esecure | SECUREVISIO

SecureVisio jedna platforma do wykrywania i zarządzania incydentami, podatnościami oraz ryzykiem. System pozwala organizacjom zautomatyzować i ujednolicić podstawowe operacje związane z zarządzaniem bezpieczeństwem w ramach jednej, zintegrowanej platformy. Dzięki temu organizacje optymalizują czas i koszty operacji bezpieczeństwa.
Osoby zarządzające bezpieczeństwem podejmują lepsze decyzje, ponieważ w jednym miejscu mają pełne informacje na temat incydentów, luk w zabezpieczeniach i związanego z nimi ryzyka.

SecureVisio adresuje następujące obszary procesu zarządzania bezpieczeństwem:

1 Świadomość sytuacyjna - inwentaryzacja, mapowanie i wizualizacja zasobów IT oraz procesów

Budowanie świadomości sytuacyjnej w zakresie zasobów, sieci i procesów to jedna z najważniejszych aktywności w procesie zarządzania bezpieczeństwem na poziomie strategicznym i operacyjnym. SecureVisio wyposażono w zautomatyzowane, pasywne i aktywne mechanizmy inwentaryzacji zasobów IT i mapowania sieci. System wykrywa systemy, urządzenia sieciowe i aplikacje, określa ich typ i relacje między nimi. Mechanizmy inwentaryzacji umożliwiają również identyfikację procesów technicznych i biznesowych, których część stanowią zidentyfikowane zasoby lub ich grupy. W ramach inwentaryzacji system dynamicznie wylicza potencjalne wektory ataku i określa możliwe zagrożenia. Infrastruktura analizowana jest również pod kątem zabezpieczeń zastosowanych w sieci i na punktach końcowych. Wszystkie wyniki pracy modułu inwentaryzacji prezentowane są w formie zwizualizowanej, interaktywnej mapy logicznej sieci. Zgromadzone informacje wykorzystywane są przez pozostałe moduły systemu:

- **Stanowią jeden z parametrów korelacji zdarzeń;**
- **Wzbogacają kontekst incydentów w procesie obsługi incydentów;**
- **Są wykorzystywane w trakcie doboru scenariuszy i przydzielania zadań do zespołów obsługi;**
- **Mają wpływ na priorytety incydentów;**
- **Stanowią podstawę automatycznej analizy ryzyka cyberzagrożeń;**
- **Mają wpływ na priorytety i obsługę podatności;**

2 Analiza ryzyka cyberzagrożeń

Analiza ryzyka cyberzagrożeń to strategiczna aktywność w procesie zarządzania bezpieczeństwem. Świadomość ryzyka związanego z cyberzagrożeniami pozwala na efektywne stosowanie zabezpieczeń. Wyniki analizy ryzyka stanowią ważny element świadomości sytuacyjnej i wpływają na działania operacyjne takie jak procesy obsługi incydentów i podatności. Platforma SecureVisio obejmuje mechanizmy automatycznej, dynamicznej analizy ryzyka cyberzagrożeń dla procesów i zasobów, na podstawie danych zgromadzonych i stale aktualizowanych w procesie inwentaryzacji. Zaawansowane algorytmy analityczne uwzględniają macierze zagrożeń i zabezpieczeń, wektory ataków oraz potencjalne konsekwencje dla systemów, procesów i danych. Kontekstowe reguły analizy ryzyka umożliwiają dostosowanie mechanizmów ryzyka do specyficznych potrzeb każdej organizacji. Wyniki analiz prezentowane są w graficznym panelu oceny ryzyka oraz w graficznym modelu sieci. Stanowią one również ważny parametr korelacji zdarzeń i wpływają na priorytety incydentów i podatności.

3 SecureVisio SIEM

Gromadzenie i przechowywanie informacji o zdarzeniach

SecureVisio wyposażono w zaawansowane, wydajne mechanizmy zbierania i przechowywania informacji o zdarzeniach z całej infrastruktury IT. System umożliwia gromadzenie logów za pośrednictwem protokołu syslog, mechanizmu Windows Event Forwarding, interfejsów API, odczyt danych z plików tekstowych, baz danych a nawet skrzynek pocztowych. Zastosowanie bazy danych opartej na plikach płaskich pozwoliło na uzyskanie bardzo wysokiej wydajności. Wbudowane, automatyczne mechanizmy archiwizacji umożliwiają długotrwałe, centralne lub rozproszone, przechowywanie danych na wskazanej przez administratora przestrzeni dyskowej.

Analiza i korelacja zdarzeń

System wyposażono w stale uzupełniany zestaw parserów zdarzeń dla różnych rodzajów źródeł. Mechanizmy parsowania r**egex, xml, json, parsowanie warunkowe** i podrzędne oraz graficzny interfejs tworzenia parserów wraz z wbudowanym debuggerem to potężne narzędzia, które są w stanie przetworzyć i znormalizować dane z dowolnego źródła. Zgromadzone dane dzięki procesowi normalizacji stają się informacjami, które mogą być przeszukiwane i przetwarzane. System wyposażono w automatyczne mechanizmy korelacji zdarzeń i stale rozwijany zestaw reguł korelacyjnych opartych między innymi na matrycy **MITRE ATT&CK**. Zaawansowany, niezwykle elastyczny silnik korelacyjny wyposażono w unikalny zestaw możliwości:

- **Tworzenie zdarzeń na podstawie innych zdarzeń;**
- **Tworzenie incydentów na podstawie zdarzeń;**
- **Nadawanie priorytetów w zależności od kontekstu;**
- **Mechanizm scoringowy uzależniony od profili zasobów;**
- **Tworzenie i odwoływanie się do tablic referencyjnych;**
- **Uwzględnianie w korelacji kontekstu zasobów związanych ze zdarzeniami (typ zasobu i jego rola w organizacji, zagrożone procesy techniczne i biznesowe, rodzaj przetwarzanych danych, potencjalne konsekwencje incydentu, wektory ataku, wyniki analizy ryzyka);**
- **Graficzny interfejs do tworzenia reguł korelacji.**

SecureVisio SOAR

Implementacja procesu obsługi incydentów bezpieczeństwa oraz podatności
W platformie SecureVisio zaimplementowano, zaawansowany moduł SOAR (Security Orchestration Automation and Response). Rozwiązanie pozwala na implementację procesów i procedur obsługi incydentów bezpieczeństwa zgodnie z najlepszymi praktykami (między innymi: ISO- 270035, NIST SP 800-61R2, ENISA, Carnegie Mellon University). Każdy potencjalny incydent bezpieczeństwa utworzony w wyniku pracy mechanizmów korelacyjnych staje się elementem procesu, w ramach którego, SecureVisio automatycznie wzbogaca dane, śledzi status, czas reakcji i obsługi, eskaluje, bada potencjalne konsekwencje oraz dostarcza scenariusze postępowania na każdym etapie analizy i reakcji.
Automatyzacja zadań analizy i reakcji na incydenty
SecureVisio automatycznie przydziela zadania członkom zespołu SOC na podstawie zdefiniowanych parametrów i kontekstu zdarzeń. Przebieg prac odbywa się zgodnie ze scenariuszami dostosowanymi do każdego etapu procesu obsługi incydentu.

Do zaawansowanych funkcji SOAR należą między innymi:

- **Graficzny interfejs do tworzenia scenariuszy;**
- **Plany działań podzielone na etapy i kroki;**
- **Interakcja z użytkownikiem, zadawanie pytań i uzależnienie dalszych kroków od odpowiedzi;**
- **Zmiana scenariusza lub skok do innego kroku na podstawie okoliczności;**
- **Wbudowane, automatyczne lub zautomatyzowane akcje systemowe w ramach scenariuszy;**
- **Wiele scenariuszy stosowanych automatycznie w zależności od statusu, kontekstu oraz parametrów incydentu/zdarzenia;**
- **Powiadamianie zespołów obsługi, właścicieli zasobów i procesów na podstawie zdefiniowanych parametrów takich jak: typ zasobu, zagrożone procesy, ważność zasobu, priorytet incydentu/zdarzenia;**
- **Powiadamianie przy zmianie statusu incydentu/zdarzenia;**
- **Powiadamianie w przypadku przekroczenia ustalonych czasów reakcji i obsługi;**
- **Czasy reakcji i obsługi uzależnione od priorytetu incydentu/zdarzenia;**

Moduł obsługi incydentów zawiera gotowe scenariusze i setki akcji, które umożliwiają automatyczne lub zautomatyzowane interakcje z zewnętrznymi systemami w ramach prac związanych z uzupełnianiem informacji, pivotingiem oraz reakcją na incydenty.
Implementacja procesu zarządzania podatnościami
Proces zarządzania podatnościami jest jednym z najważniejszych aspektów zarządzania bezpieczeństwem. Dlatego system SecureVisio obejmuje moduł, który umożliwia kompleksowe podejście do obsługi podatności. System dysponuje interfejsami integracji z wiodącymi rozwiązaniami do skanowania podatności. Interfejsy te umożliwiają zarządzanie procesami skanowania wielu skanerów oraz import wyników ich pracy. W ramach podsystemu zarządzania podatnościami SecureVisio wspomaga organizację w następujących zadaniach:

- **Ustalanie priorytetów podatności na podstawie danych kontekstowych z pozostałych modułów;**
- **Automatyczne przydzielanie zadań dla zespołów obsługi w zależności od kontekstu;**
- **Automatyczne przydzielanie scenariuszy obsługi podatności w zależności od kontekstu;**
- **Automatyczne powiadamianie zespołów obsługi, właścicieli zasobów i właścicieli procesów;**
- **Automatyczne śledzenie czasów reakcji i obsługi;**
- **Automatyczna eskalacja;**
- **Wzbogacanie informacji o podatności o informacje kontekstowe z pozostałych modułów.**

5. Ochrona Danych Osobowych

Moduł ochrony danych osobowych wspomaga organizację w obsłudze czynności, kategorii przetwarzania oraz raportowaniu. Moduł oferuje także:

- **Wyszukiwanie systemów IT przetwarzających dane osobowe oraz grup i kategorii danych, jakie tam się znajdują;**
- **Wyznaczanie dostępnych zabezpieczeń technicznych przed potencjalnymi źródłami zagrożeń dla wszystkich „ systemów IT, które przetwarzają dane osobowe;**
- **Automatyczne generowanie „Raportu naruszenia ochrony danych osobowych dla organu nadzorczego" łącznie z wyznaczeniem możliwych konsekwencji naruszenia bezpieczeństwa;**
- **Przeprowadzanie, obowiązkowej w RODO, oceny skutków dla ochrony danych (analizy ryzyka) w obszarze cyberzagrożeń , w sposób w pełni zautomatyzowany.**
- **Automatyczną analizę ryzyka utraty dostępności, poufności i integralności danych;**
- **Informacje przetwarzane w ramach modułu stanowią dodatkowy kontekst uwzględniany w procesie obsługi**