



Outnumbering cybercriminals all together





CrowdSec helps you be proactive

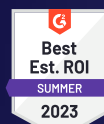
Introducing CrowdSec

CrowdSec is a modern, collaborative cybersecurity company committed to proactively safeguarding your digital assets. With its open source software developed for the SOC and DevSecOps community, CrowdSec is revolutionizing cybersecurity by capitalizing on collective intelligence to detect and mitigate emerging and targeted threats in real time.

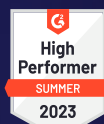
With a growing community of 65,000+ active installations contributing to a robust, constantly updated global IP reputation database, the CrowdSec Security Engine offers an unprecedented layer of security, transforming individual experiences into collective knowledge. This collaborative approach empowers every user and provides an evolving defense against cyber threats.



Threat
Intelligence



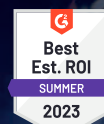
Threat
Intelligence



Threat
Intelligence



Intrusion Detection &
Prevention Systems



Intrusion Detection &
Prevention Systems



Why is CrowdSec unique?

CrowdSec is the ultimate prevention tool to protect your exposed workloads. Contrary to post-intrusion tools like SIEM, CrowdSec provides a proactive response before an intrusion takes place.

CrowdSec helps you maintain your security stance over time and constantly adapt to emerging threats. As soon as an IP address is attempting exploitation and is detected by a member of the CrowdSec community, the collective intelligence kicks in. If enough trusted peers in the CrowdSec network validate they witnessed the same signals, the response is an immediate ban of the aggressive IP for all members. This attacker will never again be able to crack down and penetrate an infrastructure or deposit ransomware using this IP. Forcing the attacker to move to another IP loses them money and time, one being a function of the other, and the CrowdSec network organizes the shortage of this precious supply, choking their automated operations.

Since every part of the process is fully automated and API-driven, it offers a seamless way of maintaining a security posture and prevents decay over time.

Your company will be attacked, but CrowdSec helps you be proactive.

“ Since the implementation of CrowdSec on our entire information system at Crédit Mutuel Arkea in 2021, the solution has helped us block countless waves of brute force attacks on the group’s subsidiaries. Today, we use it to build business-oriented models with detection approaches specific to different applications. We also plan to use the solution to detect cross-functional attacks within our information system.”

Guillaume Roussel – Operations Manager in charge of IS security at Crédit Mutuel Arkea

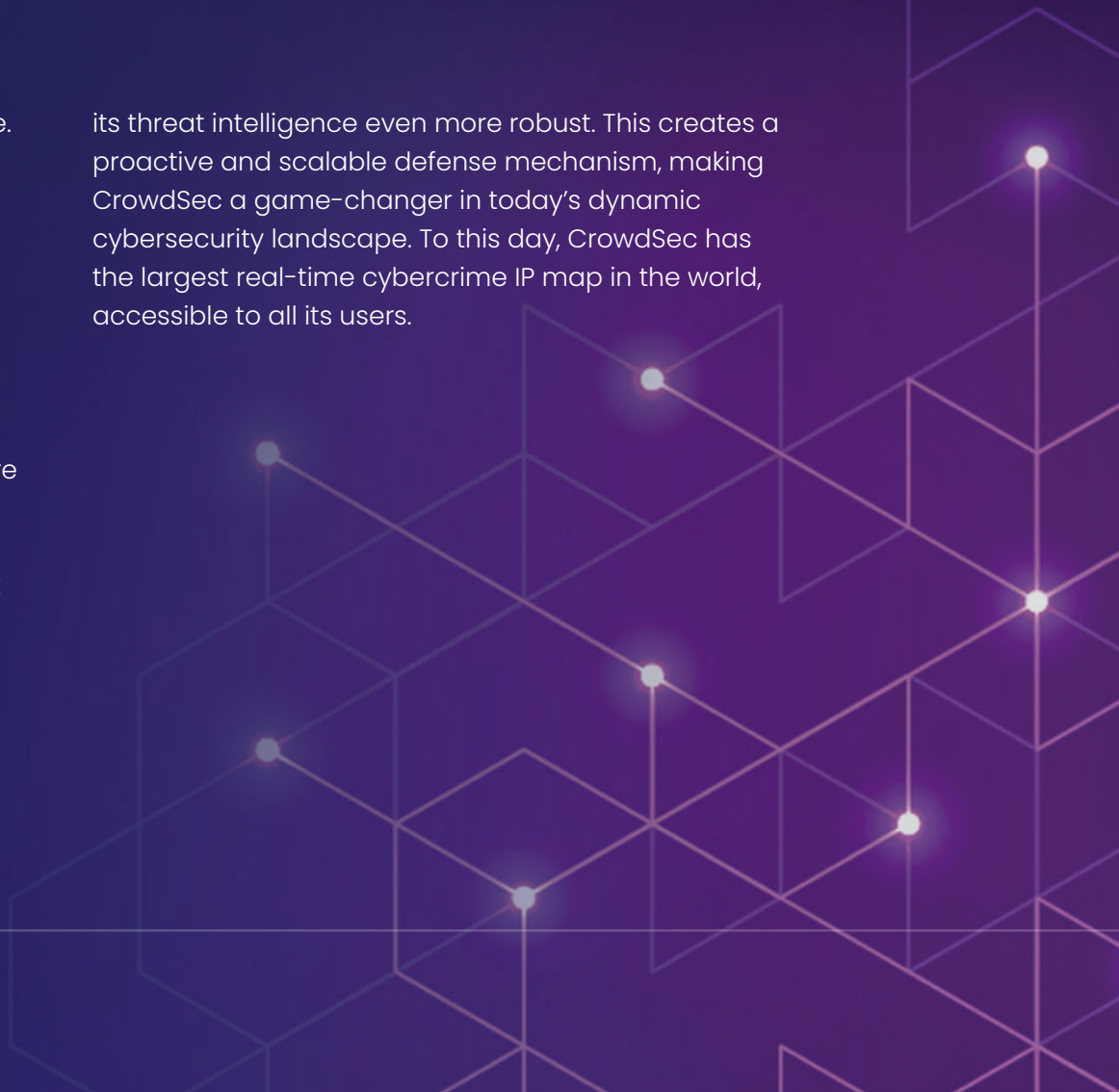


How CrowdSec works

The efficiency of CrowdSec lies in its simplicity and scale. As an adaptive behavior detection and remediation system, it operates by analyzing user behavior in OS, servers, and applications logs, identifying malicious patterns, and responding accordingly. Regardless of where your logs live — the cloud, on-prem, in a SIEM, or on a Windows, BSD, or Linux environment — they can be ingested. When CrowdSec detects a threat from a specific IP, it swiftly applies remedial measures, such as blocking the IP, sending a CAPTCHA, activating Cloudflare attack mode, alerting you, slowing down the traffic, etc.

These actions not only safeguard the local environment but, through the power of collective intelligence, also benefit the wider CrowdSec community. The identified IP is shared with the CrowdSec consensus system, and included in a global blocklist if validated, enhancing security posture for all users. CrowdSec continuously evolves with each new attack pattern detected, making

its threat intelligence even more robust. This creates a proactive and scalable defense mechanism, making CrowdSec a game-changer in today's dynamic cybersecurity landscape. To this day, CrowdSec has the largest real-time cybercrime IP map in the world, accessible to all its users.



CrowdSec products

Our products are tailored to meet your diverse security needs.

1>

CrowdSec Security Engine: This open source and lightweight software identifies malicious behavior and shares the related IP across the network, instantly protecting all users from the identified threat. Coded in Golang, it uses marginal resources and can be deployed in any environment — containers, on-prem, cloud, or hybrid. CrowdSec provides its users with a hub of numerous analysis, detection, and remediation components to quickly and easily integrate the solution with the various elements of the security infrastructure.

2>

CrowdSec Console: The CrowdSec Console is a centralized dashboard providing insight into your security events. It offers real-time visibility into threat detection, mitigation, and IP reputation, and oversees multiple CrowdSec Security Engine installations, giving an aggregated macro overview of all your exposed workloads. Detailed analytics and metrics provide SOC managers and CISOs with actionable intelligence to further strengthen security defenses.

3>

CrowdSec CTI: CrowdSec's Cyber Threat Intelligence is a force multiplier for SOC teams providing exhaustive, diverse, and precise intelligence on malicious IPs. The dynamic and global insights of the CrowdSec CTI enable the swift detection and neutralization of threats. With its proactive mechanism to pre-empt attacks and adapt in real-time to emerging threats, enterprises gain an edge in cybersecurity. With the API interface, users have access to a set of granular information including Autonomous Systems, country of origin, aggressiveness, and the types of attacks performed by an IP. The blocklist is just 0.3% of CrowdSec's data — the larger data lake can be accessed through our API or locally synchronized to use with any CTI tool.

Benefits of the **enterprise plan**



Crowdsourced — Throwing money at the cybersecurity problem has been proven ineffective. Attempts to outsmart cybercriminals were also met with marginal success. CrowdSec's goal is to outnumber cybercriminals, which is factually doable with a ratio of 10000:1 in our favor.



Open source — Proprietary software is audited less than open source components, leading to potential private exploits. Also, if your use case requires adaptation, it's easier to make it happen in half the time when using open source.



Proactive defense mechanism — Instead of merely reacting to threats, CrowdSec's solution empowers your security posture to be proactive, preemptively blocking threats before they can impact your systems. It prevents your security stance from decaying over time by enforcing proper cybersecurity hygiene.



Behavior-based — Signatures tend to be one step behind. Hashes vary. Binary analysis can have a hard time with obfuscation. Domain names can be relocated and are in infinite numbers. Behavior, however, leaves trails in logs and those trails allow us to counteract attacks, even on-logic standpoint, and not just based on a pure exploitation approach. As an example, bot scalping an e-commerce website won't trigger any EDR but their behavior is easy to spot.



Actionable — The main difference between a real-time, zero-false-positive, crowd-curated blocklist and a CTI feed is that the former can be operationalized directly in a firewall. The information allows you to know — actionable blocklists allow you to remedy.



Versatile — Continuous Integration and Continuous Delivery is part of our DNA. That is why we designed CrowdSec to be fully integrated, operational 24/7, and a means for reducing the admin burden.

Benefits of the **enterprise plan**



Real-time threat intelligence — Benefit from immediate and real-time shared intelligence about threats detected across the globe, ensuring the highest level of protection.



Scalable security — CrowdSec products are designed to scale and adapt to your business growth, making them ideal for enterprises of all sizes.



Seamless integration — CrowdSec's solutions are compatible with most platforms and systems, making integration with your existing security infrastructure effortless.



Cost-effective — One size does not fit all. Instead of paying for a standard Enterprise plan, CrowdSec allows you to pay as you grow your business, and scale up and down according to your specific needs. The CrowdSec pricing plan is based on the size of the business and the data it protects against attackers and ransomware groups.

**CrowdSec
products are
designed to
scale and adapt
to your business
growth**



● Outnumbering cybercriminals all together

Secure your digital landscape today with CrowdSec, the cutting-edge cybersecurity solution designed for the modern enterprise. Embrace the power of collective intelligence and protect your systems against cyber threats because together, we are stronger.

Try the CrowdSec Security Engine today! Installation takes five minutes, it is non-intrusive and shows immediate results. We will be happy to assist you if needed.

For more information, visit www.crowdsec.net or contact us directly at www.crowdsec.net/contact-crowdsec to arrange a demo or discussion for your specific business requirements.





Embrace the power of collective intelligence and protect your systems.

Want to make the internet a safer place?

Try the **CrowdSec Security Engine** today!



github.com/crowdsecurity



[@Crowd_Security](https://twitter.com/Crowd_Security)



[CrowdSec](https://www.linkedin.com/company/crowdsec)



[@crowdsec6295](https://www.youtube.com/@crowdsec6295)



crowdsec.net



academy.crowdsec.net