Měsíční přehled bezpečnostních incidentů

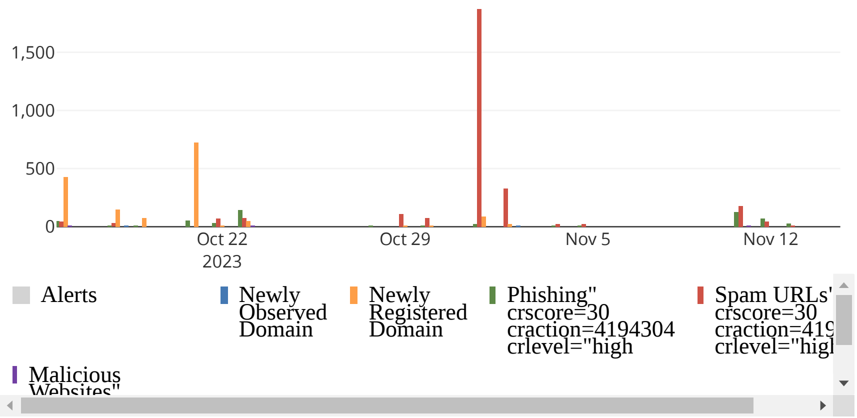
All times are displayed in the time zone UTC.

WEBFILTR.CZ

This report uses the following parameters and values:

Parameter	Value
$VarFGT_Report_SRCIP$	(srcip:172.25.254.42)

1.1 Datum blokace a kategorie bezpečnostního incidentu



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 2023-11-14 15:46:22.

1.2 Počty blokací a kategorie bezpečnostního incidentu

catdesc	count()
Spam URLs" crscore=30 craction=4194304 crlevel="high	2870
Newly Registered Domain	1533
Phishing" crscore=30 craction=4194304 crlevel="high	560
Malicious Websites" crscore=30 craction=4194304 crlevel="high	10
Newly Observed Domain	5

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 2023-11-14 15:46:23.

1.3 Typy blokací a kategorie bezpečnostního incidentu

subtype	count()
webfilter	4978
app-ctrl	17

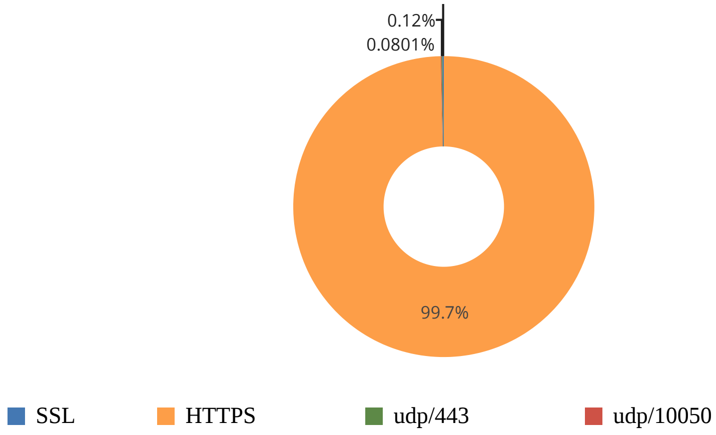
Data table aggregating count() by subtype for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (action:deny OR action:blocked OR action:block)* and was calculated at 2023-11-14 15:46:23.

1.4 Počty blokací a kategorie kritického bezpečnostního incidentu

attack	count()
malicious-url	5

Data table aggregating count() by attack for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$* and was calculated at 2023-11-14 15:46:23.

2.1 Blokované služby procentuálně



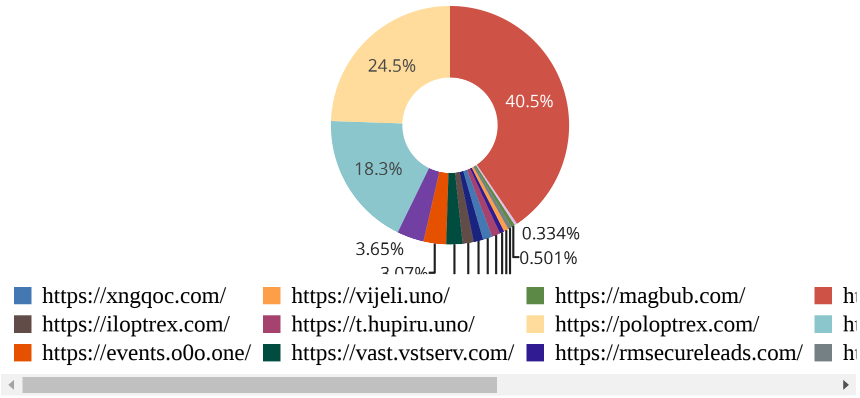
Pie chart aggregating count() by service for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (action:deny OR action:blocked OR action:block)* and was calculated at 2023-11-14 15:46:24.

2.2 Blokované služby / počty

service	count()
HTTPS	4978
SSL	7
udp/443	6
udp/10050	4

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 2023-11-14 15:46:23.

3.1 Zablokované URL adresy procentuálně



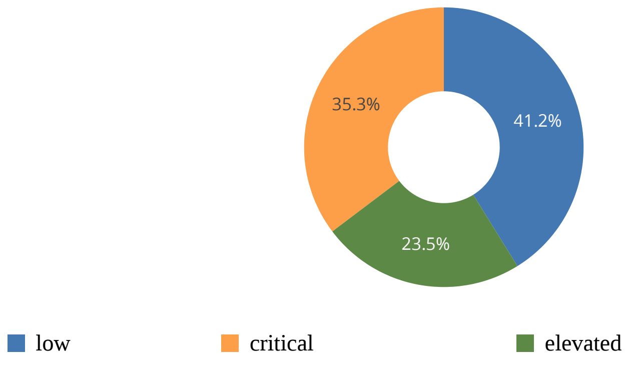
Pie chart aggregating count() by url for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (action:deny OR action:blocked OR action:block)* and was calculated at 2023-11-14 15:46:24.

3.2 Zablokované URL adresy / počty

url	count()
https://bts.a11k.com/	1941
https://poloptrex.com/	1172
https://go.fxmnba.com/	878
https://tn.hdzog.com/	175
https://events.o0o.one/	147
https://vast.vstserv.com/	106
https://iloptrex.com/	72
https://boloptrex.com/	62
https://xngqoc.com/	61
https://t.hupiru.uno/	54
https://rmsecureleads.com/	30
https://vijeli.uno/	30
https://trk.cloudtraff.com/	25
https://magbub.com/	24
https://3f2f1a20ba.1ecfd63507.com/	16

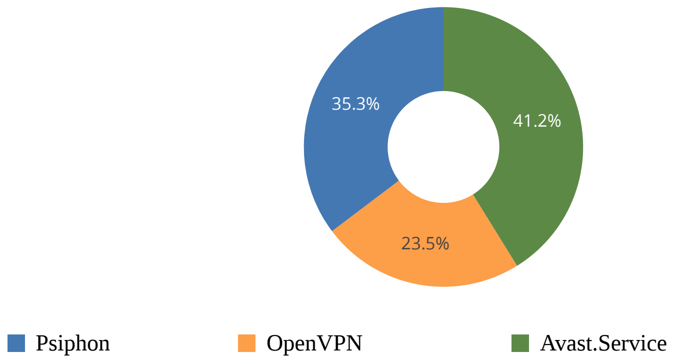
Data table aggregating count() by url for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (action:deny OR action:blocked OR action:block) AND NOT dstcountry:Reserved* and was calculated at 2023-11-14 15:46:24.

4.1 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 2023-11-14 15:46:25.

4.2 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 2023-11-14 15:46:25.

4.3 Blokované aplikace / počty

app	count()
Avast.Service	7
Psiphon	6
OpenVPN	4

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 2023-11-14 15:46:25.

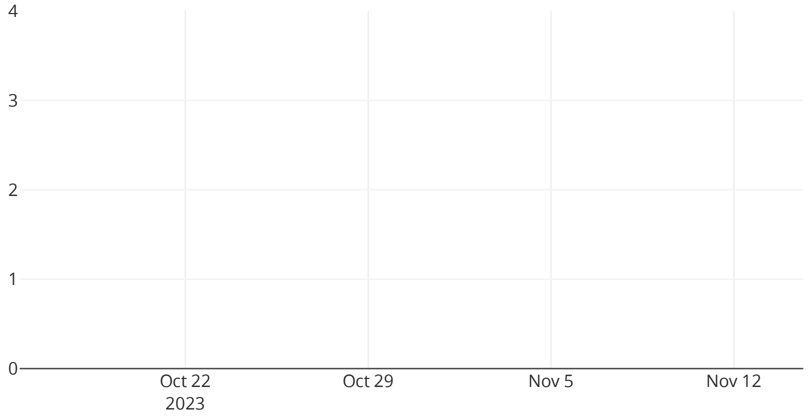
4.4 Trend kritické závažnosti

17

+7 / +70%

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 2023-11-14 15:46:25.

5.1 Blokované viry v čase



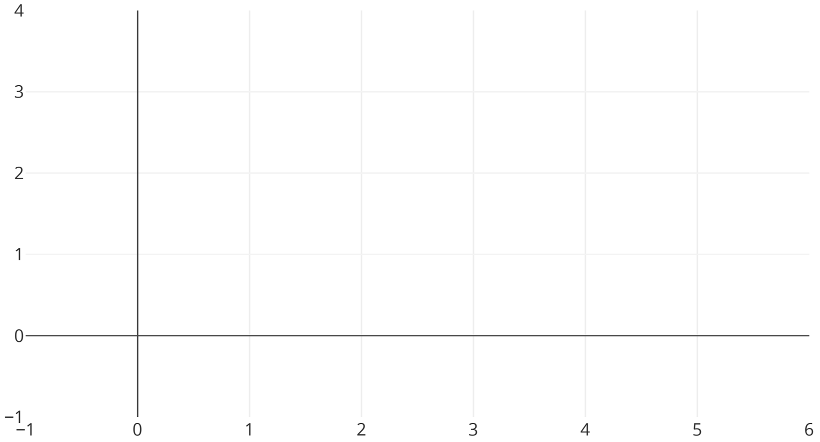
Bar chart aggregating count() by timestamp for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND subtype:virus AND action:blocked* and was calculated at 2023-11-14 15:46:25.

5.2 Blokované viry a jejich původ / počty

url	count()

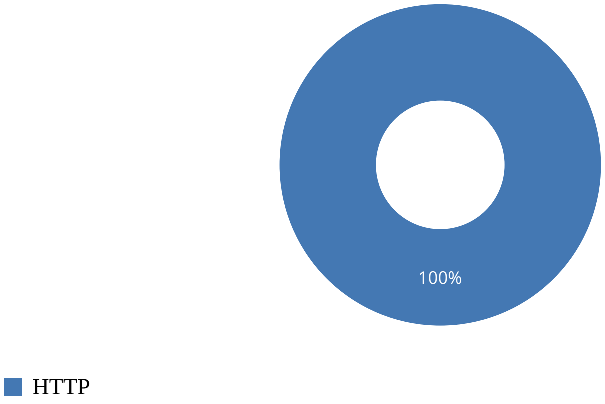
Data table aggregating count() by url for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND subtype:virus AND action:blocked* and was calculated at 2023-11-14 15:46:26.

5.3 Blokované viry procentuálně



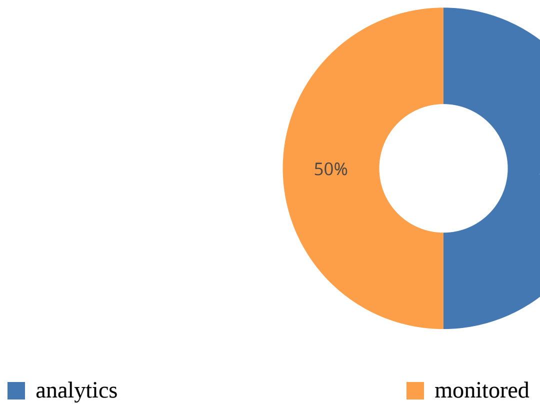
Pie chart aggregating count() by virus for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND subtype:virus* and was calculated at 2023-11-14 15:46:26.

5.4 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 2023-11-14 15:46:26.

5.5 Provedené akce procentuálně



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 2023-11-14 15:46:26.