



GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

MSS-UTM REPORT

ACME FINANCIAL SERVICES

May 19, 2023



MSS-UTM REPORT

ACME FINANCIAL SERVICES 05/19/2023

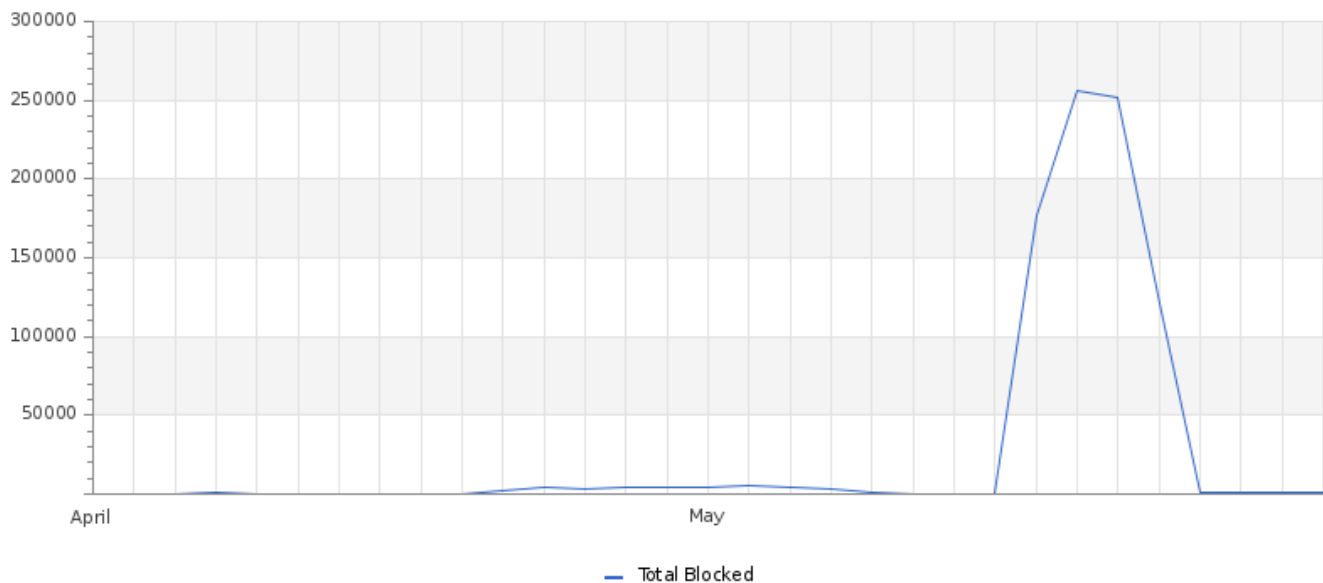
TLP AMBER

MSS-UTM REPORT

About this report

This is a SKYWATCH report that presents the most up-to-date information for the MSS-UTM as displayed in the service dashboard.

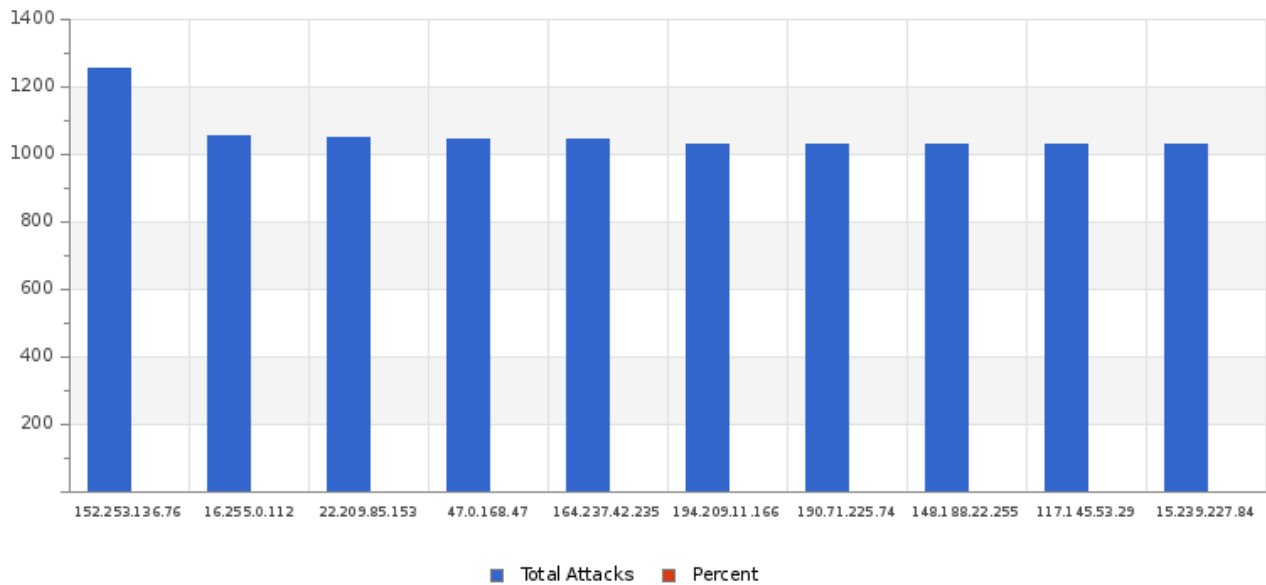
MAIN

Total Attacks Per Month ***Total Attacks Blocked *****850,484**

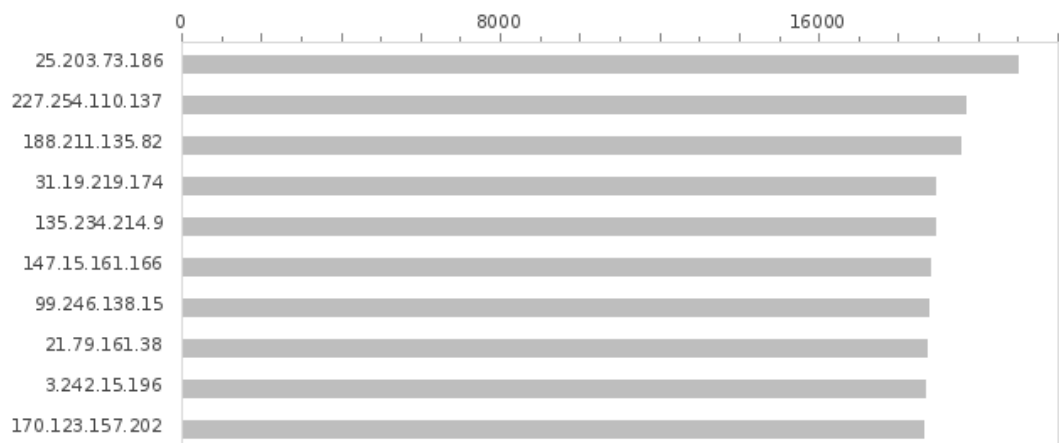
MSS-UTM REPORT

ACME FINANCIAL SERVICES 05/19/2023

Top Attack Sources *



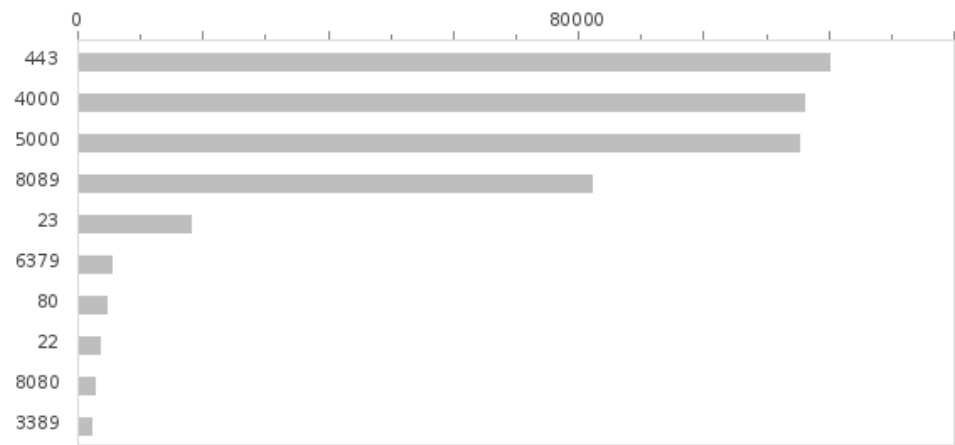
Top Blocked Traffic Destinations *



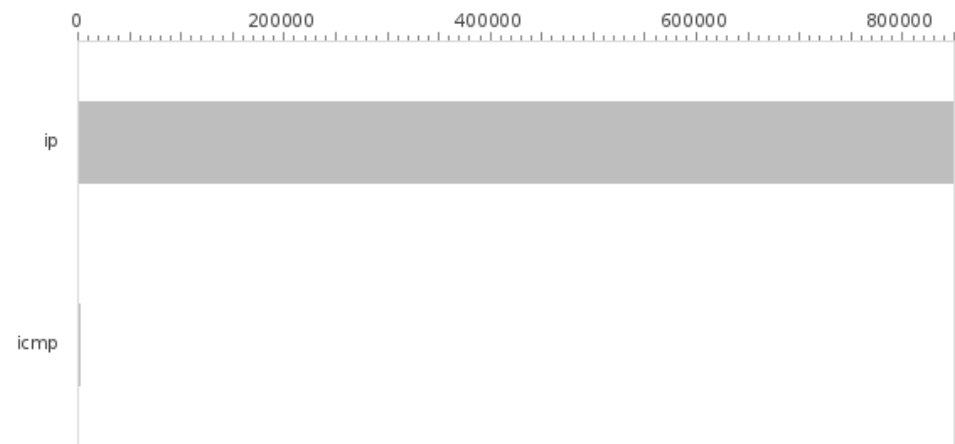
MSS-UTM REPORT

ACME FINANCIAL SERVICES 05/19/2023

Traffic Blocked by Destination Port *



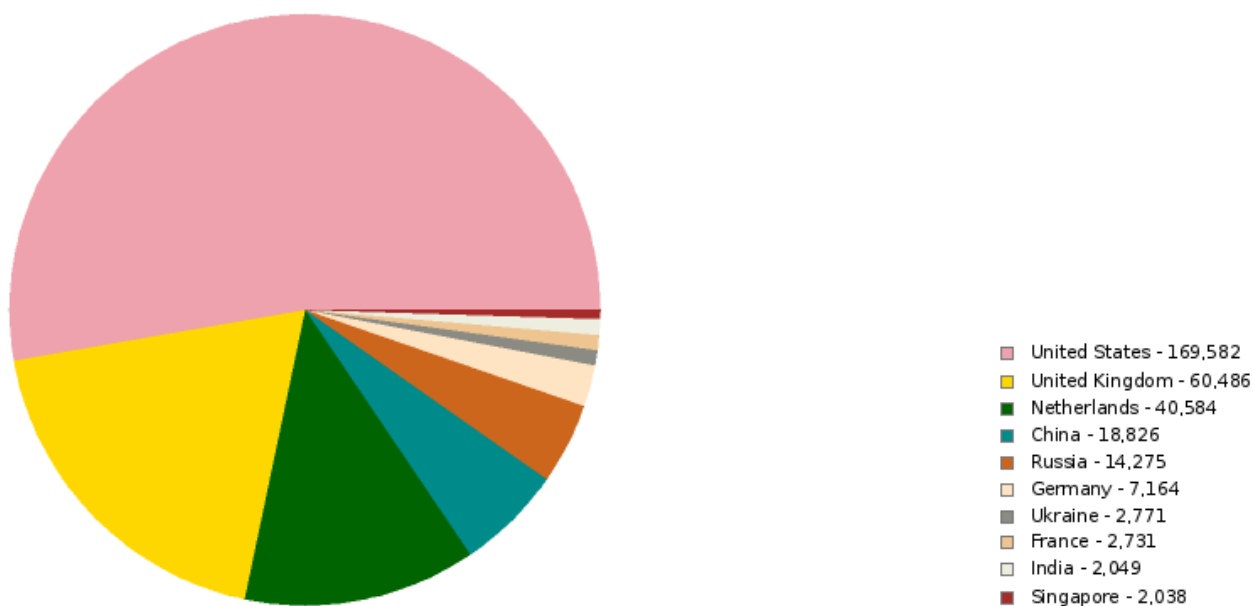
Traffic Dropped By Protocol *



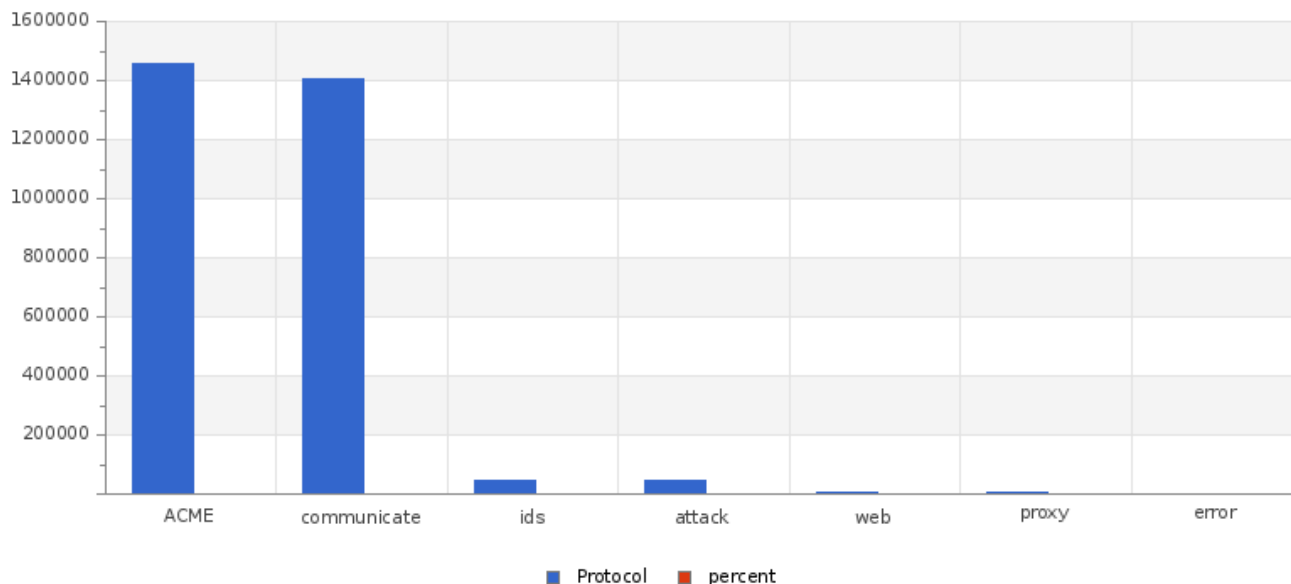
MSS-UTM REPORT

ACME FINANCIAL SERVICES 05/19/2023

Top Attacking Countries *



Network Activity *



MSS-UTM REPORT

ACME FINANCIAL SERVICES 05/19/2023

Traffic blocked by rule *



Blocked Traffic & Security Alert Destination IP Addresses



Blocked Traffic & Security Alert Source IP Addresses



USER BEHAVIOR

SaaS Events

6,294

Top Web Categories

http_category	count
any	20,116,318
computer-and-internet-info	3,903,969
ACME	2,174,495
business-and-economy	1,813,052
license-expired	430,264
government	153,816
private-ip-addresses	72,034
medium-risk	31,356
news	4,683
search-engines	3,447



MSS-UTM REPORT

ACME FINANCIAL SERVICES 05/19/2023

Top Applications

app	count
dns-base	9,878,296
ssl	7,053,900
pfsense:filterlog	4,198,052
incomplete	3,783,575
ping	1,459,912
splunk	643,315
not-applicable	542,030
web-browsing	362,427
ntp-base	273,317
ssh	117,792

SAAS ACTIVITY

SaaS Applications

18

Users

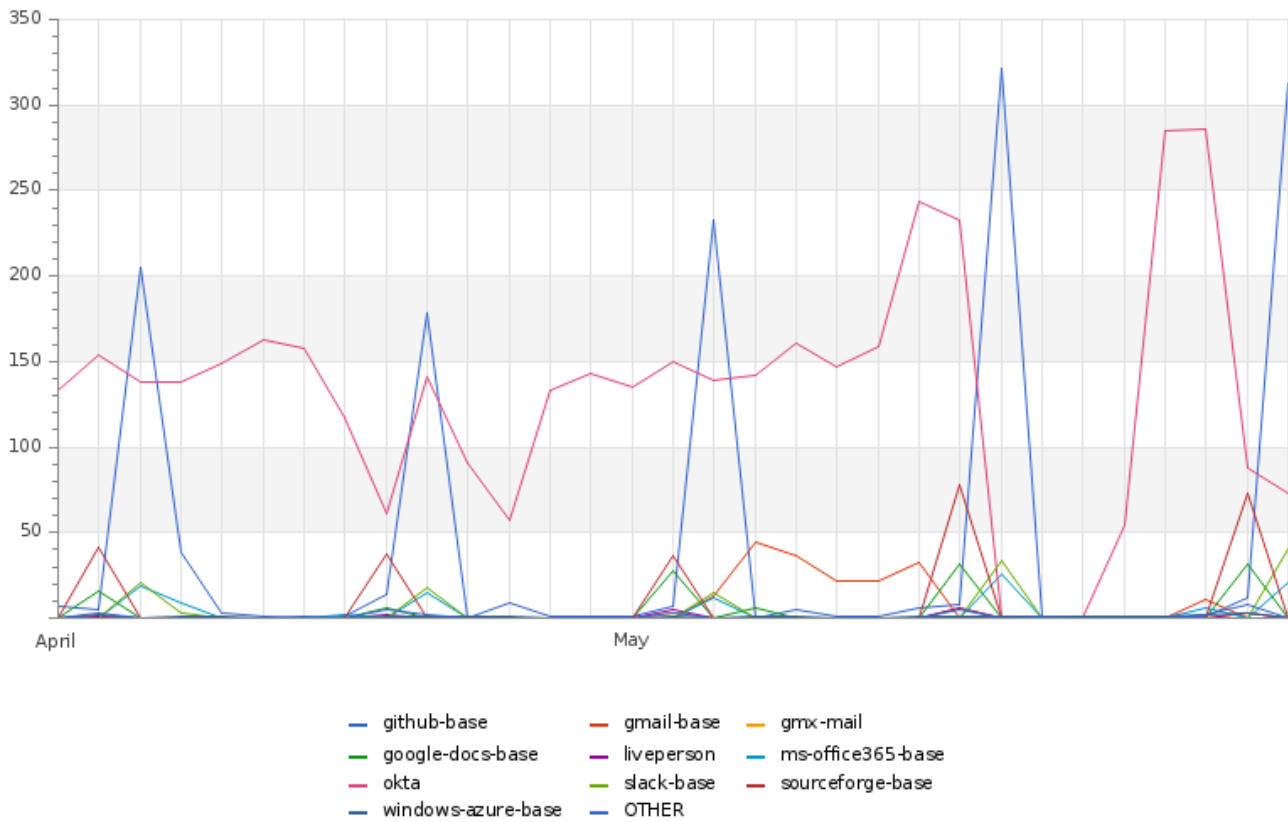
278



MSS-UTM REPORT

ACME FINANCIAL SERVICES 05/19/2023

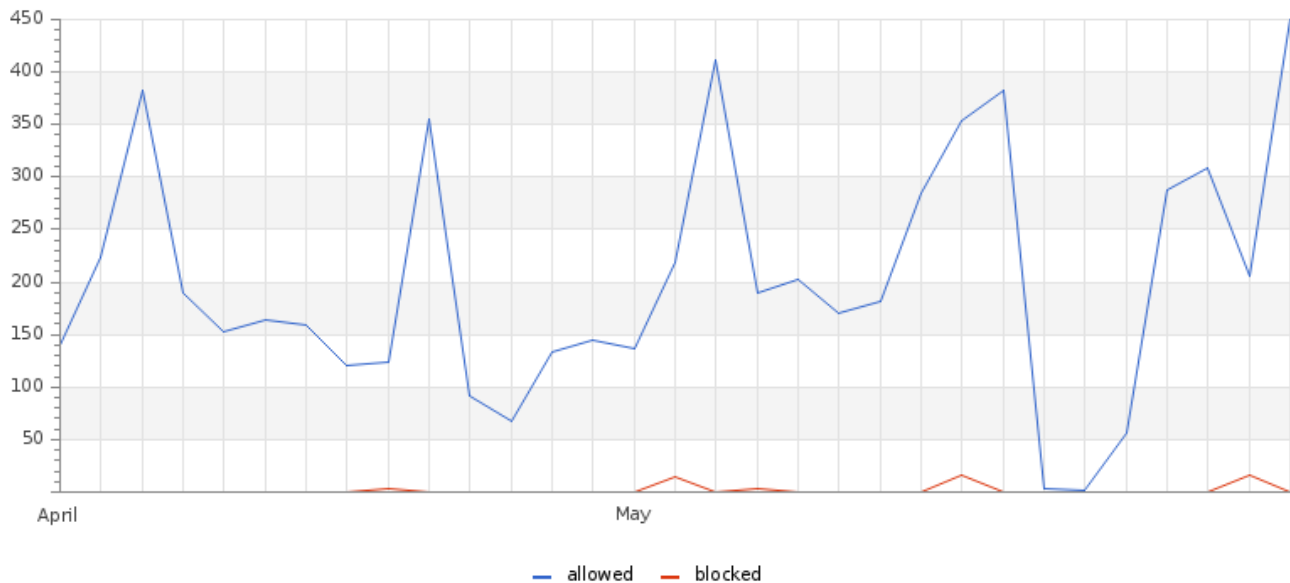
SaaS Usage



MSS-UTM REPORT

ACME FINANCIAL SERVICES 05/19/2023

SaaS Actions



Non-Sanctioned SaaS Applications

app	count	percent
dns-base	11,685,736	38.76
ssl	8,344,861	27.68
incomplete	4,531,689	15.03
ping	1,797,976	5.96
not-applicable	1,084,429	3.60
splunk	804,476	2.67
web-browsing	540,585	1.79
ntp-base	316,684	1.05
ms-update	223,134	0.74
ldap	145,002	0.48
ssh	144,792	0.48
ms-ds-smbv3	117,023	0.39
kerberos	72,032	0.24
insufficient-data	64,808	0.21
syslog	55,872	0.19
msrpc-base	41,532	0.14

MSS-UTM REPORT

ACME FINANCIAL SERVICES 05/19/2023

app	count	percent
smtp-base	26,972	0.09
ms-local-security-management	25,899	0.09
snmp-base	19,478	0.06
active-directory-base	17,348	0.06
google-base	13,406	0.04
ms-netlogon	12,829	0.04
unknown-udp	10,302	0.03
sip	9,827	0.03
quic	5,286	0.02
okta	4,093	0.01
unknown-tcp	3,642	0.01
ACME	3,252	0.01
mysql	2,137	0.01
apt-get	1,898	0.01
radius	1,880	0.01
http-proxy	1,777	0.01
icmp	1,536	0.01
upnp	1,468	0.00
github-base	1,376	0.00
ocsp	1,124	0.00
gitlab-base	1,108	0.00
telnet	1,102	0.00
stun	932	0.00
ipsec-esp-udp	908	0.00
windows-remote-management	608	0.00
ms-service-controller	586	0.00
twitter-base	443	0.00
iheartradio	369	0.00
portmapper	364	0.00
ipfs	356	0.00
git-base	273	0.00
sourceforge-base	265	0.00
youtube-base	252	0.00
ms-rdp	247	0.00
reddit-base	228	0.00



MSS-UTM REPORT

ACME FINANCIAL SERVICES 05/19/2023

app	count	percent
gmail-base	181	0.00
google-play	146	0.00
soap	142	0.00
slack-base	131	0.00
ms-wmi	128	0.00
google-docs-base	120	0.00
rss	117	0.00
ms-office365-base	110	0.00
tumblr-base	84	0.00
ms-ds-smb-base	65	0.00
vimeo-base	63	0.00
flickr-base	53	0.00
yelp-base	44	0.00
imgur-base	41	0.00
socks	36	0.00
windows-push-notifications	29	0.00
tftp	29	0.00
gre	29	0.00
myspace-base	25	0.00
windows-azure-base	23	0.00
vkontakte-base	23	0.00
ms-win-dns	20	0.00
rmcp	19	0.00
mssql-mon	19	0.00
google-update	19	0.00
netbios-ns	18	0.00
liveperson	17	0.00
flash	16	0.00
pinterest-base	15	0.00
ntp-non-rfc	15	0.00
gmx-mail	13	0.00
ipv6	12	0.00
t.120	11	0.00
outlook-web	11	0.00
pandora	10	0.00

MSS-UTM REPORT

ACME FINANCIAL SERVICES 05/19/2023

app	count	percent
mail.ru-base	10	0.00
web-crawler	9	0.00
rtsp	9	0.00
outlook-web-online	9	0.00
mssql-db-base	9	0.00
teredo	8	0.00
xing	7	0.00
stocktwits-base	7	0.00
wetransfer-base	6	0.00
odnoklassniki-base	6	0.00
meetup-base	6	0.00
mail.ru-mail	6	0.00
deezer	6	0.00
corba	6	0.00

Top Sanctioned Categories

count

7,419

FILE ACTIVITY

Blocked Files

94,101

Allowed Files

7,421

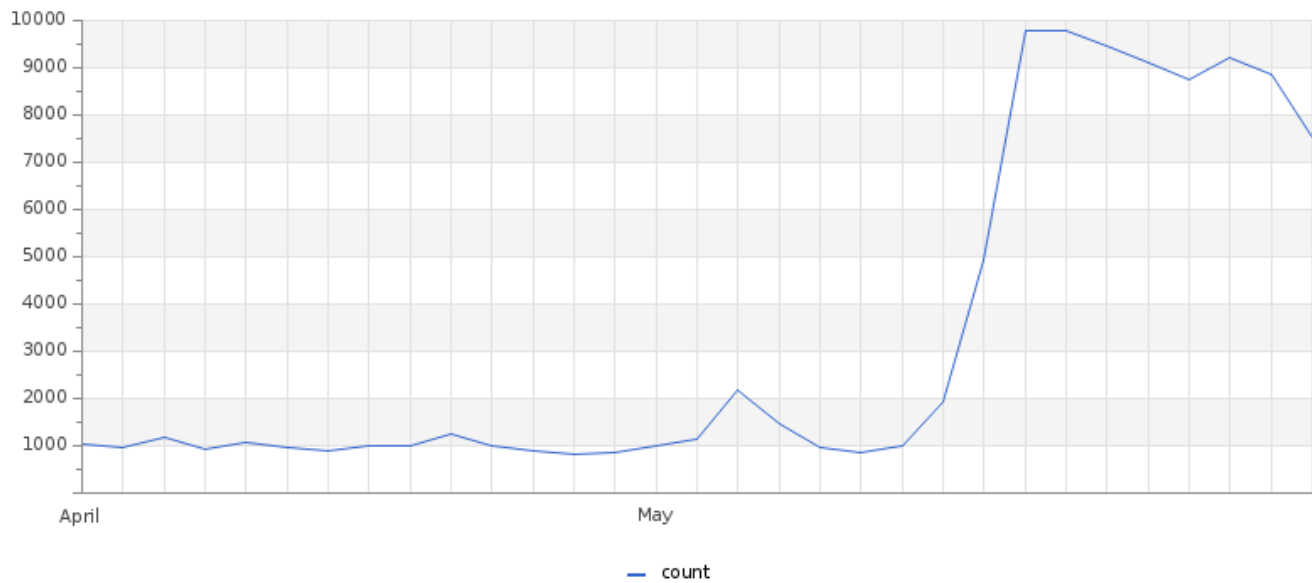
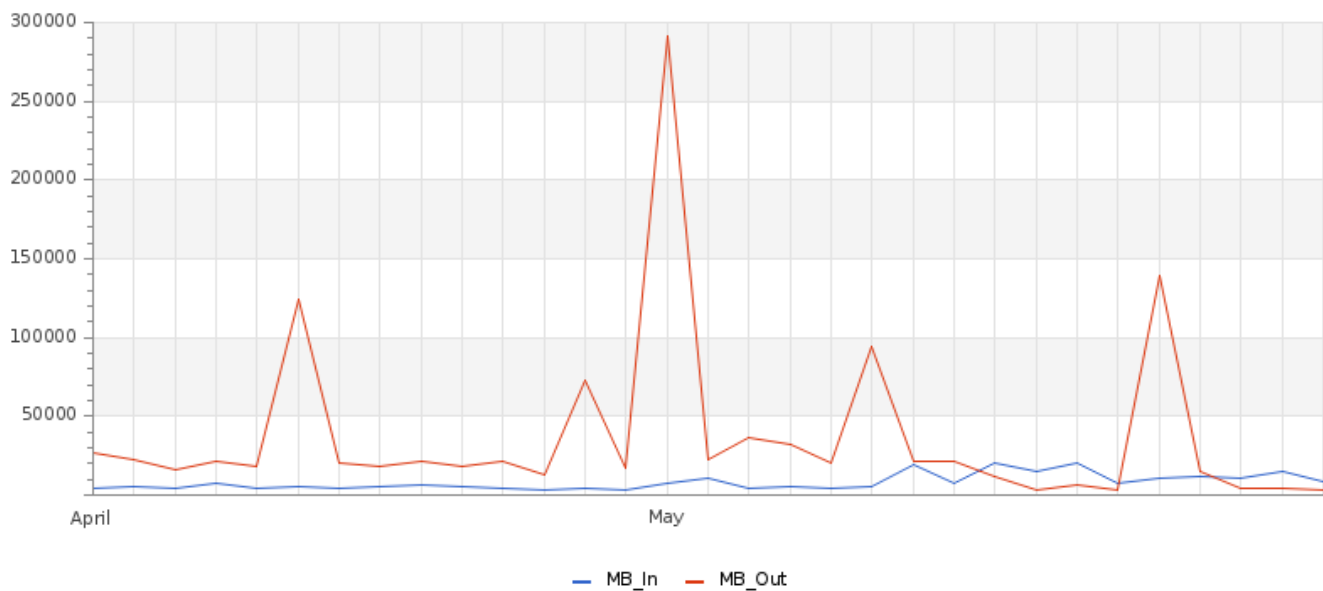
Total Files

101,659



MSS-UTM REPORT

ACME FINANCIAL SERVICES 05/19/2023

File Actions Over Time**Bytes Transferred Over Time**

MSS-UTM REPORT

ACME FINANCIAL SERVICES 05/19/2023

File Direction

direction	count
client-to-server	3,978
server-to-client	98,004

File Activity

action	app	dest	src	user	file_name	session_id	src_zone	dest_zone
blocked	ms-update	134.58.170.82	135.234.214.9	unknown	ACME	79,070	Protect	Protect
blocked	ms-update	243.165.26.123	135.234.214.9	unknown	ACME	166,344	Protect	Protect
blocked	ms-update	19.44.114.159	135.234.214.9	unknown	ACME	78,626	Protect	Protect
blocked	ms-update	78.132.23.125	135.234.214.9	unknown	ACME	67,003	Protect	Protect
allowed	smtp-base	35.38.147.228	219.202.57.133	To: acme@acme.com;		71,145	Protect	Protect
blocked	ms-update	78.132.23.125	135.234.214.9	unknown	ACME	69,826	Protect	Protect
allowed	smtp-base	35.38.147.228	219.202.57.133	To: acme@acme.com;		71,943	Protect	Protect
blocked	ms-update	2.125.43.58	135.234.214.9	unknown	ACME	73,119	Protect	Protect
blocked	ms-update	38.198.139.14	135.234.214.9	unknown	ACME	73,115	Protect	Protect
blocked	ms-update	134.58.170.82	135.234.214.9	unknown	am_engine_patch_1.1.19900.2_82b6fc54d01dc6abe88a00157629cc79aa3	72,951	Protect	Protect
blocked	ms-update	134.58.170.82	135.234.214.9	unknown	ACME	67,657	Protect	Protect
blocked	ms-update	19.44.114.159	25.203.73.186	unknown	ACME	68,490	Protect	Protect
blocked	ms-update	38.198.139.14	135.234.214.9	unknown	ACME	160,806	Protect	Protect
blocked	ms-update	150.164.136.69	135.234.214.9	unknown	ACME	59,281	Protect	Protect
blocked	ms-update	19.44.114.159	25.203.73.186	unknown	ACME	154,832	Protect	Protect
blocked	ms-update	243.165.26.123	135.234.214.9	unknown	ACME	156,687	Protect	Protect
blocked	ms-update	150.164.136.69	135.234.214.9	unknown	am_base_4adc1d9568b3c30dad3901bce9c9a8b3bc9d7bd1.exe	153,826	Protect	Protect
blocked	ms-update	19.44.114.159	135.234.214.9	unknown	am_engine_patch_1.1.20100.6_569a944f2c64ddf892a6620e70dc9da1313	146,952	Protect	Protect
blocked	ms-update	234.34.64.56	170.123.157.202	unknown	ACME	154,660	Protect	Protect
blocked	ms-update	134.58.170.82	135.234.214.9	unknown	ACME	156,173	Protect	Protect
blocked	ms-update	134.58.170.82	135.234.214.9	unknown	ACME	148,871	Protect	Protect
blocked	ms-update	38.198.139.14	135.234.214.9	unknown	ACME	64,959	Protect	Protect
blocked	ms-update	150.164.136.69	135.234.214.9	unknown	ACME	56,672	Protect	Protect
blocked	ms-update	149.215.33.47	170.123.157.202	unknown	ACME	89,805	Protect	Protect
blocked	ms-update	245.84.105.88	170.123.157.202	unknown	ACME	90,406	Protect	Protect
blocked	ms-update	225.221.27.211	135.234.214.9	unknown	ACME	88,274	Protect	Protect
blocked	ms-update	38.198.139.14	135.234.214.9	unknown	ACME	91,488	Protect	Protect
blocked	ms-update	38.198.139.14	135.234.214.9	unknown	ACME	91,376	Protect	Protect
blocked	ms-update	38.198.139.14	135.234.214.9	unknown	ACME	181,063	Protect	Protect
blocked	ms-update	134.58.170.82	135.234.214.9	unknown	ACME	185,222	Protect	Protect
blocked	ms-update	31.27.181.156	135.234.214.9	unknown	ACME	180,758	Protect	Protect
blocked	ms-update	19.44.114.159	135.234.214.9	unknown	ACME	179,180	Protect	Protect
blocked	ms-update	19.44.114.159	135.234.214.9	unknown	ACME	73,015	Protect	Protect
blocked	ms-update	134.58.170.82	135.234.214.9	unknown	ACME	40,198	Protect	Protect
blocked	ms-update	134.58.170.82	135.234.214.9	unknown	ACME	179,703	Protect	Protect
blocked	ms-update	31.27.181.156	135.234.214.9	unknown	ACME	175,268	Protect	Protect
blocked	ms-update	38.198.139.14	135.234.214.9	unknown	ACME	88,049	Protect	Protect
blocked	ms-update	38.198.139.14	135.234.214.9	unknown	ACME	180,012	Protect	Protect
blocked	ms-update	38.198.139.14	135.234.214.9	unknown	ACME	180,941	Protect	Protect
blocked	ms-update	38.198.139.14	135.234.214.9	unknown	ACME	87,754	Protect	Protect
blocked	ms-update	95.11.133.168	170.123.157.202	unknown	ACME	85,217	Protect	Protect
blocked	ms-update	47.13.245.26	135.234.214.9	unknown	ACME	144,146	Protect	Protect

MSS-UTM REPORT

ACME FINANCIAL SERVICES 05/19/2023

action	app	dest	src	user	file_name	session_id	src_zone	dest_zone
blocked	ms-update	19.44.114.159	135.234.214.9	unknown	ACME	89,096	Protect	Protect
blocked	ms-update	134.58.170.82	135.234.214.9	unknown	ACME	86,904	Protect	Protect
blocked	ms-update	0.159.71.74	170.123.157.202	unknown	ACME	175,762	Protect	Protect
blocked	ms-update	134.58.170.82	135.234.214.9	unknown	ACME	176,527	Protect	Protect
blocked	ms-update	47.13.245.26	135.234.214.9	unknown	ACME	144,183	Protect	Protect
blocked	ms-update	2.125.43.58	135.234.214.9	unknown	ACME	176,095	Protect	Protect
blocked	ms-update	38.198.139.14	135.234.214.9	unknown	ACME	82,659	Protect	Protect
blocked	ms-update	134.58.170.82	135.234.214.9	unknown	ACME	175,254	Protect	Protect
blocked	ms-update	38.198.139.14	25.203.73.186	unknown	ACME	175,161	Protect	Protect
blocked	ms-update	162.197.175.153	135.234.214.9	unknown	ACME	108,194	Protect	Protect
blocked	ms-update	150.164.136.69	135.234.214.9	unknown	ACME	206,111	Protect	Protect
blocked	ms-update	150.164.136.69	135.234.214.9	unknown	ACME	107,523	Protect	Protect
blocked	ms-update	150.164.136.69	135.234.214.9	unknown	ACME	200,299	Protect	Protect
blocked	ms-update	206.11.55.179	135.234.214.9	unknown	ACME	197,392	Protect	Protect
blocked	ms-update	150.164.136.69	135.234.214.9	unknown	ACME	201,052	Protect	Protect
blocked	ms-update	206.11.55.179	135.234.214.9	unknown	ACME	200,907	Protect	Protect
blocked	ms-update	38.198.139.14	135.234.214.9	unknown	ACME	103,369	Protect	Protect
blocked	ms-update	206.11.55.179	135.234.214.9	unknown	ACME	102,490	Protect	Protect
blocked	ms-update	19.44.114.159	135.234.214.9	unknown	ACME	103,066	Protect	Protect
blocked	ms-update	38.198.139.14	135.234.214.9	unknown	ACME	119,877	Protect	Protect
blocked	ms-update	38.198.139.14	135.234.214.9	unknown	ACME	218,034	Protect	Protect
blocked	ms-update	2.125.43.58	135.234.214.9	unknown	ACME	211,863	Protect	Protect
blocked	ms-update	80.92.150.7	135.234.214.9	unknown	ACME	214,422	Protect	Protect
blocked	ms-update	80.92.150.7	135.234.214.9	unknown	ACME	215,355	Protect	Protect
blocked	ms-update	38.198.139.14	135.234.214.9	unknown	ACME	120,782	Protect	Protect
blocked	ms-update	243.165.26.123	135.234.214.9	unknown	ACME	117,437	Protect	Protect
blocked	ms-update	38.198.139.14	135.234.214.9	unknown	ACME	115,943	Protect	Protect
blocked	ms-update	19.44.114.159	135.234.214.9	unknown	ACME	214,695	Protect	Protect
blocked	ms-update	135.104.43.122	135.234.214.9	unknown	ACME	115,593	Protect	Protect
blocked	ms-update	150.164.136.69	135.234.214.9	unknown	ACME	110,143	Protect	Protect
blocked	ms-update	162.197.175.153	135.234.214.9	unknown	ACME	114,956	Protect	Protect
blocked	ms-update	135.104.43.122	135.234.214.9	unknown	ACME	114,923	Protect	Protect
blocked	ms-update	150.164.136.69	135.234.214.9	unknown	ACME	113,379	Protect	Protect
blocked	ms-update	162.197.175.153	135.234.214.9	unknown	ACME	213,508	Protect	Protect
blocked	ms-update	162.197.175.153	135.234.214.9	unknown	am_engine_patch_1.1.19900.2_82b6fc54d01dc6abe88a00157629cc79aa3	113,220	Protect	Protect
blocked	ms-update	135.104.43.122	135.234.214.9	unknown	ACME	114,321	Protect	Protect
blocked	ms-update	135.104.43.122	135.234.214.9	unknown	ACME	113,273	Protect	Protect
blocked	ms-update	243.165.26.123	135.234.214.9	unknown	am_base_4adc1d9568b3c30dad3901bce9c9a8b3bc9d7bd1.exe	210,906	Protect	Protect
blocked	ms-update	38.198.139.14	135.234.214.9	unknown	ACME	188,706	Protect	Protect
blocked	ms-update	150.164.136.69	135.234.214.9	unknown	ACME	199,894	Protect	Protect
blocked	ms-update	38.198.139.14	135.234.214.9	unknown	ACME	209,800	Protect	Protect
blocked	ms-update	95.11.133.168	170.123.157.202	unknown	ACME	166,951	Protect	Protect
blocked	ms-update	95.11.133.168	25.203.73.186	unknown	ACME	79,099	Protect	Protect
blocked	ms-update	2.125.43.58	135.234.214.9	unknown	am_base_patch1_2469efc3ff612b06fcee2915bdcdbd511b81f51d9.exe	73,513	Protect	Protect
blocked	ms-update	78.132.23.125	135.234.214.9	unknown	ACME	76,973	Protect	Protect
blocked	ms-update	19.44.114.159	135.234.214.9	unknown	ACME	78,478	Protect	Protect
blocked	ms-update	243.165.26.123	135.234.214.9	unknown	am_delta_patch_93.70.0.156_2a62b55d6343d95eb87fa6ae34ebc5c7853d	165,887	Protect	Protect
blocked	ms-update	134.58.170.82	135.234.214.9	unknown	am_base_patch1-dbeb26c931d795c2fdc7c2923cc56afe127d4c66.exe	167,448	Protect	Protect
blocked	ms-update	19.44.114.159	135.234.214.9	unknown	am_engine_patch_1.1.20000.2_78ef46f633c81b9bdf5e5642ab3eb23d9fe	166,755	Protect	Protect
blocked	ms-update	134.58.170.82	135.234.214.9	unknown	ACME	75,269	Protect	Protect
blocked	ms-update	134.58.170.82	135.234.214.9	unknown	ACME	70,925	Protect	Protect
blocked	ms-update	19.44.114.159	135.234.214.9	unknown	ACME	67,767	Protect	Protect
blocked	ms-update	134.58.170.82	135.234.214.9	unknown	ACME	72,414	Protect	Protect
blocked	ms-update	46.241.176.199	25.203.73.186	unknown	ACME	69,432	Protect	Protect
blocked	ms-update	243.165.26.123	135.234.214.9	unknown	updateplatform_cca39b7c461f636e4d94fa20ac9ee842ae7a9caf.exe	164,189	Protect	Protect

MSS-UTM REPORT

ACME FINANCIAL SERVICES 05/19/2023

action	app	dest	src	user	file_name	session_id	src_zone	dest_zone
blocked	ms-update	134.58.170.82	135.234.214.9	unknown	ACME	51,827	Protect	Protect
blocked	ms-update	134.58.170.82	135.234.214.9	unknown	ACME	69,288	Protect	Protect
blocked	ms-update	19.44.114.159	135.234.214.9	unknown	ACME	161,130	Protect	Protect

WEB ACTIVITY

GLOBAL PROTECT

Events by User

src_user	count
acme@acme.com	863
acme@acme.com	717
acme@acme.com	647
acme@acme.com	601
acme@acme.com	518
acme@acme.com	453
251,589	429
21,989	417
acme@acme.com	394
acme@acme.com	322
acme@acme.com	314
acme@acme.com	260
645,260	257
206,196	239
474,876	231
acme@acme.com	196
993,762	194
658,588	180
369,353	177
acme@acme.com	152
923,241	138
145,113	137
726,445	122
jane37	106



MSS-UTM REPORT

ACME FINANCIAL SERVICES 05/19/2023

src_user	count
serhii.lukhverchyk	101
407,677	97
acme@acme.com	88
bdoe	88
eduard.volkov	75
doe.john	74
jane.doe	73
acme@acme.com	70
doe.john	70
jane32	65
test	60
754,641	57
828,937	55
acme-84.com\serhii.lukhverchyk	53
odoe	50
929,955	49
udoe	48
,	47
'))	47
')	47
)	46
))	46
acme@acme.com	46
jane28	45
mdoe	42
doe.jane	37
vitaliy.osnovenko	37
doe.john	33
zzLog In	33
doe.john	33
doe.john	31
acme-84.com\eduard.volkov	30
edoe	27
jane.doe	26
sdoe	25



MSS-UTM REPORT

ACME FINANCIAL SERVICES 05/19/2023

src_user	count
' AND 0 IN (SELECT SLEEP(3)) --	24
' AND SLEEP(3)='	24
AND SLEEP(3)=0	24
AND 0 IN (SELECT SLEEP(3)) --	24
admin	23
' 'Log In	22
and 1=0	22
or 1=0	22
and 1=1	22
acme-84.com\vitaliy.osnovenko	21
acme-95.com	18
738,244	18
jane.doe	15
acme@acme.com	13
' or '1'='0	11
' or 'b'='a	11
') or ('1'='1	11
') or 1=0 or ('1'='0	11
') or 1=1 or ('1'='1	11
') or (('1'='0	11
')) or (((1'='1	11
'Log In	11
) or (1=1	11
) or 1=0 or (1=0	11
) or 1=1 or (1=1	11
)) or ((1=0	11
))) or (((1=1	11
))) or 1=0 or (((1=0	11
))) or 1=1 or (((1=1	11
+ 0	11
+ 42	11
and 1=1)	11
vitalii.loievskyi	11
' or '1'='1	11
' or 'b'='b	11

MSS-UTM REPORT

ACME FINANCIAL SERVICES 05/19/2023

src_user	count
' or 1=0 or '1'='0	11
' or 1=1 or '1'='1	11
') or ('1'='0	11
') or (('1'='1	11
') or 1=0 or (('1'='0	11
') or 1=1 or (('1'='1	11

Events by Source IP

src_ip	count
65.243.40.82	32,560
31.19.219.174	26,303
39.207.215.175	26,301
146.188.163.44	1,032
4.189.106.8	594
152.165.170.242	542
251.225.165.126	532
205.20.160.243	519
133.33.153.116	505
8.114.57.46	385
27.57.20.100	383
254.158.189.136	251
236.41.127.26	246
143.108.199.35	206
126.177.9.23	165
161.20.20.148	155
17.238.69.8	144
150.61.207.153	119
76.200.24.233	112
153.96.184.214	97
175.87.197.39	90
85.251.171.54	89
41.249.184.189	69
197.104.48.80	67
180.84.125.112	67



MSS-UTM REPORT

ACME FINANCIAL SERVICES 05/19/2023

src_ip	count
237.78.195.24	61
59.64.174.193	60
190.103.133.224	55
216.232.123.170	55
225.176.54.44	51
80.201.3.74	47
24.0.94.205	45
219.39.151.195	42
113.218.210.71	41
223.13.11.146	41
131.46.127.17	40
149.88.65.105	40
30.158.115.208	38
162.107.87.52	38
254.228.0.69	36
32.134.121.110	35
248.14.9.84	33
167.168.58.242	33
219.89.158.200	32
76.106.93.130	31
235.167.25.117	28
122.10.4.76	27
143.84.80.130	27
197.45.187.194	25
77.170.17.13	24
144.15.102.35	24
112.13.101.71	24
235.30.71.61	24
206.118.1.176	24
117.227.11.181	23
216.58.166.15	22
23.166.34.85	21
177.196.252.171	20
216.197.87.242	20
40.123.87.207	20



MSS-UTM REPORT

ACME FINANCIAL SERVICES 05/19/2023

src_ip	count
38.85.7.240	19
109.206.75.188	18
54.130.162.237	18
186.186.155.229	18
232.3.4.99	16
86.235.44.21	16
42.30.55.98	15
202.247.234.21	15
233.156.110.91	15
29.240.248.195	14
203.226.76.47	12
138.197.233.242	12
85.52.123.73	12
49.157.187.45	12
140.18.119.245	12
171.85.81.5	12
195.125.237.130	11
151.253.74.4	10
73.184.28.112	10
91.252.220.19	9
222.197.194.54	9
70.190.213.116	8
230.181.104.32	8
31.68.93.139	8
25.114.101.208	8
35.84.68.73	8
219.133.61.154	8
54.244.211.109	8
30.187.236.165	7
50.120.115.156	7
103.178.75.249	6
222.119.238.175	6
31.222.35.198	6
133.140.208.76	6
6.79.148.166	6



MSS-UTM REPORT

ACME FINANCIAL SERVICES 05/19/2023

src_ip	count
137.159.3.182	6
7.142.212.74	6
53.97.194.175	6
193.20.204.170	6
51.181.16.227	6

Failed Login by User

src_user	count
251,589	429
21,989	417
645,260	257
206,196	239
474,876	231
993,762	194
658,588	180
369,353	177
923,241	138
145,113	137
726,445	122
407,677	97
john.doe	75
acme@acme.com	69
doe.jane	62
serhii.lukhverchyk	61
test	60
754,641	57
828,937	55
929,955	49
')	47
'	47
'))	47
))	46
)	46
john39	44



MSS-UTM REPORT

ACME FINANCIAL SERVICES 05/19/2023

src_user	count
eduard.volkov	40
doe.jane	39
ddoe	38
zzLog In	33
doe.jane	32
jane.doe	32
vitaliy.osnovenko	28
doe.john	28
AND 0 IN (SELECT SLEEP(3)) --	24
' AND 0 IN (SELECT SLEEP(3)) --	24
' AND SLEEP(3)='	24
AND SLEEP(3)=0	24
admin	23
and 1=1	22
' 'Log In	22
and 1=0	22
or 1=0	22
738,244	18
acme-95.com	18
acme@acme.com	17
john.doe	16
' or '1'='1	11
' or 'b'='b	11
' or 1=0 or '1'='0	11
' or 1=1 or '1'='1	11
') or ('1'='0	11
') or (('1'='1	11
') or 1=0 or (('1'='0	11
') or 1=1 or (('1'='1	11
')) or (((1'='0	11
) or (1=0	11
) or ((1=1	11
) or 1=0 or ((1=0	11
) or 1=1 or ((1=1	11
))) or (((1=0	11



MSS-UTM REPORT

ACME FINANCIAL SERVICES 05/19/2023

src_user	count
and 1=0)	11
or 0=0	11
or 1=0 or 1=0	11
or 1=1	11
or 1=1 or 1=1	11
' or '1'='0	11
' or 'b'='a	11
') or ('1'='1	11
') or 1=0 or ('1'='0	11
') or 1=1 or ('1'='1	11
')) or (('1'='0	11
')) or (('1'='1	11
' 'Log In	11
) or (1=1	11
) or 1=0 or (1=0	11
) or 1=1 or (1=1	11
)) or ((1=0	11
)) or ((1=1	11
)) or 1=0 or (((1=0	11
)) or 1=1 or (((1=1	11
+ 0	11
+ 42	11
and 1=1)	11
' and 'b'<'a	10
' and 'b'>'a	10
finance	10
')) or 1=0 or (('1'='0	10
')) or 1=1 or (('1'='1	10
law	9
shipping1	9
helpdesk	8
conference	7
jane.doe	7
vitalii.loievskyi	7
http://acme-96.com/rfi.txt	6

MSS-UTM REPORT

ACME FINANCIAL SERVICES 05/19/2023

src_user	count
jane.doe	6
acme-96.com/.	6
currency	6
acme@acme.com	6

ALL INCIDENTS

TLP:AMBER = Limited disclosure, restricted to participants' organizations. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**





GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

MSS-UTM REPORT

HOW CAN WE HELP?

Contact us today for more information on
our services and security solutions.

