



# Soc- Analyst

## تحلیل گر مرکز عملیات

انور عبداللہ زادہ

فناوری اطلاعات و ارتباطات

پتروشیمی مہاباد



# Soc- Analyst

## تحلیل گر مرکز عملیات

### ساختار مرکز عملیات امنیت (SOC)

عنوان مرکز عملیات امنیت یا ( Security Operations Center ) SOC به یک واحد در یک سازمان اطلاق می گردد که به صورت متمرکز، تمامی رخدادهای حادثه یی و امنیتی مربوط به زیرساختهای حوزه فناوری اطلاعات و ارتباطات در سازمان را به صورت جامع و یکپارچه، شبانه روزی و بلادرنگ نظارت و مدیریت نموده و در صورت بروز هر گونه رخداد که برای سازمان ریسک ایجاد نماید، اقدامات مناسبی را جهت کاهش اثرات و رفع آن صورت می دهد.

در حقیقت ایجاد مرکز SOC، راهکاری مناسب جهت جلوگیری و مقابله با حوادث فضای سایبری می باشد.

# سطوح SOC

- ▶ Tier1: بصورت مداوم در همان لحظه در شبکه یا سازمان حملات سایبری/ رخدادهای را شناسایی و به Tier2 می دهد.
- ▶ Tier2: تشخیص کارشناس ۱ را تحلیل و بررسی می کند.
- ▶ Tier3: همان مدیر SOC است که صرفاً متخصص نیست و وظیفه ی آن مدیریت فرایندهای تهدیدات و نحوه ی چیدمان شیفت کارشناسان SOC
- ▶ مدیر تکنیکال: هیچ کاری با تحلیل و هک ندارد ، وظیفه ی آن طراحی و پیاده سازی بستر لازم جهت SOC
- ▶ **توانایی های SOC:**
- ▶ ۱- در لحظه ای که سیستم فعالیت مخرب داشت بایستی ببیند و متوجه شود.
- ▶ ۲- بروز بودن در زمینه انواع حملات در جهان ( چه حمله ای در حال حاضر بیشتر در جهان اتفاق می افتد)
- ▶ ۳- پاسخگویی و تحلیل حوادث
- ▶ ۴- اسکن سیستم های موجود جهت ارزیابی باگ
- ▶ ۵- تحلیل بدافزار و جرم شناسایی شده
- ▶ ۶- آگاهی سازی، مشاوره و آموزش (امنیتی) پرسنل

# فرایند SOC

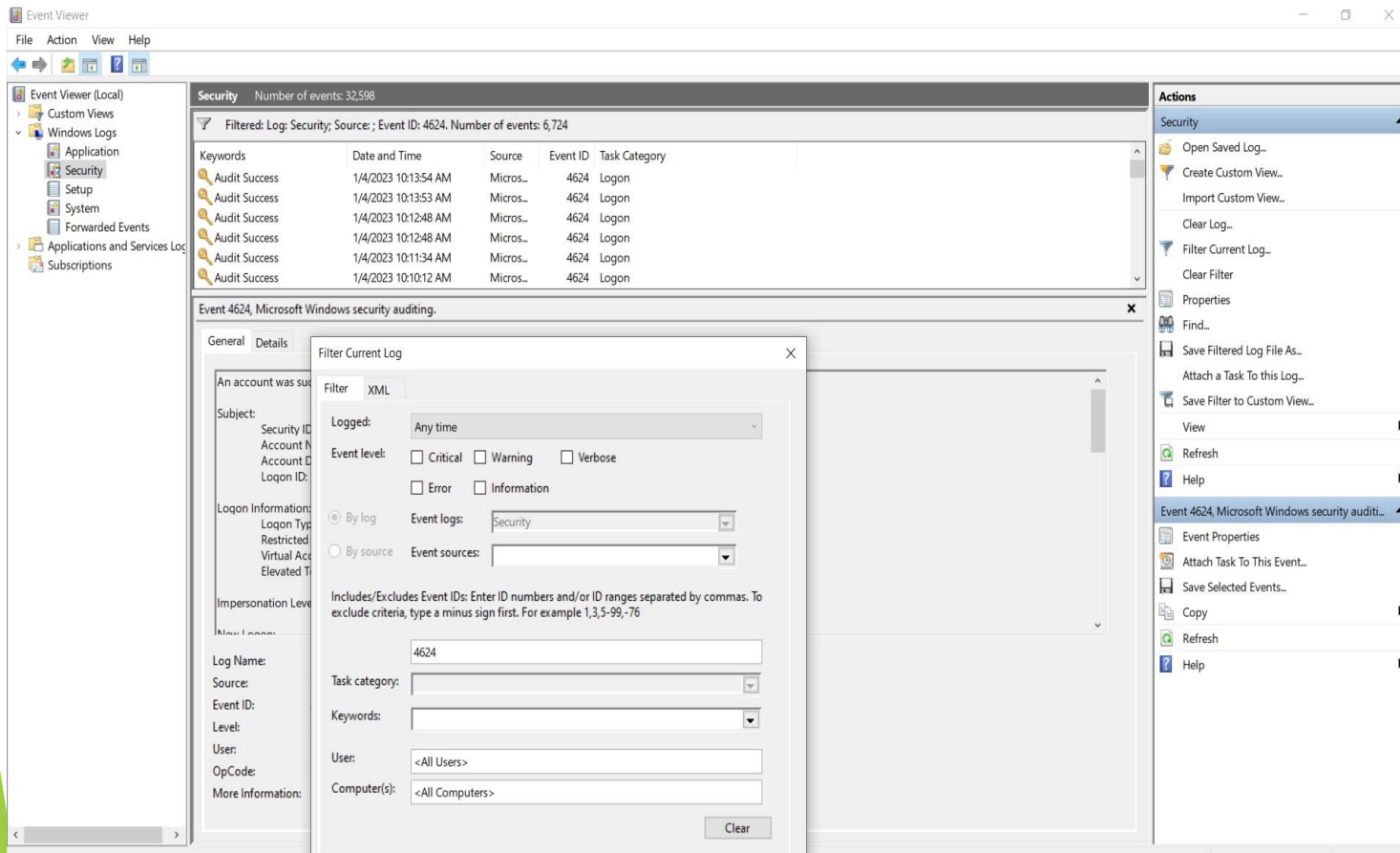
- ۱- شروع با جمع آوری لاگ ها
- ۲- بررسی و نشانه های حملات جدید در جهان
- ۳- با استفاده از دیتاهایی که داریم مدل های امنیتی جدید ساخته شود و دنبال تهدیدات سایبری باشد.
- ۴- تاثیری که مدل امنیتی روی سازمان می گذارد را تشخیص و به حداقل برسانیم.
- ۵- بصورت مستمر (۲۴ ساعته) فعالیت کند.
- ۶- وقایع شناسایی شده را گزارش و مستندسازی کند.

# چالش های SOC

- ۱- کمبود نیروی ماهر
- ۲- ابزار خوبی در دسترس هست ولی بصورت تخصصی نمی توانند استفاده کنند.
- ۳- معمولا دانش خوبی در این بخش ندارند..
- ۴- کمبود نیروی SOC

# Windows Log

جهت بررسی در هر سیستم در قسمت Event Viewer... Windows Log قابل مشاهده می باشد. ►



4625: Logon Field  
4624: Logon Success  
کیبورد 2  
3 از طریق شبکه  
4 Batch file  
5 سرویس ویندوز  
6 unlook

4778: remote desktop reconnected  
4779:remote desktop disconnected  
4647:user logoff  
4634:user login  
1100;system shutdown  
4720:user created  
1101/104:clear event

# SIEM

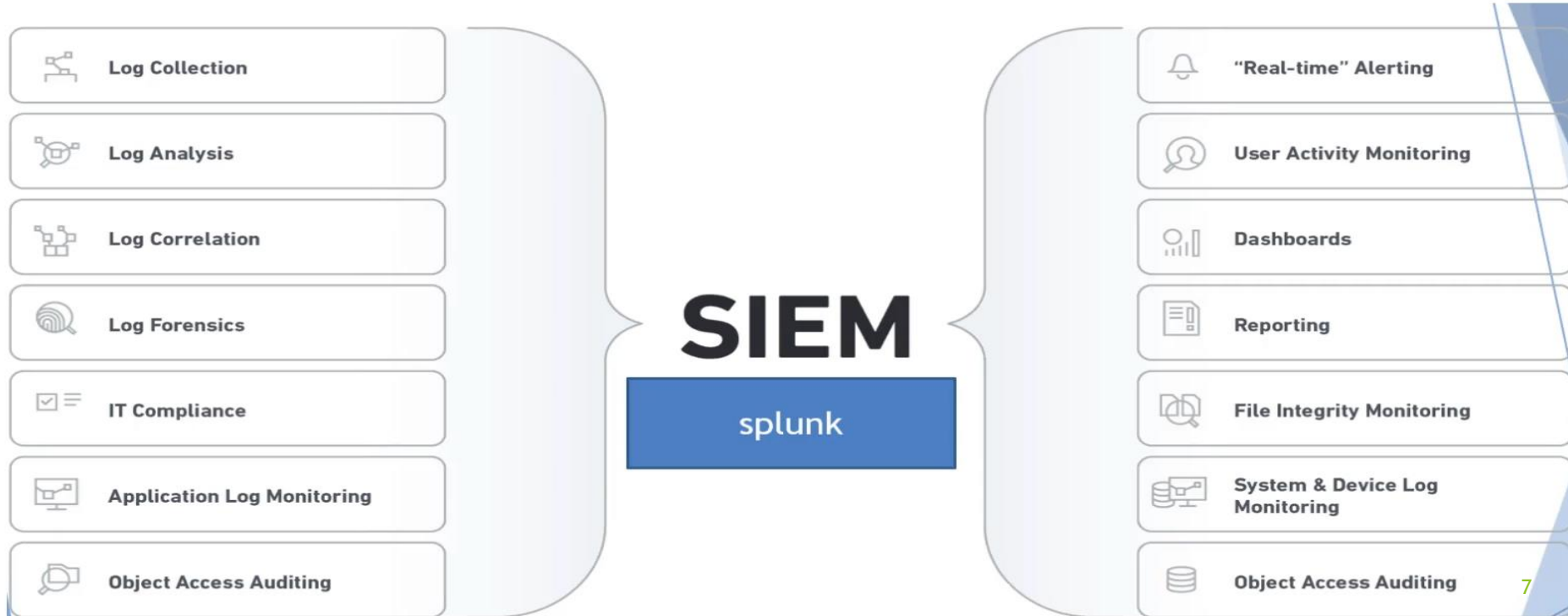
## Security Information Event Management

مجموعه ابزاری است که قابلیت مدیریت رخدادها و تحلیل و بررسی لحظه ای رویداد و رخداد را به ما می دهد. ▶



# What is splunk?

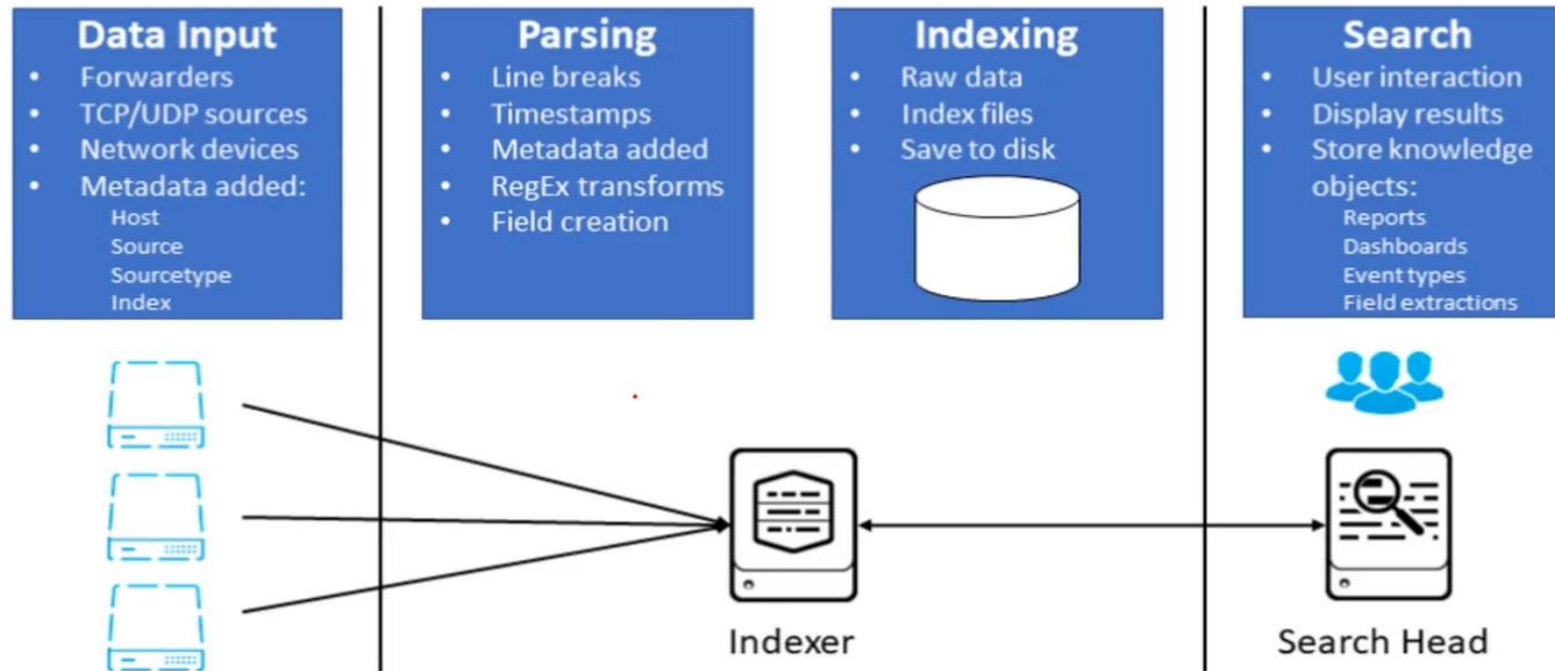
- ▶ Splunk ابزاری قوی از SEIM می باشد که جهت تحلیل Big Data ها استفاده می شود.
- ▶ همیشه بروز بوده و جز ۴ ابزار اول دنیا می باشد و گزارش گیری راحت و کامل را دارا می باشد.





# ساختار کار Splunk Enterprise

## Splunk Enterprise Data Pipeline





# نحوه کار با Splunk

۱- روی سیستمی که می خواهیم Log هایش را داشته باشیم ابزاری مانند Log Forwoder یا Sysmon نصب می کنیم.

۲- یک سرور جدا با حجم دلخواه (حجم بر حسب نیاز سازمان) راه اندازی می کنیم و Splunk را روی آن نصب می کنیم که Log های سیستم ها روی آن ارسال و ذخیره شوند. (Indexer)

۳- با استفاده از Splunk به تجزیه و تحلیل Log های ارسالی می پردازیم.

# نمونه از فایل Splunk

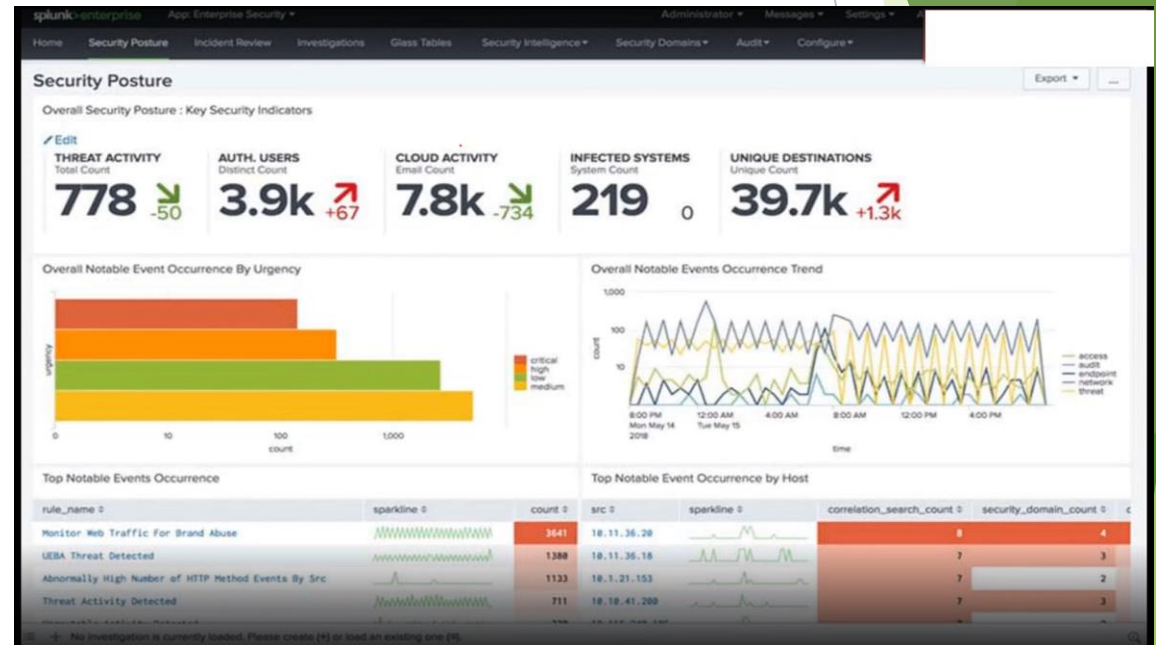
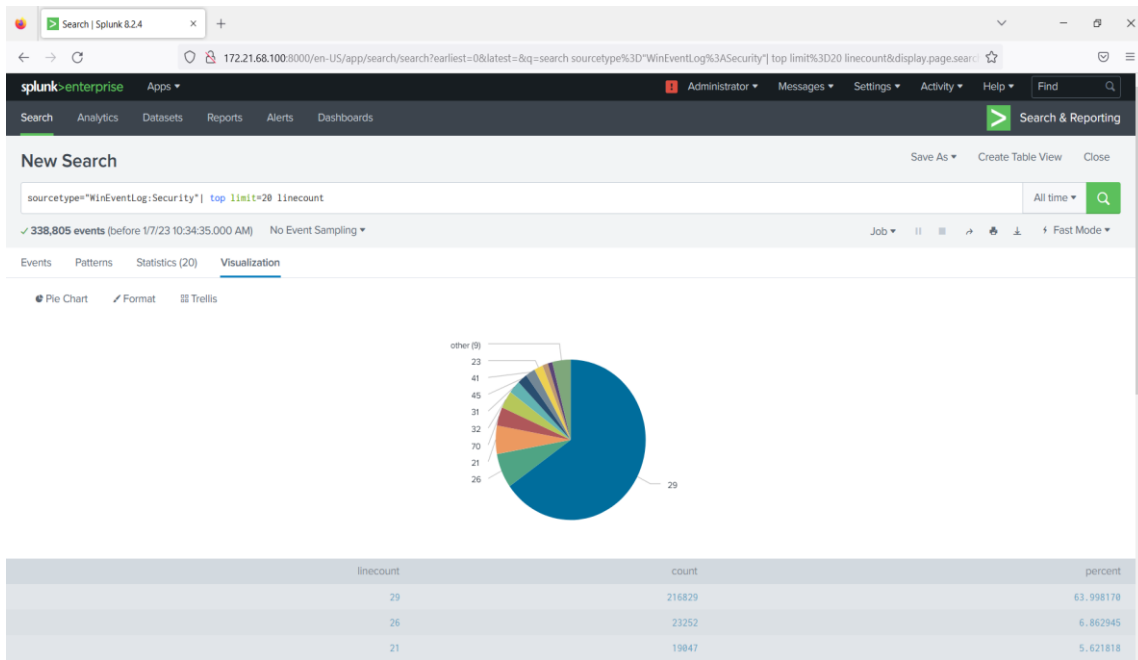
The screenshot shows the Splunk Data Summary window with the 'Hosts' tab selected. The table displays the following data:

Host	Count	Last Update
ICT5	93,869	1/7/23 10:44:26.000 AM
WNSERVER2019	306,473	1/7/23 10:44:27.000 AM

The screenshot shows the Splunk Data Summary window with the 'Sources' tab selected. The table displays the following data:

Source	Count	Last Update
PerfmonAvailable Memory	3,442	1/7/23 10:45:09.000 AM
PerfmonCPU Load	6,484	1/7/23 10:45:09.000 AM
PerfmonFree Disk Space	18	12/11/22 12:45:34.000 PM
PerfmonNetwork Interface	13,185	1/7/23 10:45:09.000 AM
WinEventLogApplication	15,714	1/7/23 10:43:09.000 AM
WinEventLogSecurity	342,225	1/7/23 10:45:08.000 AM
WinEventLogSetup	116	12/7/22 9:23:31.000 AM
WinEventLogSystem	19,354	1/7/23 10:43:10.000 AM

# گزارش گیری و داشبورده سازی



## New Search Save As Close

index=botsv\* sourcetype =linux\_secure "invalid user" OR "Failed password" All time Q

27,344 of 54,355 events matched No Event Sampling Job [Controls] Verbose Mode

Events (27,344) Patterns Statistics Visualization



Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

List Format 20 Per Page < Prev 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields	All Fields	i	Time	Event
SELECTED FIELDS		>	8/29/17 4:11:32.000 AM	Aug 29 11:11:32 eridanus sshd[27380]: Failed password for root from 116.31.116.17 port 48585 ssh2 host = eridanus source = /var/log/secure sourcetype = linux_secure
a host 2		>	8/29/17 4:11:31.000 AM	Aug 29 11:11:31 eridanus sshd[27378]: Failed password for root from 116.31.116.17 port 47411 ssh2 host = eridanus source = /var/log/secure sourcetype = linux_secure
a source 1		>	8/29/17 4:11:30.000 AM	Aug 29 11:11:30 eridanus sshd[27380]: Failed password for root from 116.31.116.17 port 48585 ssh2 host = eridanus source = /var/log/secure sourcetype = linux_secure
a sourcetype 1		>	8/29/17 4:11:29.000 AM	Aug 29 11:11:29 eridanus sshd[27378]: Failed password for root from 116.31.116.17 port 47411 ssh2 host = eridanus source = /var/log/secure sourcetype = linux_secure
INTERESTING FIELDS				
# date_hour 12				
# date_mday 5				
# date_minute 60				
- date_month 4				

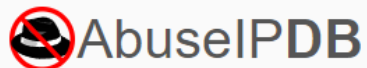




Check an IP Address, Domain Name, or Subnet  
e.g. 80.191.215.194, microsoft.com, or 5.188.10.0/24

80.191.215.194

CHECK



making the internet safer, one IP at a time

Report abusive IPs engaging in hacking attempts or other malicious behavior and help fellow sysadmins!

REPORT IP NOW

Check the report history of any IP address to see if anyone else has reported malicious activities.

Check IP or Domain



Use our powerful free API to both report abusive IPs and instantly check if an IP has been reported!

REGISTER NOW FOR API KEY

#### What is AbuseIPDB?

AbuseIPDB is a project dedicated to helping combat the spread of hackers, spammers, and abusive activity on the internet.

Our mission is to help make Web safer by providing a central blacklist for webmasters, system administrators, and other interested parties to report and find IP addresses that have been associated with malicious activity online.

You can [report an IP address](#) associated with malicious activity, or check to see if an IP address has been reported, by using the search box above.

Power user? Consider [registering an account](#) to gain access to our [powerful, free API](#) for both reporting and checking the report status of IP addresses. We also support [integration with Fail2Ban](#) for automated reporting of abusive IPs.

Please read our [FAQ](#) to learn more about AbuseIPDB!

#### Recently Reported IPs:

114.219.173.1  
 202.95.12.121  
 119.99.229.73  
 79.174.186.163  
 39.101.206.176

76.189.178.105  
 61.177.173.35  
 137.184.77.74  
 159.203.240.18  
 23.105.201.79

180.245.35.188  
 188.170.13.225  
 43.156.7.128  
 15.223.33.75  
 221.141.253.208

180.168.111.34  
 192.241.224.12  
 123.145.84.189  
 176.94.150.90  
 175.10.32.32

© 2023 AbuseIPDB. All rights reserved. [View IP List](#). Usage is subject to our [Terms and Privacy Policy](#).

Support AbuseIPDB - donate Bitcoin to [1DqaKKSh6d31GqCTdd4LGHeraqHFv9CmTN](#)

[Blog](#) | [About Us](#) | [Frequently Asked Questions](#) | [API \(Status\)](#) | [Donate](#)



ممنون از اینکه همراه ما بودید  
لطفاً نظرات خود را با ما در میان بگذارید.

04431931256

aabdollahzadeh@mapc.ir