# CYBER DEFENSE

Autor: Yustyna Utlik

# IDS (H/N/HYBRID) – *I*NTRUSION *D*ETECTION *S*YSTEM.

Zadaniem IDS jest wykrywanie i rejestrowanie ataków, a także alarmowanie o uruchomieniu określonej reguły. [1]

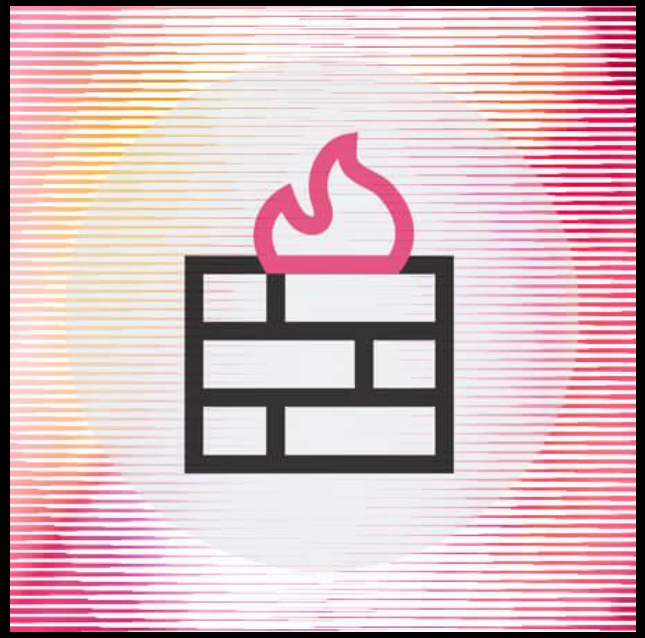
***W zależności od typu, IDS może:***

- wykrywać różnego rodzaju ataki sieciowe
- wykrywać próby nieautoryzowanego dostępu lub eskalacji uprawnień
- pojawienia się złośliwego oprogramowania
- śledzić otwarcie nowego portu itp. [2]


2 wiodące produkty rynkowe:
Snort 2.9.15.1 - https://www.snort.org; Suricata - https://suricata-ids.org;

# NG-FIREWALL

NGFW jest urządzeniem z kontrolą ruchu na poziomie aplikacji, wbudowanym systemem wykrywania włamań .Ważną cechą jest możliwość identyfikacji ruchu i powiązania go z określonym użytkownikiem.



GARTNER definiuje NGFW w następujący sposób:

Next-generation firewall - to urządzenia, które wykonują głęboką kontrolę pakietów (poza portem / protokołem), z możliwością inspekcji i blokowania ruchu na poziomie aplikacji, w tym wbudowane systemy zapobiegania włamaniom i inteligentne przetwarzanie ruch oparty na integracji z systemami zewnętrznymi. [3]

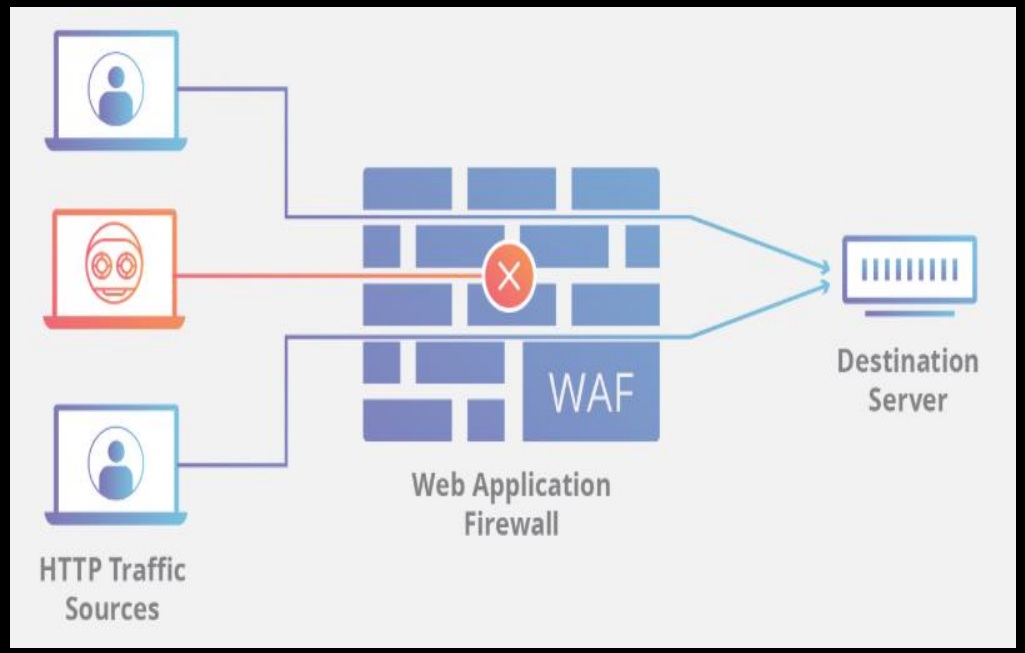
***2 wiodące produkty rynkowe:***

Barracuda CloudGen Firewall - https://www.barracuda.com/products/cloudgenfirewall;

Palo Alto Networks - https://www.paloaltonetworks.com;

# WAF - *W*EB *A*PPLICATION *F*IREWALL

WAF - Zbiór monitorów i filtrów zaprojektowanych do wykrywania i blokowania ataków sieciowych na aplikację internetową. Pliki WAF odnoszą się do warstwy aplikacji modelu OSI.

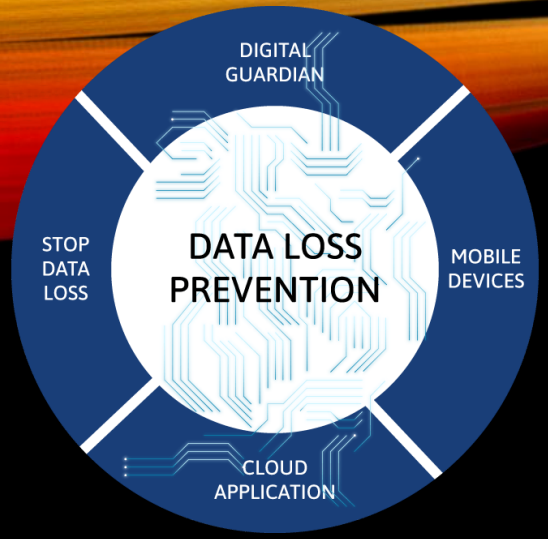



WAF obejmuje możliwość ochrony przed wszystkimi znanymi atakami informacyjnymi, co pozwala na przekazanie mu funkcji ochrony.

Dzięki temu programiści mogą skoncentrować się na implementacji logiki biznesowej aplikacji bez obawy o bezpieczeństwo. stosowany jako narzucony środek bezpieczeństwa. Oznacza to, że znajduje się przed główną aplikacją internetową i analizuje ruch przychodzący i wychodzący. W czasie rzeczywistym decyduje, czy przyznać, czy odmówić dostępu.

Warto zauważyć, że WAF nie są absolutnym środkiem ochrony informacji. Zazwyczaj są one zawarte w ogólnym systemie bezpieczeństwa aplikacji internetowej w połączeniu z innymi elementami.

# DLP - *D*ATA *L*EAK *P*REVENTION




Systemy DLP to systemy, które zapobiegają wyciekaniu poufnych informacji z systemów informatycznych firmy na zewnątrz

***W jakim celu wykorzystywane są systemy DLP?***

- minimalizacja szkód poprzez zmniejszenie ryzyka wycieku poufnych informacji od firmy;
- zapewnianie możliwości badania incydentów związanych z bezpieczeństwem informacji;
- stworzenie bazy dowodowej w celu przedstawienia jej sądowi w przypadku incydentów związanych z bezpieczeństwem informacji;
- optymalizacja wykorzystania czasu pracy przez pracowników;
- przeprowadzanie wywiadu gospodarczego w celu ustalenia stopnia lojalności pracowników w stosunku do firmy. [4]

# JAKIE ZADANIA ROZWIĄZUJE SYSTEM DLP?

- kontrola ruchu w sieci;
- kontrola ruchu pocztowego; komunikatorach internetowych (Skype / Lync, Telegram, WhatsUp, Mail.ru agent, Jabber, ICQ itp.);
- kontrola transferu danych do chmur (aplikacje chmurowe);
- kontrola wymiany informacji na stanowiskach pracy pracownika poprzez porty komunikacyjne (porty COM, LPT, USB, IrDA itp.), urządzenia wejścia-wyjścia (CD, napędy wymienne itp.), dostęp bezprzewodowy (Bluetooth, FireWire, Wi-Fi itp.), Drukowanie na drukarkach lokalnych i sieciowych;
- kontrola działań pracowników na stanowiskach pracy: kontrola schowka, keyloggera, monitorowanie odwiedzanych
- kontrola korespondencji w stron, kontrola zapytań, kontrola miejsca pracy użytkownika (audio, wideo, zrzuty ekranu), kontrola korzystania z aplikacji;
- kontrola przechowywania informacji na stacjach roboczych firmy i magazynach sieciowych;
- kopiowanie w tle wszystkich przechwyconych plików;

***2 wiodące produkty rynkowe:***

Symantec DLP - https://www.symantec.com/products/dlp;

McAfee - https://www.mcafee.com/enterprise/ru-ru/products/total-protection-for-data-loss-prevention.html#;

# ***SIEM*** — **S**ECURITY **I**NFORMATION AND **E**VENT **M**ANAGEMENT

** Jest potrzebny specjalnie do gromadzenia i analizy informacji*

System ten został zaprojektowany do analizy informacji z różnych innych systemów, takich jak DLP, IDS, antywirusy, różne urządzenia (Fortinet, routery itp.) Oraz do dalszej identyfikacji odchyleń od normy według kryteriów. Gdy tylko wykryje odchylenie, generuje incydent.

SIEM nie pełni żadnych funkcji ochronnych.

Raczej niewygodne jest ręczne przeglądanie dzienników z dużej liczby źródeł. Ponadto zdarzają się sytuacje, w których nieszkodliwe zdarzenia otrzymane z różnych źródeł wspólnie stanowią zagrożenie. SIEM jest w stanie zapewnić wszystkie niezbędne podstawy dowodowe, odpowiednie zarówno dla dochodzeń wewnętrznych, jak i sądowych. W rzeczywistości to jest jej celem.[5]

# SIEM JEST W STANIE ZAPOBIEC INCYDENTOM?

NIE! Sam SIEM nic nie może zapobiec. Jeśli zdarzenie jest w nim zarejestrowane, to już się wydarzyło. SIEM jest w stanie zapewnić całą niezbędną bazę dowodową, odpowiednią zarówno do dochodzeń wewnętrznych, jak i do sądu lub podczas demonstracji wobec sprawcy naruszenia.

Z dodatkowych funkcji, SIEM, po wdrożeniu, może pośrednio pomóc firmie zakupić inne narzędzia bezpieczeństwa informacji: na przykład uzasadniasz raport, który pokazuje, że większość otrzymanych incydentów jest zamykana przez żądane narzędzie.[6]

***2 wiodące produkty rynkowe:***
***IBM QRadar SIEM - https://www.ibm.com/pl-pl/marketplace/ibm-qradar-siem;***
***LogRhythm - https://logrhythm.com;***

# AV - ANTIVIRUS


AV - specjalny program do wykrywania wirusów komputerowych, a także niechcianych (uważanych za szkodliwe) programów i odzyskiwania plików zainfekowanych (zmodyfikowanych) przez wirusy oraz zapobiegania infekcji (modyfikacji) plików lub systemu operacyjnego złośliwym kodem.[7]

***Aby chronić się przed wirusami, stosuje się trzy grupy metod:***

- Metody oparte na analizie zawartości. Ta grupa obejmuje skanowanie sygnatur wirusów, a także sprawdzanie integralności i skanowanie podejrzanych poleceń.

- Metody oparte na śledzeniu zachowania programów podczas ich wykonywania. Metody te polegają na rejestrowaniu wszystkich zdarzeń zagrażających bezpieczeństwu systemu i występujących zarówno podczas faktycznego wykonania sprawdzonego kodu, jak i podczas emulacji jego oprogramowania.

- Metody regulowania procedury pracy z plikami i programami. Metody te dotyczą administracyjnych środków bezpieczeństwa.[8]

***2 wiodące produkty rynkowe:***
***Symantec Endpoint Protection (dla Europy) - https://www.symantec.com/products/endpoint;***
***On dla USA – Norton - https://us.norton.com/antivirus;***

# EDR - *E*NDPOINT *D*ETECTION AND *R*ESPONSE

EDR to dodatkowe narzędzie do analizy SOC z intuicyjnym interfejsem do wyszukiwania zagrożeń w czasie rzeczywistym, który umożliwia składanie złożonych zapytań w poszukiwaniu podejrzanych działań, złośliwych działań, z uwzględnieniem funkcji chronionej infrastruktury.

Zaawansowane mechanizmy wykrywania stosowane w EDR pozwalają zespołom szybko identyfikować zagrożenia i szybko reagować, zapobiegając potencjalnym szkodom dla firmy.


Złożone zagrożenia i ukierunkowane ataki przy użyciu nieznanego złośliwego kodu, przejęte konta, wymagają wielopoziomowego podejścia do wykrywania za pomocą zaawansowanych technologii czym i zajmuje się EDR.[9]

***2 wiodące produkty rynkowe:***
***mcafee mvision-edr - https://www.mcafee.com/enterprise/en-us/products/mvision-edr.html;***
***Kaspersky Endpoint Detection and Response - https://www.kaspersky.ru/enterprise-security/endpoint-detection-response-edr;***

# SOAR

SOAR to specjalne narzędzie do podsumowywania informacji o zagrożeniach bezpieczeństwa pochodzących z różnych źródeł, z późniejszą analizą tych danych.

***Główne funkcje SOAR obejmują:***

- integrację technologii / narzędzi niezbędnych w przypadku podejmowania decyzji na podstawie otrzymanych informacji o stanie systemu bezpieczeństwa,
- automatyzację procesów;
- zarządzanie incydentami przy użyciu kompleksowego podejścia;
- wizualizacja danych sprawozdawczych dla pracowników firmy - dokumentacja.

Ogromną zaletą SOAR jest pełna automatyzacja procesów zarządzania bezpieczeństwem informacji: od ustalania priorytetów po reagowanie na incydenty.


Korzystanie z SOAR pozwala integrować informacje z różnych źródeł na temat zagrożeń bezpieczeństwa. Osiąga się to za pomocą trzech głównych modułów.[5]

***2 wiodące produkty rynkowe:***
***IBM Resilient Security Orchestration, Automation and Response (SOAR)***
***https://www.ibm.com/pl-pl/marketplace/resilient-soar-platform;***
***D3 Security D3 SOAR https://d3security.com/platform/;***

# SOC - SECURITY OPERATIONS CENTER

**SOC** - to usługa zapewniająca **reakcję w przypadku wystąpienia ataku na zasoby teleinformatyczne**. Stałe monitorowanie sieci, systemów oraz zabezpieczeń teleinformatycznych umożliwia **identyfikację cyberzagrożeń oraz ataków**.

- Priorytetem SOC jest **ochrona danych** organizacji oraz **przeciwdziałanie zagrożeniom płynącym z sieci**.

- Usługa jest projektowana pod potrzeby Klienta, w taki sposób aby reakcja na incydent była możliwie szybka oraz zapewniała skuteczną obronę przez atakiem.

- Usługa składa się z grupy procesów, które są realizowane przez wybrane linie wsparcia inżynierów oraz specjalistów BLUEsec. Security Operations Center zapewnia zarówno podstawowe monitorowanie bezpieczeństwa oraz odpowiednią reakcję, jak i bardziej zaawansowane procesy, czyli zarządzanie podatnościami, analizę ryzyka, konfigurację i utrzymanie narzędzi bezpieczeństwa, analizę poincydentalną (forensic) czy szkolenia. [10]

# CSIRT - *COMPUTER SECURITY INCIDENT RESPONSE TEAM*

“Computer Security Incident Response Team (CSIRT)”, or

“Computer Emergency Response Team (CERT)”

CERT Polska to pierwszy powstały w Polsce zespół reagowania na incydenty.


CERT.PL

# CERT - **C**OMPUTER ***E***MERGENCY ***R***ESPONSE ***T***EAM

**Do głównych zadań zespołu CERT Polska należy:**

- rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci;
- aktywne reagowanie w przypadku wystąpienia bezpośrednich zagrożeń dla użytkowników;
- udział w krajowych i międzynarodowych projektach związanych z tematyką bezpieczeństwa teleinformatycznego;
- działalność badawcza z zakresu metod wykrywania incydentów bezpieczeństwa,
- analizy złośliwego oprogramowania i systemów wymiany informacji o zagrożeniach;
- rozwijanie własnych narzędzi do wykrywania, monitorowania, analizy i korelacji zagrożeń;
- publikowanie informacji o bezpieczeństwie na blogu cert.pl oraz w serwisach społecznościowych Facebook i Twitter;
- niezależne analizy i testy rozwiązań z dziedziny bezpieczeństwa teleinformatycznego. [11]

# WYKAZ LITERATURY:


[1] https://xakep.ru/2012/10/29/ids-ips/ (Data modyfikacji: 29.10.2012)
[2] https://www.sciencedirect.com/science/article/pii/S0045790609000020 (Data modyfikacji: May, 2009)

[3] https://habr.com/ru/company/hpe/blog/262123/ (Data modyfikacji: 09.07.2015)

[4] http://styletele.com/Solutions/informatsionnaya-bezopasnost/sistemy-dlp/ (Data modyfikacji: 10.11.2019)

[5] https://www.anti-malware.ru/analytics/Technology_Analysis/UBA-SIEM-SOAR (Data modyfikacji: 10.07.2018)
[6] https://habr.com/ru/post/172389/ (Data modyfikacji: 12.03.2013 )

[7] https://kapitanhack.pl/2019/06/26/akronimy/co-to-jest-av/ (Data modyfikacji: 26.06.2019)
[8] https://en.wikipedia.org/wiki/AV_Security_Suite (Data modyfikacji: 14.07.2019)

[9] https://habr.com/ru/post/457838/ (Data modyfikacji: 27.06.2019)

[10] https://www.bluesec.pl/uslugi/security-operations-center/

[11] https://www.cert.pl/o-nas/