**Wir bieten**

- Maximierung der CrowdStrike-Falcon-Sicherheitsvorteile durch strukturierte Discovery & Aktionsplan
- Entwicklung maßgeschneiderter Use Cases zur Stärkung der Next-Gen-SIEM-Erkennung
- Laufende Weiterentwicklung durch neue Datenquellen, Regeln, Dashboards & Schulungen
- Proaktive Sicherheitschecks: Penetrationstests, Social Engineering, externe Angriffsflächenanalyse

# Der Serviceware Wingman for CrowdStrike Falcon Next-Gen SIEM

Der Wingman für CrowdStrike Falcon Next-Gen SIEM ist ein Service, der entwickelt wurde, um die Sicherheitsvorteile Ihrer CrowdStrike-Lösung zu maximieren. Ausgehend von einer umfassenden Discovery-Bewertung arbeiten Expert:innen mit Ihnen zusammen, um wichtige Datenquellen zu identifizieren und die digitale Angriffsfläche Ihres Unternehmens zu analysieren. Es werden maßgeschneiderte Anwendungsfälle entwickelt, um einen greifbaren Mehrwert zu schaffen und Ihre Next-Gen-SIEM-Fähigkeiten zur Erkennung von Bedrohungen zu verbessern.

Ein maßgeschneiderter Aktionsplan definiert klare Meilensteine für die Integration von Next-Gen SIEM in Ihre Sicherheitsinfrastruktur und dient als strategischer Fahrplan zur Erhöhung Ihres Sicherheitsniveaus.

**Anfängliche Discovery-Bewertung**

- Bewertung Ihrer geschäftlichen und sicherheitstechnischen Anforderungen
- Identifizierung und Bewertung aller möglichen Datenquellen
- Anfängliche Bewertung der Angriffsfläche, Entwicklung erster Anwendungsfälle
- Priorisierung von Datenquellen und Anwendungsfällen, Entwicklung eines Aktionsplans

**Kontinuierliche Weiterentwicklung Ihres Next-Gen SIEMs**

- Anbindung neuer Protokollquellen oder Konnektoren



SERVICEWARE

- Erstellung neuer Erkennungsregeln, Berichte oder Dashboards
- Entwicklung von Workflows, Reaktionsmaßnahmen und Runbooks
- Unterstützung des Übergangs zum Betrieb durch Schulungen

**Proaktive Sicherheitsdienste zur Aufdeckung von Risiken**

- Automatisierte interne Penetrationstests mit realen Exploits
- Social-Engineering-Angriffe wie Spear-Phishing, speziell auf Ihre VIPs zugeschnitten
- Untersuchung der externen Angriffsfläche einschließlich einer Darknet-Analyse
- Empfohlene Maßnahmen zur Schließung von Lücken und zur Erweiterung der Transparenz in Next-Gen SIEM

## Paketstufen

| | SILBER | GOLD | PLATIN |
|---|---|---|---|
| NG SIEM Discovery Assessment & Onboarding | • | • | • |
| Monatliche Stunden Next-Gen-SIEM-Entwicklung* | 8 | 12 | 16 |
| Unterstützung für andere Falcon Module | • | • | • |
| Proaktive Security Services pro Jahr* | 1 | 2 | 3 |
| Aktionsplan und Projektsteuerung | • | • | • |
| Feste:r Projektmanager:in, regelmäßige Jourfixes | | | • |
| Feste Solution Architect Ansprechperson | | | • |

**Eine Erhöhung der monatlichen Stunden oder Anzahl der proaktiven Services kann zusätzlich erworben werden.*



# Über Serviceware

Serviceware bietet seit mehr als 25 Jahren Software, Beratung und Managed Services zur Digitalisierung moderner Unternehmensprozesse. Von Enterprise Service Management über IT Financial Management bis Security, Data und Endpoint Management – hochautomatisiert und sicher.

**Serviceware SE**
Serviceware-Kreisel 1
65510 Idstein • Germany
+49 6434 9450 0
contact@serviceware-se.com
www.serviceware-se.com

02/2026

SERVICEWARE