Měsíční přehled bezpečnostních incidentů

WEBFILTR.CZ

This report uses the following parameters and values:

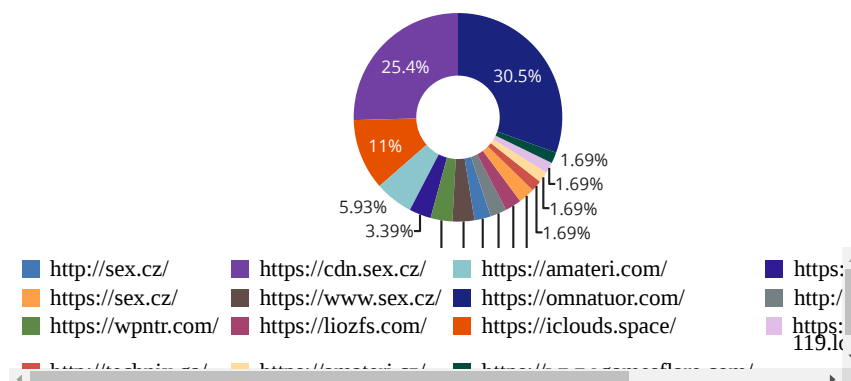| Parameter	Value
$VarFGT_Report_SRCIP$	srcip:172.25.1.43

Blokované kategorie v čase
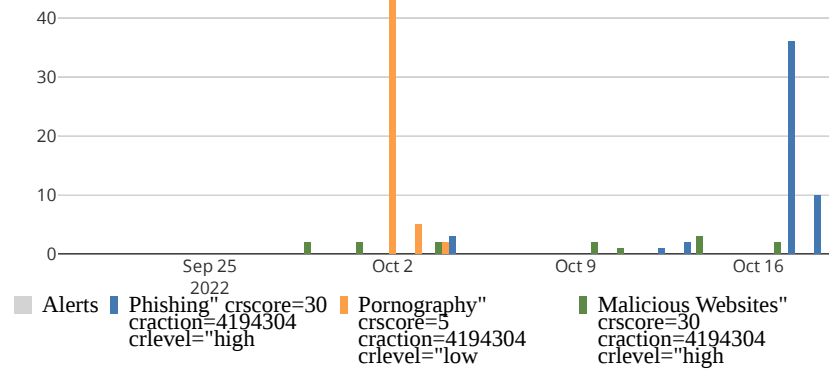
Bar chart aggregating count() by timestamp for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (action:deny OR action:blocked OR action:block)* and was calculated at Wednesday 19 October 2022, 04:30 +0000.

Blokované kategorie / počty

catdesc	count()
Phishing" crscore=30 craction=4194304 crlevel="high	52
Pornography" crscore=5 craction=4194304 crlevel="low	52
Malicious Websites" crscore=30 craction=4194304 crlevel="high	14

Data table aggregating count() by catdesc for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (action:deny OR action:blocked OR action:block)* and was calculated at Wednesday 19 October 2022, 04:30 +0000.

Zablokované URL adresy procentuálně

■ http://sex.cz/	■ https://cdn.sex.cz/	■ https://amateri.com/	■ https:
■ https://sex.cz/	■ https://www.sex.cz/	■ https://omnatuor.com/	■ http:/
■ https://wpntr.com/	■ https://liozfs.com/	■ https://iclouds.space/	■ https: 119.l
■ http://technix.ga/	■ https://amateri.cz/	■ https://www.gamesflare.com/	

Pie chart aggregating count() by url for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (action:deny OR action:blocked OR action:block)* and was calculated at Wednesday 19 October 2022, 04:30 +0000.

Zablokované URL adresy / počty

url	count()
https://omnatuor.com/	36
https://cdn.sex.cz/	30
https://iclouds.space/	13
https://amateri.com/	7
https://candycrushsoda.king.com/	4
https://wpntr.com/	4
https://www.sex.cz/	4
http://sex.cz/	3
http://webfiltr.cz/eicar/eicar.com	3
https://liozfs.com/	3
https://sex.cz/	3
http://technix.ga/	2
https://amateri.cz/	2
https://s-172-105-167-119.lolshot.io/	2
https://www.gamesflare.com/	2

Data table aggregating count() by url for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (action:deny OR action:blocked OR action:block) AND NOT dstcountry:Reserved* and was calculated at Wednesday 19 October 2022, 04:30 +0000.
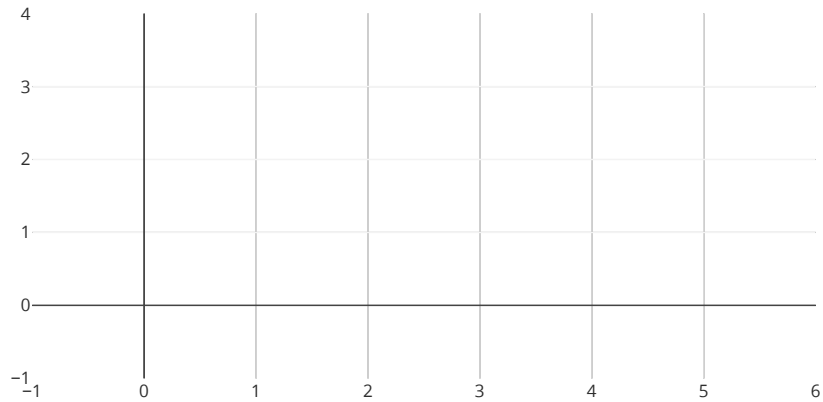
Blokované aplikace procentuálně
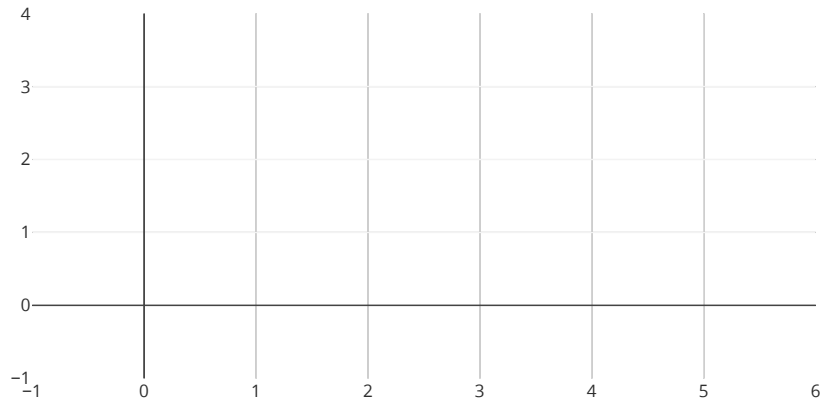
Pie chart aggregating count() by app for messages in stream *Fortigate Application Control Logs = type:utm subtype:app-ctrl* from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (action:deny OR action:blocked OR action:block)* and was calculated at Wednesday 19 October 2022, 04:30 +0000.

Blokované aplikace / počty

| app	count()

Data table aggregating count() by app for messages in stream *Fortigate Application Control Logs = type:utm subtype:app-ctrl* from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (action:deny OR action:blocked OR action:block)* and was calculated at Wednesday 19 October 2022, 04:30 +0000.

Blokované aplikace podle rizikovosti

Pie chart aggregating count() by apprisk for messages in stream *Fortigate Application Control Logs = type:utm subtype:app-ctrl* from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (action:deny OR action:blocked OR action:block)* and was calculated at Wednesday 19 October 2022, 04:30 +0000.

Blokované služby procentuálně
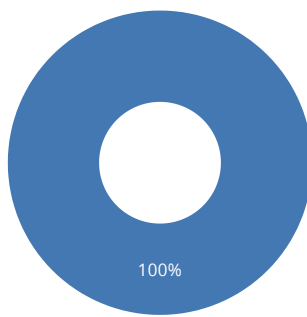

6.72%

93.3%
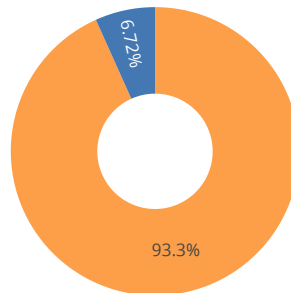
■ HTTP   ■ HTTPS

Pie chart aggregating count() by service for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (action:deny OR action:blocked OR action:block)* and was calculated at Wednesday 19 October 2022, 04:30 +0000.

Blokované služby / počty

service	count()
HTTPS	111
HTTP	8

Data table aggregating count() by service for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (action:deny OR action:blocked OR action:block)* and was calculated at Wednesday 19 October 2022, 04:30 +0000.

Blokované viry procentuálně

■ EICAR_TEST_FILE
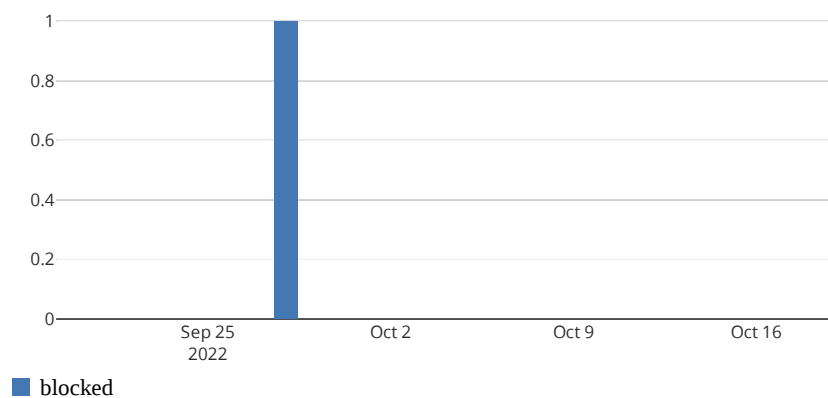
Pie chart aggregating count() by virus for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND subtype:virus* and was calculated at Wednesday 19 October 2022, 04:30 +0000.

Blokované viry a jejich původ / počty

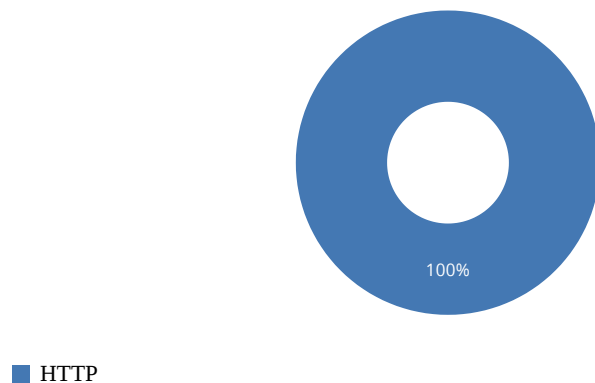| url	count()
http://webfiltr.cz/eicar/eicar.com	1

Data table aggregating count() by url for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND subtype:virus AND action:blocked* and was calculated at Wednesday 19 October 2022, 04:30 +0000.
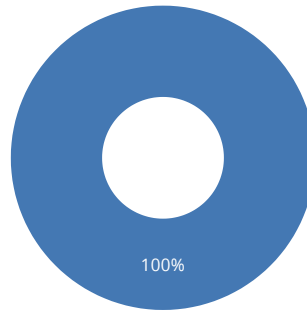
Blokované viry v čase

Bar chart aggregating count() by timestamp for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND subtype:virus AND action:blocked* and was calculated at Wednesday 19 October 2022, 04:30 +0000.

Původ virů procentuálně

Pie chart aggregating count() by service for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND subtype:virus* and was calculated at Wednesday 19 October 2022, 04:30 +0000.

Provedené akce procentuálně

■ blocked

Pie chart aggregating count() by action for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND subtype:virus* and was calculated at Wednesday 19 October 2022, 04:30 +0000.

Trend kritické závažnosti

0

+0 / --

Single number aggregating count(critical) for messages in stream *Fortigate Application Control Logs = type:utm subtype:app-ctrl* from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (action:deny OR action:blocked OR action:block)* and was calculated at Wednesday 19 October 2022, 04:30 +0000.