Solution Brief

Security Operations Center (SOC) as a Service

Separating the signals from noise

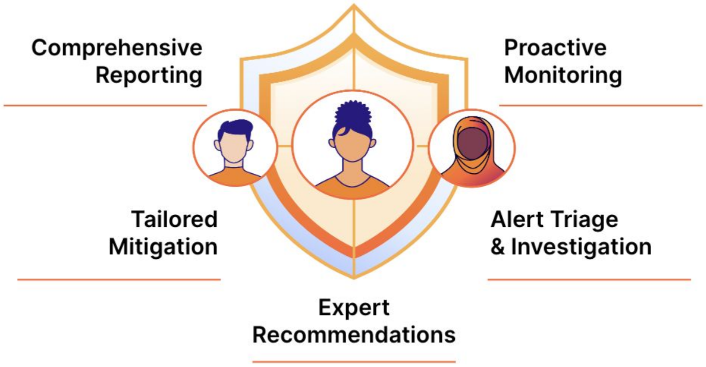
Decrease Threat Complexity & Exposure Risk

In today's complex digital world, legacy perimeter infrastructure coupled with the ever expanding threat landscape, can leave organizations struggling to separate signal from noise. Which alerts and incidents are false positives, and which require investigation? And which new aspects the threat landscape represent the biggest risk to the organization?

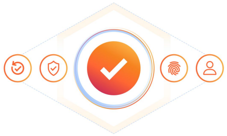
Cloudflare's SOC-as-a-Service combines our award winning security products with our dedicated team of cybersecurity experts that monitor your enterprise environment for security threats and potential operational disruptions; perform deep analysis to identify attack vectors, and implement countermeasures to mitigate incidents. Service highlights include:

- Direct access to Cloudflare SOC team
- Security incident response SLA of <30 mins
- Global, 24/7/365 protection
- Summary reports delivered on recurring basis

Cloudflare SOC Service

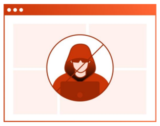


Cloudflare's SOC-as-a-Service team ensures time-sensitive incidents are properly triaged, investigated and remediated. Cloudflare SOC proactively communicates regarding events and provides recurring reports with attack summaries and network incidents.



Achieve Consistency

Cloudflare SOC team follows programmatic threat monitoring and response process - bringing immediate consistency across incident triage, investigation, and remediation.



Respond with Confidence

Identify suspicious activity with high confidence, leveraging threat intelligence across Cloudflare's massive network, which runs 20% of the world's internet traffic.

Protect Against Burn Out

The service includes offloading routine, administrative tasks, enabling lean security teams to focus on higher priority, strategic needs. Including wading through false positives and providing weekly/monthly reports of threats, rules created, log retention, attacks.

SOC Service Features & Supported Products	SOC for Core Applications	SOC for Network
Proactive Monitoring & Alerting for Anomalous Events	✓	✓
Custom Rules to Mitigate Active Attacks	✓	✓
Summary Reporting	✓	✓
Layer 7 Attack Analysis and Mitigation	✓	
Layer 3 & 4 Network Attack Analysis and Mitigation		✓
RE Tunnel Health Check Monitoring		✓
Supported Products	• DDoS • Rate Limiting • WAF	• Magic Transit

**Bot Management* *is supported reactively for mitigating an attack by the Cloudflare SOC. There is no specific alert available for this product.*

Cloudflare Alerting Innovation & Scale

Cloudflare's alerting technology leverages advanced proprietary algorithms rather than simple threshold-based triggers. These high-fidelity alerts give the SOC team confidence to react and respond decisively in near real-time. Cloudflare's SOC-as-a-Service experts ensure that time-sensitive incidents are properly triaged, investigated and remediated. Cloudflare SOC team proactively communicate regarding events and provide regular detailed reports on attacks and network incidents.

Cloudflare's network spans 200+ cities globally, and more than 1 billion unique IP addresses pass through it every day. This diversity and scale provides unique intelligence that enables Cloudflare's SOC team to identify suspicious activities across the network with high confidence.

Want to learn more about our SOC service? Contact your Cloudflare representative today.

About Cloudflare

Cloudflare is unifying network, application, and security solutions to transform organizations and power the future of the Internet.

See why Cloudflare is recognized over 60 times by the top analysts firms such as Gartner, Forrester, and IDC.