



INNOVATION DESTINATION

VISIFI CUSTOMER CONFERENCE 2023

Security

Roberto Endrizzi

JUNE 23, 2023

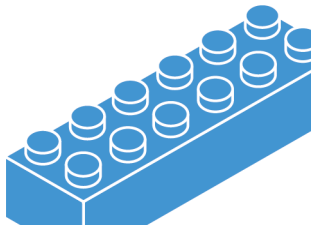


Roberto Endrizzi

I'm a 44-year-old, climbing enthusiast living in the Alps.

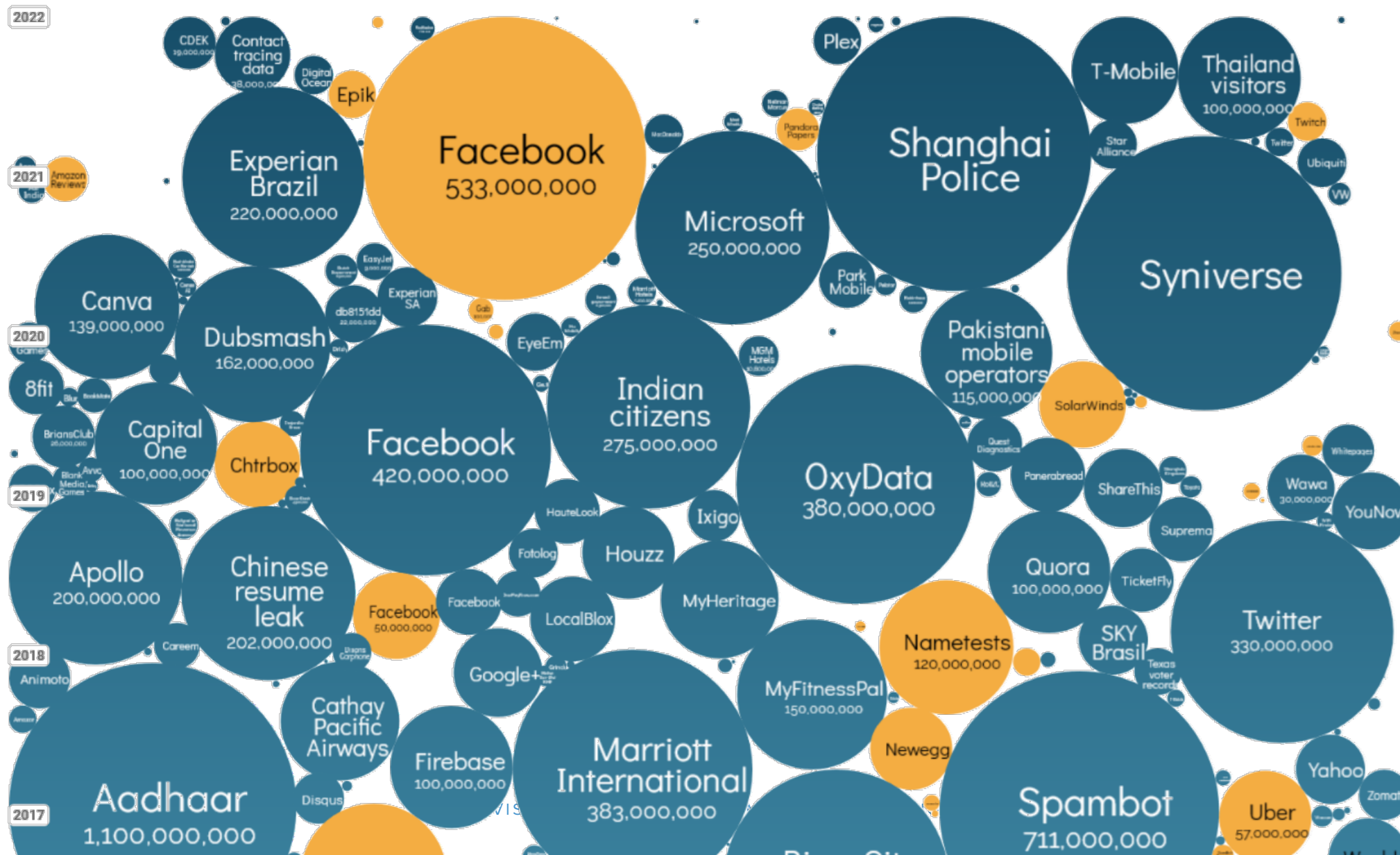
With two decades of experience in IT, now leading the IT department for Dedagroup ICT Network's international division.

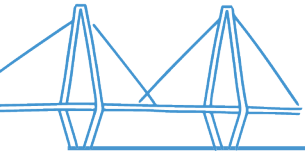
Let's break barriers, create wonders, and set the IT world ablaze!



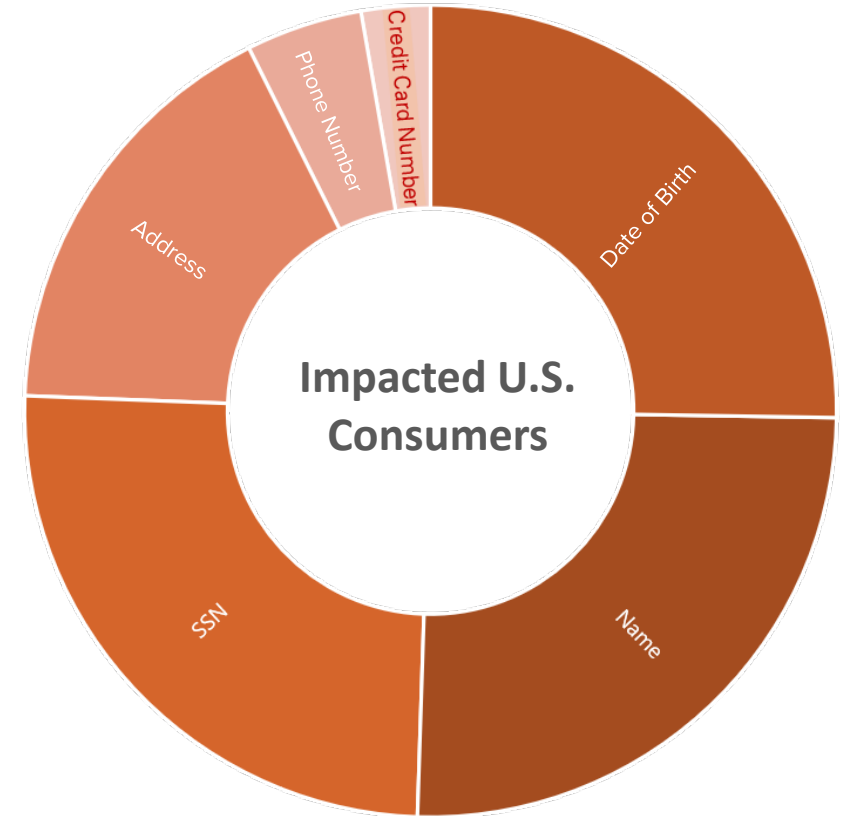


World's Biggest Data Breaches in the Last 5 years





EQUIFAX
147 million impacted





Why does a hacker do this...?

DATA = \$\$\$



How much is personal data worth on the dark web?

Personal data: from 40 cents to \$8

Credit card details: from 5 cents to \$16

Driver's license scan: from 4 cents to \$21

Clinical records: from 84 cents to \$25

Bank account: from 1 to 10% of the value

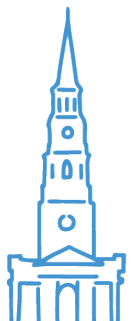




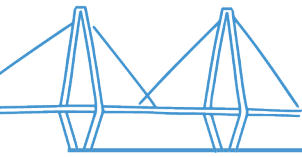
What does this Teach Us?

- Robust and updated security systems
- Education is key

VISIFI CONFIDENTIAL - LIMITED DISTRIBUTION



good safety systems and a good safety culture
for you and suppliers



What we already have – Rapid7

Overview Security Operations Activity

1.258 Users
As of Now

92M Events Processed
↓ -142M (-60.53%)

320 Notable Behaviors
↑ 116 (56.86%)

0 New Alerts
No change

389 Endpoint Agents
Last 30 Days

1 Data Collection Issues
As of Now

Investigations by Priority
Last 28 days

- 2 Investigations
- 0 Critical
- 0 High
- 0 Medium
- 2 Low

Users
Last 28 days

Risky	Watchlist
1 Carlos Amaya	F 673 0 0
2 Brad Pruitt	F 497 0 0
3 Angel Garcia	F 448 0 0
4 David Torres	F 205 0 0
5 Davide Pellerano	F 51 0 0
6 Melvin Benavides	F 27 0 0
7 Melissa Bragwell	F 24 0 0
8 David Hays	F 21 0 0

Ingress Locations
Last 24 hours

Legend: Success (Green), Failure (Red), Unspecified (Grey)

1.258 Active Users

1.831 Non-Expiring Users

45 Admin Accounts

0 Watchlist

50 Shared Accounts

143 Linked Accounts

1.413 Disabled Users

Risky Users
Last 28 days

1 Carlos Amaya	F 673 0 0
2 Brad Pruitt	F 497 0 0
3 Angel Garcia	F 448 0 0
4 David Torres	F 205 0 0
5 Davide Pellerano	F 51 0 0

Firewall Activity
Last 28 days

Ingress Locations
Last 24 Hours

Authentications
Last 28 days

1 healthmailbox11b8569083146138e482	477.648
2 marcos leon	466.648
3 036 Teller	279.205
4 corey	270.856
5 vc admin	246.132

Vulnerabilities
Last 28 days

1 David Hays	Last Seen: Jun 7, 2023 11:28:28 PM	78
2 Paul Morton	Last Seen: Jun 7, 2023 11:28:29 PM	75
3 Jennifer Hosmer	Last Seen: Jun 7, 2023 11:28:29 PM	41

IDS
Last 28 days

We don't see any data for IDS at this time.

If you are a new customer, this may be normal while we analyze your network.

Virus Alerts
Last 7 days

We don't see any data for Virus Alerts at this time.

If you are a new customer, this may be normal while we analyze your network.

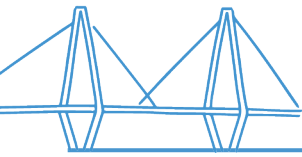
Web Proxy
Last 28 days

1 Cherice Kagunye	351.100
2 Gregory Burton	295.791

All our assets under monitoring

VISIFI CONFIDENTIAL - LIMITED DISTRIBUTION





What we already have – Rapid7

Investigations

Filters Close

Applied Filters 3 filters applied

Medium X High X Close X Clear all

28 Investigations

High

- Custom Inactivity Alert: Firewall ASASM Inactivity was triggered**
Priority: High Assignee: Pietro De Simone
Created: 06 Jun, 2023 2:25 PM · Recent detection: 06 Jun, 2023 2:25 PM
- Custom Inactivity Alert: Firewall Inactivity Internet ASA was triggered**
Priority: High Assignee: Pietro De Simone
Created: 06 Jun, 2023 2:25 PM · Recent detection: 06 Jun, 2023 2:25 PM
- Custom Inactivity Alert: Firewall InactivityDFW ASASM was triggered**
Priority: High Assignee: Pietro De Simone
Created: 06 Jun, 2023 2:24 PM · Recent detection: 06 Jun, 2023 2:24 PM
- Crowdstrike Falcon: Command and Control - Bash has created an interactive terminal for a...**
Priority: High Assignee: Alvise Bacco

Filters

Date Range Close
Date Range
Select range

Priority Level Clear
2/5 selected

- Critical 0
- High 4
- Medium 24
- Low 0

Status Reset
1/4 selected

- Open 0
- Investigating 0
- Waiting 0
- Close 28

Alert Type Close
7 filter options
Search Alert Types

Agents Agent Log Archives Settings

Filters

Agent Status

- Stale (1)
- Offline (37)
- Online (352)

Errors

- Agents with Errors (39)
- Agents with No Errors (351)

OS Families

- Linux (171)
- Windows (219)

Version

- 3.1.4.47 (1)
- 3.2.4.63 (1)
- 3.3.0.2 (1)
- 3.2.5.31 (27)
- 3.3.1.20 (360)

Queries Enter your query here Search Save

390 Agents

352 Online

37 Offline

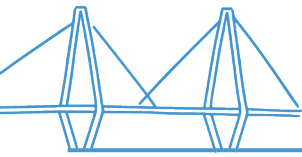
1 Stale

Agents (390) Export to CSV

Hostname	Status	IP Address	Version	Operating System	Connection Path	Last Seen
paysmon02	Online	10.2.250.25	3.3.1.20	centos Linux 7	poollect01.eplinc.com-FW	2023-06-08 T13:41:15+02:00
toore07	1 error	10.2.65.219	3.3.1.20	rocky Linux 8.8	Direct to platform	2023-06-08 T13:43:16+02:00
polbapp03	Online	10.2.91.23	3.3.1.20	Microsoft Windows Server 2019 Datacenter	Direct to platform	2023-06-08 T13:42:18+02:00
pslr02	Online	10.2.105.35	3.3.1.20	centos Linux 7	Direct to platform	2023-06-08 T13:41:40+02:00
tipapp18	Online	10.2.60.152	3.3.1.20	centos Linux 8	poollect02.eplinc.com domain dns	2023-06-08 T13:46:03+02:00
CSR12	Offline	192.168.1.6	3.3.1.20	Microsoft Windows 10 Pro	Direct to platform	2023-06-06 T05:16:16+02:00
tipapp09	Online	10.2.65.139	3.3.1.20	centos Linux 8	Direct to platform	2023-06-08 T13:44:36+02:00
eplmde02	Online	10.2.50.72	3.2.5.31	Microsoft Windows Server 2012 R2 Datacenter	poollect02.eplinc.com domain dns	2023-06-08 T13:45:19+02:00
pvcl02	1 error	10.1.250.17	3.3.1.20	centos Linux 7	poollect04.eplinc.com	2023-06-08 T13:40:58+02:00
Sales42-10	Offline	192.168.4.48	3.3.1.20	Microsoft Windows 10 Pro	Direct to platform	2023-06-08 T04:37:43+02:00
al1-ctblog01	1 error	10.1.250.142	3.3.1.20	centos Linux 7	poollect04.eplinc.com	2023-06-08 T13:43:44+02:00
atdoc01	Online	10.2.90.36	3.3.1.20	centos Linux 7	Direct to platform	2023-06-08 T13:45:28+02:00
pwebseense03	1 error	10.2.250.235	3.3.1.20	centos Linux 7	poollect01.eplinc.com-FW	2023-06-08 T13:42:06+02:00
tipapp02	Online	10.2.65.132	3.3.1.20	centos Linux 8	Direct to platform	2023-06-08 T13:45:02+02:00
prdweb01	Online	10.2.50.32	3.3.1.20	Microsoft Windows Server 2019 Datacenter	poollect02.eplinc.com domain dns	2023-06-08 T13:40:54+02:00
finann11	Online	10.2.65.61	3.3.1.20	centos Linux 8	Direct to platform	2023-06-08 T13:44:74+02:00

Incident Management Response Team 24/7





What we already have - Cloudflare

Requests
95.67M

Data transfer
1.82 TB

Page views
12.9M

Visits
4.25M

API requests
7.27M

New You're using our new Web Traffic analytics.

Traffic for cue-branch.com

[Print report](#) [Download data](#)

[Add filter](#) Previous 30 days

Requests summary

An HTTP request. A typical page view requires many requests.

[All](#) [Referer](#) [Host](#) [Country](#) [Path](#) [Edge status code](#) ...

Total requests
95.67M

Requests

Time (local)

Requests by source

5 items

Referers

www.cue-branch.com	89.22M
None (direct)	5.26M
www.peachstatefcu.org	534k
www.guadalupecu.org	46.88k
www.acipcofcu.org	36.2k

Paths

/CU030MB/Login.aspx	1.18M
/peachstatefcu/Account/Handlers/Activi...	1.08M
/CU030MB/Account/AccountSummary.a...	995.6k
/CU030MB/Account/AccountDetails.aspx	757.6k
/favicon.ico	746.4k

Hosts

www.cue-branch.com	89.22M	Filter Exclude
cue-branch.com	1.08k	
demo.cue-branch.com	4.08k	
cue-branch.com:2095	80	
cue-branch.com:2082	40	

Source browsers

Unknown	56.72M
MobileSafari	9.92M
Chrome	9.19M
ChromeMobile	8.44M
Edge	3.55M

Source operating systems

Unknown	56.73M
Windows	11.77M
iOS	11.76M
Android	10.15M
MacOSX	4.56M

Source device types

Mobile	59.73M
Tablet	18.2M
Desktop	17.74M

95 million requests on our Online System





What we already have - Cloudflare

Threats

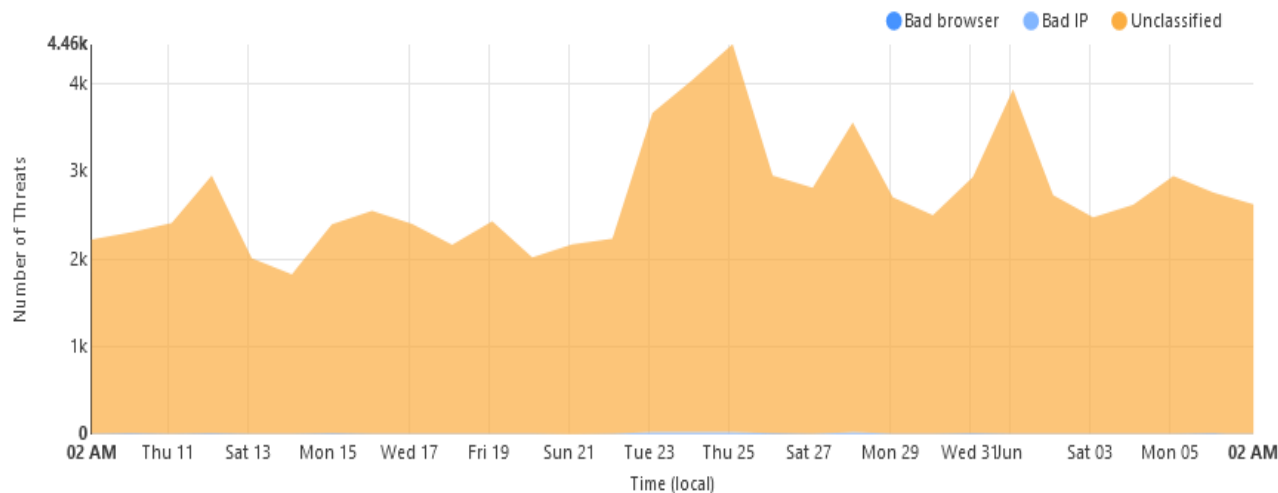
Previous 30 days

Threats

Total Threats
Previous 30 days
81.87k

Top Country
Previous 30 days
DE

Top Threat Type
Previous 30 days
Bad browser



Threats by Country

Previous 24 hours



Top Threat Countries / Regions

Previous 24 hours

Country / Region	Requests
Germany	477
Mexico	191
France	190
Italy	157
Singapore	113

Top Crawlers / Bots

Previous 24 hours

Crawler/Bot	Pages Crawled
Google	316
applebot	19

[Help](#)

We have blocked 81K attacks in the last 30 days





NEW Cloudflare functionality

+ Add filter

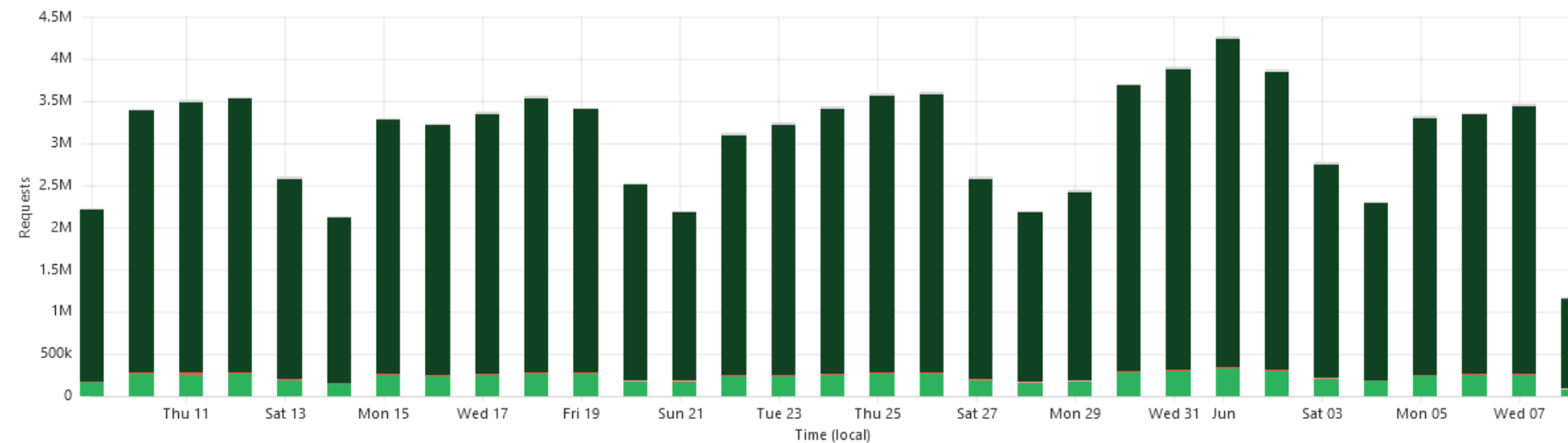
+ Create custom rule

Previous 30 days

HTTP requests Attack analysis

Total **95.67M**

- Likely clean **7.29M**
- Likely attack **489.84k**
- Clean **87.17M**
- Attack **40.68k**
- Not scored **674.76k**



Insights

39.16k not mitigated requests scored as attack [Filter](#)

489.24k not mitigated requests scored as likely attack [Filter](#)

350.56k requests with a non-Mozilla-compatible user agent [Filter](#)

Attack analysis

- Attack **40.68k**
- Likely attack **489.84k**
- Not scored **674.76k**
- Clean **87.17M**
- Likely clean **7.29M**

Gain deeper control with granular attack scores, including various sub attack vectors such as SQLi, XSS and RCE.

[Upgrade to Enterprise](#)

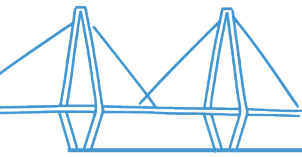
Bot analysis

Bot score



let's block "anything" that pretends to be a human





What we have **NEW** - InsignVM



Goals and SLAs

8 Goals

- 0 Compliant/On Track
- 2 At Risk
- 6 Not Compliant/Not Met
- 0 Owned By Me
- 8 Owned By Others

Name	Assets	Status
Assets without rapid7 agent installed	971	Not Compliant
Ensure credential success	857	Not Compliant
Remediate 90% of criticals at quarterlies	265	At Risk
Remediate all AS400 vulnerabilities	3	Not Compliant
Remediate all critical vulnerabilities within 30 days	265	Not Compliant
Remediate all Windows update critical vulnerabilities at quarterlies	108	At Risk
Remediate Microsoft Patch Tuesday vulnerabilities	221	Not Compliant
Remove Obsolete OS	142	Not Met

vulnerability management platform integrated within our suite





Some suggestions for you

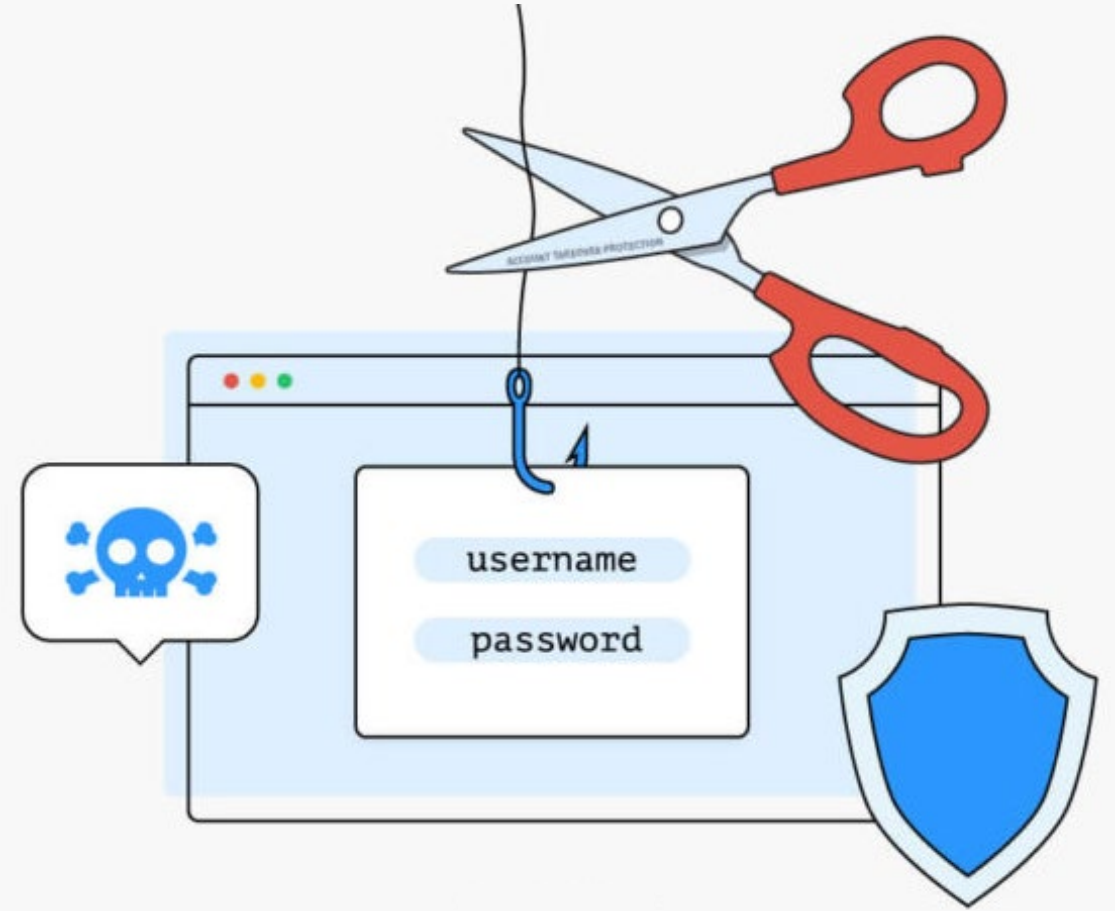
- Protect from phishing
- Social engineering
- Keep your passwords safe
- Mobile device security tips



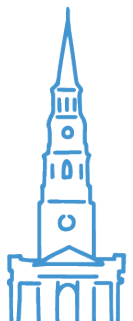


Protect from phishing

- A good antivirus
- 2FA wherever you can
- Training, training, and training!



KnowBe4



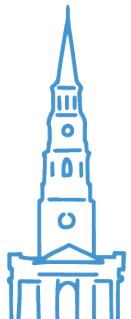


Social engineering

- Be aware
- Verify Identity
- Protect your information online



Company culture





Keep your passwords

- Use unique and strong passwords
- Change Passwords Regularly
- Keep your passwords in a safe place



KeePass



Mobile device security tips

- Phone lock & encrypt the content
- Use only official store & keep updated
- Antivirus



Norton / Bitdefender / McAfee

Mobile Security suites



Don't click on the unknown links!

Thank you

