Projekt WCYB

Michał Wawrzyńczak

January 2020

Contents

1 Zadanie 4

1.1 (H/N/hybrid)IDS – Host/Network/hybrid Intrusion Detection System

[1][2] Systemy monitorujace ruch sieciowy, w poszukiwaniu podajrzanych aktywności, alarmuje o problematycznych i podejrzliwych zdarzeniach gdy zostana wykryte. Systemy te skanuja sieć a także analizuja logi systemowe, przetwarzajace według zdefiniowanych zasad i sygnatur.
Popularne produkty: Snort, Bro, OSSEC
Zastosowanie w KillChain: Delivery, Exploitation, Instalation, C2, Actions on Objective

1.2 Firewall

[3] Najcześciej wykorzystywany sposób zabezpieczania sieci i systemów przed intruzami. Jest to oprogramowanie na urzadzeniu końcowym lub osobne urzadzenie wpinany przed maszyna końcowa, a do jego głównych zadań należy filtrowanie pakietów zgodnie z zdefiniowanymi wcześniej zasadami.
Popularne produkty: Cisco ASA, Barracuda NextGen Firewall
Zastosowanie w KillChain: Delivery, (Exploitation) https://pl.wikipedia.org/wiki/Zapora_sieciowa

1.2.1 Next-Generation Firewall

[4][5] Nowa generacja firewalli, można o niej powiedzieć, że łaczy w sobie funkcje tradycyjnych firewalli i IDP/IPS. NG-Firewall przeprowadzaja głeboka inspekcje pakietów i w inteligentny" sposób decyduja a blokowaniu badź przepuszczeniu ruchu.

1.2.2 Web Application Firewall

[6] Czesto wystepujacy jako moduł do serwera webowego. Filtruje, monitoruje i blokuje ruch sieciowy do i z aplikacji sieciowych przy wykorzystaniu wcześniej zdefiniowanych zasad. W głównej mierze opiera sie na modelu black i white listy.

1.3 DLP – Data Loss Prevention

[7][8] Rozwiazanie softwere'owe majace na celu zapobieganie wycieka danych, poprzez blokowanie czynności, które moga prowadzić do wycieku, np. zgrywania ważnych danych na nośniki fizyczna, wysyłania ich poczta elektroniczna, blokowanie maili wiekszych od danego limitu, czy nawet robienie screanshotów lub drukowania niektórch dokumentów.
Popularne produkty: Symantec DLP, SecureTrust DLP, McAfee Total Protection for DLP
Zastosowanie w KillChain: Instalation, C2, Actions on Objective

1.4 SIEM - Security Information and Event Management

[9] Systemy zapewniajace całościowy wglad w to co dzieje sie w systemie operacyjnym i sieci, w znaczacym stopniu ułatwiajace zarzadzanie i reagowania na incydenty. Systemy te zbieraja informacje z różnych źródeł, gromadzac je w scentralizowanej platformie, a nastepnie koreluja je ze soba, porównuja z sygnaturami, dziela na kategorie i umożliwiaja przeszukiwanie i wyświetlanie ich dla użytkownika.
Popularne produkty: SolarWinds, McAfee ESM, Kibana
Zastosowanie w KillChain: Delivery, Exploitation, Instalation, C2, Actions on Objective

1.5 AV/AM – AntiVirus/AntiMalwere

[10][11] Program komputerowy używany do prewencji detekcji i usówania złośliwego oprogramowania. Pierwszy program tego typu został zaprojektowany by walczyć z wirusami komputerowymi stad nazwa AntiVirus, dziś jednak odpowiedniejsza jest nazwa AntiMalwere gdyż softwere ten zwalcza wiele rodzajów malweru (robaki, trojany, ransomwere, rootkit). Programy te wyposażone sa w róznego rodzaju skanery, monitory itp. Do AntiVirus'ów możemy zaliczyć także szczepionki, czyli programy skierowane przeciwko konkretnemu malwere'owi
Popularne produkty: Norton, Avast, Kaspersky
Zastosowanie w KillChain: Delivery, Exploitation, Instalation, C2, Actions on Objective

1.6 EDR-Endpoint Detection and Response

[12] Jest to narzedzie służace do wykrywania i reagowania na zagrożenia i podejrzana aktywność na urzadzeniach końcowych. Monitoruje i analizuje ono zdarzenia majace miejsce już w systemie operacyjnym, takich jak tworzenie procesów, modyfikowanie rejestrów czy połaczenia sieciowe. Takie działanie daje możliwość szybkiej reakcji na zdarzenie, jeśli wcześniejsze urzadzenia takie jak firawall czy IDS ze wzgledu na tzw. silently fail" przeocza zagrożenie, które nie spełni zaimplementowanych reguł.
Popularne produkty: FireEye Endpoint Security, Carbon Black Cb Response
Zastosowanie w KillChain: Instalation, C2, Actions on Objective

1.7 SOAR- Security Orchestration, Automation And Response

[13] Jest to system umożliwiajacy zbieranie informacji z różnych źródeł i gromadzenie w jednym miejscu. Wyposażony w wiele narzedzi usprawniajacych analizowanie, reagowanie i zarzadzanie wieloma aspektami zwiazanymi z cyberbezpieczeństwem. Systemy SOAR pozwalaja usprawnić operacje w trzech kluczowych aspektach bezpieczeństwa:

Kluczowe aspekty systemów SOAR

- Reagowania na incydenty bezpieczeństwa
- Zarzadzanie zagrożeniami oraz podatnościami
- Automatyzacja operacji cyberbezpieczeństwa

Popularne produkty: LogRhythm, DFLabs
Zastosowanie w KillChain: Delivery, Exploitation, Instalation, C2, Actions on Objective

2 Zadanie 5

2.1 SOC - Security Operations Cente

2.1.1 Opis

[14][15] Usługa monitorowania bezpieczeństwa. Ze wzgledu na swoja złożoność jest ona czesto dostarczana przez zewnetrznego dostawce, w ramach której daje klientowi gotowe rozwiazania w ramach analizy, narzedzi, technologi, informowania oraz procesów służacych do skutecznej detekcji i obsługi incydentów, a także integracji z procesami bezpieczeństwa w organizacji. Takie rozwiazanie umożliwia szybkie i skuteczne reagowanie na zdarzenia, dzieki połaczeniu ze soba wielu różnych systemów bezpieczeństwa ze specjalistyczna obsługa przez wykwalifikowana kadre.

- **Ludzie** - grupa ekspertów z dziedziny cyberbezpieczeństwa.
- **Technologie** - zaimplementowanie najnowszych technologi.
- **Procesy i procedury** - Określenie procedur, priorytetyzacja i selekcja zagrożeń.

2.1.2 Zakres usług i zadania

- **Monitorowanie** - zbieranie, analizowani i kolerowanie logów systemowych i sieciowych ze zdarzeń.
- **Wykrywanie** - detekcja incydentów i zdarzeń bezpieczeństwa
- **Ocena** - Analiza i ocana zdarzeń wykrytych w sieciach i systemach
- **Reakcja na incydenty** - Zapewnienie zdalnej reakcji na incydenty, analizy malwere'u
- **Cyber Threat Intelligence (CTI)** - Natychmiastowe udzielanie informacji, w nagłych przypadkach, a także w dalszej perspektywie
- **Prewencja** - przeprowadzanie audytów bezpieczeństwa, testów penetracyjnych, wyszukiwanie podatności, analiza i tworzenie map topologi sieciowej.

2.1.3 KillChain, a SOC

- **Delivery** – Prewencja
- **Exploitation** – Monitorowanie, Wykrywanie, Ocena
- **Instalation** - Monitorowanie, Wykrywanie, Ocena
- **C2** - Monitorowanie, Wykrywanie, Ocena
- **Action on Objective** - Reakcja, CTI, Ocena

2.2 CERT/ CSIRT - Computer Emergency Response Team/Computer Security Incident Response Team

2.2.1 Opis

[16][17] Sa to zespoły reagowania na zdarzenia w sieci. Ich głównym zadaniem jest nieustanne nadzorowanie ruchu sieciowego w danym obszarze bezpieczeństwa telekomunikacyjnego oraz podejmowanie w razie potrzeby natychmiastowych decyzji i działań wobec pojawiajacych sie zagrożeń celem ich zneutralizowania. Zespoły CERT zaczeły powstawać w 1988 r. po incydencie MorrisWorm.

2.2.2 Główne zadaia zespołów CERT

- Rejestrowanie i obsługa zdarzeń naruszajacych bezpieczeństwo sieci;
- Aktywne reagowanie w przypadku wystapienia bezpośrednich zagrożeń dla użytkowników
- Niezależne analizy i testy rozwiazań z dziedziny bezpieczeństwa teleinformatycznego
- Współpraca z innymi zespołami CERT na świecie
- Udział w krajowych i miedzynarodowych projektach zwiazanych z tematyka bezpieczeństwa teleinformatycznego;
- Działalność badawcza z zakresu metod wykrywania incydentów bezpieczeństwa
- Analizy złośliwego oprogramowania i systemów wymiany informacji o zagrożeniach
- Rozwijanie własnych narzedzi do wykrywania, monitorowania, analizy i korelacji zagrożeń
- Publikowanie Raportów o bezpieczeństwie zasobów Internetu
- Działania informacyjno-edukacyjne, zmierzajace do wzrostu świadomości w zakresie bezpieczeństwa teleinformatycznego
- Publikowanie informacji o bezpieczeństwie

2.2.3 KillChain, a CERT

- **Delivery** – Publikacja informacji, majacych na celu zwiekszanie świadomości społeczeństwa z zagrożeń wystepujacych w sieci. Działania takie maja prowadzić do uniemożliwienia/utrudnienia przestepca ich "prace"
- **Exploitation** – Badania prowadzace do wykrywania podatności w systemach informatycznych oraz ich łatanie. Współpraca na tym gruncie z innymi zespołami CERT na całym świecie. A także analiza zdarzeń które już doszły do skutku.
- **Instalation** - Monitorowanie i analiza logów systemowych w poszukiwaniu zagrożeń. Próba wprowadzania nowych rozwiazań i narzedzi służacych analizie malwere'u.
- **C2**- Monitorowanie oraz analiza ruchu sieciowego celem wykrycia trwajacych ataków
- **Action on Objective** – Reagowanie na zdarzenia celem ich neutralizacji oraz ich analiza.

References

[1] https://en.wikipedia.org/wiki/Intrusion$_d etection_s ystem$.

[2] https://en.wikipedia.org/wiki/Intrusion$_d etection_s ystemhttps$: $//pl.wikipedia.org/wiki/Intrusion_P revention_S ystem$.

[3] https://pl.wikipedia.org/wiki/Zapora$_s ieciowa$.

[4] https://en.wikipedia.org/wiki/Next-generation$_f irewall$.

[5] https://digitalguardian.com/blog/what-next-generation-firewall-learn-about-differences-between-ngfw-and-traditional-firewalls.

[6] https://sekurak.pl/czym-jest-web-application-firewall-czesc-pierwsza-na-przykladzie-naxsi/.

[7] https://www.ekransystem.com/pl/blogpolska/co-jest-dlp-data-loss-prevention-i-komu-sie-przyda.

[8] https://en.wikipedia.org/wiki/Data$_l oss_p revention_s oftware$.

[9] https://kapitanhack.pl/2019/06/26/akronimy/czym-jest-siem/.

[10] https://malware.wikia.org/wiki/Antivirus$_S oftware$.

[11] https://en.wikipedia.org/wiki/Antivirus$_s oftware$.

[12] https://kapitanhack.pl/2019/09/23/akronimy/co-to-jest-edr/.

[13] https://searchsecurity.techtarget.com/definition/SOAR?fbclid=IwAR1bwI3lQHQwbubVluS2JD6s8q1SVs
WgnoVWIGOxxuga-FWJ0GB8HpaQ.

[14] https://www.forcepoint.com/cyber-edu/threat-intelligence.

[15] https://exatel.pl/cyberbezpieczenstwo/security-operations-center/.

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

[17] https://en.wikipedia.org/wiki/Computer$_e mergency_r esponse_t eam$.