%this file explains the meaning of columns for the competition data files: cybersecurity_training.csv and cybersecurity_test.csv

alert_ids - an identifier of the alert, values from this column should be used to match the corresponding records from the event_logs files

client_code - encrypted identifiers of clients for which alerts were generated

notified - a binary column indicating whether a client was notified about the alert (the target column in this task); this column is missing in the test data!

categoryname - a category name of the alert that corresponds to its severity

ip - an encrypted IP address corresponding to the alert; the first two octets were encrypted for public addresses, and for addresses from private networks, the second and third one; each octet was encrypted independently (the same code on different octets corresponds to different values) but values of the same octet are consistent, e.g. addresses AB.CD.1.1 and AB.CD.1.10 come from the same sub-network

ipcategory_name - a category of the corresponding IP, created based on https://en.wikipedia.org/wiki/Reserved_IP_addresses

ipcategory_scope - a domain of the corresponding IP category, created based on https://en.wikipedia.org/wiki/Reserved_IP_addresses

parent_category - a parent category of the IP category name

grandparent_category - a grandparent category of the IP category name

overallseverity - an estimation of the alert severity generated by the system rules

timestamp_dist - a time period (in seconds) between the first and the last log event corresponding to the alert

start_hour - an hour of the first log event that is assumed to be the first of the events corresponding to the alert

start_minute - a minute of the first log event that is assumed to be the first of the events corresponding to the alert

start_second - a second of the first log event that is assumed to be the first of the events corresponding to the alert

weekday - a day of week of the first log event that is assumed to be the first of the events corresponding to the alert

correlatedcount - a number of records denoted by the system in an auxiliary table with localized alerts, that corresponds to the alert

n1 - a binary field indicating whether a standard system query1 returned value > 0 (it can be understood as a result of a standard analytical query)

n2 - a binary field indicating whether a standard system query2 returned value > 0 (it can be understood as a result of a standard analytical query)

n3 - a binary field indicating whether a standard system query3 returned value > 0 (it can be understood as a result of a standard analytical query)

n4 - a binary field indicating whether a standard system query4 returned value > 0 (it can be understood as a result of a standard analytical query)

n5 - a binary field indicating whether a standard system query5 returned value > 0 (it can be understood as a result of a standard analytical query)

n6 - a binary field indicating whether a standard system query6 returned value > 0 (it can be understood as a result of a standard analytical query)

n7 - a binary field indicating whether a standard system query7 returned value > 0 (it can be understood as a result of a standard analytical query)

n8 - a binary field indicating whether a standard system query8 returned value > 0 (it can be understood as a result of a standard analytical query)

n9 - a binary field indicating whether a standard system query9 returned value > 0 (it can be understood as a result of a standard analytical query)

n10 - a binary field indicating whether a

standard system query10 returned value > 0 (it can be understood as a result of a standard analytical query)
score - a score related to the alert, issued by an autonomous analytical model
srcip_cd - a number of different source IP addresses in an auxiliary table with localized alerts, that corresponds to the alert
dstip_cd - a number of destination IP addresses in an auxiliary table with localized alerts, that corresponds to the alert
srcport_cd - a number of different source ports in an auxiliary table with localized alerts, that corresponds to the alert
dstport_cd - a number of different destination ports in an auxiliary table with localized alerts, that corresponds to the alert
alerttype_cd - a number of triggered alert types, denoted in an auxiliary table with localized alerts
direction_cd - a number of different event directions denoted in an auxiliary table with localized alerts, that corresponds to the alert
eventname_cd - a number of different event names (names of events that are dependent on the hardware) denoted in an auxiliary table with localized alerts, that corresponds to the alert
severity_cd - a number of different severity values associated with individual events denoted in an auxiliary table with localized alerts, that corresponds to the alert
reportingdevice_cd - a number of different reporting devices (devices that register the events) denoted in an auxiliary table with localized alerts, that corresponds to the alert
devicetype_cd - a number of different reporting device types denoted in an auxiliary table with localized alerts, that corresponds to the alert
devicevendor_cd - a number of different reporting device vendors denoted in an auxiliary table with localized alerts, that corresponds to the alert
domain_cd - a number of different domains denoted in an auxiliary table with localized alerts, that corresponds to the alert
protocol_cd - a number of different protocols denoted in an auxiliary table with localized alerts, that corresponds to the alert
username_cd - a number of different usernames denoted in an auxiliary table with localized alerts, that corresponds to the alert
srcipcategory_cd - a number of different source IP categories denoted in an auxiliary table with localized alerts, that corresponds to the alert
dstipcategory_cd - a number of different destination IP categories denoted in an auxiliary table with localized alerts, that corresponds to the alert
isiptrusted - a binary field indicating whether the IP address corresponding to the alert is controlled by the customer
untrustscore - a score based on what is known about the external portion of the communication (network traffic) associated with the alert
flowscore - a behavioral score based on behavioral indicators adjusted for the alert
trustscore - a score based on what is known about the internal portion of the communication (network traffic) associated with the alert
enforcementscore - an adjustment score based on whether or not the activity associated with the alert was mitigated by a security control
dstipcategory_dominate - the most frequent ipcategory_name for the destination addresses denoted in an auxiliary table with localized alerts, that corresponds to the alert
srcipcategory_dominate - the most frequent ipcategory_name for the source addresses denoted in an auxiliary table with localized alerts, that corresponds to the alert
dstportcategory_dominate - the most frequent destination port category denoted in an auxiliary table with localized alerts, that corresponds to the alert
srcportcategory_dominate - the most frequent source port category denoted in an auxiliary table with localized alerts, that corresponds to the alert
thrcnt_month - a number of records from an auxiliary table with threat watch alerts, denoted for the same IP address as the alert, during the previous month
thrcnt_week - a number of records from an auxiliary table with threat watch alerts, denoted for the same IP address as the alert, during the previous week
thrcnt_day - a number of records from an auxiliary table with threat watch alerts, denoted for the same IP address as the alert, during the previous day

```
p6                                                  -       a result of an analytical query p6
for the corresponding alert, on an auxiliary table with threat watch alerts
p9                                                  -       a result of an analytical query p9
for the corresponding alert, on an auxiliary table with threat watch alerts
p5m                                                 -       a result of an analytical query p5m
for the corresponding alert, on an auxiliary table with threat watch alerts
p5w                                                 -       a result of an analytical query p5w
for the corresponding alert, on an auxiliary table with threat watch alerts
p5d                                                 -       a result of an analytical query p5d
for the corresponding alert, on an auxiliary table with threat watch alerts
p8m                                                 -       a result of an analytical query p8m
for the corresponding alert, on an auxiliary table with threat watch alerts
p8w                                                 -       a result of an analytical query p8w
for the corresponding alert, on an auxiliary table with threat watch alerts
p8d                                                 -       a result of an analytical query p8d
for the corresponding alert, on an auxiliary table with threat watch alerts
```