Paweł SZYNKIEWICZ [1], Adam KOZAKIEWICZ[2]

Naukowa i Akademicka Sieć Komputerowa (NASK) (1), Politechnika Warszawska (2)

doi:10.15199/48.2019.03.32

Filtracja i korelacja zdarzeń bezpieczeństwa – modele i metody

Abstract. *The paper is concerned with the problem of filtration and correlation of security incidents - suspicious events in computer networks. Each event is specifiable by a set of attributes and whole dataset is filtered w.r.t. these attributes to identify the suspicious events. Correlation is accomplished by looking for and analyzing relationships between suspicious events and vulnerabilities from heterogeneous datasets. The aim is to group data with the similar values of attributes. A brief survey of a set of techniques to investigate event patterns and combine suspicious events into meaningful entities is provided. The attention is focused on classification and grouping techniques. (**Filtration and correlation of security incidents - models and methods**)*

Streszczenie. *Praca dotyczy zagadnień filtracji i korelacji zdarzeń bezpieczeństwa w sieciach teleinformatycznych. Filtracja jest wykonywana względem pewnych zdefiniowanych atrybutów charakteryzujących zdarzenie. Korelacja jest rozumiana jako proces kojarzenia ze sobą informacji o możliwych incydentach naruszenia bezpieczeństwa i zagrożeniach w sieci pozyskanych z różnych źródeł. Kojarzone są ze sobą zdarzenia o podobnych wartościach wspomnianych wcześniej atrybutów. Oba problemy są zdefiniowane i omówione są różne podejścia, które można zastosować do ich rozwiązania. Szczególna uwaga jest zwrócona na techniki grupowania i klasyfikacji.*

Keywords: cybersecurity, security incidents, filtration, correlation, classification methods, grouping techniques.
Słowa kluczowe: cyberbezpieczeństwo, zdarzenia bezpieczeństwa, filtracja, korelacja, metody klasyfikacji, techniki grupowania.

Wprowadzenie

Rozważania koncentrują się na zagadnieniach przetwarzania danych o zdarzeniach bezpieczeństwa w sieci w celu budowania świadomości sytuacyjnej oraz oceny możliwości wystąpienia potencjalnych zagrożeń. Przyjmuje się, że dane o sytuacji w sieci mogą być pozyskiwane z różnych źródeł, tj. instytucji, organizacji z kraju i świata, a więc są to zazwyczaj dane różnego typu. W ogólności można wyróżnić trzy podstawowe rodzaje rozważanych danych:

- Dane typu podstawowego, których format jest ściśle określony, posiadające jednoznaczną interpretację, czyli dane atomowe, nie składające się z danych innych typów, (np.: adres IP, URL, skróty), surowe dane binarne, tj. próbki malware, ruchu sieciowego itd.
- Dane ustrukturyzowane (zagregowane), grupujące logicznie powiązane ze sobą dane różnych typów, np. IoC (*Indicators of Compromise*), dane o incydentach, podatnościach, uczestnikach. Ich format jest określony przez zbiory składowych wymaganych i składowych opcjonalnych.
- Dane nieustrukturyzowane, bez ściśle określonej struktury, które mogą zawierać dane innych typów, np.: komentarze, analizy, dyskusje.
- Dane asocjacyjne, określające relacje między obiektami w systemie.

Do reprezentacji danych o cyberzagrożeniach stosuje się coraz częściej standard STIX (Structured Threat Information Expression, https://stixproject.github.io/about/) – obecnie najpełniejszy język i format serializacji danych do wymiany informacji o zdarzeniach bezpieczeństwa w sieci. STIX pozwala na definiowanie i rozszerzanie typów, wersjonowanie, opisywanie relacji między obiektami i określanie profili użycia języka. Podstawowe encje standardu STIX to: obserwacje, indykatory, incydenty, taktyki techniki i procedury, kampanie, aktorzy, cele, działania. Do wymiany informacji reprezentowanych w języku STIX służy protokół TAXII (Trusted Automated eXchange of Indicator Information, https://taxiiproject.github.io/) - mechanizm wymiany danych z poziomu aplikacji wykorzystujący protokół HTTPS.

Ważnym elementem każdego systemu do analityki biznesowej (ang. *Business Intelligence*) [1], a do takich należą systemy, których zadaniem jest uzyskanie obrazu sytuacyjnego w sieci, są dobrze opracowane procesy integracji danych, zwane potocznie procesami ETL (ang. e*xtracton, transformation, loading*). Poprawnie zdefiniowane procesy ETL umożliwiają zastąpienie ogromnej ilości różnorodnych danych pozyskiwanych z różnych źródeł łatwo dostępnymi, usystematyzowanymi i użytecznymi dla użytkowników systemu informacjami. Wyróżnia się następujące etapy ETL:

1. Import (wydobycie) danych z systemów źródłowych. Dane mogą być reprezentowane w różnych formatach, przewiduje się wiele różnych protokołów wymiany danych.
2. Transformacja danych źródłowych w jednolity, zintegrowany zestaw informacji. W trakcie transformacji wykonywane są dowolne konwersje, agregacje, filtracje, korelacje i przeliczania na danych źródłowych, zgodnie z algorytmami biznesowymi. Sprawdzana jest ich integralność i spójność. Wykorzystane do tego celu są mechanizmy zarządzania jakością danych.
3. Wprowadzenie przetworzonych informacji do systemów docelowych.

W większości systemów, w tym w systemach, których zadaniem jest uzyskanie obrazu sytuacyjnego w sieci najtrudniejszą operacja jest odpowiednia transformacja danych. Ze względu na różny charakter pozyskiwanych informacji oraz ograniczoną możliwość kontroli nad procesem napływania danych utrzymanie wysokiej jakości danych stanowi poważne wyzwanie [2,3]. Wymagane jest zazwyczaj wdrożenie zaawansowanych technik integracji danych, obejmujących [1,4]: asymilację danych, weryfikację jakości, usuwanie błędów, automatyczne scalanie, rozstrzyganie konfliktów, deduplikację, standaryzację i normalizację. Kolejnymi operacjami na danych są filtracja i korelacja, które stanowią temat przewodni niniejszej pracy. Filtracja zdarzeń występujących w sieci polega na przeprowadzeniu wstępnej analizy polegającej na wybraniu danych przez zastosowanie zdefiniowanych filtrów, czyli takich, które warto poddać dalszej analizie. Korelacja zdarzeń jest rozumiana jako proces kojarzenia ze sobą przefiltrowanych wcześniej informacji o możliwych incydentach naruszenia bezpieczeństwa i zagrożeniach oraz grupowanie zdarzeń o podobnych lub wspólnych cechach. Kolejnym krokiem jest odkrywanie asocjacji, czyli w tym przypadku zależności między incydentami w sieci i danymi o innych, powiązanych z nimi zdarzeniami m.in. w celu określenia wzajemnych powiązań pomiędzy aktywnymi zagrożeniami dla sieci i systemów oraz słabymi punktami tych zasobów. Przetworzone dane stanowią podstawę do oszacowania poziomu zagrożenia w skali kraju, oceny

ryzyka rozprzestrzeniania się zagrożenia i podjęcia właściwych środków bezpieczeństwa, zgodnie z ustalonymi priorytetami. Różnorodne metody i techniki służą do osiągnięcia dwóch związanych ze sobą celów: ujawnienia wszystkich realnych zagrożeń oraz wyeliminowania fałszywych alarmów.

Dane Opisujące zdarzenia bezpieczeństwa

Przyjmijmy, że analizy są wykonywane dla różnych typów danych opisujących zdarzenia bezpieczeństwa. Wśród możliwych danych można wyróżnić:

- wskaźniki infekcji (*Indicators of Compromise* - IoC),
- obserwacje (ang. *sightings*),
- podejrzenia incydentu (infekcja, *abuse*),
- incydenty,
- wystąpienia podatności (obserwacje podatnych systemów),
- podatności w systemach, oprogramowaniu lub/oraz konfiguracji,
- informacje o jakości / komentarze,
- raporty / analizy,
- dane o powiązaniach między podmiotami, przepływy, dane surowe, np. *spamtrap,* pliki binarne, kontekst (np. konfiguracja statyczna *malware*), itp.

Wymienione rodzaje danych mogą być opisywane w bardzo różny sposób, trudne jest ich przetwarzanie. Automatyczna filtracja wymaga ustrukturyzowania oraz ujednolicenia opisu danych o różnym typie zdarzeń. Stąd definicje i propozycje zapisu formalnego przedstawione w następnym rozdziale.

Filtracja i korelacja zdarzeń bezpieczeństwa - modele

Rozważania poświęcone filtracji i korelacji zdarzeń bezpieczeństwa rozpoczniemy od przedstawienia zestawu pojęć i ogólnych definicji filtra i korelatora zdarzeń bezpieczeństwa.

Definicja 1: Zbiór zdarzeń bezpieczeństwa: *Iloczyn kartezjański* $Z = Z_1 \times Z_2 \times \ldots \times Z_N$, *zbiorów wartości* N *atrybutów* Z_i, $i = 1, \ldots, N$ *charakterystycznych dla incydentów bezpieczeństwa w sieci*.

Definicja 2: Zdarzenie bezpieczeństwa (incydent bezpieczeństwa): *Element zbioru* Z, *czyli* $z = (z_1, \ldots, z_N) \in Z$.

Przyjmujemy, że wszystkie zdarzenia bezpieczeństwa opisujemy za pomocą N-elementowej krotki zawierającej wartości atrybutów (dziedzina wnioskowania ma wymiar N).

Definicja 3: Atrybut zdarzenia bezpieczeństwa: *Funkcja* f_i *przypisująca zdarzeniu bezpieczeństwa* z *wartość jego* i*-tego elementu* z_i *należącą do zbioru* Z_i ($z_i \in Z_i$).

(1) $f_i(z)\colon Z \to Z_i, i = 1, \ldots, N,$

czyli zdarzenie bezpieczeństwa z definiuje krotka:

$z = (z_1, \ldots, z_N) = \big(f_1(z), \ldots, f_N(z)\big)$.

Atrybuty mogą przyjmować wartości różnego typu. Mogą to być zbiory wartości liczbowych (liczby całkowite lub rzeczywiste), łańcuchy znaków, jak też dane złożone, np. rekordy, struktury danych itd. Podsumowując, każdy zbiór Z_i może zawierać dane innego typu. W przypadku, gdy dla danego zdarzenia nie jesteśmy w stanie określić wartości *i*-tego atrybutu przypisujemy mu wartość $NULL$, czyli z_i=$NULL$.

Poniżej przedstawiamy przykład zdarzenia bezpieczeństwa:

z = (192.168.11.2, http://ab, {80,443}, 03.06.2018, 15.10.20, 15, 6)

z_1 – numer IP,
z_2 – domena,
z_3 – zbiór docelowych portów,
z_4 – data identyfikacji ataku,
z_5 – czas identyfikacji ataku (znacznik czasu),
z_6 – czas trwania zdarzenia (w ustalonej jednostce czasu),
z_7 – intensywność zdarzenia (liczba wystąpień w ustalonej jednostce czasu).

Filtracja zdarzeń bezpieczeństwa

Celem jest wyselekcjonowanie ze zbioru wszystkich zarejestrowanych zdarzeń bezpieczeństwa, tych których atrybuty przyjmują wartości z zadanych zbiorów wzorcowych.

Definicja 4: Wzorzec i-tego atrybutu: *Podzbiór wartości* i*-tego atrybutu* $F_i \subseteq Z_i$ *określający warunki nałożone na wartość tego atrybutu.*

Wzorzec służy do wyselekcjonowania podzbioru zdarzeń spełniających warunek

(2) $f_i(z) \in F_i$.

Definicja 5: Wzorzec: *Iloczyn kartezjański wzorców dla* N *atrybutów*

(3) $F = F_1 \times \ldots \times F_N.$ $\qquad F \subseteq Z.$

Definicja 6: Filtr zdarzeń bezpieczeństwa: *Funkcja* $\psi\colon Z \to \{0,1\}$ *stwierdzająca przynależność zdarzenia* z *do wzorca* (2)

(4) $\psi(z) = \begin{cases} 1, & z = \big(f_1(z), \ldots, f_N(z)\big) \in F, \\ 0, & w\ przeciwnym\ razie, \end{cases}$

gdzie $z = \big(f_1(z), \ldots, f_N(z)\big) \in F \equiv \Lambda_{i=1}^{N} f_i(z) \in F_i$. Zakładamy, że filtracja może być dokonywana względem L atrybutów ($L \leq N$). Domyślnie przyjmuje się $F_i \equiv Z_i$.

Informacja wzbogacająca

Dane o zdarzeniu bezpieczeństwa mogą być istotnie wzbogacone. Dodatkowymi danymi mogą być wyniki analiz przeprowadzonych na podstawie aktualnych wartości atrybutów zdarzenia, np. obliczone statystyki, oszacowania itd. Istotne może okazać się również uwzględnienie aktualnie dostępnych dodatkowych informacji, które nie dotyczą bezpośrednio incydentów sieciowych, ale mogą w znacznym stopniu wzbogacić naszą wiedzę o potencjalnych możliwościach wystąpienia zagrożeń bezpieczeństwa w chronionej infrastrukturze. Dane te pochodzą zazwyczaj z różnych, odseparowanych źródeł. Przykładami informacji wzbogacającej mogą być dane o historycznych atakach, rekordy bazy podatności, wyniki ankiety, pozycje katalogu infrastruktury i oprogramowania. Przyjmijmy przedstawioną poniżej definicję informacji wzbogacającej.

Definicja 7: Informacja wzbogacająca: *Zbiór dodatkowych danych* W*, które mogą mieć znaczenie w kontekście zdarzeń bezpieczeństwa.*

Przykład informacji wzbogacającej: W={w_1, w_2, w_3,…}

w_1 – statystyka wyznaczona na podstawie wybranych atrybutów (wartość numeryczna),
w_2 – rekord bazy danych podatności (wartość numeryczna),
w_3 – pozycja w katalogu sprzętu (wartość numeryczna),
w_4 – pozycja w katalogu oprogramowania (wartość numeryczna).
w_5 – wynik ankiety przeprowadzonej w chronionej instytucji (ciąg znaków lub wartość numeryczna).

Przyjmijmy, że w danej chwili *t* dysponujemy zbiorem W zawierającym M informacji wzbogacających. Informacje wzbogacające mogą powodować zmianę wartości atrybutów zdarzeń, zwiększenie liczby możliwych ich wartości lub zidentyfikowanie nowych zdarzeń o innych atrybutach. W wyniku zastosowania przekształcenia *g* do wszystkich zidentyfikowanych zdarzeń i danych wzbogacających otrzymujemy nowy zbiór zdarzeń, który jest poddawany dalszej analizie. W pierwszym przypadku, tj. wzbogacenie skutkujące modyfikacją wartości aktualnych

atrybutów zdarzeń i ewentualnie zwiększeniem zestawu wartości jakie mogą przyjmować atrybuty, przekształcenie *g* przyjmuje następującą postać

(5) $g_i(z,W)\colon Z \times W \to Z_i^*$.

Nowy, wzbogacony zbiór zdarzeń $Z^* = Z_1^* \times Z_2^* \times \ldots \times Z_N^*$, $z^* = (z_1^*, \ldots, z_N^*)$ spełnia warunek $\overline{Z^*} \geq \overline{Z}$.

W drugim przypadku, gdy informacje wzbogacające zawierają dane innego typu, które np. nie dotyczą bezpośrednio ataków sieciowych, w wyniku fuzji danych otrzymujemy zbiór zdarzeń Z^{**}. Lista zdarzeń jest rozszerzana o nowe zdarzenia, które mogą być opisywane przez M nowych, nie rozważanych w zbiorze Z atrybutów. Zwiększa się nie tylko wymiar zbioru Z, ale też liczność elementów krotki opisującej zdarzenie bezpieczeństwa. Elementy wzbogaconego zbioru zdarzeń Z^{**} przyjmują następującą postać $z^{**} = \left(z_1^{**}, \ldots, z_{N,}^{**} z_{N+1}^{**}, \ldots, z_{N+M}^{**}\right)$.

Korelacja zdarzeń bezpieczeństwa

Celem jest wyselekcjonowanie ze zbioru zarejestrowanych incydentów bezpieczeństwa K powiązanych (skorelowanych) zdarzeń, tzn. takich, których wartości rozważanych atrybutów są podobne, a w szczególności takie same. Podstawowym wymaganiem jest zdefiniowanie miary podobieństwa (ang. *similarity measure*). Jest to funkcja, która dla dwóch porównywanych obiektów zwraca wartość liczbową określającą ich podobieństwo. Miara podobieństwa najczęściej jest metryką na zbiorze porównywanych obiektów, może być nazywana funkcją odległości lub po prostu odległością.

Definicja 8: Metryką w dowolnym niepustym zbiorze X nazywa się funkcję $d\colon X \times X \to [0, +\infty)$, która dla dowolnych elementów *a*, *b*, *c* tego zbioru spełnia warunki:

1. $d(a,b) = 0 \Leftrightarrow a = b$ (identyczność nierozróżnialnych),
2. $d(a,b) = d(b,a)$ (symetria),
3. $d(a,b) \leq d(a,c) + d(c,b)$ (nierówność trójkąta).

W praktyce miary odległości obiektów takich jak zdarzenia są konstruowane z miar określonych dla poszczególnych atrybutów. Konstrukcja zazwyczaj oparta jest na prostym schemacie wzorowanym na metrykach pierwszego rzędu, najczęściej na metryce miejskiej, czyli dla zdarzeń $z^l, z^k \in Z$ $d_m(z^l, z^k) = \sum_{i=1}^{N} d_i\left(z_i^l, z_i^k\right)$, zazwyczaj ważonej, tzn.

(6) $d_m(z^l, z^k) = \sum_{i=1}^{N} \propto_i d_i\left(z_i^l, z_i^k\right)$,

zwykle $\sum_i \propto_i = 1$, rzadziej na metryce Czebyszewa, czyli

(7) $d_\infty(z^l, z^k) = \max_{i=1,\ldots,N} d_i(z_i^l, z_i^k)$.

Często stosowane są bardziej złożone kombinacje, np. średnia. Odległości dla poszczególnych atrybutów definiowane są zależnie od ich postaci. Dość często są to metryki binarne, oparte na mniej lub bardziej skomplikowanych regułach porównań. Dla wartości numerycznych (czasy trwania zdarzenia, różnie wyrażana intensywność, rozmiary pakietów, itp.) stosowane są proste funkcje – moduł różnicy lub jego prosta funkcja skalująca, np. logarytmiczna lub wykładnicza. Dla wartości ze zbiorów dyskretnych zazwyczaj używana jest prosta, identycznościowa metryka binarna. Dla ciągów znaków stosuje się różne formy odległości edycyjnej, tzn. zliczające minimalną liczbę operacji niezbędnych do przekształcenia jednego ciągu znaków w drugi. Poszczególne warianty odległości edycyjnej różnią się zbiorem dopuszczalnych operacji. W szczególności rozważane są:

- Odległość Hamminga – jedyną dopuszczalną operacją jest wymiana pojedynczego znaku na inny; ponieważ operacja ta nie zmienia długości ciągu. Miara ta ma zastosowanie jedynie dla ciągów o równej długości.
- Najdłuższy wspólny łańcuch (LCS) – dopuszczalne jest jedynie dodanie lub usunięcie pojedynczego znaku.
- Odległość Levenshteina – dopuszczalne operacje to dodanie, usunięcie lub wymiana pojedynczego znaku.
- Odległość Damerau-Levenshteina – dopuszczalne operacje to dodanie, usunięcie lub wymiana pojedynczego znaku na inny oraz zamiana sąsiednich znaków miejscami.

Odległość edycyjna jest powszechnie stosowana, niemniej spotykane są też inne rozwiązania. Na przykład w systemie Nebula [5] wykorzystywane są skróty *spamsum* [6]. Spotykane są także rozwiązania porównujące zbiory skrótów Rabina-Karpa [3]. Zważywszy, że miary podobieństwa różnych atrybutów często znacznie różnią się zakresami przyjmowanych wartości, często przy tworzeniu łącznej miary prawdopodobieństwa obiektów konieczna jest pewna normalizacja. Na przykład odległość edycyjna ciągów znaków to liczba całkowita, która może osiągać wartości bliskie długości porównywanych ciągów znaków, podczas gdy podobieństwo dla wartości z zamkniętego wyliczenia, jak np. protokół, to wartość binarna.

Wykorzystując definicję metryki zdefiniujemy pojęcie korelatora zdarzeń bezpieczeństwa ze zbioru *Z.*

Definicja 9. Korelator zdarzeń bezpieczeństwa**:** *Funkcja* $\theta\colon (z^k, z^l, I) \to \{0,1\}$ *stwierdzająca korelację zdarzenia* z^k *ze zdarzeniem* z^l *względem atrybutów o indeksach ze zbioru* I

(8) $\theta(z^k, z^l, I) = \begin{cases} 1, & d(z^k, z^l) \leq \varepsilon, \\ 0, & w\ przeciwnym\ razie, \end{cases}$

gdzie $d(z^k, z^l)$ to zdefiniowana metryka podobieństwa zdarzeń pierwszego rzędu, np. $d\left(z^k, z^l\right) = \sum_{i \in I} \propto_i d\left(z_i^k, z_i^l\right)$, a ε do założona wartość progowa odległości, w szczególności ε = 0, gdy wymagana jest identyczność wybranych atrybutów zdarzeń. Korelator może być stosowany do zdarzeń $z \in Z$ lub zdarzeń wzbogaconych $z^* \in Z^*$. W szczególnym przypadku, gdy zbiór *I* jest jednoelementowy oceniamy podobieństwo zdarzeń względem jednego atrybutu.

W wyniku zastosowania korelatora do wszystkich par zdarzeń otrzymamy zbiór zdarzeń skorelowanych, czyli takich, których atrybuty przyjmują podobne wartości. W praktyce postać i złożoność korelatora θ zależy od postawionego zadania. Zadanie determinują również dane, które będą korelowane. Przykłady są przedstawione poniżej.

- *Korelacja intruza i źródła* polega na prostej identyfikacji konkretnych intruzów i określeniu jak bardzo inwazyjne są ich działania w chronionej infrastrukturze. Przyjmuje się, że rozważane zdarzenia zostały zakwalifikowane jako incydenty bezpieczeństwa. Ze zbioru incydentów wybiera się te, które mają identyczne (lub podobne) wartości atrybutów charakterystycznych dla źródła zdarzenia. Korelacja intruzów pozwala na dokładne monitorowanie zachowania konkretnego intruza w dłuższym okresie czasu.
- *Korelacja incydentów*. Kojarzone są zdarzenia bezpieczeństwa $z = (z_1, \ldots, z_N) \in Z$, które wystąpiły w określonym czasie. Po wzbogaceniu danych, wybraniu atrybutów względem, których będą badane powiazania zdarzeń korelator (8) wyznacza zbiór zdarzeń skorelowanych, które są poddawane dalszej analizie. Szczególne przypadki korelacji incydentów to:
    - *Korelacja kierunkowa* polega na kojarzeniu ze sobą incydentów i zdarzeń na podstawie kierunku ataku. Jest ona bardzo ważna we wstępnej fazie rozpoznania ataku. Sprawdza się, czy zdarzenia są skierowane z zewnętrznych źródeł do wnętrza organizacji, czy z źródeł wewnątrz organizacji są

kierowane na zewnątrz, czy też w całości zachodzą wewnątrz organizacji.
- o *Korelacja zdarzeń dotyczących zasobów kluczowych* polega na kojarzeniu ze sobą zdarzeń, które dotyczą elementów krytycznej infrastruktury pojedynczej instytucji lub krytycznych infrastruktur wielu instytucji, w których dany element występuje.
- o *Korelacja z danymi historycznymi,* porównanie zagrożeń z zidentyfikowanymi wcześniej jako działania nieuprawnione.

Dalsza analiza skorelowanych incydentów pozwala na wyznaczenie liczby podejrzanych atakujących i/lub systemów, które są celami ataków. Pozyskane w ten sposób informacje pozwalają na podjęcie konkretnych działań.

Algorytm filtracji i korelacji zdarzeń bezpieczeństwa

Zakładając dostępność danych wzbogacających W proponowany jest następujący algorytm filtracji i korelacji zdarzeń bezpieczeństwa. Jest to algorytm trzyetapowy.

1. *Filtracja danych:* wybór atrybutów do filtracji, ustalenie wzorca (3) i zastosowanie filtra (4).
2. *Wzbogacenie danych*: wyznaczenie zbioru zdarzeń Z^* o zmodyfikowanych atrybutach (5) lub fuzja danych (zbiór Z^{**}).
3. *Wyznaczenie zbioru/zbiorów skorelowanych zdarzeń*:

a. ustalenie listy indeksów atrybutów, które będą porównywane (zbiór *I* w formule (8)),

b. wybranie pary zdarzeń ze zbioru Z^* lub Z^{**} i wyznaczenie wartości odległości d dla założonej miary oraz zastosowanie korelatora (8),

c. powtórzenie kroku b dla wszystkich możliwych par z analizowanego zbioru zdarzeń (Z^* lub Z^{**}).

Krok b algorytmu może być wykonany na kilka sposobów, w zależności od wymagań jakie ma realizować moduł korelacji zdarzeń. Rozważane są następujące warianty:

Wariant A: Kojarzone są wszystkie zarejestrowane zdarzenia lub zdarzenia wybrane (każdy z każdym) oraz wyznaczane są zbiory zdarzeń o podobnych (lub identycznych) wartościach atrybutów. Liczność zbiorów zależy od liczby podobnych atrybutów.

Wariant B: Wybierane są grupy atrybutów, względem których wyznaczane są zbiory skorelowanych zdarzeń. Wybór atrybutów może być losowy lub decyduje o nim użytkownik. Efektem końcowym jest zestaw zbiorów zdarzeń o podobnych (lub identycznych) wartościach atrybutów z wybranych zestawów.

Pozyskanie danych ruchowych w sieci

Działania, których celem jest ocena bezpieczeństwa sieci oraz identyfikacja istniejących i potencjalnych zagrożeń poprzedza proces zbierania danych niezbędnych do wykonania analiz. Kluczowymi danymi są dane ruchowe. Pozyskanie ruchu wymaga nagrywania przepływów pakiet po pakiecie (ang. *sniffing*). Niezbędne jest zapisywanie pełnego binarnego zrzutu pakietu. Standardowo tego rodzaju zrzuty ruchu zapisywane są w formacie PCAP (ang. *packet capture*), ale istnieje kilka różnych sposobów ich rejestracji.

- *Monitorowanie systemowe* polega na rejestracji ruchu przez jego monitorowanie na poziomie interfejsu. Istnieją gotowe narzędzia do takich celów, np. *tcpdump* (http://www.tcpdump.org/). Zrzuty na tym poziomie odbywają się najczęściej na poziomie pojedynczych pakietów, które nie są powiązane w przepływy. Wymaga to skomplikowanego przetwarzania zebranych danych.

- *Monitorowanie bocznikowe* polega na kopiowaniu przez urządzenie sieciowe całości ruchu przekazywanego przez łącze na dodatkowy interfejs, na którym prowadzony jest nasłuch. Zaletą tego rozwiązania jest możliwość zebrania ruchu z wielu miejsc w jednym punkcie oraz uniknięcie wprowadzania wykrywalnych opóźnień w przekazywanym ruchu.
- *Monitorowanie na poziomie honeypota* może być stosowane tylko w przypadku zbierania ruchu przez honeypoty - inaczej pułapki [8]. Niektóre rozwiązania honeypotowe zawierają wbudowaną funkcjonalność zbierania przepływów, która często bywa dość rozbudowana. Możliwe jest wiązanie pakietów w pełne przepływy, a nawet powiązanie ruchu ze zdarzeniami zarejestrowanymi na honeypocie, co pozwala z dużą pewnością na wskazanie przepływów rzeczywiście złośliwych.
- *Zbieranie ruchu na poziomie IDS* wykorzystuje możliwości rejestracji ruchu dostępne w rozwiązaniach IDS (*Intrusion Detection System*). Zwykle zapewnione jest łączenie w całość wielopakietowych przepływów, a niezaprzeczalną zaletą rozwiązania jest to, że zbierane przepływy mogą od razu być dopasowywane do już istniejących, dowolnie skomplikowanych reguł. Daje to możliwość odmiennego traktowania przepływów, które są rozpoznawane przez znane sygnatury i nie wymagają ponownej analizy.

Najwygodniejszym z praktycznego punktu widzenia, choć jednocześnie najtrudniejszym, sposobem rejestracji ruchu jest wykorzystanie systemu IDS. W zastosowaniach badawczych zdecydowanie dominującym rozwiązaniem tego typu jest Snort [9]. Jest to narzędzie o otwartych źródłach, dalece rozszerzalne i elastyczne, którego język opisu reguł jest praktycznie standardem. Możliwość stosowania wtyczek pozwala na bardziej złożoną analizę pakietów i przepływów, niż w przypadku języka reguł. Od niedawna jednak wybór otwartego, darmowego rozwiązania do celów badawczych nie jest w pełni oczywisty. Suricata (https://suricata-ids.org/) jest kompatybilna ze Snortem. Podobnie jak Snort, Suricata jest systemem modularnym, o otwartych źródłach, łatwym do dostosowania. Znacznie bardziej zaawansowana wielowątkowość pozwala liczyć na większą wydajność na nowoczesnym sprzęcie i zdolność do wykorzystywania bardziej złożonych analiz. Dzięki zaawansowanej bibliotece HTP, odpowiadającej za normalizację i parsowanie protokołu HTTP, Suricata szczególnie dobrze radzi sobie z ruchem tego typu (WWW, serwisy internetowe, itp.). Obecnie trudno wskazać jednoznacznie lepsze rozwiązanie. Za Snortem przemawia jego dojrzałość i doświadczenie twórców. Suricata jest projektem młodszym i godnym uwagi.

Selekcja zbioru podejrzanych przepływów - filtracja

Pierwszym krokiem przy jakimkolwiek przetwarzaniu danych o zagrożeniach jest wyodrębnienie zbioru przepływów uważanych za podejrzane oraz zbioru ruchu normalnego, najczęściej nazywanego zbiorem normalnym lub zbiorem niezłośliwym. Do tego celu wykorzystywane są różnego rodzaju filtry pozwalające na klasyfikację przepływów. Automatyczne systemy nie mają zwykle żadnej możliwości realnej oceny złośliwego charakteru rejestrowanego przepływu. Muszą jednak klasyfikować zbierane przepływy jako złośliwe lub nie. Wprowadzenie do nich jednoznacznych reguł nie ma sensu. Stosowane są zatem heurystyki, najczęściej wykorzystujące znane charakterystyki dotychczas zarejestrowanych ataków, takie jak:

- stałość portów, co najmniej docelowego,
- występowanie skanowań, tzn. łączenie się tego samego nadawcy z wieloma odbiorcami,
- wykładniczy wzrost liczby przepływów na odpowiednim porcie, jak i liczby nadawców.

Istnieje też możliwość wykorzystania szybkich metod klasyfikacji z wykorzystaniem wiedzy pozyskanej z zewnętrznych źródeł, np. poprzez uczenie maszynowe [10]. Popularne techniki to klasyfikator bayesowski, metoda *k*-sąsiadów, czy maszyna wektorów podpierających [4,10,11]. Wykorzystują one zbiór normalnego ruchu w charakterze punktu odniesienia. Posiadanie takiego zbioru umożliwia odrzucanie błędnych identyfikacji podejrzanych danych. Główną słabością rozwiązań tworzących ruch normalny równolegle ze złośliwym jest ich podatność na atak zwany *normal pool poisoning*. W takim ataku napastnik wysyła dużą ilość legalnego ruchu, który w większości wykorzystywanych w klasyfikatorach heurystyk nie wzbudzi podejrzeń, przy czym ruch ten celowo zawiera fragmenty przepływu typowe dla nowego ataku. Skuteczny atak nasyca zbiór normalny przepływami zawierającymi podejrzane fragmenty, przez co utrudnia wykrycie danych podejrzanych (np. z wykorzystaniem sygnatur ataku [3,5,7]). Z tego względu zalecane jest wykorzystywanie w roli zbioru normalnego starszych próbek ruchu, które w efekcie nie powinny jeszcze zawierać żadnych śladów ewentualnej, rozpoczynającej się właśnie epidemii. Dobrym rozwiązaniem są zbiory kilkumiesięczne – w tak krótkim czasie nie dojdzie zwykle do dużych zmian w popularności protokołów, dane można uznać za aktualne. Dodatkową korzyścią jest dostępność i jakość takich zbiorów. Odpowiednie zbiory przepływów można pobrać z publicznych źródeł, można też wytworzyć je na własne potrzeby monitorując ruch produkcyjny.

Selekcja zbioru podejrzanych przepływów - honeypot

Obecnie dość powszechne jest wykorzystanie ruchu zbieranego przez systemy honeypot [8]. Są to systemy, które emulują rzeczywiste usługi i rejestrują swoją interakcję z napastnikiem. Ich przeznaczeniem jest bycie atakowanym. Przechodzący przez nie ruch jest z definicji w całości podejrzany – decyduje sam fakt skierowania go na nieużywany produkcyjnie adres IP. Niestety jakość takiego zbioru podejrzanego jest w praktyce daleka od doskonałości. Pewna część ruchu rejestrowanego przez honeypoty to w rzeczywistości szum: poprawne, niezłośliwe próby połączeń wynikające z różnego rodzaju błędów w konfiguracjach, albo odbicia, czyli prawidłowe pakiety wysyłane przez ofiarę ataku (zwykle DDoS) w odpowiedzi na złośliwe pakiety ze sfałszowanym IP źródłowym. W tym przypadku należy więc również traktować zbiór jako zaszumiony. Ponadto ruch o złośliwych zamiarach nie musi być próbą ataku. Znaczna jego część to różnego rodzaju próby skanowań. W praktyce to ostatnie zastrzeżenie ma ograniczone znaczenie, gdyż skanowania są zwykle podobnie niepożądane, jak same ataki.

Korelacja manualna a automatyczna

Filtracja i kojarzenie ze sobą dynamicznie pojawiających się danych o zagrożeniach w sieci są w większości instytucji realizowane w sposób manualny. Administratorzy systemów dopasowują np. znane sygnatury ataku ze znanymi podatnościami systemu docelowego aby oszacować prawdopodobieństwo sukcesu lub porażki takiego ataku. Ze względu na konieczność przeanalizowania olbrzymiej liczby kombinacji jest to zadanie bardzo trudne. Stąd filtracja i korelacja manualna są obecnie zastępowane przez specjalizowane, automatyczne systemy kojarzenia danych [2,3,5,7,12,13,14]. Zbierają one i konsolidują wszystkie informacje w jednorodnych bazach danych. Następnie, zdarzenia te są agregowane, filtrowane i korelowane. Rezultatem jest skonsolidowany obraz warunków bezpieczeństwa i zagrożenia dla chronionej infrastruktury teleinformatycznej. Automatyczna filtracja i korelacja pozwalają zredukować szum informacyjny i skoncentrować uwagę na krytycznych naruszeniach bezpieczeństwa, a tym samym podnieść skuteczność ochrony cybernetycznej dzięki m.in. możliwości przyspieszenia procesu wykrywania ataków lub nieuprawnionych działań w sieci.

Różne metody przetwarzania danych mogą być wykorzystane do automatycznej filtracji i korelacji zdarzeń bezpieczeństwa. W niniejszej pracy skoncentrujemy się na technikach grupowania zdarzeń.

Grupowanie obiektów w klastry – przegląd metod

Jednym z możliwych podejść do problemu filtracji i korelacji rozumianej jako wyszukiwanie podzbiorów podobnych obiektów są automatyczne metody grupowania (klasteryzacji) [1,15]. Zasadniczo wynikiem grupowania jest podział zbioru na rozłączne podzbiory charakteryzujące się wzajemnym podobieństwem należących do nich obiektów – jest to zatem forma automatycznej klasyfikacji, przy czym zazwyczaj prowadzonej bez uprzedniej znajomości klas, a często nawet ich liczby, jak zakładają to popularne metody klasyfikacji wykorzystane w pracach [4,11]. W zastosowaniu do korelacji wymaganie na rozłączność uzyskiwanych podzbiorów nie występuje, co w niektórych przypadkach może zostać uwzględnione przez prostą modyfikację algorytmu.

Metody automatycznego grupowania są skutecznym podejściem przy poszukiwaniu szerokich klas podobnych obiektów w zbiorze w celu identyfikacji ich wspólnych cech. W rozważanym zastosowaniu obiektami są różnego rodzaju zdarzenia bezpieczeństwa opisane definicją 1.

Istnieje wiele metod grupowania, o różnych cechach, a więc i o różnej wartości praktycznej w poszczególnych zastosowaniach. Przede wszystkim należy wspomnieć o podziale na metody grupowania miękkiego i twardego, różniące się definicją przynależności do klastra. W metodach grupowania twardego przynależność jest określona binarnie – element należy do klastra lub nie. W metodach grupowania miękkiego możliwa jest przynależność niepewna, lub w pewien sposób stopniowana, a więc powstające klastry są zbiorami rozmytymi lub przybliżonymi. W systemach bezpieczeństwa grupowanie miękkie ma zwykle ograniczoną użyteczność, toteż skupimy się na grupowaniu twardym. Istotną cechą metod jest również ich zupełność, czyli to, czy dopuszczają występowanie obiektów niezgrupowanych, najczęściej określanych jako szum (ang. *noise*) lub obiekty odstające (ang. *outliers*). Ponieważ w cyberbezpieczeństwie duża część zbieranych danych jest zaszumiona, większą wartość praktyczną mają metody, które nie wymagają ujęcia wszystkich obiektów w klastry. Niemniej nie dyskwalifikuje to metod zupełnych – ich użyteczność zależy od konkretnego przypadku. Najważniejsze klasy algorytmów grupowania znajdujących zastosowanie praktyczne to:

- metody połączeniowe,
- metody centroidowe,
- metody gęstościowe,
- metody rozkładowe.

Podstawowym wymaganiem przy stosowaniu wszelkich metod automatycznego grupowania jest oczywiście prawidłowe zdefiniowanie miary podobieństwa (definicja 8). W kolejnych podrozdziałach zaprezentowano w zarysie rodziny metod nadających się do wykorzystania w korelacji danych dotyczących cyberbezpieczeństwa.

Metody połączeniowe

W metodach połączeniowych zakłada się, że jeśli dwa obiekty są podobne, powinny należeć do jednej grupy. Liczba klastrów może być zakładana z góry, może też wynikać z założonych wymagań na maksymalną odległość

obiektów w jednym klastrze. Przykładem takich metod są metody hierarchiczne i grafowe.

Metody hierarchiczne. W metodach hierarchicznych na podstawie odległości między parami węzłów są iteracyjnie konstruowane zbiory klastrów. W podejściu aglomeracyjnym obliczenia rozpoczynają się od zbioru singletonów, a klastry tworzone są przez łączenie mniejszych, skupiających obiekty charakteryzujące się największym wzajemnym podobieństwem. W podejściu deglomeracyjnym kierunek działania jest odwrotny – obliczenia rozpoczynają się od jednego, dużego klastra, a w każdym kroku klaster, w którym odległości między elementami są największe, jest dzielony na mniejsze. W obu rozwiązaniach wyniki mogą być przedstawione jako dendrogram. Jakość wyników w dużym stopniu zależy od przyjętego punktu odcięcia, czyli wymaganej maksymalnej odległości między elementami należącymi do tego samego klastra. Metody deglomeracyjne są rzadko używane, gdyż ich złożoność jest wykładnicza i dla dużych zbiorów danych wydajność jest niewystarczająca. Metody aglomeracyjne są pod tym względem znacznie bardziej użyteczne praktycznie.

Istnieje wiele metod z tej rodziny, o różnej charakterystyce wydajności i jakości uzyskiwanych wyników. Należą do nich m.in. metody tworzące drzewa binarne. Ich dużą wadą jest jednak stosunkowo niska jakość uzyskiwanego grupowania – narzucona odgórnie liczność tworzonych zbiorów często skutkuje występowaniem podzbiorów grupujących elementy o niskim podobieństwie, które w rzeczywistości powinny być członkami sąsiednich grup. W niektórych zastosowaniach używane bywają też metody zakładające stały punkt odcięcia, czyli wymuszające jednolity rozmiar klastra – zwiększają one w oczywisty sposób uciążliwość tego problemu.

Metody grafowe. Narzędziem do tworzenia klastrów w tej grupie metod jest graf odległości. Ideowo algorytmy tej rodziny można przedstawić jako różne rozwiązania problemu przycinania grafu, które usuwają z niego krawędzie o największych długościach, co prowadzi do rozpadu na podgrafy, które interpretowane są jako klastry. Warto zwrócić uwagę, że w metodach tej klasy istnienie jednego węzła, którego odległość od jednego z elementów dwóch różnych podgrafów wystarcza do połączenia ich w klaster skutkuje powstawaniem dużych, rozciągniętych klastrów, których odległe elementy mogą znacznie się różnić. Zależnie od zastosowania może to być poważną wadą, może jednak także ujawniać nieoczywiste zależności. W przypadku zbiorów silnie, losowo zaszumionych, prowadzi to jednak do nadmiernego rozrostu klastrów w wyniku występowania przypadkowych „łączników".

Konstrukcja i przycinanie pełnego grafu odległości dla dużych zbiorów wejściowych nie jest oczywiście efektywną implementacją. Najczęściej klastry budowane są przyrostowo – każdy kolejny element porównywany jest ze wszystkimi już przetworzonymi (co oznacza złożoność kwadratową) i krawędzie tworzone są jedynie jeśli odległość jest mniejsza od założonego progu. Dołączenie nowego obiektu prowadzi do utworzenia nowego klastra, kiedy łączy się on tylko z obiektami „samotnymi", nie należącymi do klastrów. Połączenie z obiektami należącymi do jednego klastra powiększa ten klaster o nowy obiekt, jeśli natomiast podobne są obiekty należące do więcej, niż jednego klastra, dochodzi do scalenia sąsiednich klastrów przez zamknięcie luki między nimi. Elementy, dla których nie utworzono żadnych krawędzi, umieszczane są w osobnym zbiorze elementów odstających i mogą wejść w skład przyszłych klastrów, kiedy pojawią się inne, podobne do nich.

Algorytmy grafowe w wersjach przyrostowych są szczególnie dogodne jako rozwiązanie problemu grupowania ciągłego, tzn. utrzymywania wiedzy o grupach występujących aktualnie w stałym strumieniu danych, bez analizy całego zbioru. Grupowanie ciągłe jest bardzo użytecznym narzędziem korelacji danych w czasie rzeczywistym, pozwalającym wskazać podobne zdarzenia w ostatnim okresie. W tym zastosowaniu liczność zbioru pogrupowanych elementów utrzymywana jest na względnie stałym poziomie, co pozwala uniknąć problemu kwadratowej złożoności. Konieczne jest stosowanie odpowiednich metod usuwania starych obiektów. Nie jest to zadanie bardzo trudne, ale wymaga przemyślanego algorytmu – mechaniczne usuwanie wszystkich obiektów starszych od pewnej wartości progowej może prowadzić do rozpadu dobrych w istocie klastrów. Zjawisko to jest trudne do uniknięcia, chyba że możliwe jest sformułowanie innego niż odległość kryterium oceny jakości istniejących klastrów.

Metody centroidowe

Grupowanie centroidowe to rodzina metod, w których grupę definiuje odległość od obiektu (rzeczywistego, lub sztucznego) stanowiącego jej centrum. Liczba klastrów zakładana jest z góry. Powszechnie znaną techniką jest algorytm k-średnich i jego warianty. Zasadniczo wszystkie metody z tej rodziny opierają się na iteracyjnym ulepszaniu zbioru elementów centralnych („rdzeni") w celu minimalizacji zróżnicowania (najczęściej wyrażanego wariancją) elementów klastrów, które wynikają z wyboru rdzeni. Ogólny schemat postępowania jest więc następujący:

1. Wyznacz zbiór *n* rdzeni – każdy rdzeń odpowiada jednemu klastrowi.
2. Przypisz każdy element do klastra, którego rdzeń jest najbardziej do niego podobny.
3. Zbadaj zróżnicowanie w ramach klastrów, jeśli jest wystarczająco małe lub jeśli poprawa względem poprzedniej iteracji jest dostatecznie mała, STOP.
4. Wyznacz centroid każdego klastra (nowy rdzeń).
5. Wróć do kroku 2.

Algorytmy są stosunkowo proste i efektywne, jednak możliwości ich zastosowania do korelacji zdarzeń w cyberbezpieczeństwie są dość ograniczone. Przyczyną są dwie istotne wady rozwiązań tej klasy. Po pierwsze, liczba klastrów jest z góry założona – najczęściej taka informacja nie jest dostępna. Po drugie, jakość wyników często istotnie zależy od początkowego wyboru rdzeni.

Metody gęstościowe

Algorytmy gęstościowe to rodzina metod ogólnego zastosowania, które tworzą grupy odpowiadające naturalnym skupieniom danych, czyli ciągłym obszarom o zwiększonej gęstości. Podobnie jak w metodach centroidowych, wiele metod tej rodziny zakłada istnienie „rdzenia", wokół którego skupione są pozostałe elementy, jednak rdzeń jest wybierany dla znalezionego skupienia, a nie odwrotnie, toteż liczba klastrów nie jest ustalana z góry. Popularnym reprezentantem tej grupy jest algorytm DBSCAN [15], często wykorzystywany ze względu na dobrą jakość uzyskiwanych wyników i wystarczającą wydajność. Klastry tworzone algorytmem DBSCAN posiadają wyróżnione rdzenie – wybrane obiekty podobne do wystarczająco wielu innych. Klaster jest tworzony z obiektów, których odległość od jego rdzenia jest mniejsza od pewnej wartości progowej. Stosowany jest prosty algorytm zachłanny, w którym nowe klastry tworzone są natychmiast, kiedy uda się zebrać odpowiednią ilość podobnych obiektów, które nie trafiły do istniejących już klastrów. Dzięki temu jest to algorytm dość szybki i skuteczny, jednak jakość tworzonych klastrów nie zawsze jest zadowalająca. Podobieństwo do opisanych wcześniej metod centroidowych nie jest przypadkowe, algorytm jest

bardzo podobny. Kluczową różnicą jest to, że ani liczba klastrów, ani początkowy zbiór rdzeni nie są zadawane z góry, a wynikają z analizy danych. Istotną cechą algorytmu DBSCAN w niektórych zastosowaniach jest możliwość działania przyrostowego z zachowaniem trwałości klastrów, co pozwala wiązać z nimi użyteczne metadane. Nie ma w tym przypadku potrzeby ponownej klasteryzacji całego zbioru obiektów – obiekty już pogrupowane pozostają w istniejących klastrach, zaś nowe dane zostają do nich dopisane, sklasyfikowane jako szum, albo powiązane z podobnymi obiektami wcześniej uznanymi za szum. Powstanie nowego klastra jest zatem istotną informacją i oznacza pojawienie się całej grupy podobnych do siebie obiektów, których nie można dopasować do istniejących klastrów.

Metody rozkładowe

W metodach rozkładowych przyjmuje się, że struktura grup jest z góry założona przez przyjęcie, że obiekty należą z natury do grup, ale są rozrzucone z pewnym rozkładem. Na przykład założenie rozkładu normalnego wymusza grupy elipsoidalne. Tego typu metody są bardzo użyteczne w analizie danych będących wynikiem silnie zaszumionych fizycznych pomiarów, czy też przy grupowaniu obiektów, których własności są losowo zaburzone, a zatem wtedy, gdy zaburzenia dają się w uzasadniony sposób modelować losowo. W zastosowaniu w systemach ochrony cybernetycznej najczęściej nie jest to możliwe – zróżnicowanie danych wynika często z celowego zaciemniania lub z innych zjawisk nie poddających się tak prostemu modelowaniu, toteż użyteczność metod z tej rodziny jest bardzo ograniczona.

Odkrywanie asocjacji zdarzeń bezpieczeństwa

Wykorzystując zbiory zdarzeń pogrupowanych względem wartości atrybutów oraz dysponując dodatkowymi informacjami poza tymi, które były uwzględnione w procesie grupowania możemy w łatwy sposób odkryć interesujące nas zależności między zdarzeniami bezpieczeństwa oraz obserwacjami dotyczącymi stanu sieci i chronionych systemów – wyznaczyć zbiór reguł asocjacyjnych [16]. Reguły asocjacyjne przedstawiane są w postaci implikacji. Każda reguła składa się z dwóch zbiorów atrybutów: zbioru wartości warunkujących (poprzednika) oraz zbioru wartości warunkowanych (następnika). Reguła z poprzednikiem X i następnikiem Y jest zapisywana w następujący sposób: $X \Longrightarrow Y$ a jej interpretacja brzmi: w przypadku wystąpienia wszystkich wartości ze zbioru X często występują również wszystkie wartości ze zbioru Y". Reguły asocjacyjne przypominają reguły decyzyjne, przy czym w ich przypadku decyzja nie jest z góry określona. W przypadku danych zbieranych przez systemy monitorowania bezpieczeństwa sieci będą to ilościowe reguły wielowymiarowe (dane reprezentują różne dziedziny wartości) i wielopoziomowe (dane charakteryzują się różnym poziomem abstrakcji). Wyznaczone reguły asocjacyjne kojarząc nieoczywiste zależności między wartościami atrybutów zdarzeń wzbogacają wiedzę o sytuacji w sieci i umożliwiają wykrycie wzorców charakteryzujących ataki. Wpływają w ten sposób na przyspieszenie wykrycia i identyfikacji ataku oraz wskazanie grup potencjalnych ofiar. Stanowią również wsparcie przy szacowaniu ryzyka rozprzestrzenienia się zagrożeń [17,18].

Podsumowanie

Praca jest poświęcona technikom wspierającym ocenę bezpieczeństwa sieci teleinformatycznych i identyfikację zagrożeń. Przedstawiono ogólne podejście do problemu filtracji i korelacji zdarzeń bezpieczeństwa w sieciach zakładające ujednoliconą reprezentację zdarzeń przez zdefiniowaną listę charakteryzujących je atrybutów. Wskazano rodzaje możliwych danych opisujących zdarzenia identyfikowane w sieciach oraz dokonano przeglądu technik, grupowania które mogą znaleźć zastosowanie w zadaniach filtracji i korelacji zdarzeń. Prezentując wybrane metody szczególną uwagę zwrócono na ich potencjalną skuteczność w zastosowaniach ochrony przed cyberzagrożeniami i wydajność.

Automatyczne grupowanie jest uniwersalnym narzędziem, możliwym do wykorzystania w różny sposób w korelowaniu zdarzeń bezpieczeństwa. Najbardziej obiecujące jest grupowanie ciągłe – dla przetwarzanych w systemach ochrony sieci strumieni danych możliwe jest prowadzenie ciągłej analizy, dzięki czemu dla każdego nowego obiektu (np. zdarzenia) w systemie są od razu identyfikowane powiązania z niedawnymi podobnymi obiektami. W tym przypadku ważny jest dobry wybór i parametryzacja funkcji odległości, gdyż każda jej zmiana narusza ciągłość grupowania. Taka analiza jest też atrakcyjna jako mechanizm priorytetyzacji dla analityków. Nowe zdarzenie może być dobrze dopasowane do istniejącego klastra, który został już przebadany i wiadomo, jakim zjawiskom odpowiada – w takim przypadku priorytet obsługi zdarzenia jest powiązany z wagą przypisaną do tego klastra podczas analizy. Zdarzenia kwalifikowane jako szum, niepasujące do klastrów, mogą być interesujące lub wręcz przeciwnie, zależnie od specyfiki danego strumienia danych. Najciekawszym zaś wariantem jest powstanie nowego klastra – sugeruje to, że pojawiła się nowa klasa zdarzeń, wymagająca pilnej analizy.

Podsumowując, należy podkreślić, że wyniki filtracji i korelacji mogą istotnie wspierać ocenę szacowania ryzyka rozprzestrzeniania się zagrożeń w chronionym systemie.

Praca wykonana w ramach projektu CYBERSECIDENT/369195/I/NCBR/2017, współfinansowanego przez Narodowe Centrum Badań i Rozwoju w ramach programu CyberSecIdent.

***Autorzy**: Mgr. inż. Paweł Szynkiewicz, Naukowa i Akademicka Sieć Komputerowa (NASK), ul. Kolska 12, 01-045 Warszawa, E-mail: pawelsz@nask.pl.*
Dr inż. Adam Kozakiewicz, Politechnika Warszawska, Instytut Automatyki i Informatyki Stosowanej, ul. Nowowiejska 15/19, 00-665 Warszawa, E-mail: akozakie@elka.pw.edu.pl.

LITERATURA

[1] Surma, J, Business Intelligence. Systemy wspomagania decyzji biznesowych, PWN, 2009
[2] Salour Li, M., Su X., A Survey of Internet Worm Detection and Containment, *IEEE Communications Surveys & Tutorials*, 10(2008), No. 1, 20-35
[3] Szynkiewicz P., Kozakiewicz A., Design and Evaluation of a System for Network Threat Signatures Generation, *Journal of Computational Science* 22 (2017), 187-197
[4] Kruczkowski M., Kozakiewicz A., Niewiadomska-Szynkiewicz, E., FP-tree and SVM for Malicious Web Campaign Detection, *Proc. of 7th Asian Conference, ACIIDS, Series: Lecture Notes in Computer Science*, 2015, No. 9012, 193–201
[5] Werner, T., Fuchs C., Gerhards-Padilla E., Martini P., Nebula – Generating Syntactical Network Intrusion Signatures, *4th International Conference on Malicious and Unwanted Software (MALWARE)*, 2009, 31-38
[6] Roussev V., Richard III G. G., Marziale L., Multiresolution Similarity Hashing, *Digital Investigation*, 4(2007), 105-113
[7] Newsome J., Karp B., Song D., Polygraph: Automatically Generating Signatures for Polymorphic Worms, *proc. of IEEE Symposium on Security and Privacy (S&P'05)*, 2005, 226 – 241
[8] Bandakkanavar R. Honeypot, *Technical paper*, Krazytech, 2017

[9] Roesch M., Snort – Lightweight Intrusion Detection for Networks, *Proc. of the 13th Conference on Systems Administration*, 1999, 229–238
[10] Vapnik V. N., The Nature of Statistical Learning Theory, Springer-Verlag, 1995
[11] Kruczkowski M., Niewiadomska-Szynkiewicz E., *Support vector machine for malware analysis and classification*, *Proc.of IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology*, 2(2014), 280-283
[12] Kreibich C., Crowcroft J., Honeycomb – Creating Intrusion Detection Signatures Using Honeypots, *ACM SIGCOMM Computer Communication Review,* 34(2004), 51-56
[13] Sounak P., Mishra B.K., Survey of Polimorphic Worm Signatures, *Inter. Journal of u- and e-Service, Science and Technology*, 7(2014), No. 3, 129-150
[14] Kozakiewicz A., Pałka T., Kijewski P., Wykrywanie adresów serwerów c&c botnetów w danych ze środowisk sandbox, *Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne*, 2015, No. 8-9, 1223-1231
[15] Ester M., Kriegel H.-P., Sander J., Xu X., A density-based algorithm for discovering clusters in large spatial databases with noise, *Second International Conference on Knowledge Discovery and Data Mining (KDD-96)*, 1996, 226-231
[16] Agrawal C., Srikant R., Fast Algorithms for Mining Association on Rules in Large Databases, Proc. of the 20-th International Conference on Very Large Data Bases, 1994, 487-499
[17] Jones A., Ashenden D., Risk Management for Computer Security, Elsevier, 2005
[18] El Fray I, Pejaś J., Hyla T., Nowe podejście w zarządzaniu ryzykiem dla systemów informacyjnych organizacji, Rozproszona kontrola dostępu w praktyce, *Przegląd Elektrotechniczny*, 2015, No 11, 186-190