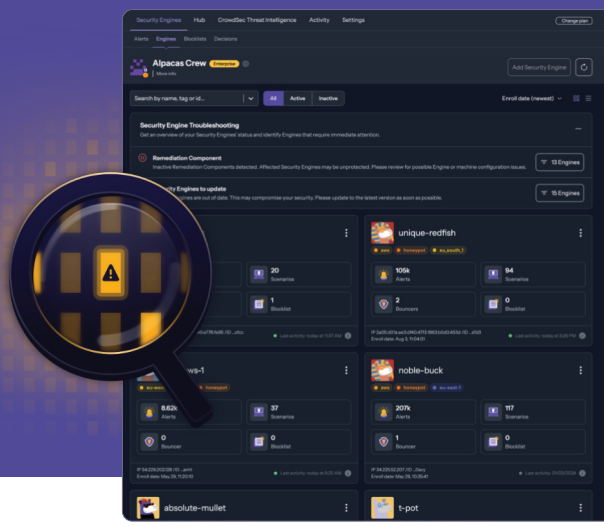
CrowdSec

The CrowdSec Security Stack

Protect against Targeted Attacks with CrowdSec's Behavior-Based IDPS & WAF

Reduce SOC time by 15%, cloud egress costs by 20%, SIEM costs by 40%, and background noise by up to 80%. Try it for free.



Intrusion Protection with the CrowdSec Security Stack

CrowdSec Security Stack is a combination of two components. Our renowned ultra-low footprint FOSS Security Engine detects suspicious behaviors in any log source and acts as an all-in-one IDS/IPS and WAF. Combining it with the CrowdSec Console provides a clustering effect capable of detecting complex attacks over your entire internet-exposed perimeter. Those two components work hand in hand to offer advanced detections, centralized configurations, data retentions, and deployment industrialization.

I Need to Protect Exposed Applications

Proactively block targeted attacks and mass exploitation attempts to protect your applications or even virtually patch the vulnerable ones.

I Need Maximum SOC Efficiency

Internet background noise makes it hard to identify targeted attacks. Suppress noise sources like scans, brute force, and mass-exploitation attempts from your security alerts to maximize efficiency and reduce risks.

> *"Log4J was virtually patched in 15 minutes and 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

DevOps Approved, SecOps Acclaimed!

Protecting More Than 250,000 Workloads

Tens of Millions of Attacks Processed Daily

50M IPs Tracked from over 3000 AS and 185 Countries

Nearly 500 Scenarios and Rules to Deter 10+ Types of Cyber Attacks

- Scans (Web/Ports/VOIP)
- Botnets (L7 DdoS, etc.)
- Credentials (Brute-forcing Reuse)
- Stuffing (Credit card, credentials)
- Bots (Scropping, scalping, etc.)
- CVE exploitation (SQLi, overflows, XSS, etc.)
- Policy violations
- Impossible traveler
- Application-level (Injections, scripting, etc.)

Meet Our Collaborative and FOSS Security Engine

Behavioral Detection

With hundreds of attack scenarios, the CrowdSec Security Engine identifies exploitation attempts targeting your infrastructure and applications.

Automated Protection

Leverage the Security Engine detection and remediation in your existing firewall, load balancer, reverse proxy, CDN, or web server to block aggressors.

Proactive and Collaborative Security

Your filtering devices receive curated, zero-false-positive blocklists to proactively block dangerous IPs, ensuring they never reach your servers.

Production Environments Need Enterprise-Level Security. Explore the CrowdSec Security Stack

Key Features	Key Benefits
Enhanced Visibility and Monitoring: Gain deep insights into unusual attack patterns or IPs probing your exposed perimeter. Manage your Security Engines with a unified control panel, focus on what matters, and leverage our premium blocklists.	Improve Your Detection Capabilities: Combining advanced behavior detection and collective wisdom from the Network Effect, eliminate threats targeting your systems before they reach your applications and possibly gain access to sensitive data.
Alert Context: Get an unprecedented level of detail about the triggers behind every security alert to swiftly react to any threat targeting your infrastructure or your web applications. Fine-tune to suppress any noise and to highlight what is really dangerous.	Protect Your Security Perimeter: Effortlessly counter and analyze complex attack behaviors, such as scalping, credential stuffing, impossible travel, and more, as well as other well-known attacks, including DDoS, brute force, CVE exploitation, and XSS attacks.
Real-time Decision Management: Automate and graduate your response to security events on any part of your infrastructure. MFA, HTTP notification, BGP sinkhole, Block, 403, CAPTCHA — it's your call.	Unify Your Security Response: Protect your workloads, wherever they are deployed, on-premise or in the cloud, with the same level of security and tailored response.
Background Noise Filtering: Proactively block mass exploitation attempts that constitute the internet background noise, which accounts for up to 80% of overall security alerts.	Improve Your SOC Efficiency: Reduce background noise in your security logs to focus on real threats, reduce alert fatigue, store fewer log lines in your SIEM, and improve your overall response time.
Premium Blocklists: Unlock the full potential of the Security Engine with the Premium Blocklists to enable top-notch proactive protection based on ultra-curated data collected by the CrowdSec Network of 70,000+ active Security Engines, deployed on real servers and in real production environments.	Community-Powered Security Insights: Gain access to a wealth of shared knowledge and insights, further enhancing your security measures. This collaborative approach to cybersecurity not only improves your defensive capabilities but also contributes to a safer digital environment for all.

Compatible with Your Existing Infrastructure

ELK, aws, Azure, Linux, Windows, FreeBSD, paloalto NETWORKS, FORTINET, CISCO, CLOUDFLARE, CHECK POINT, NGINX, APACHE HTTP SERVER PROJECT, træfik proxy, and more

Leverage the power of the crowd to enhance your application and infrastructure security every step of the way with the CrowdSec Security Stack.

Trusted by

Google for Startups, Deloitte., PARIS 2024, Le Monde, Crédit Mutuel ARKEA, Ministère des Affaires sociales et de la Santé, as software, https://scale.sc commerce, DOCAPOSTE

crowdsec.net info@crowdsec.net CrowdSec