SIEM Use Cases

SECURIVY

Logsign

Spis treści:

Czym są use case’y?

Przypadki użycia (use case’y) są kluczowe dla identyfikacji operacji osoby atakującej we wczesnych, środkowych i końcowych fazach. **Niewielki, drobny incydent może wskazywać na większe ataki**, dlatego monitorowanie najdrobniejszych zachowań jest tak istotne. Konieczne jest również posiadanie scenariusza postępowania (playbook) dotyczącego reakcji. Przypadkiem użycia może być stworzona przez nas **zasada lub warunek**, który będzie odnosił się do logów wprowadzanych do SIEM. Use case’y opisują aktywności, które użytkownik wykonuje w systemie oraz odpowiedzi systemu na te zachowania. Mogą również uwzględniać różne scenariusze i warunki, w jakich system będzie działał.

Zdefiniowanie i obserwacja use case’ów pomaga odpowiedzieć na pytanie: "Co system powinien w danym przypadku zrobić dla swoich użytkowników?" Przykładem będzie wykrycie szkodliwego ruchu na kluczowych serwerach infrastruktury lub zbyt wiele prób logowania w ciągu ostatniej minuty.

Najlepsze praktyki korzystania z przypadków użycia:

- Upewnij się, że zawsze masz przy sobie klarowną listę przypadków użycia.
- Przypadki użycia powinny być powiązane z fazami MITRE ATT&CK, aby można było określić, jak bardzo atakujący osiągnął swój cel. Etykietowanie i powiązanie z matrycą MITRE ATT&CK pomaga w wykrywaniu (jakie logi należy monitorować) i łagodzeniu zagrożeń. Pomaga również w przypisaniu do grupy APT.
- Każdy use case powinien mieć klarowny priorytet zgodny z polityką twojej organizacji.
- Każdy use case powinien mieć źródło logów, które musi być wprowadzone do SIEM.

Dlaczego ważne jest posiadanie dużej liczby use case’ów?

- Prawdziwe ataki cybernetyczne są złożone, a analiza i obserwacja wielu przypadków użycia pozwoli być zespołowi SOC o krok przed atakującym.
- Przypadki użycia to reguły, które wywołują alert. Pozwalają one zdefiniować scenariusze postępowania, znaleźć odpowiedzi na pytania: jak na nie reagować, jakie kroki do przeprowadzenia analizy należy wykonać i jak załagodzić zagrożenie.
- Proces tworzenia scenariuszy postępowania jest bardzo ważny. Znacznie pomaga on w przygotowaniu do radzenia sobie z cyberatakami.

Windows

- Wyłączenie/włączenie serwera
- Wykrycie nośnika wymiennego
- Nietypowe wyłączenie systemu Windows
- Próby logowania na to samo konto z różnych komputerów
- Wykrycie wyłączenia i ponownego uruchomienia serwera po godzinach pracy
- Zmiana przynależności do grupy administracyjnej
- Nieautoryzowane logowanie na domyślne konta
- Interaktywne korzystanie z konta usługi
- Logowanie zdalne - sukces i niepowodzenie
- Zatrzymanie/ponowne uruchomienie usługi systemowej w systemie Windows
- Ustawienie uprawnień ACL dla członków grupy administratorów
- Włączenie/wyłączenie konta w systemie Windows
- Wielokrotne zablokowanie kont w systemie Windows
- Wielokrotne logowania na jedno konto w systemie Windows
- Atak Brute force z tego samego źródła
- Logowania poza normalnymi godzinami pracy
- Logowanie na wiele kont użytkowników z tego samego źródła
- Atak Brute Force z tego samego źródła z udanym zalogowaniem
- Tworzenie/usuwanie kont w systemie Windows
- Awaria sprzętu w systemie Windows
- Nieudane logowanie do wielu miejsc docelowych z tego samego źródła
- Wielokrotne nieudane logowania na konta administracyjne
- Wykrycie dodania/usunięcia konta użytkownika w grupie administratorów
- Wykrycie zmiany czasu systemowego (czas uruchomienia)
- Wykrycie użycia domyślnych kont dostawców produktów
- Usunięcie użytkownika w ciągu 24 godzin od utworzenia
- Zatrzymanie ważnej usługi na serwerach Windows
- Pełny dziennik zdarzeń bezpieczeństwa w systemie Windows
- Wielokrotne zmiany hasła w krótkim czasie
- Zmiana typu grupy w systemie Windows
- Zmiana polityki audytu
- Wyczyszczenie dziennika audytu
- Wykrycie dodania konta użytkownika
- Nieudane logowanie - próba logowania na wygasłe konto
- Duża liczba tworzonych/usuwanych użytkowników w krótkim czasie
- Wykrycie ruchu wychodzącego z serwerów do Internetu
- Nieudane logowanie/próba zalogowania na konto wyłączonego/byłego pracownika/konta z wygasłą ważnością
- Usunięcie pliku/folderu w systemie Windows
- Zmiana uprawnień plików/folderów w systemie Windows
- Duża liczba tworzonych/usuwanych użytkowników w krótkim czasie

Unix

- Import i eksport plików FTP w systemie Unix
- Pełny system plików Unix
- Wyłączenie serwera Unix
- Tworzenie/usuwanie użytkowników w krótkim czasie
- Tworzenie/usuwanie grup użytkowników w krótkim czasie
- Próby logowania na to samo konto z różnych komputerów w systemie Unix
- Nieudane logowania
- Nieudane logowania na wyłączone konta
- Zalogowanie się do serwera FTP
- Wiele połączeń SFTP
- Nieudane logowania z dostępem roota
- Wiele nieudanych logowań jako użytkownik SU
- Próby zdalnego logowania jako użytkownik root na węźle produkcyjnym
- Dostęp sudo od nieprzywilejowanych użytkowników
- Wykrycie użycia domyślnych kont dostawców produktów
- Dodawanie lub usuwanie użytkowników do grupy "root" w systemie Unix
- Zatrzymanie ważnej usługi
- Duża liczba nieudanych logowań na to samo konto w krótkim czasie
- Zmiana hasła
- Dodawanie, usuwanie i modyfikowanie zadań cron
- Nieudane logowania jako użytkownik SU
- Wykrycie zmiany konfiguracji syslog
- Wykrycie zmiany konfiguracji sieciowej

Firewall, Antywirus, IPS i VPN

- Nieudane logowanie jako administrator
- Atak Brute Force z udanymi zmianami konfiguracji
- Przełączenie się Firewalla na Firewalla awaryjnego
- Udana komunikacja z adresu IP z Internetu po wcześniejszych blokadach w Firewallu
- Próby dostępu do niezidentyfikowanych protokołów i portów
- Przeskanowanie hosta poprzedzone incydentem z wykorzystaniem exploita
- Dostęp do nieprawidłowych docelowych adresów IP
- Udana autoryzacja poza godzinami pracy
- Ponowne uruchomienie Firewalla
- Wykrycie modyfikacji kont użytkowników/grup
- Dodanie/usunięcie użytkownika do bazy danych Firewalla
- Wykrycie niezabezpieczonego ruchu, takiego jak FTP, telnet na ważnych serwerach
- Wykrycie dodania/usunięcia administratora Firewalla
- Odmowa logowania (atak Brute force)
- Duża liczba wystąpienia odmowy dostępu
- Wykrycie zmiany konfiguracji
- Utrata łącza do urządzenia równorzędnego z powodu problemów z okablowaniem fizycznym lub konfiguracją NSRP
- Skanowanie portów sieciowych i hostów
- Wykrycie przełączenia między głównym a zapasowym urządzeniem
- Administrator udzielił/odwołał dostęp do Firewalla z określonego adresu IP
- Wykrycie ruchu typu P2P
- Alerty o wysokim obciążeniu procesora przez Firewalla
- Firewall nie mógł przydzielić pamięci RAM
- Wykrycie dowolnego rodzaju awarii związanej ze stanem zapasowego Firewalla
- Zarejestrowanie najczęściej blokowanego ruchu sieciowego pochodzącego z obszaru zdemilitaryzowanego (DMZ) i Firewalla
- Obserwacja ruchu wychodzącego na ważnych portach
- Udany wykonanie ruchu sieciowego wychodzącego do adresu IP umieszczonego na czarnej liście
- Wiele nieudanych prób wykonania ruchu sieciowego wychodzącego do adresu IP zagrożonego umieszczonego na czarnej liście

Urządzenia zabezpieczające

- Wykrycie krytycznego alertu Firewalla
- Wykrycie zmiany konfiguracji VPN
- Wykrycie nieudanych logowań na konto administratora
- Udana autoryzacja poza godzinami pracy
- Udana próba dostępu z podejrzanych krajów
- Restart usług
- Zmiana konfiguracji klastra Firewalla/Gatewaya
- Wysokie obciążenie procesora
- Konfiguracja polityki bezpieczeństwa systemu
- Duża liczba odmowy dostępu
- Alert oparty na sygnaturze Smart-Defense
- Błąd weryfikacji certyfikatu VPN
- Wykrycie zmiany konfiguracji
- Ponowne uruchomienie Firewalla

Poczta elektroniczna

- 10 najczęściej wysyłających wiadomości do domen zewnętrznych
- 10 najczęściej odbierających/wysyłających wiadomości e-mail
- Wykrycie wycieku danych
- Wysyłanie dużych plików za pomocą wiadomości e-mail
- Wykrycie podejrzanych/złośliwych załączników
- Identyfikatory grup wykorzystania poczty elektronicznej
- Monitorowanie wiadomości wychodzących z domeny firmy do innych domen poza godzinami pracy
- Wysokie wykorzystanie przepustowości e-mail przez poszczególnych użytkowników
- Wykrycie nieudanych dostarczeń wiadomości
- Dostęp do skrzynki pocztowej przez innego użytkownika
- Wysyłanie wiadomości używając imienia innego użytkownika
- Wysyłanie wiadomości w imieniu innego użytkownika
- Wykrycie logowania użytkowników do skrzynki pocztowej, która nie jest ich kontem głównym
- Wykrycie automatycznego przekierowywania wiadomości
- 10 najczęściej wysyłających wiadomości wewnętrznie
- Nagły wzrost przychodzących wiadomości SMTP przez bramę pocztową
- Duża liczba odrzuconych wiadomości z jednego adresu "od"

Sieć bezprzewodowa / VPN:

- Wykrycie nieautoryzowanego ruchu w sieci
- Najważniejsze konta VPN zalogowane z wielu zdalnych lokalizacji
- Najważniejsze konta VPN zalogowane z VPN i lokalnej sieci
- Nieautoryzowane próby logowania w sieci bezprzewodowej
- Serwer autoryzacji sieci bezprzewodowej jest niedostępny
- Anonimowe logowanie z nieznanego adresu IP
- Logowanie do konta VPN z wielu lokalizacji w krótkim czasie lub z podejrzanych krajów
- Jednoczesne logowanie z wielu lokalizacji dla jednego użytkownika
- Połączenie VPN trwające dłużej niż 24 godziny
- Dostęp VPN z wewnętrznego adresu IP
- Dostęp VPN z zagranicznych lokalizacji
- Ponowne uruchomienie punktu dostępowego bezprzewodowej sieci lokalnej
- Wykrycie niezabezpieczonego punktu dostępu bezprzewodowego
- Dostęp VPN zespołu pracowników znajdujących się w tym samym kraju
- Dostęp VPN i karta dostępu wewnątrz kraju

IPS (na przykład Cisco IPS):

- Próba dostępu do pliku z hasłami UNIX
- Ważne powiadomienie IPS
- Możliwe wykorzystanie podatności
- Prawdopodobne skanowanie portów w sieci
- Próba ataku typu SQL Injection
- Ruch wirusów w sieci
- Ataki oparte na sygnaturach

Routery i przełączniki:

- Komunikaty o błędach krytycznych routera
- Zmiana statusu relacji sąsiadujących BGP
- Awaria zasilania routera
- Zmiana konfiguracji
- Zarejestrowane krytyczne komunikaty pochodzące z Switcha
- Zarejestrowane alerty pochodzące z Switcha
- Wykrycie antyspamu
- Odrzucenie pliku z powodu dużej wielkości
- Wykrycie procesu aplikacji proxy
- Wykrycie ataku typu land
- Wykrycie ataku typu ping of death
- Wykrycie dodania nowej polityki
- Wykrycie naruszenia polityki
- Ruch sieciowy wirusów
- Wykrycie filtrowania treści
- Nieudana/udana autoryzacja

Proxy:

- Próby dostępu do niezidentyfikowanych protokołów i portów
- Raport dotyczący dostępu do domen złośliwego oprogramowania
- Podsumowanie raportu kategorii proxy
- Raport dotyczący dostępu do adresów IP związanych z złośliwym oprogramowaniem
- Dostęp do potencjalnie niechcianego oprogramowania
- Host dynamicznego DNS
- Złośliwy kod/Malnety
- Złośliwe wychodzące dane/Botnety
- Peer-to-Peer (P2P)
- Unikanie proxy
- Narzędzia zdalnego dostępu
- Dostęp z nietypowym agentem użytkownika
- Zapytania POST na niezidentyfikowane strony po godzinach pracy
- Niechciany dostęp do internetu
- Zmiany konfiguracji proxy
- Nieudane próby logowania do proxy
- Naruszenie dostępu do zawartości
- Anonimowy dostęp do proxy
- Dostęp do stron z narzędziami hakerskimi
- Próby dostępu identyfikowane jako BOTNET na podstawie nagłówka żądania HTTP

Bazy danych:

- Wygaśnięcie hasła
- Używanie poleceń wprowadzających duże zmiany
- Wykonywanie poleceń wprowadzających duże zmiany w bazie danych poza godzinami pracy
- Polecenia aktualizacji lub wstawienia
- Tworzenie/usuwanie użytkowników w bazie danych
- Wiele nieudanych logowań do bazy danych
- Tworzenie/modyfikacja schematu bazy danych
- Najczęstsze niepowodzenia wykonania zapytania
- Monitorowanie prób logowania do bazy danych
- Użycie domyślnych kont dostawców produktów wobec polityki
- Dostęp do baz danych poza godzinami pracy
- Nieudane logowania dla kont sys/system lub kont uprzywilejowanych
- Połączenie z bazami danych produkcyjnymi z niedozwolonych segmentów sieciowych

Antywirus (AV):

- Wykrycie wirusa przez antywirusa
- Wykrycie ruchu tylnymi drzwiami w sieci przez AV
- Wykrycie nośników wymiennych
- Wykrycie zainfekowania malwarem przez antywirusa (nie poddano kwarantannie/czyszczeniu/usunięciu/przeniesieniu)
- Wykrycie wielu zainfekowań malwarem przez AV z tego samego hosta
- Wiele źródeł uzyskuje dostęp do tego samego adresu URL związanego z malwarem
- Wykryto wiele różnych typów zainfekowań malwarem przez antywirusa z tego samego hosta
- Błąd wykrycia aktualizacji definicji antywirusowych w maszynach użytkowników końcowych
- Wykrycie rozprzestrzeniającego się robaka w sieci
- Wykrycie rozprzestrzeniania się wirusa
- Próba zatrzymania planowych/rozkładanych skanów ad hoc
- Wykrycie ruchu związanego z nielegalnym połączeniem sieciowym
- Próba zatrzymania usług antywirusa
- Próba zatrzymania kluczowych modułów antywirusa
- Antywirus zidentyfikował podejrzane maszyny w sieci (rogue machines)
- Wykrycie skanu, który został zatrzymany przed zakończeniem
- Wykrycie zatrzymania/wstrzymania (opóźnienia) planowanego skanu
- Wykrycie komputera, który nie jest chroniony najnowszymi definicjami
- Wykrycie nowo zainstalowanego oprogramowania klienta
- Wykrycie odinstalowania oprogramowania klienta
- Wykrycie rozprzestrzeniania się malwaru przez antywirusa na wielu maszynach w tej samej podsieci/innej podsieci
- Wiele powtórzeń tego samego zainfekowania z tej samej maszyny (AL i Trend - historyczne dane)
- Wiele powtórzeń unikalnego zainfekowania z tej samej maszyny (AL i Trend - historyczne dane)
- Monitorowanie czarnych list domen/IP, ruchu wychodzącego/dochodzącego do/z zainfekowanej maszyny (AL i Trend - czas rzeczywisty)
- Próba ataku Brute force/przeskanowania portów lub hosta/zdobywania uprawnień na zainfekowanej maszynie (AL i Trend - czas rzeczywisty)
- Próba restartu usługi lub procesu antywirusa, modułów antywirusa na zainfekowanej maszynie

Inne:

- Używanie domyślnego konta użytkownika
- Nieaktywne konta użytkowników
- Monitorowanie dostępu VPN poza godzinami pracy
- Najczęściej komunikujące się urządzenia z Firewalem
- Ruch P2P
- Rozproszone skanowanie portów hosta
- Rozproszone skanowanie hostów sieciowych
- Atak SYN Flood według IDS/Firewalla
- Wysoka liczba odrzuconych połączeń dla jednego hosta
- Wykrycie rozprzestrzenianie się robaka/wirusa
- Skanowanie sieci wychodzącej/wejściowej
- Błąd aktualizacji antywirusa
- Dostęp do zainfekowanych adresów IP przez malware
- Dostęp do zainfekowanych adresów URL przez malware
- Próba hakowania portalu internetowego
- Wyciek danych
- Wykryto zainfekowanie BOTNET w sieci wewnętrznej LAN
- Nieautoryzowany dostęp z sieci osób trzecich lub dostawców
- Aktywność zainfekowanego hosta
- Działania budzące podejrzenia, adware, phishing i aktywności związane z hakowaniem
- Niechciane oprogramowanie
- Wykryto rozprzestrzenianie się malwarem przez Antywirusa na wielu maszynach
- Monitorowanie dostępu zespołu developerskiego do systemów produkcyjnych
- Czarna lista adresów IP
- Przejście na czarną listę adresu IP po wielokrotnym blokowaniu przez Firewalla
- Czarna lista adresów URL
- Trendy analizy danych
- Ruch sieciowy wychodzący do podejrzanych krajów
- Ruch sieciowy wychodzący na podejrzane porty
- Ruch sieciowy wychodzący do podejrzanych usług
- Zakończona aktywność użytkownika
- Podejrzany ruch sieciowy do wrażliwych zasobów
- Komunikacje do złych domen
- Komunikacje do domen/IP z czarnej listy
- Przesyłanie danych do domen/IP z czarnej listy
- Ruch sieciowy wychodzący dotyczący bazy danych
- Atak typu Cross Site Scripting
- Script Injection
- Złośliwa aktywność
- Wykryto zmiany/awarie stanu interfejsu Firewalla
- Użycie niezabezpieczonych protokołów - wykrycie niezabezpieczonego ruchu takiego jak FTP, telnet, VNC na kluczowych serwerach

Inne:

- Dostęp do VPN z zagranicy
- Podejrzane próby logowania do VPN
- Wykrycie zatrzymania usługi na serwerach ESX
- Wykrycie wielu nieudanych logowań użytkowników na serwerach ESX z tego samego źródła
- Wykrycie wyłączenia/włączenia serwera ESX
- Wykrycie uruchamiania/zatrzymywania/wznowienia/restartu maszyny wirtualnej
- Wykrycie dodania/usunięcia hosta na vCenter
- Wykrycie tworzenia/usuwania maszyny wirtualnej na vCenter
- Zaobserwowanie prawdopodobnego ataku typu XSS zaobserwowany
- Zaobserwowanie prawdopodobnego ataku typu Directory Traversal
- Zaobserwowanie podejrzanej metody http
- Zapytanie HTTP inne niż GET, POST, HEAD i OPTIONS
- Zaobserwowanie prawdopodobnych ataków typu SQL Injection
- Atak internetowy - skanowanie podatności za pomocą Nessusa

Źródła:

https://www.siemusecases.com/

https://playbooks.flexibleir.com/soc-siem-use-cases/

https://www.linkedin.com/pulse/soc-siem-use-cases-khalid-alateeq/

Skontaktuj się z nami,
aby **dowiedzieć się więcej**

Odwiedź nas na:
www.securivy.com

Obserwuj nas:

Kontakt:
Securivy Sp. z o.o.
NIP: 7792534607
biuro@securivy.com
tel. +48 573 568 234

Logsign

SECURIVY