygląda analogicznie w przypadku pozostałych kategorii podlegających kontroli, dostępnych w osobnych oknach menu. W ten sposób łatwo zweryfikować chociażby najczęściej wykorzystywane urządzenia zewnętrzne podpinane do komputerów, jak chociażby pamięć masowa USB czy sprzęt sparowany za pośrednictwem protokołu Bluetooth lub podłączony poprzez FireWire. Analogicznie sprawa wygląda w przypadku komunikacji e-mailowej, ruchu sieciowego czy wydruków – w każdym przypadku można łatwo prześledzić źródło, miejsce docelowe, czas, rozmiar oraz inne szczegóły charakteryzujące aktywność każdego użytkownika czy komputera.

Safetica ONE Enterprise rozszerza funkcjonalność pakietu o rozbudowane możliwości integracji z systemami zewnętrznymi, jak chociażby urządzenia Fortigate, rozwiązania klasy SIEM czy narzędzia analityczne.

Szczególnie ciekawy jest monitoring stron internetowych i wiadomości e-mail. W przypadku tych pierwszych bez trudu przeanalizować można najczęściej odwiedzane witryny WWW, z których część niekoniecznie musi być wykorzystywana w celach służbowych, z uwzględnieniem czasu spędzonego w każdej z nich dla wszystkich użytkowników. Analiza poczty elektronicznej pozwala z kolei sprawdzić np. rodzaj wysłanych załączników lub domeny, pomiędzy którymi odbywała się komunikacja. Moduł Discovery to doskonałe źródło informacji o tym, co się dzieje na komputerach firmowych w zakresie komunikacji elektronicznej oraz przepływu danych, dzięki czemu łatwo zidentyfikować incydenty związane z nieprzestrzeganiem wewnętrznych regulacji.

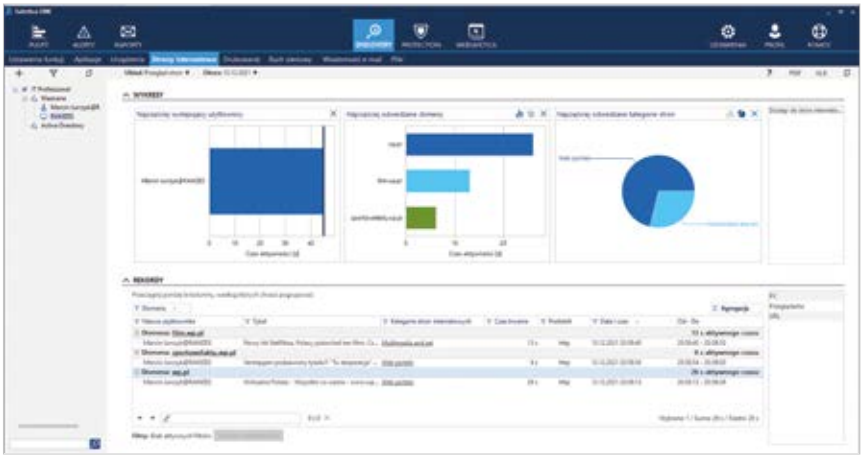
PROTECTION

Safetica Protection rozszerza możliwości pakietu o warstwę ochronną bazującą na regułach i politykach DLP definiowanych

zgodnie z wymaganiami danego przedsiębiorstwa. W tym przypadku poza funkcjami analitycznymi i czysto informacyjnymi dostępne są mechanizmy pozwalające skutecznie zablokować niedozwolone operacje, aby uniknąć przejęcia danych. Oczywiście w pierwszym etapie wdrożenia istnieje możliwość wymuszenia pracy w trybie czysto informacyjnym, jedynie ostrzegającym użytkowników o potencjalnej próbie naruszenia reguł bezpieczeństwa. W takim przypadku wymagane jest potwierdzenie przez pracownika, że dana czynność wykonywana jest w pełni świadomie wbrew obowiązującym zasadom, co ewentualnie pomoże w wyciągnięciu dalszych konsekwencji. Oczywiście możliwe jest także narzucenie twardych reguł uniemożliwiających transfer danych wrażliwych poza firmę.

Ochrona danych w module Protection opiera się na kilku elementach. Najważniejsze z nich to kategorie danych oraz reguły DLP. Oba komponenty są ze sobą ściśle powiązane. Dostępne są trzy typy polityk bezpieczeństwa DLP – ogólna, aplikacyjna oraz bazująca na klasyfikacji danych. W przypadku tej ostatniej konieczna jest wcześniejsza klasyfikacja informacji ze względu na ich rangę. Jednym z najlepszych przykładów będą dane wrażliwe, gdzie wśród kryteriów z pewnością znajdą się takie składniki jak chociażby nr dowodu osobistego, identyfikator PESEL czy chociażby numer karty kredytowej. Producent przewidział predefiniowaną listę słowników, którą z powodzeniem można rozszerzyć o własne wyrażenia regularne RegEx. Warunki można grupować w relacji AND lub OR, dzięki czemu możliwe jest precyzyjne zdefiniowanie wystąpienia dopasowania reguły. Można również zaimportować do 50 własnych słowników w formacie TXT zawierających do 500 tys. słów kluczowych.

Oczywiście możliwe jest określenie wielu polityk DLP. W tym przypadku przetwarzanie odbywa się od góry do dołu i kończy w momencie wystąpienia pierwszego dopasowania. Sama polityka może działać w czterech trybach – od tymczasowego wyłączenia, poprzez logowanie w dzienniku zdarzeń, logowanie z powiadamianiem, po logowanie z blokowaniem. Wbudowana lista reguł może dotyczyć takich elementów jak dyski chmurowe (z rozróżnieniem dla Box Sync, Dropboksa, Google Drive'a, OneDrive Personal, OneDrive Business oraz Sharepointa), przesyłanie danych do usługi hosting plików, do poczty webowej, stron internetowych, poprzez wiadomości e-mail, komunikatory (tylko dla plików), urządzenia wymienne czy chociażby schowek systemowy, zrzuty ekranowe, wydruki, a nawet operacje git push. Dostępne opcje mogą się różnić w zależności od tego, czy wybierzemy politykę ogólną, która pozwala na zarządzanie konkretnym rodzajem komunikacji – jak chociażby kopiowanie danych na urządzenia zewnętrzne – czy też politykę danych, która pozwala na bardziej granularną kontrolę.



Raporty na temat aktywności użytkowników pozwalają w łatwy sposób przeanalizować pozasłużbowe działania w czasie pracy.

ENTERPRISE

Tworzenie polityk opartych na predefiniowanej liście kategorii aplikacyjnych dostępne jest w najwyższej wersji – Safetica ONE Enterprise. Poza automatyczną klasyfikacją danych ze względu na ich kategorię czy też aplikację, z której dane pochodzą, użytkownicy mogą również oznaczać pliki ręcznie, przypisując je do odpowiedniej klasy.

Poza wspomnianymi mechanizmami kategoryzacji danych i polityk DLP możliwe jest także kontrolowanie użytkowników i danych za pomocą definicji stref, stanowiących dodatkową warstwę abstrakcji w zarządzaniu przepływem informacji. W ten sposób można np. zagregować wybrane urządzenia, lokalizacje sieciowe, adresy e-mail czy IP w grupy, którymi można łatwo zarządzać za pośrednictwem reguł DLP. Mechanizm jest szczególnie przydatny w tworzeniu zaufanego środowiska pracy z przypisanymi zasobami, co do których wykorzystania jesteśmy pewni. Inne funkcje dostępne w ramach Safetica ONE Protection to zarządzanie szyfrowaniem dysków na podstawie integracji z BitLockerem.

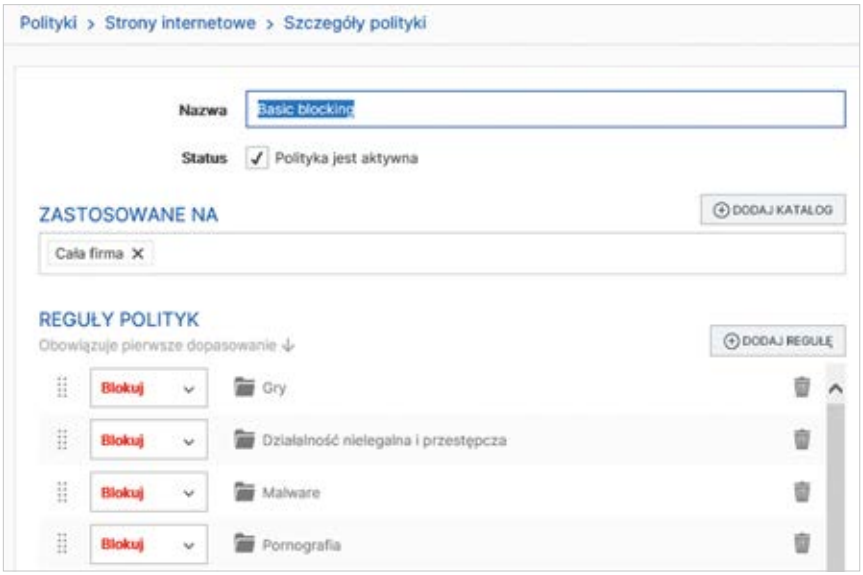
PORÓWNANIE MODUŁÓW

Reasumując – przygodę z Safetica ONE można rozpocząć od zakupu modułu Discovery, za pomocą którego możliwa jest realizacja audytu bezpieczeństwa ze względu na przepływy informacji, zgodność z wybranymi standardami, jak chociażby GDPR lub HIPAA, po wykrywanie podejrzanych aktywności na stacjach roboczych. Aby efektywnie chronić dane i urządzenia końcowe, warto sięgnąć po moduł Protection, za pośrednictwem którego możliwa jest zaawansowana kategoryzacja danych oraz efektywna

kontrola przepływu informacji w firmie wraz z podstawowymi mechanizmami ochrony danych, takimi jak szyfrowanie z wykorzystaniem BitLockera. Na tym poziomie dostępne są również dodatkowe mechanizmy, jak chociażby wsparcie dla funkcji shadow copy, dzięki której można zachować kopie danych będące częścią incydentu bezpieczeństwa. Również na poziomie funkcjonalnym dostępne są opcje blokowania urządzeń przenośnych oraz wydruku, a także kontrola danych we wspomnianych już usługach chmurowych. Safetica ONE Enterprise rozszerza funkcjonalność pakietu o rozbudowane możliwości integracji z systemami zewnętrznymi, jak chociażby urządzenia Fortigate, rozwiązania klasy SIEM czy narzędzia analityczne. Ponadto w tej edycji wspieranych jest także wiele domen AD, a także możliwe jest dopasowanie szaty graficznej do własnych standardów.

Jednym z dwóch dodatkowych modułów, które można dokupić niezależnie od wersji Safetica ONE, jest Safetica UEBA. Rozszerzenie to wprowadza dodatkowe opcje w zakresie analizy aktywności użytkowników, dzięki czemu funkcjonalność DLP zostaje uzupełniona o możliwości dostępne w oprogramowaniu do monitoringu pracowników. Zestawienia na temat aktywności i wykorzystania wspomnianych już wcześniej zasobów rozbudowano o dedykowane alerty i raporty.

Warto również dodać, iż informacje z modułu UEBA dostępne są zarówno z poziomu dedykowanej aplikacji klienckiej, jak również z przeglądarkowej wersji pulpitu o nazwie WebSafetica. Interfejs webowy wykorzystywany jest głównie do wyświetlania raportów i analiz w formie graficznej. Umożliwia także przeprowadzenie podstawowych czynności administracyjnych. Co do zasady jest to interfejs dedykowany mniej technicznym użytkownikom, takim jak analitycy czy kadra menedżerska. Ostatni z opcjonalnych modułów, czyli Safetica Mobile, to uzupełnienie oferty o funkcje zarządzania urządzeniami mobilnymi pracującymi pod kontrolą Androida lub iOS-a. W tym przypadku mamy do czynienia z funkcjami MDP, pozwalającymi wymusić na użytkownikach odpowiednie polityki dotyczące np. złożoności haseł, konfiguracji sieci Wi-Fi czy zdalnego blokowania w przypadku utraty urządzenia. Nasza testowa licencja obejmowała najwyższy pakiet Safetica ONE Enterprise wraz z modułem UEBA, dlatego zarządzania urządzeniami mobilnymi nie udało nam się sprawdzić.



Użyteczną funkcją dostępną w pakiecie jest monitorowanie i kontrola odwiedzanych stron internetowych.

> WYMAGANIA I INSTALACJA

Jak już wcześniej wspomniano, oprogramowanie Safetica ONE można wdrożyć na pojedynczej maszynie, która będzie pełniła funkcję serwera aplikacji w tandemie z usługą bazodanową. Ta sama maszyna udostępnia również interfejs przeglądarkowy – WebSafetica. Dla wdrożeń w środowiskach nieprzekraczających 250 urządzeń końcowych minimalne wymagania sprzętowe to czterordzeniowy procesor, 8 GB pamięci operacyjnej, a także około 100 GB przestrzeni dyskowej. Rozwiązanie można wdrożyć na systemach serwerowych Microsoftu od wersji 2012 w górę. WebSafetica wymaga także zainstalowania i skonfigurowania usługi IIS (przeprowadzana automatycznie podczas instalacji) co najmniej w wersji 7.5. Konieczny jest także .NET w wersji 4.5.2+. Wraz ze wzrostem liczby chronionych końcówek zwiększa się również wymagana moc obliczeniowa. W zakresie od 500 do 2000 użytkowników wystarczy osiem rdzeni procesora i 16–32 GB RAM-u, a także odpowiednio 250–500 GB przestrzeni dyskowej. Powyżej granicy 2000 użytkowników producent zaleca rozdzielenie funkcji serwera aplikacji od bazy danych i przydzielenie odpowiednich zasobów dla każdej z nich. Wśród wspieranych silników bazodanowych znaleźć można jedynie produkty Microsoftu, począwszy od wersji 2012. Producent przewidział także możliwość implementacji swojego rozwiązania w chmurze Microsoftu – Safetikę znaleźć można w Azure Marketplace. W ten sposób możliwa jest kontrola nad przepływem danych i aktywnością użytkowników bez konieczności posiadania dedykowanych zasobów sprzętowych wewnątrz organizacji.

Na liście chronionych systemów klienckich są oczywiście wszystkie wersje okienek, począwszy od wersji Windows

7 SP1 i, co ciekawe, macOS od wersji 10.10 (pełna funkcjonalność DLP od wersji 10.15). Instalację agenta można przeprowadzić ręcznie lub z wykorzystaniem reguł GPO. Ze względu na głęboką ingerencję w zaawansowane funkcje chronionego systemu operacyjnego warto także zweryfikować kompatybilność z używanym oprogramowaniem antywirusowym. W przypadku niektórych wersji produktów AV od różnych producentów może dojść do konfliktu, a sama Safetica może zostać potraktowana jako oprogramowanie szkodliwe.

Safetica ONE licencjonowana jest ze względu na liczbę chronionych urządzeń klienckich. Minimalny zakup to 10 licencji, które można nabyć w formie jedno-, dwu- lub trzyletniej licencji, a także w formie licencji bezterminowej z rocznym wsparciem w cenie.

> ZARZĄDZANIE

Wszystkie czynności administracyjne, począwszy od konfiguracji wszystkich parametrów, poprzez definicję reguł bezpieczeństwa, polityk i zasad, można przeprowadzić za pośrednictwem przeznaczonej do tego aplikacji do zarządzania – Safetica Management Console. Jest to panel sterowania, który można zainstalować na dowolnej stacji roboczej. Do połączenia z serwerem konieczne będzie podanie adresu IP lub nazwy domenowej, portu, na którym dostępna jest usługa, a także danych uwierzytelniania. Interfejs nie jest nadto przeładowany, a nawigacja po menu jest całkiem intuicyjna.

W górnej belce dostępne są trzy sekcje z ikonami menu. Pierwsze trzy ikony od lewej pozwalają na wgląd w status monitorowanych urządzeń wraz z analizą zebranych informacji. Mowa tu o Pulpicie, Alertach oraz Raportach. Kolejne trzy ikony w sekcji środkowej pozwalają na konfigurację funkcji w ramach modułów Discovery oraz Protection. Dostępny jest tu także kafelek przekierowujący do przeglądarki internetowej, w której otwierane jest okno WebSafetiki. Ostatnia grupa trzech ikon to Ustawienia, Profil oraz Pomoc. Sama konfiguracja poszczególnych opcji konfiguracyjnych systemu DLP jest dość przejrzysta i już po kilku minutach łatwo zorientować się w konwencji narzuconej przez producenta. W przypadku poszczególnych ustawień, zmienianych charakterystycznymi suwakami, przydałoby się dodać odnośniki do ustawień wyższego poziomu. Informacja na temat dziedziczenia niektórych ustawień bez wskazania, z którego poziomu to dziedziczenie następuje, może powodować konsternację. IT

Autor jest architektem w międzynarodowej firmie z branży IT. Zajmuje się infrastrukturą sieciowo-serwerową, wirtualizacją infrastruktury i pamięcią masową.

PODSUMOWANIE

Safetica ONE to ciekawa propozycja stanowiąca uzupełnienie podstawowych mechanizmów bezpieczeństwa, które zostały już zaimplementowane w firmie na innych poziomach. Jest to kolejna warstwa ochrony danych tuż obok zapór sieciowych, systemów IPS/IDS, WAF-ów czy rozwiązań typu endpoint protection. Możliwość łatwej i intuicyjnej klasyfikacji danych ze względu na ich znaczenie, a następnie równie szybkie tworzenie reguł dostosowanych do wewnętrznej polityki przedsiębiorstwa, to główne zalety tego rozwiązania. Podstawowe wdrożenie dla niewielkiego środowiska nie powinno zająć więcej niż kilka godzin. Sama obsługa programu jest relatywnie prosta, a dodatkowym ułatwieniem podczas zarządzania systemem jest całkiem dobre spolszczenie interfejsu i to zarówno dedykowanej konsoli administracyjnej, jak również webowego interfejsu dla mniej technicznych użytkowników. Rozbicie oprogramowania na moduły odpowiadające określonej funkcji to dobre posunięcie, pozwalające rozpocząć przygodę z Safetiką nieco mniejszym kosztem. O ile różnica pomiędzy wersjami Discovery, Protection i Enterprise na pierwszy rzut oka jest dość jasna, o tyle zdobycie stuprocentowej pewności, czy dana funkcja aby na pewno jest dostępna w konkretnej edycji, wymaga już zagłębienia się w dokumentację producenta lub bezpośredni kontakt z supportem. Na uwagę zasługuje także możliwość integracji z rozwiązaniami firm trzecich. Dodatkową zaletą z kolei jest możliwość analizy wykorzystania zasobów firmowych. W ten sposób łatwo zweryfikować chociażby wykorzystanie licencji na oprogramowanie oraz przeanalizować czas spędzony przez użytkowników na aktywnościach pozasłużbowych w godzinach pracy.

Werdykt

Safetica ONE

Zalety

- ⊕ rozbudowane możliwości kontroli przepływu danych
- ⊕ wsparcie dla shadow copy oraz rozpoznawania OCR
- ⊕ szeroki wachlarz integracji z oprogramowaniem zewnętrznym
- ⊕ możliwość implementacji w chmurze
- ⊕ szybkość wdrożenia
- ⊕ dostępny język polski

Wady

- ⊖ nieco zawiła dokumentacja

Ocena **9**/10