DATENBLATT

CLOUDFLARE

Security Operations Center (SOC) as a Service von Cloudflare

+49 89 2555 2276 | enterprise@cloudflare.com | www.cloudflare.com/de-de/

Eine unübersichtliche Bedrohungslandschaft

In der heutigen digitalen Welt sind Cyberangriffe an der Tagesordnung und Netzwerke werden immer komplexer. Selbst den wachsamsten Unternehmen fällt es oft schwer, Wichtiges von Unwichtigem zu unterscheiden. Bei welchen Warnmeldungen und Vorfällen handelt es sich um Fehlalarme und welche müssen eingehender untersucht werden? Und welche neuen Aspekte der sich ständig weiterentwickelnden Bedrohungslandschaft stellen das größte Risiko für das Unternehmen dar?

Die Komplexität des Netzwerks resultiert aus heterogenen Umgebungen und einem veralteten Perimeter-basierten Infrastrukturmodell. In der Folge setzen Unternehmen heute eine Vielzahl von Einzeltools zur Sicherheit- und Performance-Überwachung ein. Sicherheits- und IT-Teams müssen ständig Protokolle, Warnmeldungen und Richtlinien verschiedener Umgebungen interpretieren und miteinander in Einklang bringen. Die Folge sind kostspielige, ineffiziente und fehleranfällige Betriebsabläufe.

All diese Komplexität erhöht nicht nur die Angriffsfläche und die Gefahranfälligkeit, sondern kann auch schnell zu Ermüdung und Burnout von Beschäftigten führen und Unternehmen daran hindern, sich auf neue Wachstumschancen zu konzentrieren.

Klarheit ins Chaos bringen mit SOC as a Service von Cloudflare

SOC as a Service von Cloudflare verbindet unsere preisgekrönten Sicherheitsprodukte mit unserem engagierten Team von Cybersicherheitsexperten, die Ihre Unternehmensumgebung rund um die Uhr auf Bedrohungen und potenzielle Betriebsstörungen überwachen, zur Identifizierung von Angriffsvektoren tiefgreifende Analysen durchführen und bei Sicherheitsvorfällen Gegenmaßnahmen ergreifen.

SOC as a Service von Cloudflare wurde für Unternehmen jeder Größe und Komplexität entwickelt und wird in Layer 3, Layer 4 und Layer 7 allen Anforderungen an die Sicherheitsüberwachung, die Bedrohungserkennung und die Reaktion auf Vorfälle gerecht. Der früheste Hinweis auf Sicherheitsvorfälle kann manchmal ein beeinträchtigter Anwendungs- oder Netzwerkzustand sein. Aus diesem Grund wird hinsichtlich Erreichbarkeit, Verfügbarkeit und Latenz des Ursprungsservers eine proaktive Benachrichtigungsstrategie angewandt. Das macht nicht nur den Gesamtzustand des Netzwerks transparent, sondern beugt auch Netzwerkstörungen und -ausfällen vor.

Für das Benachrichtigungssystem von Cloudflare werden keine einfachen schwellenwertbasierten Trigger eingesetzt, sondern ausgefeilte selbstentwickelte Algorithmen. Diese äußerst zuverlässigen Benachrichtigungen geben dem SOC-Team die Sicherheit, nahezu in Echtzeit reagieren und entschlossen handeln zu können. Die SOC as a Service-Experten von Cloudflare stellen eine ordnungsgemäße Ersteinschätzung, Untersuchung und Behebung zeitkritischer Vorfälle sicher. Das SOC-Team von Cloudflare informiert proaktiv über Zwischenfälle und liefert regelmäßig ausführliche Berichte zu Angriffen und Netzwerkvorfällen.

Das Netzwerk von Cloudflare umfasst mehr als 200 Städte weltweit und wird täglich von mehr als 1 Milliarde eindeutiger IP-Adressen durchlaufen. Diese Größenordnung und Vielfalt bildet die Grundlage für ein einzigartiges Wissen, anhand dessen das SOC-Team von Cloudflare verdächtige Aktivitäten im gesamten Netzwerk mit hoher Zuverlässigkeit identifizieren kann.

Vorteile der SOC as a Service-Lösung von Cloudflare

Ganzjähriger Schutz, rund um die Uhr

Die Sicherheitsexperten von Cloudflare halten kontinuierlich nach Bedrohungen Ausschau und reagieren darauf, bevor sich daraus kritische Ereignisse entwickeln können.

Schnellere Erkennung und Behebung

Maßgeschneiderte Abwehr und Konfiguration durch das SOC-Team tragen dazu bei, die Zeitspanne zwischen dem Auftreten eines Vorfalls, seiner Erkennung und seiner Behebung zu verkürzen.

Proaktive Kommunikation und Berichterstellung

Proaktive Kommunikation über verschiedene Kanäle wie Telefon, E-Mail und WebHooks, wenn im Traffic-Unregelmäßigkeiten auftreten oder das Netzwerk angegriffen wird. Regelmäßige Berichte über erstellte Regeln und blockierte Angriffe, mit Empfehlungen zu Konfigurationsänderungen.

Geringere Sicherheitskosten

Dank des SOC von Cloudflare müssen weniger Sicherheitsspezialisten für die Überwachung und Reaktion auf Warnmeldungen eingesetzt und geschult werden, wodurch die Sicherheitsausgaben insgesamt sinken.

Schneller und einfacher Start

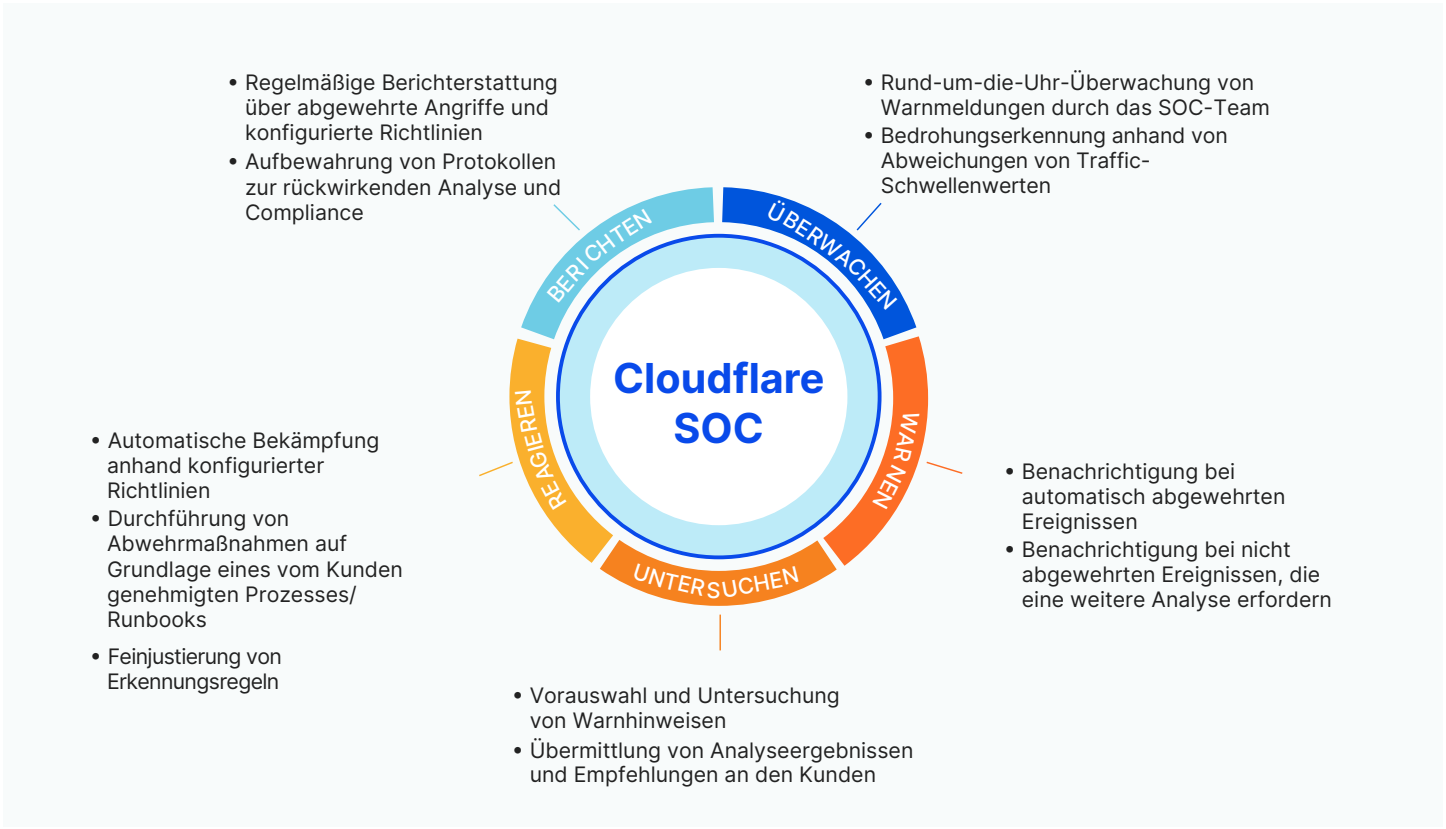
Eine SOC-Basiskonfiguration lässt sich schnell und einfach erstellen. Für die Aktivierung des SOC-Dienstes müssen keine zusätzlichen Endpunkt-Agenten oder -Tools eingesetzt werden.

Auslagerung der Sicherheit an Cloudflare-Experten

Ihr Sicherheitsteam muss sich nicht mehr mit Fehlalarmen auseinandersetzen und kann sich auf andere vorrangige Projekte konzentrieren, denn die Sicherheitsexperten von Cloudflare erkennen jede verdächtige Aktivität sofort und reagieren schnell mit Lösungsempfehlungen.

Monatliche/Vierteljährliche Berichte

Unser SOC-Team erstellt regelmäßig Berichte, um Einblicke in die Schutzmaßnahmen zu bieten, die von Cloudflare zur Abwehr von Sicherheitsbedrohungen ergriffen werden.



Service-Optionen

	SOC für Kernanwendungen	SOC für Netzwerke
Proaktive Überwachung und Benachrichtigung bei anomalen Ereignissen	✔	✔
Benutzerdefinierte Regeln zur Abwehr laufender Angriffe	✔	✔
Berichterstellung	✔	✔
Analyse und Abwehr von Angriffen auf Layer 7	✔	✕
Früherkennung von Erreichbarkeits-, Verfügbarkeits- und Latenzproblemen des Ursprungsservers	✔	✕
Analyse und Abwehr von Netzwerkangriffen auf Layer 3 und 4	✕	✔
Überwachung und Integritätsprüfung des GRE-Tunnel	✕	✔
Unterstützte Produkte	DDoS Durchsatzbegrenzung WAF	Magic Transit

Erste Schritte: Kontaktieren Sie noch heute Ihren Cloudflare-Kundenbetreuer, um loszulegen.