

UNITED STATES EXPOSURE INTELLIGENCE

Dataset summary – Leviathan OffSec (leviathan.ac) – derived, risk-classified host telemetry

Coverage

Metric	Value
Unique IP addresses	159,601
Host:service observations	199,400
Risk-flagged hosts	70,370
Hosts with hostname/domain join	101,156
Hosts with SSL certificate detail	50,481
Geography	United States (all records)
Refresh cadence	Continuous collection; snapshot rebuild on demand

Risk segments

Segment	Hosts	Signal
outlier_multiport	33,108	
ntp_amplifier	18,432	NTP service – DDoS amplification vector
panel_exposed	7,152	Hosting/admin panel answering publicly
media_server_exposed	2,700	Media server exposed (Plex class)
mail_exposed	2,648	Mail transfer agent exposed (Exim class)
adb_exposed	2,509	Android Debug Bridge reachable – device takeover class
router_cwmp_exposed	1,635	TR-069/CWMP router management exposed
ftp_exposed	1,442	FTP service exposed
db_exposed	730	Database (MySQL/Postgres/Redis/Mongo/MSSQL) on the public internet
rdp_exposed	141	RDP exposed
k8s_api_exposed	76	Kubernetes API server exposed
winrm_exposed	67	WinRM remote management exposed
smb_exposed	59	SMB – EternalBlue-class exposure
vnc_exposed	38	VNC – unauthenticated remote desktop
mqtt_exposed	29	MQTT broker exposed
docker_exposed	22	Docker daemon exposed
telnet_exposed	16	Telnet – plaintext remote shell
ipmi_exposed	3	IPMI out-of-band management exposed

Risk score distribution

Tier	Hosts	Meaning
critical	4,713	score 85-100 – immediate exposure, takeover/control class
high	13,340	score 65-84 – significant exposure, priority patching
medium	27,904	score 40-64 – exposed service, routine hardening
low	153,443	score 0-39 – minimal or well-configured exposure

Infrastructure classification

ASN type	Observations
----------	--------------

enterprise	68,705
cloud	40,967
isp	34,579
other	26,639
cdn	19,607
hosting	6,399
education	1,711
government	793
Host type	Observations
organization	71,209
datacenter	60,574
isp_subscriber	34,579
unknown	26,639
shared_hosting	6,399

Service mix

Service class	Hosts
other	75,306
web_tls	44,288
web	20,191
ntp	18,432
imaps	9,742
panel	7,152
media_server	2,700
mail	2,648
adb	2,509
ssh	2,101
dns	1,807
mgmt	1,644
cwmp	1,635
ftp	1,442
pop3s	1,067
oracle	835
snmp	719
x11	524
isakmp	520
afp	375
iscsi	296
winrm_tls	280
pop3	209
redis	206
imap	202
proxy	193
mysql	191

pptp	188
printer	186
mongodb	178
rpcbind	176
rdp	141
rtsp	122
ajp	85
socks	82
postgres	76
k8s_api	76
msrpc	73
winrm	67
smb	59
ephemeral	55
kafka	52
openvpn	50
sip	47
mssql	43
amqp	39
vnc	38
finger	38
elasticsearch	36
modbus	35
mqtt	29
ldap	24
docker	22
salt	21
kibana	20
zookeeper	18
docker_tls	18
memcached	16
telnet	16
ldaps	15
ipp	14
mdns	11
nfs	6
wsdiscovery	5
netbios	4
ipmi	3
svn	1
upnp	1

Top operating organizations

Organization	Observations
Cloudflare, Inc.	14,909

Amazon Technologies Inc.	9,363
Amazon.com, Inc.	5,158
Bitly Inc	5,012
Wal-Mart Stores, Inc.	4,864
Google LLC	4,799
Microsoft Corporation	4,298
Egnyte Inc.	4,224
Metaverse Limited.	4,216
Linode	4,182

Method & compliance

Derived intelligence only: every record is a normalized, risk-classified host observation with network attribution. No raw capture payloads, no third-party raw records, no personal data. Fields: ip, asn/asn_org, isp, port, service_class, product/version, risk_flags, hostname/registered_domain, geo, ssl issuer/expiry, first_seen/last_seen. Delivery: Parquet or CSV snapshots (monthly) with weekly delta feeds; per-IP lookup API available on request. Licensed for security, attack-surface management, insurance analytics, and research use cases. Buyers must hold authorization for any domain they act on.

Generated 2026-10-23 18:32:15 UTC · source accounting verified: 199,400 lines read, 199,400 unique out, 0 duplicates dropped, 0 non-parsed