Techniczne możliwości Platformy Zarządzania Incydentami SecureVisio™: Porównanie z systemami SIEM.

SecureVisio posiada pełną funkcjonalność systemu SIEM. Dla wdrożonych już rozwiązań SIEM innych producentów (m.in. IBM Qradar[1], Splunk[2], McAfee ESM[3]) platforma dostarcza narzędzia znacznie rozszerzające ich funkcjonalność i użyteczność.

Systemy SIEM służą do wykrywania incydentów bezpieczeństwa w oparciu o korelację zdarzeń pochodzących z posiadanych systemów informatycznych oraz systemów zabezpieczeń. Ich działanie kończy się w momencie wykrycia potencjalnych incydentów bezpieczeństwa, przenosząc cały ciężar dalszej analizy na operatorów tych systemów którzy (na bazie swojej wiedzy, posiadanej dokumentacji oraz integracji z narzędziami organizującymi ich obsługę, np.: systemami ticketowymi) muszą dokonać weryfikacji i kwalifikacji zdarzeń – a w przypadku stwierdzenia, iż zdarzenie jest incydentem bezpieczeństwa – adekwatnie zareagować poprzez odpowiednie działania naprawcze.

Systemy SIEM (na bazie reguł korelacyjnych) nadają potencjalnym incydentom priorytet techniczny, wynikający bezpośrednio ze zdarzenia i nieuwzględniający kontekstu (specyfiki) organizacji. Dlatego też, zdecydowana większość zakwalifikowanych incydentów okazuje się w rzeczywistości fałszywymi alarmami. W praktyce takie podejście wydaje się być mało skuteczne. Systemy SIEM generują dziennie setki potencjalnych alarmów, co uniemożliwia ich właściwą analizę. W przypadku wykrycia przez SIEM prawdziwego incydentu bezpieczeństwa, stwarzającego realne zagrożenie dla organizacji, zaginie on w gąszczu innych alarmów i najprawdopodobniej nie zostanie obsłużony na czas, doprowadzając tym samym do dalszych, znacznie poważniejszych konsekwencji.

Aby uniknąć podobnych sytuacji, przy wykorzystaniu tradycyjnych systemów SIEM, należałoby zatrudnić cały zespół ekspertów bezpieczeństwa, który nieprzerwanie, 24 godziny na dobę/ 7 dni w tygodniu będzie analizował dziesiątki a nawet setki potencjalnych incydentów dziennie, poszukując wyłącznie tych rzeczywiście dla organizacji niebezpiecznych. Następnie, po zlokalizowaniu konkretnych alarmów, ów eksperci – korzystając z systemów zewnętrznych, bazując na posiadanej dokumentacji teleinformatycznej oraz zdobytej wcześniej wiedzy o sposobie działania usług krytycznych (w tym związanych z nimi zależnościami, formie ich zabezpieczenia, itp.) musieliby przystąpić do ich rozwiązania. Innymi słowy: zarządzanie systemami SIEM i eliminacja fałszywych alarmów wymaga ciągłego strojenia i dużego zaangażowania zasobów ludzkich, co ze względu na trudną dostępność oraz utrzymanie zespołu ekspertów, jest procesem ciągłym i wysoce kosztownym.

SecureVisio wychodzi naprzeciw tym wyzwaniom. System automatyzuje i ułatwia pracę operatorów odpowiedzialnych za zarządzanie incydentami, poprzez dostarczanie im wszystkich niezbędnych informacji (w tym biznesowych), uzupełniających kontekst techniczny zdarzenia (Workflow). Automatyzacja SecureVisio to także wbudowane scenariusze obsługi incydentów (Playbook) i możliwość dokonywania automatycznych akcji. SecureVisio posiada znacznie wyższą efektywność dostrojenia rozwiązania do

[1] IBM Qradar, https://www.ibm.com/pl-pl/marketplace/ibm-qradar-siem
[2] Splunk, https://www.splunk.com/
[3] McAfee ESM, https://www.mcafee.com/enterprise/en-us/products/enterprise-security-manager.html

kontekstu organizacji niż tradycyjne systemy SIEM, dzięki czemu proces eliminacji fałszywych alarmów nie wymaga zaangażowania zespołu ekspertów i ciągłego dostrajania reguł korelacyjnych. W tym celu SecureVisio tworzy – w większości przy pomocy narzędzi autodiscovery - elektroniczną dokumentację. Wbudowane w system reguły korelacyjne korzystają z tych informacji i automatycznie eliminują znaczną część fałszywych alarmów. Wówczas operatorzy mogą przystąpić do strojenia już wtedy wyłącznie pojedynczych reguł.

Poniższa tabela przedstawia podsumowanie możliwości, oferowanych przez SecureVisio w zakresie zastąpienia lub rozszerzenia funkcjonalności systemów SIEM.

Lp.	Funkcjonalność i użyteczność	SIEM	SecureVisio
1.	Reguły korelacyjne bazujące na różnych źródłach zdarzeń	●	●
2.	Priorytetyzacja techniczna potencjalnych incydentów	●	●
3.	Zaawansowane prasowanie zdarzeń (regex, xml, json) w oparciu o podstawowe formaty pobierania zdarzeń m.in. Windows Event forwarding, syslog, konektory baz danych, e-mail oraz pliki płaskie	●	●
4.	Wzbogacanie i normalizacja zdarzeń	●	●
5.	Workflow uporządkowujący pracę osób odpowiedzialnych za zarządzanie incydentami	○	●
6.	Playbook automatyzujący i ułatwiający pracę osób odpowiedzialnych za zarządzanie incydentami	○	●
7.	Konsola zarządzania i raporty dostępne jednocześnie w polskiej i angielskiej wersji językowej	○	●
8.	Informacja o priorytecie biznesowym oraz niebezpieczeństwie (konsekwencji) związanym z potencjalnym incydentem względem organizacji.	◑ Systemy SIEM pozwalają tylko na budowanie list zasobów o określonej ważności dla organizacji	●
9.	Automatyczne szacowanie ryzyka (wg metodyki ISO-27005) i prezentacja wielkości ryzyka w odniesieniu do różnych typów zagrożeń (w celu ułatwienia oceny, czy potencjalne incydenty bezpieczeństwa zostały ocenione jako wysoce prawdopodobne)	○	●
10.	Graficzna prezentacja potencjalnych ścieżek ataków uławiająca operatorom ocenę rzeczywistego zagrożenia ich wystąpienia względem analizowanego zasobu z różnych obszarów sieci	○	●
11.	Wizualizacja na mapie sieci zagrożonych wektora ataku bazującego na informacji w logach dotyczących potencjalnego incydentu bezpieczeństwa.	○	●
12.	Definiowanie czasów SLA dla czynności obsługi incydentów względem biznesowego ryzyka dla organizacji	○	●
13.	Automatyczne powiadamianie osób odpowiedzialnych o nowych incydentach krytycznych dla biznesu organizacji (np. zagrożenia dla krytycznych procesów biznesowych, zagrożenie	◑ Powiadamianie bez szacowania potencjalnych szkód dla biznesu	●

	wycieku danych osobowych i innych wrażliwych danych) oraz przekroczeniu SLA w obsłudze incydentów bezpieczeństwa	organizacji. Systemy SIEM nie uwzględniają BIA.	
14.	Symulacja skutków biznesowych dla organizacji w razie zmaterializowania się wykrytych zagrożeń zakwalifikowanych jako potencjalne incydenty.	○	●
15.	KPI, KRI - obliczanie i wizualizacja wskaźników efektywności i wskaźników ryzyka biznesowego w procesie zarządzania incydentami	◑ Ogólne statystki ilościowe dotyczące wykrywanych incydentów bezpieczeństwa	●
16.	Biblioteka skryptów SSH i WMI/PowerShell do analizy i wiarygodnej eliminacji false positive, czynności sprawdzających, kwalifikacji oraz działań naprawczych.	○	●
17.	Narzędzia definiowania organizacji zespołu obsługi incydentów	○	●
18.	Eliminacja fałszywych alarmów na bazie kontekstu organizacji	○	●