graylog
API SECURITY

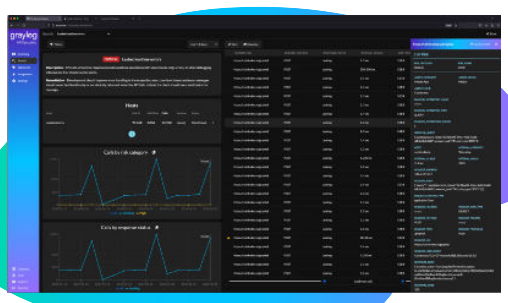
Graylog API Security – gewinnen Sie neue Einblicke und die Kontrolle über Ihre API-Angriffsfläche

Vollständige API-Erkennung, Identifizierung von Bedrohungen und Reaktion auf sicherheitsrelevante Vorfälle

Graylog API Security ist die erste API-Sicherheitslösung, die speziell dafür entwickelt wurde, Ihren Security-Teams eine vollständige Beobachtung der Runtime-API-Aktivitäten innerhalb des Perimeters zu ermöglichen. Da Angreifer immer neue Wege finden, sich als autorisierte Benutzer auszugeben und so uneingeschränkten Zugriff auf kritische operative APIs erhalten, können Sie sich nicht mehr ausschließlich auf die Perimeter-Verteidigung verlassen. Ihre Security-Teams können jetzt Graylog API Security nutzen, um Ihr Sicherheitsniveau für APIs zu erhöhen und die wachsende API-Angriffsfläche zu verringern – auch Post-Perimeter. Graylog API Security bietet Funktionen zur Erkennung von APIs, zur Identifizierung von Bedrohungen und zur Reaktion auf sicherheitsrelevante Vorfälle. Die Lösung schafft vollkommene Transparenz in Ihrer IT-Umgebung und ermöglicht eine Überwachung auf Angriffe in Echtzeit. Zudem können Sie die End-to-End-API-Request- und API-Response-Daten umfassend analysieren.

Sprechen Sie mit unseren Experten und erleben Sie Graylog API Security in Aktion

Überzeugen Sie sich selbst! Graylog möchte, dass Sie noch vor einem Kauf Antworten auf alle Ihre Fragen erhalten. Wir bieten Ihnen Produktdemos an, die die Funktionalitäten unserer Lösung aufzeigen und ausreichend Zeit für Fragen und Antworten lassen. Vereinbaren Sie noch heute einen Termin für Ihre **Graylog API Security-Demo** und erleben Sie unsere leistungsstarke Cybersecurity-Plattform in Aktion.



Die wichtigsten Vorteile von Graylog API Security

- **Kontinuierliche API-Erkennung —** Die automatische Erkennung und Kategorisierung aller APIs stellt sicher, dass keine API unter dem Radar bleibt.
- **Geführte Erkennung von Bedrohungen und Reaktionsmaßnahmen** — Sie erhalten Warnmeldungen mit klaren und praktikablen Schritten, um Bedrohungen sofort zu bekämpfen und abzuwehren.
- **Vollständige Request- UND Response-Payload** — Sie erhalten mehr als nur Header-Daten und können präzise Warnmeldungen, eine nachträgliche Bedrohungssuche sowie API-spezifische Abhilfemaßnahmen nutzen.
- **Sichere, Self-Managed-Lösung** — Behalten Sie sensible Daten im eigenen Unternehmen, vermeiden Sie Störungen durch Dritte und ersparen Sie sich Bedenken bezüglich personenbezogener Daten sowie den bürokratischen Aufwand für SaaS-Sicherheitsüberprüfungen.

graylog
API SECURITY

Leistungsstarker Funktionsumfang

API-Erfassung
Verschaffen Sie sich einen vollständigen Überblick über Ihre API-Angriffsfläche dank der Optionen für die API-Erfassung im Netzwerk, am Gateway sowie in den Anwendungen.

Klärung für alle Assets
Sparen Sie Entwicklungszeit, indem Sie die Daten, die durch jede beliebige API fließen, automatisch klassifizieren.

Kontinuierliche API-Erkennung
Entlasten Sie Entwickler- und Security-Teams von der manuellen Identifizierung der in Ihrem Unternehmen genutzten APIs.

No-Code-Regeln
Erstellen Sie mühelos Ihre eigenen benutzerdefinierten Regeln für die Erkennung von Bedrohungen und für die Alarmierung.

OWASP Top 10+
Nutzen Sie die Bedrohungssignaturen von Graylog, die über OWASP hinausgehen, um Risiken unmittelbar zu reduzieren.

Erkennung von Bedrohungen in Echtzeit
Überwachen Sie Sicherheitsprobleme zur Laufzeit und generieren Sie optimal abgestimmte Warnmeldungen mit vollständigem Kontext und individuellen Anleitungen zur Behebung.

Abhilfe schaffen
Die Alerts enthalten detaillierte, zielgerichtete und anpassbare Anweisungen, damit Sie Risiken sofort adressieren können.

Erfassung der Request- und Response-Daten
Erfassen Sie automatisch die Header- und Body-Daten aller Anfragen und Antworten für REST-APIs und GraphQL-Abfragen.

Risikobewertung
Bewerten Sie automatisch die Sicherheitssituation für Ihre APIs und erhalten Sie nützliche Informationen über aktuelle API-Sicherheitsrisiken.

Umfassende Suche
Finden Sie benötigte Informationen schnell mit Standard-SQL- und Regex-Abfragen.

Eigenständiger Data Lake
Bewahren Sie API-Transaktionen für weiterführende Untersuchungen sowie die Suche nach Bedrohungen kostengünstig auf – ohne dass eine externe Datenbank erforderlich ist.

SIEM- und SOAR-Integration
Senden Sie kritische Sicherheitswarnungen automatisch an Graylog SIEM oder Ihre SOAR-Lösung, um auf sicherheitsrelevante Vorfälle zu reagieren.

SSO
Nutzen Sie OAuth oder JWT für den sicheren Zugriff auf Graylog API Security.

Gezielte Alarmierung
Leiten Sie Warnmeldungen präzise und direkt an Ihre Security- und/oder DevOps-Teams weiter – via Slack, Teams, Gchat oder Zapier.