

**Bezpieczeństwo infrastruktury krytycznej i systemów sterowania przemysłowego IoT - Laboratorium 10 – SOC/
Wykrywanie Incydentów Part 1**

Forma: praca w samodzielna / małe zespoły (2 - 4 osoby)

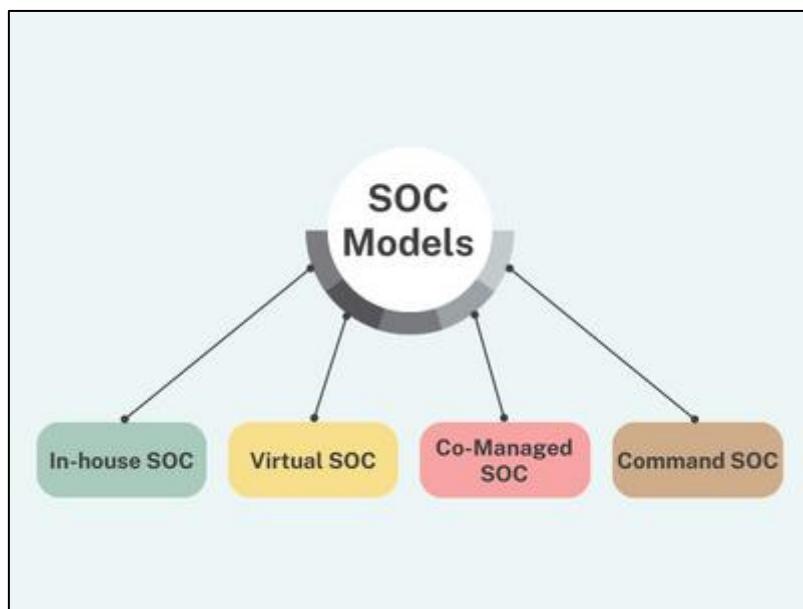
Wstęp teoretyczny

Czym jest SOC?

<https://www.microsoft.com/pl-pl/security/business/security-101/what-is-a-security-operations-center-soc>

<https://softinet.com.pl/roznica-miedzy-soc-a-siem/#:~:text=Security%20Operations%20Center%20,utrzymanie%20ci%C4%85g%C5%82o%C5%9Bci%20dzia%C5%82ania%20system%C3%B3w%20IT>

Security Operation Center (SOC) to jednostka, w której zespół ds. bezpieczeństwa informacji w sposób ciągły monitoruje i analizuje bezpieczeństwo organizacji. Głównym celem zespołu SOC jest wykrywanie, analizowanie oraz reagowanie na incydenty cyberbezpieczeństwa z wykorzystaniem technologii, ludzi i procesów.



Typy modeli SOC

W zależności od potrzeb bezpieczeństwa oraz budżetu, istnieje kilka rodzajów SOC:

SOC wewnętrzny

Ten zespół powstaje wtedy, gdy organizacja buduje własny zespół ds. cyberbezpieczeństwa. Organizacje rozważające wewnętrzny SOC powinny dysponować budżetem pozwalającym na jego ciągłe utrzymanie.

SOC wirtualny

Ten typ zespołu SOC nie posiada stałej siedziby i często pracuje zdalnie w różnych lokalizacjach.

SOC współzarządzany

SOC współzarządzany składa się z wewnętrznego personelu SOC, który współpracuje z zewnętrznym dostawcą zarządzanych usług bezpieczeństwa MSSP. Kluczowe znaczenie ma w tym modelu dobra koordynacja.

Command SOC

Ten zespół SOC nadzoruje mniejsze SOC na dużym obszarze. Organizacjami korzystającymi z tego modelu są między innymi duzi operatorzy telekomunikacyjni oraz agencje obronne.

Ludzie, procesy i technologia

Budowa skutecznego SOC wymaga bardzo dobrej koordynacji. Przede wszystkim musi istnieć silna relacja pomiędzy ludźmi, procesami i technologią. Mówiąc najprościej, omawiamy ludzi, procesy oraz technologie wymagane do funkcjonowania SOC.

Ludzie

Silny zespół SOC wymaga wysoko wykwalifikowanego personelu, który dobrze zna alerty bezpieczeństwa oraz scenariusze ataków. Ponieważ rodzaje ataków stale się zmieniają, potrzebni są członkowie zespołu, którzy potrafią łatwo dostosować się do nowych typów ataków i są gotowi prowadzić badania.

Procesy

Aby dalej rozwijać strukturę SOC, konieczne jest jej dostosowanie do wielu różnych wymagań bezpieczeństwa, takich jak NIST, PCI oraz HIPAA. Wszystkie procesy wymagają bardzo wysokiego poziomu standaryzacji działań, aby nic nie zostało pominięte.

Technologia

Zespół musi posiadać różne narzędzia do wielu zadań, takich jak testy penetracyjne, wykrywanie, zapobieganie oraz analiza. Muszą również na bieżąco śledzić rynek i rozwój technologii, aby znaleźć najlepsze rozwiązanie dla organizacji. Czasami najlepszy produkt dostępny na rynku nie jest najlepszym wyborem dla danego zespołu. Należy także uwzględnić inne czynniki, takie jak budżet organizacji.

Role w SOC

Analityk SOC

Ta rolę może być klasyfikowana jako poziom 1, 2 oraz 3 w zależności od struktury SOC. Analityk bezpieczeństwa klasyfikuje alert, poszukuje przyczyny oraz doradza w zakresie działań naprawczych.

Reagujący na incydenty

Osoba odpowiedzialna za reagowanie na incydenty jest odpowiedzialna za wykrywanie zagrożeń. Ta rola wykonuje wstępную ocenę naruszeń bezpieczeństwa.

Łowca zagrożeń

Łowca zagrożeń to specjalista ds. cyberbezpieczeństwa, który w sposób aktywny wyszukuje i bada potencjalne zagrożenia oraz podatności w sieci lub systemach organizacji. Wykorzystuje on połączenie technik manualnych oraz automatycznych do wykrywania, izolowania i neutralizowania zaawansowanych trwałych zagrożeń APT oraz innych złożonych ataków, które mogą omijać tradycyjne zabezpieczenia. Łowcy zagrożeń zazwyczaj posiadają bogatą wiedzę na temat infrastruktury IT organizacji oraz jej poziomu bezpieczeństwa, a także znajomość nowych zagrożeń i technik ataków. Ich celem jest wykrywanie i eliminowanie zagrożeń zanim spowodują one szkody lub zakłócenia w działalności firmy.

Inżynier bezpieczeństwa

Inżynierowie bezpieczeństwa odpowiadają za utrzymanie infrastruktury bezpieczeństwa rozwiązań SIEM oraz produktów centrum operacji bezpieczeństwa SOC. Na przykład inżynier bezpieczeństwa buduje połączenie pomiędzy SIEM a rozwiązaniami SOAR.

Kierownik SOC

Kierownik SOC zajmuje się zadaniami zarządzycielskimi, takimi jak planowanie budżetu, tworzenie strategii, zarządzanie personelem oraz koordynowanie działań operacyjnych. Zajmuje się przede wszystkim zagadnieniami operacyjnymi, a nie technicznymi.

Analityk SOC i jego obowiązki

Analityk SOC jest pierwszą osobą, która bada zagrożenia dla systemu. Jeśli sytuacja tego wymaga, eskaluje incydenty do swoich przełożonych, aby mogli oni przeciwdziałać zagrożeniom. Analityk SOC odgrywa bardzo ważną rolę w zespole SOC, ponieważ to on jako pierwszy reaguje na zagrożenie.

Zalety pracy jako analityk SOC

Istnieje wiele różnych technik wektorów ataku oraz złośliwego oprogramowania i ich liczba z każdym dniem stale rośnie. Jako analityk możesz czerpać dużą satysfakcję z badania tych różnorodnych typów incydentów. Pomimo tego, że systemy operacyjne, produkty bezpieczeństwa i inne narzędzia, z których korzystasz, pozostają takie same, praca nie staje się monotonna, ponieważ analizujesz różne zdarzenia. Dodatkowo niektórych technik możesz w ogóle nie spotkać, nie każdego tygodnia ani nie każdego dnia.

Dzień z życia analityka SOC

W ciągu dnia analityk SOC zazwyczaj przegląda alerty w systemie SIEM i określa, które z nich stanowią rzeczywiste zagrożenia. Aby dojść do właściwego wniosku, wykorzystuje różne narzędzia bezpieczeństwa i ochrony, takie jak Endpoint Detection and Response EDR, zarządzanie logami oraz SOAR. W dalszej części programu szkoleniowego szczegółowo wyjaśnimy, dlaczego i w jaki sposób te narzędzia są wykorzystywane.

Systemy operacyjne

Aby określić, co w systemie jest nieprawidłowe, najpierw trzeba wiedzieć, co uznawane jest za normalne. Przykładowo w systemie operacyjnym Windows działa wiele usług i bez wiedzy, które z nich są normalne, a które mogą być podejrzane, trudno jest odróżnić zagrożenie. Dlatego należy znać zasady działania systemów operacyjnych Windows oraz Linux.

Sieć

Przede wszystkim w tej roli będziesz mieć do czynienia z wieloma złośliwymi adresami IP oraz adresami URL, dlatego musisz potwierdzić, że w sieci nie znajdują się urządzenia próbujące łączyć się z tymi adresami. Po wykonaniu tego kroku możliwe jest wyznaczenie dalszego kierunku analizy. Ten etap jest nieco bardziej skomplikowany, ponieważ może być konieczne odnalezienie potencjalnego wycieku danych w sieci. Aby realizować wszystkie te zadania, należy rozumieć podstawy sieci komputerowych.

Analiza złośliwego oprogramowania

Podczas pracy z większością zagrożeń bardzo prawdopodobne jest, że napotkasz jakiś rodzaj złośliwego oprogramowania. Aby zrozumieć rzeczywisty cel działania takich programów, które czasami celowo prezentują inne zachowanie, by zmylić analityków, konieczne jest posiadanie umiejętności analizy malware. Istotne jest przynajmniej określenie, gdzie znajduje się centrum dowodzenia i kontroli złośliwego pliku oraz sprawdzenie, czy w sieci istnieje urządzenie komunikujące się z tym adresem.

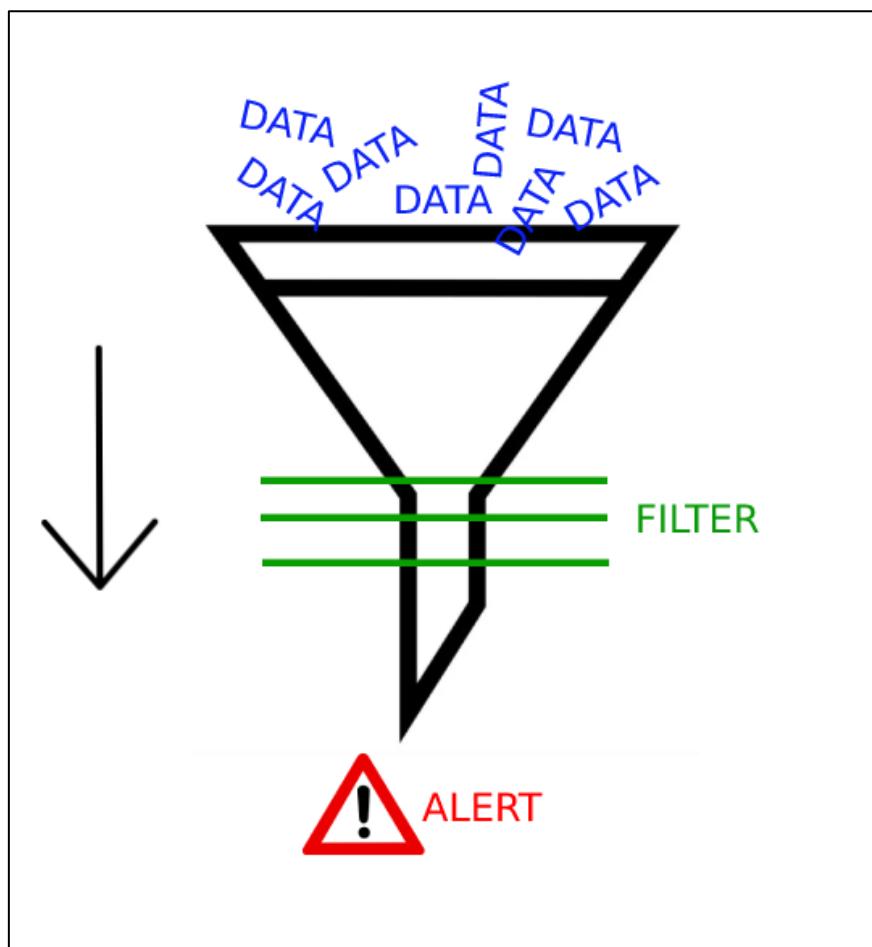
SIEM

https://app.letsdefend.io/training/lesson_detail/siem-and-analyst-relationship

SIEM to rozwiązanie z zakresu bezpieczeństwa, które łączy zarządzanie informacjami o bezpieczeństwie oraz zarządzanie zdarzeniami. Obejmuje ono rejestrowanie zdarzeń w środowisku w czasie rzeczywistym. Głównym celem rejestrowania zdarzeń jest wykrywanie zagrożeń bezpieczeństwa. Ogólnie rzecz biorąc, systemy SIEM posiadają bardzo wiele funkcji. Te, które najbardziej interesują analityków SOC, to funkcje zbierania i filtrowania danych oraz generowania alertów dla podejrzanych zdarzeń.

Przykładowy alert

Jeśli ktoś w systemie operacyjnym Windows spróbuje wprowadzić 20 błędnych haseł w ciągu 10 sekund, uznaje się to za podejrzaną aktywność. Mało prawdopodobne jest, aby osoba, która zapomniała hasła, próbowała wpisać je aż tyle razy w tak krótkim czasie. Dlatego tworzy się regułę lub filtr SIEM do wykrywania takiej aktywności, która przekracza ustalony próg. Na podstawie tej reguły SIEM generowany jest alert, gdy taka sytuacja wystąpi.



MAIN CHANNEL		INVESTIGATION CHANNEL		CLOSED ALERTS		
SEVERITY	DATE	RULE NAME		EVENTID	TYPE	ACTION
▼ High	Sept. 5, 2021, 12:43 p.m.	★ SOC153 - Suspicious Powershell Script Executed		101	Malware	🔗
▼ High	Sept. 4, 2021, 8:08 p.m.	SOC155 - Suspicious SSH Login		104	Unauthorized Access	🔗
▼ Medium	Sept. 4, 2021, 3:07 p.m.	SOC157 - Suspicious WAR File		107	Malware	🔗
▼ Medium	Sept. 4, 2021, 2:30 p.m.	SOC154 - Service Configuration File Changed by Non Admin User		102	Generic	🔗

Relacja pomiędzy analitykiem SOC a SIEM

Chociaż rozwiązania SIEM posiadają wiele funkcji, analitycy SOC zazwyczaj zajmują się głównie śledzeniem alertów. Inne zespoły lub osoby odpowiadają za tworzenie konfiguracji oraz korelacji reguł. Jak wspomniano wcześniej, alerty są generowane na podstawie danych, które przechodzą przez filtry. Alerty są najpierw analizowane przez analityka SOC. W tym miejscu rozpoczyna się jego praca w centrum operacji bezpieczeństwa. Jego głównym zadaniem jest określenie, czy wygenerowany alert jest rzeczywistym zagrożeniem, czy też fałszywym alarmem. Dla lepszego zrozumienia można ponownie odnieść się do strony Monitoring. Jak można tam zobaczyć, w interfejsie SIEM występują różne alerty. Analityk SOC powinien analizować szczegóły związane z tymi alertami przy pomocy innych narzędzi SOC, takich jak EDR, zarządzanie logami, źródła informacji o zagrożeniach i inne, a następnie ostatecznie określić, czy są to rzeczywiste zagrożenia.

MAIN CHANNEL		INVESTIGATION CHANNEL		CLOSED ALERTS		
SEVERITY	DATE	RULE NAME		EVENTID	TYPE	ACTION
▼ High	Sept. 5, 2021, 11:33 a.m.	SOC128 - Malicious File Upload Attempt		106	Malware	» ✓
▼ Medium	Dec. 1, 2020, 5:50 a.m.	SOC102 - Proxy - Suspicious URL Detected		32	Proxy	» ✓
EventID:	32					
Event Time:	Dec. 1, 2020, 5:50 a.m.					
Rule:	SOC102 - Proxy - Suspicious URL Detected					
Level:	Security Analyst					
Source Address	172.148.17.14					
Source	MikeComputer					
Hostname						
Destination	172.217.17.174					
Address						
Destination	encrypted-tbn0.gstatic.com					
Hostname						
Username	Mike01					
Request URL	https://encrypted-tbn0.gstatic.com/images?q=bn:AND9GcSJESknzLUXELhngZZWBbmGwtqfFsaemB9w&usqp=CAU					
User Agent	Mozilla/5.0 (iPhone; CPU iPhone OS 13_4_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.1 Mobile/15E148 Safari/604.1					
Device Action	Blocked					
▼ Medium	Oct. 19, 2020, 9:54 p.m.	SOC105 - Requested T.I. URL address		20	ThreatIntel	» ✓

Nowo utworzone alerty można zobaczyć w kanale głównym i można traktować go jako kanał wspólny. W tej symulacji współpracownicy nie są widoczni, ale w rzeczywistych warunkach pracy członkowie zespołu widzą ten panel. Po wybraniu alertu, którym chcesz się zająć, należy kliknąć przycisk Take Ownership w obszarze Action, aby przejąć odpowiedzialność za dany alert i skierować go do kanału dochodzeniowego. W ten sposób pozostały członkowie zespołu widzą, nad którym alertem aktualnie pracujesz. Jednocześnie pomaga im to wybrać inne alerty do analizy. Dzięki temu cały zespół może szybko przejrzeć wszystkie zgłoszenia. Po kliknięciu w alert można zobaczyć jego szczegóły. Pozwala to zebrać informacje potrzebne do dochodzenia, takie jak nazwa hosta, adres IP, skrót pliku i inne dane. Należy pamiętać, że od czasu do czasu w systemie SIEM mogą pojawić się fałszywe alerty. Dobry analityk SOC potrafi rozpoznać takie sytuacje i przekazać informację zwrotną zespołowi, przyczyniając się tym samym do zwiększenia skuteczności działania SOC.

Przykład

Załóżmy, że zespół SIEM stworzył zestaw reguł generujących alerty dla adresów URL zawierających słowo union w celu wykrywania ataków typu SQL injection. Użytkownik wykonał wyszukiwanie przy użyciu adresu <https://www.google.com/search?q=mysql+union+usage>, a w systemie SIEM został wygenerowany alert, mimo że nie występowało tam rzeczywiste zagrożenie. Alert został wygenerowany, ponieważ słowo union znajdowało się w adresie URL. Tego typu anomalie można przekazywać zespołowi SIEM w celu optymalizacji procesu generowania alertów.

Logi

Log jest chronologiczny zapis zawierający informację o zdarzeniach i działaniach dotyczących systemu informatycznego, systemu komputerowego czy komputera. Log tworzony jest automatycznie przez dany program komputerowy, a sama czynność zapisywania do logu nazywana jest też logowaniem nie należy mylić tego określenia z logowaniem w celu wykonania uwierzytelnienia. Logi są używane do analizowania pracy systemu informatycznego, np. sporządzania statystyk, wykrywania prób włamania do systemu i sposobu ich przeprowadzenia oraz wykrywania wszelkich błędów i nieprawidłowości działającego oprogramowania. Logi mogą być prowadzone mniej lub bardziej szczegółowo (jest to tak zwany poziom szczegółowości logowania) w zależności od potrzeby. Przykładowo, system domyślnie może logować tylko najpoważniejsze zdarzenia (poważne błędy), a na życzenie może rejestrować wydarzenia bardziej szczegółowo (na przykład ostrzeżenia czy rejestrować normalny przebieg pracy procesów). Zazwyczaj najbardziej szczegółowy poziom logowania służy twórcom systemu w usuwaniu błędów w jego działaniu. W niektórych systemach można zmieniać poziom szczegółowości logowania w trakcie ich pracy.

Informacje mogą dotyczyć zdarzeń podejmowanych na systemie lokalnie (np. przez pracujących na nim użytkowników lub programy) albo zdarzeń pochodzących z zewnątrz (np. pakietów wysyłanych na interfejs sieciowy systemu komputerowego), jak również może to być zapis rozmów prowadzonych za pomocą komunikatora internetowego lub czatu. Do logów zaliczyć można wykazy połączeń telekomunikacyjnych i zapisy wysłanych lub odebranych wiadomości (SMS, poczta elektroniczna).

Typowy wpis w logu zawiera m.in. następujące informacje:

- względny lub bezwzględny czas zdarzenia (np. data i godzina),
- rodzaj zdarzenia, identyfikator (często wykorzystywany do rozdzielania informacji na kilka strumieni danych),
- nazwa użytkownika, programu, procesu generującego wpis
- dane o pobieranych plikach,
- adres IP, jeżeli operacja dotyczy komunikacji przez sieć,
- kwalifikacja zdarzenia (poważny błąd, ostrzeżenie, raport z normalnego przebiegu prac, bardzo szczegółowy)
- tekstowy opis zdarzenia
- praktycznie każda informacja potrzebna administratorowi systemu, a możliwa do odczytania w sposób alfanumeryczny.

Logi mogą być zapisywane w plikach lub do baz danych, czasami są wysyłane na inne maszyny przez sieć lub na drukarkę. Niekiedy do zbierania logów z innych maszyn jest przeznaczony oddzielnny system (ze względów bezpieczeństwa).

Tworzenie, przechowywanie i archiwizacja logów niesie za sobą zagrożenia związane z ochroną informacji i prywatności. Uzyskanie przez osoby niepowołane dostępu do logów może doprowadzić do ujawnienia istotnych danych, na przykład do zapisu niejawnych transakcji biznesowych lub przebiegu komunikacji poprzez pocztę elektroniczną lub komunikator internetowy.

Niektórzy użytkownicy stosują politykę przechowywania logów przez krótki czas (na przykład siedem dni), a w niektórych przypadkach wybrane informacje w ogóle nie są zapisywane.

Z drugiej strony brak logów uniemożliwia analizę zjawisk z przeszłości, na przykład przebiegu włamania komputerowego lub wykrycia nadużyć. Trudniej jest również stwierdzić, czy nieprawidłowości w pracy systemu mają charakter jednorazowy czy też występowały już w przeszłości.

Przechowywanie zapisów logów przez dłuższy czas w celu ewentualnego przekazania ich organom ścigania to tzw. retencja danych.

Czym jest Log Management

https://app.letsdefend.io/training/lesson_detail/log-management

https://app.letsdefend.io/training/lesson_detail/log-collection

https://app.letsdefend.io/training/lesson_detail/log-aggregation-and-parsing

https://app.letsdefend.io/training/lesson_detail/log-storage

https://app.letsdefend.io/training/lesson_detail/alerting

Jak sama nazwa wskazuje, Log Management zapewnia dostęp do wszystkich logów w środowisku, takich jak logi stron internetowych, systemów operacyjnych, zapór sieciowych, serwerów proxy, EDR i innych, a także umożliwia zarządzanie nimi w jednym miejscu. Zwiększa to wydajność pracy oraz pozwala oszczędzać czas. Jeśli nie masz dostępu do logów z jednego miejsca, wtedy to samo zapytanie, na przykład celem jest ustalenie wszystkich użytkowników na letsdefend.io, musiałoby zostać wysłane do wielu różnych urządzeń. Zwiększało to ryzyko błędu oraz ilość czasu, który trzeba byłoby na to poświęcić. Jeśli wejdzieś na stronę Log Management w LetsDefend, zobaczysz różne źródła logów, takie jak Proxy, Exchange oraz Firewall oznaczone jako Type. Oznacza to, że wszystkie te źródła logów zostały zebrane w jednym miejscu, a dane z takich źródeł jak Proxy czy zapora sieciowa mogą być przeglądane za pomocą jednego zapytania.

Log Search							
Result:	7	Page:	1	Search...	Search		
#	DATE	TYPE	SOURCE ADDRESS	SOURCE PORT	DESTINATION ADDRESS	DESTINATION PORT	RAW
1	Aug, 29, 2020, 10:28 PM	Proxy	172.16.17.14	47741	198.100.45.154	80	⊕
2	Aug, 29, 2020, 10:32 PM	Proxy	172.16.17.14	57441	67.68.210.95	80	⊕
3	Aug, 29, 2020, 11:00 PM	Exchange	63.35.133.186	47847	172.16.20.3	25	⊕
4	Aug, 29, 2020, 11:09 PM	Proxy	172.16.17.88	23477	81.169.145.105	80	⊕
5	Sep, 18, 2020, 05:14 PM	Firewall	172.16.17.35	4421	173.231.198.30	587	⊕
6	Sep, 20, 2020, 10:54 PM	Firewall	172.16.17.47	54211	5.188.0.251	443	⊕
7	Sep, 20, 2020, 10:54 PM	Proxy	172.16.17.47	54211	5.188.0.251	443	⊕

Cel Log Management

Analitycy SOC zazwyczaj korzystają z Log Management, aby ustalić, czy występuje jakakolwiek komunikacja z określonym adresem oraz aby zobaczyć szczegóły tej komunikacji. Założmy, że natrafłeś na złośliwe oprogramowanie i po jego uruchomieniu odkryłeś, że komunikuje się ono z adresem letsdefend.io oraz wykonuje stamtąd polecenia. W takiej sytuacji centrum dowodzenia i kontroli znajduje się pod adresem letsdefend.io. Możesz więc wyszukać ten adres w firmowym systemie Log Management, aby sprawdzić, czy jakieś urządzenia próbowały komunikować się z tym centrum dowodzenia. Prowadzi nas to do drugiej sytuacji. Widzisz alert SIEM informujący, że urządzenie LetsDefendHost w twojej sieci wysyła dane na adres IP 122.194.229.59. Przeprowadź do tego dochodzenie, odizolowałeś urządzenie od sieci, wykonałeś niezbędne działania i teraz sytuacja jest pod kontrolą. Pozostaje jednak jeszcze jedna kwestia. Czy inne urządzenia również nie wysyłają danych na ten podejrzany adres IP 122.194.229.59? Alert mógł dotyczyć tylko LetsDefendHost, ale mimo to powinieneś wyszukać ten podejrzany adres w Log Management, aby sprawdzić, czy system nie przeoczył innych połączeń i spróbować je odnaleźć.

Splunk

<https://www.tutorialspoint.com/splunk/index.htm>

https://www.splunk.com/en_us/blog/learn/splunk-tutorials.html

Czym jest Splunk

Splunk to korporacyjna platforma analityczna stworzona do wyszukiwania, monitorowania oraz analizowania danych maszynowych w czasie rzeczywistym, takich jak logi. Działa poprzez zbieranie oraz indeksowanie danych w przeszukiwalnym indeksie, na podstawie którego użytkownicy mogą tworzyć wykresy, raporty, alerty, pulpity oraz wizualizacje. Splunk przekształca ogromne ilości surowych danych IT w informacje możliwe do wykorzystania, umożliwiając wykrywanie wzorców, rozwiązywanie problemów oraz wspieranie podejmowania decyzji biznesowych. Firmy wykorzystują Splunk do rozbijania silosów danych. Sama nazwa Splunk pochodzi od słowa spelunking oznaczającego eksplorację jaskiń i jest analogią do głębokiego odkrywania ukrytych danych w poszukiwaniu wartości.

Historia Splunk

Splunk został założony w 2003 roku przez Michaela Bauma, Roba Dasa oraz Erika Swana. Założyciele inspirowali się eksploracją jaskiń jako metaforą zagłębiania się w dane IT. Początkowo produkt koncentrował się na potężnej wyszukiwarce do skanowania i przechowywania plików logów, odpowiadając na potrzebę wydobywania wartości z wszystkiego, co generuje dane w organizacji. W 2023 roku Splunk obchodził swoje 20-lecie i ogłosił przejęcie przez firmę Cisco za kwotę 28 miliardów dolarów. Transakcja została sfinalizowana w marcu 2024 roku.

Dlaczego organizacje korzystają ze Splunk

Organizacje wdrażają Splunk, ponieważ zapewnia on jednolity sposób obsługi różnorodnych danych logów i zdarzeń do wielu celów jednocześnie. Podstawową wartością Splunka jest zamiana danych maszynowych w wiedzę. Pomaga on zespołom operacji IT szybko wyszukiwać i rozwiązywać problemy w złożonych infrastrukturach, a zespołom bezpieczeństwa wykrywać oraz badać zagrożenia z wielu źródeł w jednym miejscu. W przeciwieństwie do tradycyjnych narzędzi Splunk potrafi przyjmować dowolne dane tekstowe pochodzące z serwerów, aplikacji, urządzeń sieciowych, czujników i wielu innych źródeł oraz umożliwiać ich przeszukiwanie i korelację. Ta wszechstronność sprawia, że Splunk może być wykorzystywany zarówno do monitorowania wydajności stron internetowych, jak i do analizy zachowań użytkowników. Jego elastyczność jako technologii horyzontalnej, czyli niezwiązanej z jedną dziedziną, pozwala na zastosowanie w zarządzaniu aplikacjami, cyberbezpieczeństwie, audytach zgodności, analizie ruchu internetowego, analizie biznesowej i wielu innych obszarach. W praktyce firmy zauważają poprawę dostępności systemów dzięki szybszemu rozwiązywaniu problemów, redukcję kosztów operacyjnych poprzez automatyzację analizy logów, wzmocnienie bezpieczeństwa dzięki alertom w czasie rzeczywistym oraz lepsze raportowanie zgodności z przepisami.

Główne funkcje Splunk

Splunk jest bardzo rozbudowaną platformą, obejmującą pełen zakres pracy z danymi od ich pobierania po analizę i podejmowanie działań. Do jego kluczowych funkcji należą:

1. Pobieranie danych, indeksowanie i wyszukiwanie

Splunk może zbierać dane praktycznie z każdego źródła i w dowolnym formacie. Są to logi, metryki, zdarzenia oraz konfiguracje, niezależnie od tego, czy pochodzą z serwerów, urządzeń sieciowych, aplikacji, usług chmurowych czy baz danych. Podczas pobierania danych silnik indeksujący Splunka przetwarza surowe dane na zdarzenia możliwe do wyszukiwania, dodając znaczniki czasu oraz metadane takie jak host, źródło oraz typ źródła. Indeksowanie umożliwia bardzo szybkie wyszukiwanie i pobieranie danych z ogromnych zbiorów. Użytkownicy mogą wyszukiwać dane za pomocą języka zapytań SPL, który umożliwia wykonywanie obliczeń statystycznych, filtrowanie oraz formatowanie wyników. Funkcja wyszukiwania stanowi fundament działania Splunka, ponieważ pozwala zarówno na proste wyszukiwanie po słowach kluczowych, jak i na zaawansowane zapytania umożliwiające korelację zdarzeń z różnych źródeł.

2. Zarządzanie logami i ich analiza

Splunk bardzo często pełni rolę centralnego systemu zarządzania logami. Nieprzerwanie zbiera on oraz agreguje logi z rozproszonych systemów w jednym miejscu. Następnie udostępnia narzędzia do analizy tych danych pod kątem informacji operacyjnych. Potrafi również przekształcać surowe logi tekstowe w ustrukturyzowane pola oraz stosować transformacje, takie jak maskowanie danych wrażliwych czy odrzucanie niepożądanych zdarzeń. Umożliwia także analizę danych w czasie rzeczywistym. Przykładowo można odnaleźć wszystkie błędy w zadanym przedziale czasowym albo utworzyć zaplanowane wyszukiwania wykrywające wzorce, takie jak nagły wzrost błędów o kodzie 500. Splunk obsługuje również analizę statystyczną logów, co pozwala uzyskiwać metryki oraz trendy, na przykład tempo występowania błędów, aktywność użytkowników czy częstotliwość konkretnych komunikatów.

3. Monitorowanie w czasie rzeczywistym i alertowanie

Splunk doskonale sprawdza się zarówno w analizie historycznej, jak i w monitorowaniu danych w czasie rzeczywistym. W miarę napływu nowych danych system może na bieżąco porównywać je z wcześniej zdefiniowanymi warunkami lub progami. Wyszukiwania mogą być uruchamiane cyklicznie albo działać w czasie rzeczywistym, aktualizując się wraz z napłykiem nowych zdarzeń. Na podstawie tych wyszukiwań Splunk może generować alerty, gdy spełnione zostaną określone kryteria, na przykład gdy pojawi się konkretny komunikat o błędzie, gdy liczba nieudanych logowań przekroczy ustalony próg w ciągu pięciu minut albo gdy obciążenie procesora serwera utrzymuje się powyżej dziewięćdziesięciu procent przez dłuższy czas. Alerty mogą być wysyłane różnymi kanałami, takimi jak e-mail, SMS, tworzenie zgłoszeń w systemie ServiceNow czy uruchamianie skryptów.

4. Pulpity i wizualizacja

Aby ułatwić analizę dużych zbiorów danych, Splunk oferuje rozbudowane możliwości wizualizacji i raportowania. Użytkownicy mogą tworzyć interaktywne pulpity zawierające wykresy, tabele, mapy oraz inne wizualizacje. Pulpity są w pełni konfigurowalne i mogą prezentować różne metryki, takie jak czasy odpowiedzi strony, poziomy ważności logów czy liczba aktywnych alertów. Splunk umożliwia również generowanie raportów w formacie PDF według ustalonego harmonogramu. Dzięki temu dane stają się czytelne zarówno dla odbiorców technicznych, jak i nietechnicznych.

5. Funkcje bezpieczeństwa i wykrywania zagrożeń

Splunk rozwinał się w jedną z wiodących platform SIEM. Oferuje funkcje dedykowane analizie bezpieczeństwa, takie jak pobieranie danych z urządzeń zabezpieczających, korelację informacji z różnych źródeł oraz wykrywanie anomalii i znanych wzorców ataków. Zapewnia także mechanizmy kontroli dostępu oraz audytowania działań użytkowników. Dane mogą być szyfrowane zarówno podczas przesyłania, jak i przechowywania. Dostęp oparty na rolach ogranicza zakres danych widocznych dla poszczególnych użytkowników, a wszystkie operacje w systemie mogą być rejestrowane.

6. Integracja z narzędziami zewnętrznymi

Splunk został zaprojektowany jako platforma rozszerzalna i łatwa do integracji z innymi narzędziami IT oraz DevOps. Obsługuje wiele standardów oraz interfejsów, takich jak syslog, API, bazy danych oraz HTTP. Może pobierać dane z systemów chmurowych, klastrów Kubernetes czy systemów CRM. Udostępnia również zestaw SDK oraz interfejs REST API, dzięki czemu możliwa jest zdalna obsługa i automatyzacja.

Zastosowania Splunk

Wszechstronność Splunka pozwala na wykorzystanie go w wielu obszarach IT, bezpieczeństwa oraz biznesu. Do najczęstszych zastosowań należą monitorowanie operacji IT, cyberbezpieczeństwo oraz analiza zgodności z przepisami, a także monitorowanie wydajności aplikacji.

Architektura Splunk

Architektura Splunka jest modularna i skalowalna. Składa się z kilku kluczowych komponentów współpracujących w ramach potoku przetwarzania danych. Podstawowe elementy to forwardery, indexery oraz search heady, uzupełnione o komponenty zarządzające.

1. Forwarder

Forwarder to lekki agent instalowany na systemach źródłowych, takich jak serwery, aplikacje oraz urządzenia sieciowe. Jego zadaniem jest zbieranie danych i przesyłanie ich do indexera. W Splunku wyróżnia się forwardery uniwersalne, które przesyłają dane w postaci surowej, oraz forwardery ciężkie, które mogą wstępnie przetwarzać dane.

2. Indexer

Indexer stanowi serce architektury Splunka. Odbiera dane, przetwarza je i zapisuje w postaci zdarzeń możliwych do wyszukiwania. Dane są dzielone na pojedyncze zdarzenia, przypisywane są im znaczniki czasu oraz pola opisowe, a następnie zapisywane na dysku w postaci zoptymalizowanej pod kątem wyszukiwania.

3. Search Head

Search Head to komponent odpowiedzialny za interfejs użytkownika. Przyjmuje zapytania i przekazuje je do indexerów, które zawierają dane.

4. Pozostałe komponenty

Splunk Enterprise posiada dodatkowe elementy odpowiedzialne za zarządzanie i koordynację. Deployment Server zarządza centralnie konfiguracją innych instancji Splunka. License Master kontroluje wykorzystanie licencji opartej na wolumenie danych indeksowanych dziennie. W środowiskach klastrowych wykorzystywane są również węzły Cluster Master oraz Deployer do zarządzania konfiguracją klastrów.

Splunk vs ELK Stack vs Sumo Logic

The table below provides a clear comparison between **Splunk**, **ELK Stack (Elasticsearch, Logstash, Kibana)**, and **Sumo Logic**, three of the most popular **log management and data analytics tools**.

Feature	Splunk	ELK Stack (Elastic Stack)	Sumo Logic
Type	Proprietary, paid software	Open-source (Elastic Stack), self-hosted or managed	Cloud-based, SaaS
Ease of Use	User-friendly UI with powerful search features	Requires setup and configuration; can be complex	Fully managed, easy to use
Deployment	On-premises, cloud, hybrid	On-premises, cloud, hybrid	Cloud-only (SaaS)
Core Components	Indexers, Search Heads, Forwarders, SPL (Search Processing Language)	Elasticsearch (search), Logstash (data ingestion), Kibana (visualization)	Log collectors, query engine, dashboards
Scalability	Highly scalable but requires strong infrastructure	Scalable, but requires tuning and maintenance	Scales automatically in the cloud
Data Ingestion	Supports structured and unstructured data, real-time indexing	Uses Logstash or Beats for data ingestion	Cloud-based ingestion with auto-scaling
Search & Query Language	Uses SPL (Search Processing Language)	Uses Elasticsearch Query DSL (Domain Specific Language)	Uses SQL-like query language
Log Management	Centralized log management with built-in analytics	Requires configuration for log parsing and storage	Fully automated log ingestion and storage
Monitoring & Alerting	Advanced real-time monitoring and custom alerts	Requires third-party tools for better monitoring	In-built real-time alerting and notifications
Security & SIEM Capabilities	Splunk Enterprise Security (SIEM), SOAR (Automation)	Can be configured for SIEM but lacks built-in security features	Security analytics available but not as advanced as Splunk
Visualization & Dashboards	Highly customizable, interactive dashboards	Kibana provides visualization, but requires setup	Pre-built dashboards with easy customization
Machine Learning & AI	Built-in Machine Learning Toolkit (MLTK), AI-powered insights	Requires Elastic ML (paid feature)	AI-based anomaly detection and analytics
Integration & Extensibility	Supports third-party integrations, APIs, Splunkbase apps	Open-source with many plugins, APIs	Integrates with cloud services and security tools
Performance & Speed	Fast, optimized for large-scale data	Fast but depends on cluster optimization	Fast, but query speed depends on data storage tier
Cost	Expensive; charges based on data ingestion volume	Free and open-source, but costly at scale due to infrastructure needs	Subscription-based pricing, often cheaper than Splunk
Best For	Enterprises needing advanced security, IT monitoring, and analytics	Developers, startups, and businesses looking for a customizable, open-source solution	Companies looking for a managed, cloud-native log monitoring tool
Popular Use Cases	Security operations, IT monitoring, compliance, DevOps, cloud observability	Log analytics, DevOps monitoring, business intelligence	Cloud security, SaaS monitoring, real-time log analysis

Materiały dodatkowe:

- <https://www.youtube.com/watch?v=56NDgBOSpUg>
- https://www.splunk.com/en_us/training/splunk-fundamentals.html
- https://www.splunk.com/en_us/blog/learn/splunk-tutorials.html
- <https://www.microsoft.com/pl-pl/security/business/security-101/what-is-a-security-operations-center-soc>
- <http://smurf.mimuw.edu.pl/node/1900>
- https://education.splunk.com/Saba/Web_spf/NA10P2PRD105/guestapp/catalog/browse/categ0000000000003041
- <https://www.geeksforgeeks.org/software-engineering/what-is-elastic-stack-and-elasticsearch/>
- <https://stackify.com/syslog-101/>
- <https://docs.canary.tools/syslog/rfc5424.html#basic-structure>
- <https://cert.pl/posts/2024/05/rekomendacje-ot/>
- <https://securitybeztabu.pl/isa-iec-62443-kompletny-przewodnik-po-standardzie-cyberbezpieczenstwa-ot-ics/>
- <https://learn.microsoft.com/pl-pl/azure/defender-for-iot/organizations/iot-advanced-threat-monitoring>
- <https://tryhackme.com/path/outline/soclevel1>
- <https://github.com/MalwareCube/SOC101>
- https://github.com/MalwareCube/SOC101/blob/main/resources/bookmarks/soc_bookmarks.html

Przykłady

Gdzie są logi w linuxie i jak je odczytać/nimi zarządzać?

<https://securitybeztabu.pl/krytyczne-logi-do-monitorowania-przewodnik-dla-analitykow-soc/>

<https://www.geeksforgeeks.org/techtips/how-to-monitor-logs-in-linux/>

Log File	Description
/var/log/syslog	Records general system activity logs.
/var/log/auth.log	Contains authentication and login attempt information.
/var/log/kern.log	Logs kernel-related messages.
/var/log/boot.log	Stores boot-time events and errors.
/var/log/dmesg	Contains hardware and driver initialization messages.
/var/log/cron.log	Stores scheduled task execution details.
/var/log/secure	Tracks security-related messages and sudo activities.
/var/log/messages	General system messages (used in Red Hat-based systems).

<https://www.geeksforgeeks.org/techtips/how-to-manage-logs-in-linux/>

```
cat /var/log/auth.log
```

Output:

```
vboxuser@Ubuntu:~/gfg$ sudo cat /var/log/auth.log
2025-11-01T06:15:01.052602+00:00 Ubuntu CRON[3965]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-11-01T06:15:01.059331+00:00 Ubuntu CRON[3965]: pam_unix(cron:session): session closed for user root
2025-11-01T06:17:01.092057+00:00 Ubuntu CRON[3969]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-11-01T06:17:01.099900+00:00 Ubuntu CRON[3969]: pam_unix(cron:session): session closed for user root
2025-11-01T06:25:03.250771+00:00 Ubuntu CRON[4023]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-11-01T06:25:03.252295+00:00 Ubuntu CRON[4022]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-11-01T06:25:03.256621+00:00 Ubuntu CRON[4022]: pam_unix(cron:session): session closed for user root
2025-11-01T06:25:03.262055+00:00 Ubuntu CRON[4023]: pam_unix(cron:session): session closed for user root
2025-11-01T06:30:00.000864+00:00 Ubuntu gdm-password: gkr-pam: unlocked login keyring
2025-11-01T06:35:01.820099+00:00 Ubuntu CRON[4150]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-11-01T06:35:01.827821+00:00 Ubuntu CRON[4150]: pam_unix(cron:session): session closed for user root
2025-11-01T06:41:51.971614+00:00 Ubuntu unix_chkpwd[4177]: password check failed for user (vboxuser)
2025-11-01T06:41:51.972402+00:00 Ubuntu gdm-password: pam_unix(gdm-password:auth): authentication failure; logname=vbox
user uid=0 euid=0 tty=/dev/tty1 ruser= rhost=
2025-11-01T06:41:57.177348+00:00 Ubuntu gdm-password: gkr-pam: unlocked login keyring
2025-11-01T06:45:01.278599+00:00 Ubuntu CRON[4412]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-11-01T06:45:01.285283+00:00 Ubuntu CRON[4412]: pam_unix(cron:session): session closed for user root
2025-11-01T09:16:17.545874+00:00 Ubuntu systemd-logind[1111]: New seat seat0.
2025-11-01T09:16:17.545880+00:00 Ubuntu systemd-logind[1111]: Watching system buttons on /dev/input/event0 (Power Button)
2025-11-01T09:16:17.545885+00:00 Ubuntu systemd-logind[1111]: Watching system buttons on /dev/input/event1 (Sleep Button)
2025-11-01T09:16:17.545911+00:00 Ubuntu systemd-logind[1111]: Watching system buttons on /dev/input/event2 (AT Translate d Controller)
```

<https://www.digitalocean.com/community/tutorials/how-to-view-and-configure-linux-logs-on-ubuntu-debian-and-centos>

Dla chętnych: https://msobocinska.zsl.gda.pl/PrSO_kl2/00-2025/LogiSerwera/cw%20logowanie.pdf

Zadania praktyczne

Zadanie 1 – LetsDefend i Tryhackme

Wykonaj poniższe zadania (można wybrać które 😊):

LetsDefend:

- <https://app.letsdefend.io/training/lessons/soc-fundamentals>
- <https://app.letsdefend.io/training/lessons/siem-101>
- <https://app.letsdefend.io/training/lessons/splunk>
- <https://app.letsdefend.io/training/lessons/how-to-investigate-a-siem-alert>

Tryhackme:

- <https://tryhackme.com/room/socfundamentals>
- <https://tryhackme.com/room/socl1alertreporting>
- <https://tryhackme.com/room/socl1alerttriage>
- <https://tryhackme.com/room/introtosiem>
- <https://tryhackme.com/room/introtologanalysis>
- <https://tryhackme.com/room/introtologs>
- <https://tryhackme.com/room/linuxloggingforsoc>
- <https://tryhackme.com/room/windowsloggingforsoc>
- <https://tryhackme.com/room/loganalysiswithsiem>
- <https://tryhackme.com/room/idsevasion>

Zadanie 2 – Instalacja Splunk

- <https://github.com/splunk/docker-splunk>
- <https://www.tutorialspoint.com/splunk/index.htm>

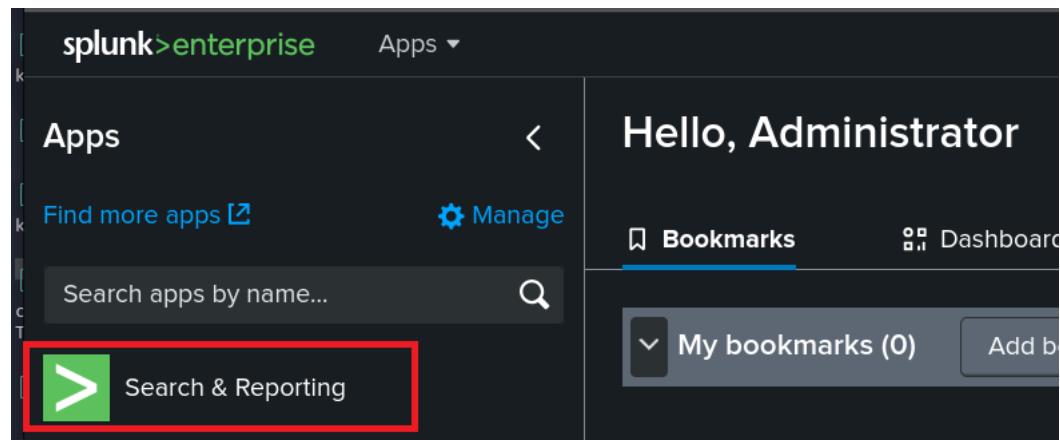
```
sudo docker run -p 8000:8000 -e "SPLUNK_PASSWORD=<password>" \
-e "SPLUNK_START_ARGS=--accept-license" \
-e "SPLUNK_GENERAL_TERMS=--accept-sgt-current-at-splunk-com" \
-it --name so1 splunk/splunk:latest
```

Po zakończeniu pobierania i uruchamiania udaj się do: <http://localhost:8000>

Login: admin

Hastło: <password> z polecenia wyżej

Uruchom Search & Reporting



Następnie uruchom tutorial:

A screenshot of a 'How to Search' tutorial page. At the top, it says 'How to Search'. Below that, a message states: 'If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.' At the bottom, there are three buttons: 'Documentation' (with a red box around it), 'Tutorial' (also with a red box around it), and 'Data Summary'. The 'Tutorial' button is currently selected.

- [About the Search Tutorial | Splunk Docs](#)

Podążaj krok po kroku za tutorialiem i wykonuj przedstawione tam zadania.

Zadanie 3 – Splunk online lab

Wykonaj zadanie:

- <https://tryhackme.com/room/splunkforloganalysis-aoc2025-x8fj2k4rqp>