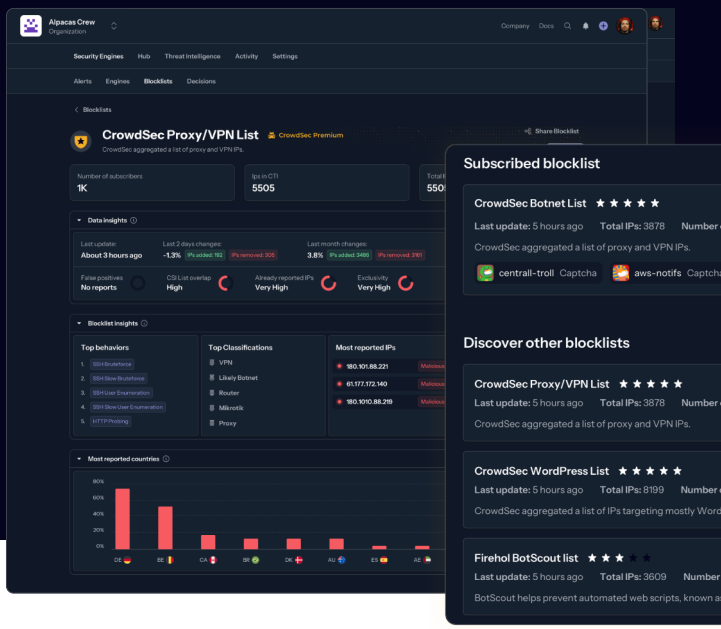
CrowdSec

CrowdSec Curated Threat Intelligence & Blocklists

"We have eliminated between 40% and 50% of the background noise, saving two FTEs worth of time in incident response." Crédit Mutuel Arkéa

"CrowdSec has 36% exclusive information compared to all other CTI sources." VirusTotal



The Difference between Suspicious and Malicious Is Proactivity

Discover a new breed of security blocklists powered by a uniquely diverse global CTI network of hundreds of thousands of production servers detecting more than 10 million potential threats daily.

Try it yourself! Book a demo and get our top 250K IPs for free for the first month.

Yes, CrowdSec Curated Threat Intelligence Is Unique

30% of malicious IPs we proactively block are unknown to any other vendor for at least one week

50% of malicious IPs in our database are known to a maximum of 3/92 threat intelligence vendors

15-20% of malicious IPs we proactively block never appear in any other blocklist

7-60 days ahead of all other security blocklists and threat intelligence vendors in blocking malicious ingress IPs

12M MITRE-Classified IoC Processed/Day

50M IP Tracked from over 3000 AS and 185 Countries

5% Daily Rotation on Average

30 Info Fields per IP Address

I Need Maximum SOC Efficiency

Internet background noise makes it hard to identify targeted attacks and generates alert fatigue for the team.
Proactively block attacks from reaching your applications and pollute your logs.

I Need to Be Prepared

Blocking IPs known for scans, brute force, CVE, XSS, SQLi exploitation, and other attacks is an efficient virtual patching strategy.
Proactively block security vulnerability exploitation attempts until you patch or find a workaround.

I Need to Reduce My Costs

Answering undue malevolent requests has a non-zero impact on your IT resources, team, and SIEM costs while it generates zero business value.
Proactively block those known malicious IPs to reduce your server, egress, and SIEM costs.

"Overall, we witnessed a reduction of 15% of our SecOps time, 60% of SIEM costs, and 20% of our web server resources."

Crédit Mutuel ARKEA

Compatible with Your Existing Infrastructure

Our blocklists are made to be consumed natively by most firewalls, reverse proxies, CDNs, cloud protections, and load balancers.

Features & benefits:

Key Features	Key Benefits
Real-Time Updates: Premium Blocklists are continuously updated, ensuring immediate protection against new and emerging threats. This approach allows for the rapid dissemination of crowd-powered intelligence across the network, enabling your defenses to adapt as quickly as cyber threats evolve.	Instant Protection from Emerging Threats: When a major vulnerability like Log4j is disclosed, mass exploitation starts within a few hours. Our Network Effect only takes a few minutes before it can broadcast the IP from aggressive attackers, preventing them from even scanning your environments and giving you time to patch.
Precision and Reliability: Leveraging advanced analytics, the Network Effect, and AI, CrowdSec Blocklists offer an exceptional accuracy rate with no false positives. This precision ensures that your operations remain uninterrupted, enhancing your overall security posture without sacrificing operational efficiency.	Enhanced SOC Efficiency: CrowdSec Blocklists enable SOC teams to operate more efficiently by reducing alert fatigue, improving response times, and enabling the allocation of strategic resources toward real threats. Now you can focus your efforts on targeted attacks that deserve your full attention.
Background Noise Reduction: Whether you are a startup or a Fortune 500 company, internet background noise accounts for 62% of your alerts on average. It consumes resources, human time, and SIEM budget. Proactively blocking this noise considerably reduces these costs.	Significant Cost Saving: Stop wasting resources on replies to undue queries, incident response, and recovery. Reduce your operational costs as the need for additional security measures and the associated overheads is significantly diminished.
Data Curated by the Network Effect: The collaborative part of CrowdSec builds a global, crowd-powered CTI network. When an attack is detected locally, the targeted machines share meta information with CrowdSec, which we curate at scale to update the blocklists constantly with more than 30 fields of contextualized information per IP.	Community-Powered Security Insights: A wealth of shared knowledge and insights further enhances your security measures. This collaborative approach not only improves your defensive capabilities but also contributes to a safer digital environment for all. Premium customers benefit from crowd-powered data without the need for a Security Engine.

Explore Our Specialized Blocklists or Create Your Own Using Our Data

1. Sign up for CrowdSec Console at app.crowdsec.net
2. Generate a CrowdSec CTI API key
3. Use our blocklists in your firewall or CDN

Do you want to block IP addresses specifically targeting authentication endpoints against your country over the last month? Your game, your rules.

Trusted by

crowdsec.net info@crowdsec.net CrowdSec