DATASHEET

CLOUDFLARE

Cloudflare's Security Operations Center (SOC) as a Service

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

The Noisy Threat Landscape

In today's digital world where cyberattacks have become common and networks have become complex, even the most attentive organizations can struggle to separate signal from noise. Which alerts and incidents are false positives, and which require investigation? And which new aspects of the ever-evolving threat landscape represent the biggest risk to the organization?

The network complexity resulting from heterogeneous environments and an outdated "perimeter" model of infrastructure now leaves organizations with an assortment of siloed security and performance monitoring tools. Security and IT teams are caught in the rut of translating logs, alerts and policies between environments, leading to costly, inefficient and error-prone operations.

In addition to increasing organizations' attack surface and risk of exposure, all of this complexity can quickly lead to alert fatigue and burnout, and prevent organizations from focusing on new growth opportunities.

Cutting Through The Noise: Cloudflare's SOC-as-a-Service

Cloudflare's SOC-as-a-Service combines our award winning security products with our dedicated team of cybersecurity experts that monitor your enterprise environment 24×7×365 for security threats and potential operational disruptions; perform deep analysis to identify attack vectors, and implement countermeasures to mitigate incidents.

Cloudflare's SOC-as-a-Service is designed to meet the security monitoring, threat detection and incident response needs of enterprises of all sizes and sophistication, across Layer 3, Layer 4, and Layer 7. Since the earliest indicators of security incidents can sometimes appear as degraded application or network health, proactive alerting for origin reachability, availability and latency is performed. This not only provides visibility into the overall health of the network but also acts as a proactive defense against network disruptions and failures.

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 SOCteam to identify suspicious activities across the network with high confidence.

Benefits of Cloudflare's SOC-as-a-Service

24×7×365 protection

Cloudflare security experts continuously monitor and respond to security threats before they become critical events.

Faster detection and remediation

Tailored mitigation and configuration by the SOC team, helps reduce lapse time between when an incident occurs, when it is detected, and when it is mitigated.

Proactive communication and reporting

Proactive communication through various channels — including phone, email and webhook — when there is a traffic anomaly or when the network is under attack. Periodic reports on rules created and attacks blocked, with recommendations on configuration changes.

Reduced overall security costs

Cloudflare's SOC reduces the need to employ and train in-house security specialists for monitoring and responding to alerts, thereby shrinking overall security spend.

Quick and easy start

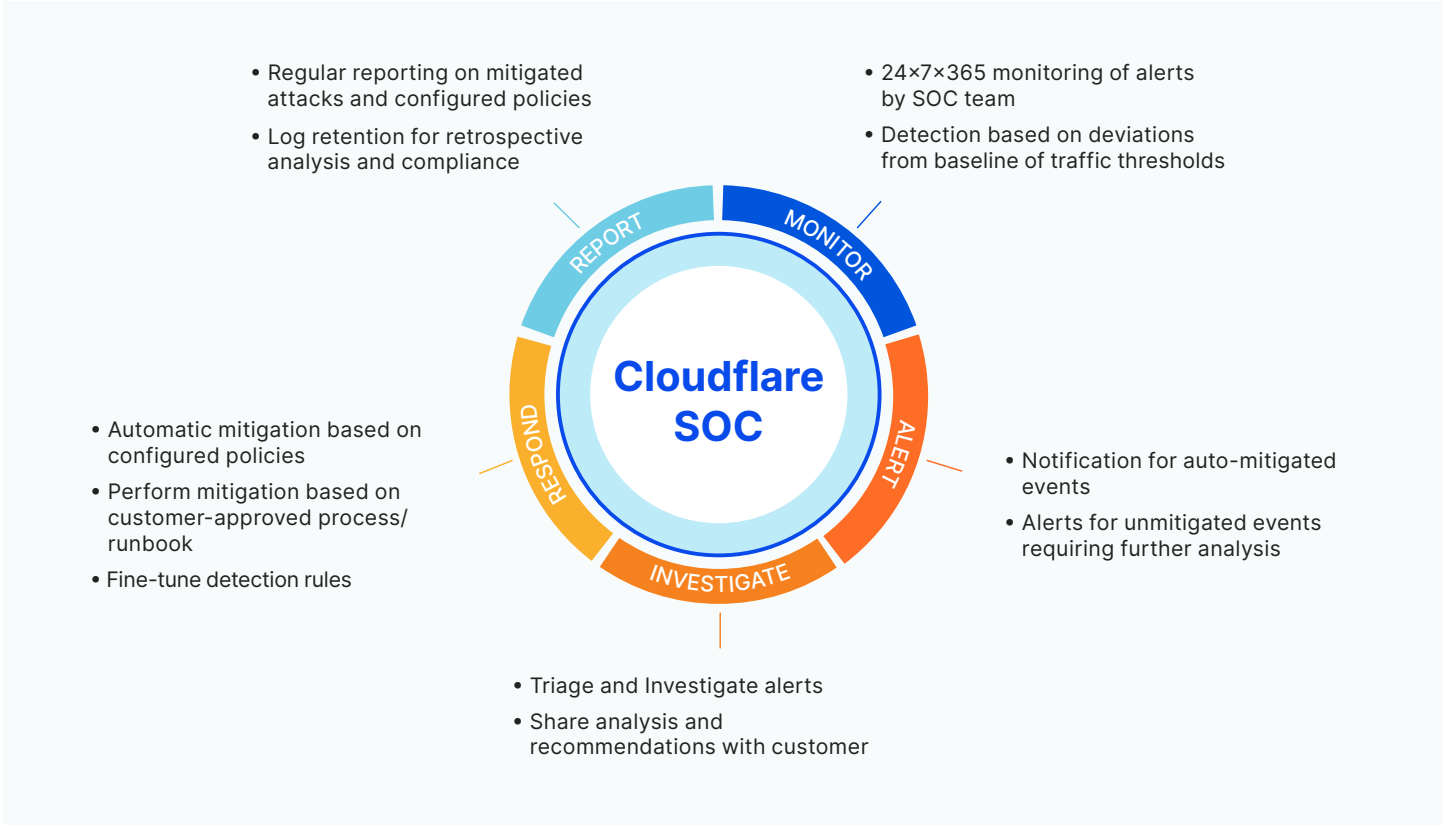
Getting to a baseline SOC configuration is quick and simple. Enabling the SOC service doesn't require deploying any additional endpoint agents or tools.

Offloading security to Cloudflare experts

Your security team no longer has to wade through the false positives and can focus on other priority projects, thanks to Cloudflare security experts who immediately identify any suspicious activity and swiftly respond with recommendations for resolution.

Monthly/Quarterly reports

Our SOC team will provide regular reporting to share insights into the Cloudflare protections mitigating security threats.



Service Options

	SOC for Core Applications	SOC for Network
Proactive Monitoring and Alerting for Anomalous Events	✔	✔
Custom Rules to Mitigate Active Attacks	✔	✔
Reporting	✔	✔
Layer 7 Attack Analysis and Mitigation	✔	✕
Early Detection/Alerting for Origin Reachability, Availability, & Latency issues	✔	✕
Layer 3 & 4 Network Attack Analysis and Mitigation	✕	✔
GRE Tunnel Health Check Monitoring	✕	✔
Supported Products	DDoS Rate Limiting WAF	Magic Transit

Getting Started: Contact your Cloudflare Account Executive today to get started.