

IT-Security Monitoring

Managed Service

Einordnung und Zielgruppe

IT-Security Monitoring ist ein Managed Service zur kontinuierlichen Überwachung definierter IT-Systeme auf sicherheitsrelevante Ereignisse. Der Service richtet sich an Unternehmen, die einen strukturierten Überblick über sicherheitskritische Vorgänge in ihrer IT benötigen, ohne selbst eine zentrale Log- und Monitoring-Infrastruktur betreiben zu müssen.

Der Fokus liegt auf Transparenz, Nachvollziehbarkeit und der frühzeitigen Erkennung relevanter Auffälligkeiten im laufenden Betrieb.

Was ist IT-Security Monitoring?

IT-Security Monitoring umfasst die zentrale Sammlung, Auswertung und Dokumentation sicherheitsrelevanter Ereignisdaten aus unterschiedlichen IT-Komponenten. Protokolle und Meldungen werden fortlaufend erfasst, zusammengeführt und anhand vordefinierter Use-Cases ausgewertet.

Überwacht werden unter anderem Firewalls, Identitäts- und Verzeichnisdienste sowie Server-Systeme. Ziel ist es, sicherheitsrelevante Vorgänge sichtbar zu machen, strukturiert aufzubereiten und bei kritischen Ereignissen gezielt zu informieren. Der Service stellt keine aktive Abwehr dar, sondern liefert die Grundlage für fundierte Entscheidungen im Umgang mit Sicherheitsvorfällen.

Was wir lösen

In vielen IT-Umgebungen existieren sicherheitsrelevante Informationen verteilt über verschiedene Systeme. Fehlgeschlagene Anmeldungen, Änderungen an Benutzerrechten oder Konfigurationsänderungen sind zwar protokolliert, werden im Alltag jedoch häufig nicht zentral ausgewertet oder nur reaktiv betrachtet.

IT-Security Monitoring löst dieses Problem, indem relevante Ereignisse systemübergreifend zusammengeführt und regelmäßig überprüft werden. Dadurch sinkt das Risiko, dass sicherheitskritische Vorgänge unbemerkt bleiben oder erst sehr spät erkannt werden. Gleichzeitig wird die interne IT entlastet, da Auswertung, Strukturierung und Grundbewertung der Ereignisse übernommen werden.

Was wir übernehmen

Der Service beinhaltet die zentrale Logsammlung aus den vereinbarten Quellen, das tägliche automatisierte Monitoring sowie die Pflege vordefinierter Standard-Use-Cases. Sicherheitsrelevante Ereignisse werden dokumentiert, eingeordnet und nachvollziehbar bereitgestellt.

Ihr Ansprechpartner:



Marco Cornelsen
Tel. 02594 9191 1334
vertrieb@easy-hood.info

EasyHood - IT since 1337.
Lise-Meiter-Str. 6 – 48301 Nottuln
Tel. 02594 9191 1337

EasyHood
IT since 1337.

High- und Critical-Events führen zu einer aktiven Benachrichtigung. Ergänzend wird ein regelmäßiger Security-Report zur Verfügung gestellt.

Das Ergebnis:
Wir betreiben für Sie eine zentrale Logsammlung und ein tägliches automatisches Monitoring der vereinbarten Systeme.
Sicherheitsrelevante Ereignisse werden anhand definierter Standard-Use-Cases erkannt und ausgewertet.

Beispiele für überwachte Use-Cases sind:

- Fehlgeschlagene Anmeldeversuche von Administratoren in Verzeichnisdiensten, Cloud-Diensten und Firewalls
- Änderungen an Benutzerrechten, insbesondere das Anlegen neuer Administrator-Konten
- Änderungen an sicherheitsrelevanten Firewall-Einstellungen wie Portfreigaben

Ereignisse mit hoher oder kritischer Relevanz werden als Security-Alerts klassifiziert. In diesen Fällen erfolgt eine reaktive Benachrichtigung per E-Mail oder Ticket, sodass der Kunde zeitnah reagieren kann. Zusätzlich erhalten Sie einen monatlichen Security-Report mit einer zusammengefassten Auswertung der erkannten Ereignisse.

Kurz gesagt
IT-Security Monitoring schafft Transparenz über sicherheitsrelevante Vorgänge in Ihrer IT. Sie erhalten eine zentrale Übersicht, automatische Überwachung definierter Use-Cases, gezielte Alerts bei kritischen Ereignissen und eine regelmäßige Auswertung – ohne selbst ein Security-Monitoring betreiben zu müssen.

Was wir unter sicherheitsrelevanten Ereignissen verstehen

Sicherheitsrelevante Ereignisse sind technische Vorgänge oder Änderungen, die auf ein erhöhtes Risiko für die IT-Sicherheit hinweisen können. Dazu zählen insbesondere ungewöhnliche oder wiederholte fehlgeschlagene Anmeldungen, Änderungen an administrativen Benutzerrechten sowie Anpassungen an sicherheitskritischen System- oder Netzwerkkonfigurationen. Die Bewertung erfolgt anhand vordefinierter Kriterien und Schweregrade.

Voraussetzungen für diese Zugriffkonzept
Voraussetzung für IT-Security Monitoring ist der Zugriff auf die Protokoll- und Ereignisdaten der zu überwachenden Systeme. Zudem müssen die Logquellen, der Überwachungsumfang sowie die Benachrichtigungswege eindeutig festgelegt sein.

EasyHood - IT since 1337.
Lise-Meiter-Str. 6 – 48301 Nottuln
Tel. 02594 9191 1337

EasyHood
IT since 1337.