Haftungsausschluss

Rechtlicher Hinweis

Dieser Leitfaden und seine Inhalte (der „Leitfaden") werden von NXGEN bereitgestellt. Alle Rechte am Leitfaden und am darin verkörperten geistigen Eigentum — einschließlich, aber nicht beschränkt auf Marken, Handelsnamen, Logos und ähnliche Kennzeichen im oder am Leitfaden — sind gesetzlich geschützt. Sämtliche Rechte, Ansprüche und Anteile am Leitfaden und an damit verbundenen Schutzrechten verbleiben bei NXGEN und seinen Lizenzgebern.

Der Leitfaden wird unentgeltlich, „wie besehen" und ausschließlich zu Informationszwecken bereitgestellt, ohne jegliche Gewährleistung. Er ist weder dazu bestimmt noch geeignet, ein Rechtsverhältnis zwischen dem Leser und NXGEN oder seinen verbundenen Unternehmen zu begründen, einschließlich, aber nicht beschränkt auf Verpflichtungen von NXGEN oder seinen verbundenen Unternehmen gegenüber dem Leser.

Die Verpflichtungen von NXGEN und seinen verbundenen Unternehmen in Bezug auf von einem Kunden erworbene NXGEN-Produkte oder -Dienstleistungen richten sich ausschließlich nach den Bedingungen des Vertrags, unter dem diese Produkte oder Dienstleistungen erworben wurden.

Zur Klarstellung

Der Leser trägt das gesamte Risiko hinsichtlich der Nutzung, der Ergebnisse und der Leistung des Leitfadens. Soweit gesetzlich zulässig, schließt NXGEN alle Gewährleistungen aus, ob gesetzlich, ausdrücklich oder stillschweigend — einschließlich, aber nicht beschränkt auf stillschweigende Gewährleistungen der Marktgängigkeit, der Eignung für einen bestimmten Zweck, des Rechtsbestands und der Nichtverletzung von Rechten Dritter — sowie jegliche Haftung oder Gewährleistung aus Vorschlägen, Spezifikationen oder Mustern im Zusammenhang mit dem Leitfaden.

Alarmkategorien

Updated 16 September 2026

Jeder Alarm, den GCXONE empfängt, wird nach der Verarbeitung in eine von zehn Kategorien eingeteilt. Diese Klassifizierung speist die Alarm-Aufschlüsselungs-Widgets im Dashboard und die Analyse-Spalte im Ereignisprotokoll.

Die Kategorien

KategorieBedeutungEchtEin echtes Ereignis, bestätigt durch die NOVA99x KI-Analyse und an einen Operator zur Bearbeitung weitergeleitet.FalschDurch die NOVA99x KI-Analyse als Fehlalarm herausgefiltert – es trat kein echtes Sicherheitsereignis auf.TechnischEin technisches oder systembezogenes Ereignis, z. B. ein HealthCheck-Fehler, und nicht eine Sicherheitsdetektion.Redundant-Ein Duplikat eines bereits ausgelösten Alarms für denselben Auslöser, das daher nicht erneut an die Operator-Warteschlange gesendet wird.IsolierenEin Alarm von einer Kamera oder einem Sensor, der von einem Operator oder Administrator vorübergehend isoliert (von der Überwachung ausgeschlossen) wurde, für eine festgelegte Dauer.DeaktiviertEin Alarm, der eingetroffen ist, während die Site oder das Gerät deaktiviert war.BlockiertEin Alarm, der durch Überlauf-Schutz unterdrückt wurde, wenn ein Gerät oder eine Site in kurzer Zeit ein ungewöhnlich hohes Alarmvolumen sendet.InaktivEin Alarm von einer Kamera oder einem Sensor, der derzeit in der Site-Konfiguration als inaktiv markiert ist.AbgelehntEin Alarm, der automatisch vor der Analyse durch einen konfigurierten Filter wie eine Blacklist-Regel, eine Maske oder eine Prioritätsregel abgelehnt wird.Kein BerichtEin Ereignis, das keinen Alarmbericht erzeugt hat.

Wo Sie diese sehen

Diese Kategorien erscheinen in der gesamten Alarm-Analytik des Dashboards: im Alarmkategorien-Aufschlüsselungs-Widget, im Vergleichs-Diagramm Echt vs Falsch vs Redundant vs Technisch, in den Aufschlüsselungs-Tabellen pro Site und pro Gerät sowie in der Analyse-Spalte des Ereignisprotokolls.

- Echt, Falsch und Technisch sind die primären Ergebnisse der NOVA99x-Analyse und bilden den Großteil des Alarmvolumens der meisten Sites.
- Isolate und Disarmed spiegeln Konfigurationsentscheidungen Ihres Teams wider – ein Sensor, der in Isolation versetzt wurde, oder eine Site/ein Gerät, das deaktiviert ist – und nicht etwas, das NOVA99x entschieden hat.
- Blockiert, Inaktiv, Abgelehnt, Redundant und Kein Bericht beschreiben Alarme, die unterdrückt, ausgeschlossen oder gefiltert wurden, bevor sie einen Operator erreichten.

> Isolate und Disarm liegen in Ihrer Kontrolle.
>
> Erzeugt eine Kamera wiederholt Isolate- oder Disarmed-Alarme, prüfen Sie, ob sie absichtlich in einem Isolations-Fenster oder einem deaktivierten Zeitplan belassen wurde – beides sind Konfigurationszustände, die Ihr Team festlegt und die in der Geräte-Konfiguration gelöscht werden können.