|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Karta projektu badawczo-rozwojowego** | | | | |
|
|
| **Tytuł projektu** | | | | |
| **Opracowanie i wdrożenie dopasowanego rozwiązania klasy SIEM**  **do monitorowania bezpieczeństwa systemów informatycznych** | | | | |
| **Numer ewidencyjny projektu** | | **BR Wazuh** | | |
| **OPIS DZIAŁAŃ BADAWCZO ROZWOJOWYCH:** | | | | |
|
| ***Cel/ Opis nowych zakładanych właściwości/ funkcjonalności rozwiązania (produktu lub procesu)*** | Celem projektu było opracowanie dopasowanego narzędzia klasy SIEM (Security Information and Event Management) do monitorowania incydentów związanych z bezpieczeństwem systemów informatycznych, w tym zapewnienie bezpiecznej i wydajnej łączności z firmową siecią dla pracowników wykonujących obwiązki służbowe zdalnie.  Projekt zakładał wdrożenie zaawansowanego systemu monitorowania i reagowania na incydenty bezpieczeństwa poprzez uruchomienie platformy Wazuh z modułem XDR. Wazuh to otwarto-źródłowe oprogramowanie klasy SIEM (Security Information and Event Management). Główne funkcje Wazuh:   * Zbieranie i analiza logów – integruje dane z systemów operacyjnych, aplikacji, sieci i urządzeń bezpieczeństwa, aby wykrywać anomalie. * Wykrywanie zagrożeń – identyfikuje próby ataków, nieautoryzowane zmiany, malware czy podejrzane zachowania użytkowników. * Monitorowanie integralności plików (FIM) – sprawdza, czy pliki i konfiguracje systemowe nie zostały zmodyfikowane bez autoryzacji. * Bezpieczeństwo punktów końcowych (endpointów) – ma lekkie agenty instalowane na serwerach, komputerach czy urządzeniach IoT, które przesyłają dane do serwera Wazuh. * Zgodność z normami i audyt – wspiera raportowanie zgodności z regulacjami (GDPR, PCI-DSS, HIPAA, ISO 27001). * Integracja z Elastic Stack i Kibana – dane z Wazuh mogą być wizualizowane w formie dashboardów i raportów, co ułatwia analizę incydentów.   Główne założenia architektury systemu:   * Agenci Wazuh – zbierają dane z urządzeń końcowych. * Serwer Wazuh – przetwarza, analizuje i koreluje zdarzenia. * ElasticSearch + Kibana – przechowuje dane i udostępnia interfejs graficzny do ich przeglądania.   Planowano wdrożenie platformy Wazuh z modułem XDR – rozbudowanego systemu open source do gromadzenia, analizowania i korelowania danych z systemów i urządzeń końcowych. Do jej obsługi stworzono dedykowaną infrastrukturę wirtualną, skonfigurowano połączenia między agentami na stacjach roboczych a serwerem oraz zaplanowano integrację z systemem ERP i urządzeniami UTM.  Faza testowa projektu miała szczególnie duże znaczenie, ponieważ nie ograniczała się jedynie do weryfikacji poprawności instalacji. Pracownicy działu IT opracowywali własne, autorskie scenariusze incydentów, które mogły wystąpić w rzeczywistym środowisku przedsiębiorstwa. Testy obejmowały m.in. symulacje prób włamań do sieci, infekcji złośliwym oprogramowaniem, nieautoryzowanego dostępu do danych czy przeciążenia usług sieciowych. Każdy scenariusz był szczegółowo opisany, a następnie uruchamiany w kontrolowanych warunkach, aby sprawdzić, czy system jest w stanie wykryć i odpowiednio zareagować zgodnie z zaplanowanymi procedurami.  W trakcie testów tworzono i modyfikowano reguły bezpieczeństwa – część z nich oparto na gotowych bibliotekach dostarczonych z systemem Wazuh, jednak wiele zostało opracowanych od podstaw przez pracowników firmy, aby uwzględnić specyfikę jej procesów i infrastruktury. Równocześnie weryfikowano skuteczność powiadomień SMS i e-mail, poprawność izolowania zainfekowanych urządzeń, a także integrację z urządzeniem UTM i przełącznikami sieciowymi.  Efektem fazy testowej było wypracowanie zestawu zoptymalizowanych reguł bezpieczeństwa oraz potwierdzenie, że cały system – od momentu wykrycia zdarzenia po automatyczną reakcję – działa zgodnie z założeniami. Dzięki temu, po przejściu do fazy produkcyjnej, platforma Wazuh z modułem XDR mogła zapewnić monitoring stanu bezpieczeństwa, centralny punkt kontroli ruchu sieciowego oraz szybkie reagowanie na incydenty. Dodatkowo projekt usprawnił pracę zdalną, zwiększając bezpieczeństwo połączeń VPN i upraszczając ich konfigurację. | | | |
|
|
|
| ***Podstawowe etapy projektu*** | | | | |
| ***Numer etapu*** | ***Nazwa etapu*** | | | ***Data realizacji*** |
| 1. | Analiza stanu obecnego i identyfikacja luk w zabezpieczeniach | | | 10.2024 |
| 2. | Projektowanie integracji platformy Wazuh XDR z istniejącą siecią | | | 11.2024 |
| 3. | Utworzenie dedykowanej infrastruktury wirtualnej dla platformy Wazuh | | | 11.2024 |
| 4. | Instalacja i integracja platformy Wazuh z modułem XDR | | | 11.2024 |
| 5. | Opracowanie reguł bezpieczeństwa i scenariuszy incydentów | | | 11.2024 |
| 6. | Faza testowa z symulacjami incydentów i optymalizacją konfiguracji | | | 11.2024 |
| 7. | Wdrożenie produkcyjne i monitorowanie działania systemu | | | 12.2024 |
| ***Wykaz najważniejszych problemów badawczych oraz sposób ich rozwiązania*** | * Integracja open‑source’owego oprogramowania Wazuh z istniejącą infrastrukturą – wyzwaniem było przygotowanie dedykowanego środowiska wirtualnego, dostosowanie konfiguracji do wymagań sieci i zapewnienie wydajności. Zbudowano osobne serwery wirtualne, zoptymalizowano parametry systemu (dostęp do CPU, pamięci, IO) i utworzono procedury backupu. * Skalowalność i stabilność instalacji – ręczna instalacja i ustawianie alertów wymagały wielokrotnych testów. Zautomatyzowano proces instalacji agentów, zastosowano repozytoria pakietów i skrypty instalacyjne, co umożliwiło szybkie wdrażanie na kolejnych urządzeniach. * Tworzenie reguł detekcji incydentów – brak gotowej biblioteki dla specyfiki firmy wymagał stworzenia reguł od podstaw (poziom aplikacji, systemu operacyjnego, sieci). Wykorzystano dokumentację Wazuh, przeanalizowano najczęstsze wektory ataku i przygotowano zestaw reguł oraz mechanizmy modyfikacji na podstawie wyników testów i próbnych incydentów. Zintegrowano system z narzędziem XDR. * Natychmiastowa reakcja na incydenty – system wymagał konfiguracji automatycznych akcji (remediacji) i szybkich kanałów powiadomień. Zintegrowano platformę z usługami SMS/e‑mail, stworzono procedury izolowania zainfekowanych hostów oraz testowano skuteczność reakcji w środowisku testowym. | | | |
| ***Podstawowe prace o charakterze twórczym w projekcie*** | opracowanie infrastruktury i instalacji platformy Wazuh/XDR – przygotowanie wirtualnych serwerów, instalacja oprogramowania, konfiguracja interfejsów komunikacyjnych, ustawienie bazy danych i silnika analitycznego.  Tworzenie i modyfikacja reguł detekcji – projektowanie własnych reguł, iteracyjne testowanie i dostosowywanie ich do specyfiki środowiska; implementacja mechanizmów reagowania (remediacja), w tym izolacja urządzeń i automatyczne skrypty.  Integracja systemu powiadomień – opracowanie skryptów i procedur wysyłania alertów SMS i e‑mail; przygotowanie panelu zarządzania incydentami.  Zastosowanie praktyk DevSecOps – automatyzacja instalacji agentów i aktualizacji oprogramowania, skrypty monitorujące kondycję systemu, dokumentacja operacyjna i tworzenie kopii bezpieczeństwa. | | | |
| ***Poziom innowacyjności projektu*** | **Innowacja**  **w skali przedsiębiorstwa** | | **Innowacja**  **w skali kraju** | |
| Tak | | Nie | |
| ***Podsumowanie projektu*** | Projekt rozwoju cyberbezpieczeństwa przedsiębiorstwa umożliwił przebudowę infrastruktury ochronnej poprzez uruchomienie zaawansowanej platformy Wazuh i narzędzia XDR.  Dzięki dedykowanej infrastrukturze serwerowej, bibliotekom reguł bezpieczeństwa i automatycznym mechanizmom korelacji zdarzeń firma uzyskała możliwość monitorowania sieci w czasie rzeczywistym, reagowania na incydenty i szybkiego informowania działu IT o zagrożeniach.  Zespół projektowy zdobył nową wiedzę w zakresie integracji otwarto‑źródłowych systemów SIEM/XDR oraz tworzenia reguł detekcji, co może zostać wykorzystane w kolejnych inicjatywach. | | | |
|
|
|
|
|
|
|
|
|
| **Dokumentacja projektowa (załączniki do karty projektu)** | | | | |
| 1. | Repozytorium kodu źródłowego | | | |