SECUREVISIO

SecureVisio™
Specyfikacja techniczna

Nowoczesne rozwiązanie zarządzania bezpieczeństwem kategorii IT GRC (Governance, Risk, Compliance), wyposażone w elektroniczną dokumentację systemu teleinformatycznego oraz narzędzia zarządzania incydentami (Incident Management), a także zintegrowane narzędzia analizy wpływu naruszeń bezpieczeństwa na procesy organizacji (Business Impact Analysis). SecureVisio™ może działać jako niezależne rozwiązanie IT GRC w organizacji lub inteligentna platforma do budowy Security Operations Center (SOC).

- Elektroniczna dokumentacja zabezpieczeń
- Baza wiedzy eksperckiej bezpieczeństwa IT
- Narzędzia modelowania zagrożeń
- Narzędzia audytowania bezpieczeństwa
- Narzędzia automatycznego szacowania ryzyka
- Narzędzia oceny konsekwencji incydentu
- Narzędzia symulacji awarii
- Rejestr incydentów bezpieczeństwa
- Moduł integracji z SIEM i zabezpieczeniami sieci
- Moduł integracji z narzędziami Vulnerability Assessment
- Moduł integracji z bazą CVE®
- Moduł raportowania i alarmowania

Elektroniczna dokumentacja zabezpieczeń

- Kreator wstępnej konfiguracji IT GRC
- Parametry techniczne i biznesowe
- Graficzne narzędzia tworzenia i przeszukiwania dokumentacji
- Automatyczne rozpoznanie systemów IT (Asset Discovery)
- Logiczna architektura zabezpieczeń IT (urządzenia bezp., strefy, warstwy ochrony)
- Schematy sieci fizycznej (łącza, przełączniki, rutery, itp.)
- Dołączanie zewnętrznych dokumentów
- Definiowanie dodatkowych parametrów
- Moduł zarządzania rolami i użytkownikami

Baza wiedzy eksperckiej

- Dobre praktyki projektowania zabezpieczeń
- Dobre praktyki audytowania bezpieczeństwa
- Efektywność zabezpieczeń sieciowych
- Efektywność zabezpieczeń lokalnych
- Metodyka szacowania ryzyka

Narzędzia modelowania zagrożeń (Threat Modelling)

- Wyznacz źródła zagrożenia zasobu IT
- Pokaż zabezpieczenia zasobów IT przed potencjalnymi źródłami zagrożenia
- Pokaż najbardziej narażone zasoby IT
- Pokaż lokalizację danych określonej kategorii
- Pokaż zakres i konsekwencje incydentu bezpieczeństwa
- Pokaż obszary sieci nie należące do organizacji
- Pokaż zabezpieczenia chroniące zasób przed określonym źródłem zagrożenia
- Pokaż lokalizację zasobów określonego rodzaju
- Pokaż zasoby posiadające określone zabezpieczenia lokalne
- Pokaż narzędzia zarządzania bezpieczeństwem dla urządzeń zabezpieczeń
- Pokaż narzędzia zarządzania bezpieczeństwem dla ważnych zasobów IT

Narzędzia automatycznego szacowania ryzyka

- Powiązanie systemów IT z procesami biznesowymi
- Ważność procesów biznesowych
- Algorytm analizy ryzyka biznesowego
- Tabela podsumowania ryzyka wszystkich najważniejszych systemów IT

Narzędzia oceny konsekwencji incydentu (Business Impact Analysis)

- Automatyczne obliczanie konsekwencji prawnych i biznesowych wystąpienia incydentu
- Automatyczne obliczanie ważności systemów IT dla organizacji
- Specyficzne zagrożenia teleinformatyczne

Narzędzia audytowania bezpieczeństwa (Security Audit)

- Pokaż narażone zasoby IT o krytycznym znaczeniu biznesowym
- Pokaż ważne zasoby IT narażone na awarie
- Zasoby IT o wysokim poziomie ryzyka
- Pokaż komunikację sieciową bez ochrony kryptograficznej
- Analiza ryzyka zasobów IT dla poszczególnych zagrożeń
- Wbudowane szablony audytu (m.in. KNF, PCI-DSS)
- Kreator definiowania własnych wymagań bezpieczeństwa: wymagania dla zabezpieczeń sieciowych, wymagania dla zabezpieczeń lokalnych, wymagania dla narzędzi zarządzania bezpieczeństwem

Moduł integracji z narzędziami Vulnerability Assessment

- Odczyt raportów skanerów podatności (m.in. Nessus, Rapid7 Nexpose)
- Selekcja podatności na podstawie ważności dla organizacji

Moduł integracji z bazą CVE®

- Automatyczny odczyt danych nt. nowych podatności z bazy CVE
- Specyfikacja oprogramowania ważnych systemów IT (OS, software)
- Selekcja podatności na podstawie ważności dla organizacji

Specyfikacja techniczna

- Virtual Appliance – VMware ESX, VMware Player
- Konsola zarządzania GUI: aplikacja instalowana w systemach Microsoft Windows 7, 8, 8.1 i 10; interfejs Web wspierany przez przeglądarki Microsoft Internet Explorer 9, 10, 11 i Firefox 4x

Narzędzia symulacji awarii

- Powiązanie elementów sieci fizycznej i logicznej
- Identyfikacja Single Point of Failure
- Aktywacja/dezaktywacja elementów sieci i systemów IT
- Wyświetlanie niedziałających procesów biznesowych

Moduł integracji z SIEM i zabezpieczeniami sieci

- Odczyt logów i alarmów z SIEM, firewalli, IPS i innych zabezpieczeń (Syslog)
- Selekcja incydentów dot. systemów IT krytycznych dla organizacji
- Selekcja logów firewall dot. systemów IT krytycznych dla organizacji

Moduł raportowania i alarmowania

- Raporty nt. krytycznych podatności
- Raporty nt. krytycznych incydentów
- Kreator własnych raportów
- Powiadomienia email
- Interaktywny kalendarz
- Export do formy drukowalnej (PDF)

Rejestr incydentów bezpieczeństwa

- Formularz rejestracji i opisu incydentów
- Automatyczny odczyt incydentów (Syslog Universal Parser)

Licencjonowanie

- Oparte na liczbie chronionych systemów IT i urządzeń w sieci
- Rozszerzenie licencji – funkcje modelowania zagrożeń (Threat Modelling), audytowania bezpieczeństwa (Security Audit) i wymagania bezpieczeństwa KNF

O eSecure:

Jesteśmy prywatną firmą z całkowicie polskim kapitałem. Posiadamy wieloletnie doświadczenie zdobyte zarówno na rynku polskim, jak i zagranicznym. Pomagamy naszym Klientom rozwiązywać ich najtrudniejsze problemy, osiągać największe wyzwania, realizować cele, które wymagają wyjątkowych umiejętności profesjonalistów branżowych, ekspertów biznesowych, audytorów, strategów i analityków.

Centrala
ul. Hoffmanowej 19
35-016 Rzeszów
tel.: +48 17 779 62 46

Biuro w Warszawie
Aleje Jerozolimskie 162 A
02-342 Warszawa

www.esecure.pl