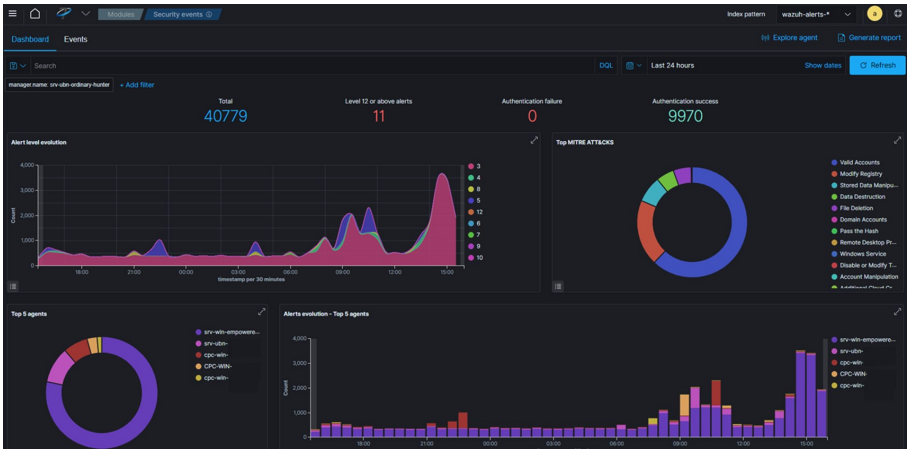
FlexSOC – der SIEM/SOC Service für KMU

*Mit **FlexSOC** überwachen wir Ihre IT rund um die Uhr, erkennen Angriffe frühzeitig und reagieren mit konkreten Massnahmen – Sie brauchen kein eigenes Security-Team.*

Echtzeitüberwachung: Unsere SIEM-Plattform analysiert die Logdaten Ihrer Netzwerke, Endpunkte und Applikationen rund um die Uhr und erkennt Unregelmässigkeiten.

Umfassende Bedrohungserkennung: Unsere fortschrittlichen Regeln & Algorithmen identifizieren nicht nur bekannte Bedrohungen, sondern erkennen auch unbekannte Angriffsmuster.

Schnelle Reaktion: Wenn eine Bedrohung erkannt wird, reagieren wir schnell. Unsere SOC-Analysten beobachten kritische Events im 5x9 Betrieb, um die Sicherheit Ihres Unternehmens zu gewährleisten.



Tiefgreifende Analyse: Wir gehen über die Oberfläche hinaus. Unsere Security-Analysten analysieren Bedrohungen im Detail, um ihre Herkunft und Absicht zu verstehen.

Überwachung verschiedener Services: Wir überwachen kontinuierlich Ihre Endpunkte, um sicherzustellen, dass sie laufen und aktuell sind und keinen Bedrohungen ausgesetzt sind. Auch Online-Services wie M365 können überwacht werden.

Kontinuierliche Optimierung: Wir passen unsere Security Rules und Sicherheitsstrategie kontinuierlich an die sich verändernde Bedrohungslage an und sorgen dafür, dass Sie immer zeitgemäss sind.

Zusammenarbeit

Sie erhalten uneingeschränkten Lesezugriff auf die Plattform—wir übernehmen die Detailarbeit und kümmern uns mit Ihrem bestehenden IT-Partner oder Ihrem IT-Team um die Stärkung der Sicherheit. Für eine umfassende Incident Response können wir Ihnen eine Cyber-Versicherung zu Vorzugskonditionen vermitteln.

Sie erhalten

- Proaktive Erkennung von Angriffen mit einer cloudbasierten XDR-Lösung
- 24x7 Monitoring Ihrer Umgebung mit Wazuh (Open Source)
- 9x5 manuelle Triage & Threat Hunting kritischer Events durch Protect7
- Basis-Unterstützung bei Sicherheitsvorfällen
- Regelmässige Anpassungen der Regeln

Überwachungen

- Win, Mac, Linux Endpunkte (Clients & Server)
- Syslog zur Integration von Firewalls, Netzwerk-Devices usw.
- Microsoft M365
- Github
- Speziallösungen

Add-Ons

- Regelmässige vertiefte Analysen weiterer relevanter Events
- Qualifizierte Vulnerability Reports
- Zugriff auf Expertenpool

Preise

- Fixpreise für Kostensicherheit
- Essentials ab CHF 555.–/Monat; mit Überwachung von bis zu 100 Endpunkten ab CHF 725.–/Monat
- abhängig von Dimensionierung und gewählten Add-Ons

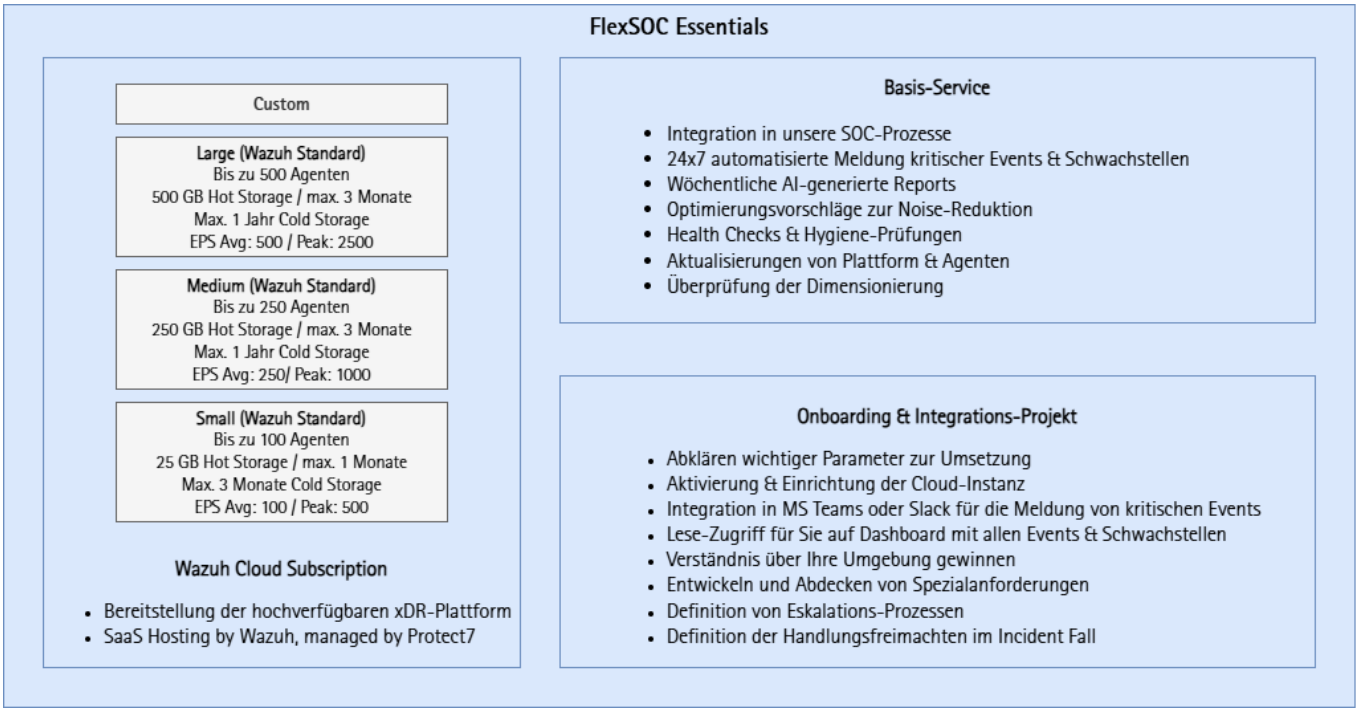
MANAGED SERVICES

Protect7 GmbH | Schaffhauserstrasse 418 | 8050 Zürich | Tel. +41 44 515 68 68 | www.protect7.com | info@protect7.com

Service-Gestaltung und Optionen

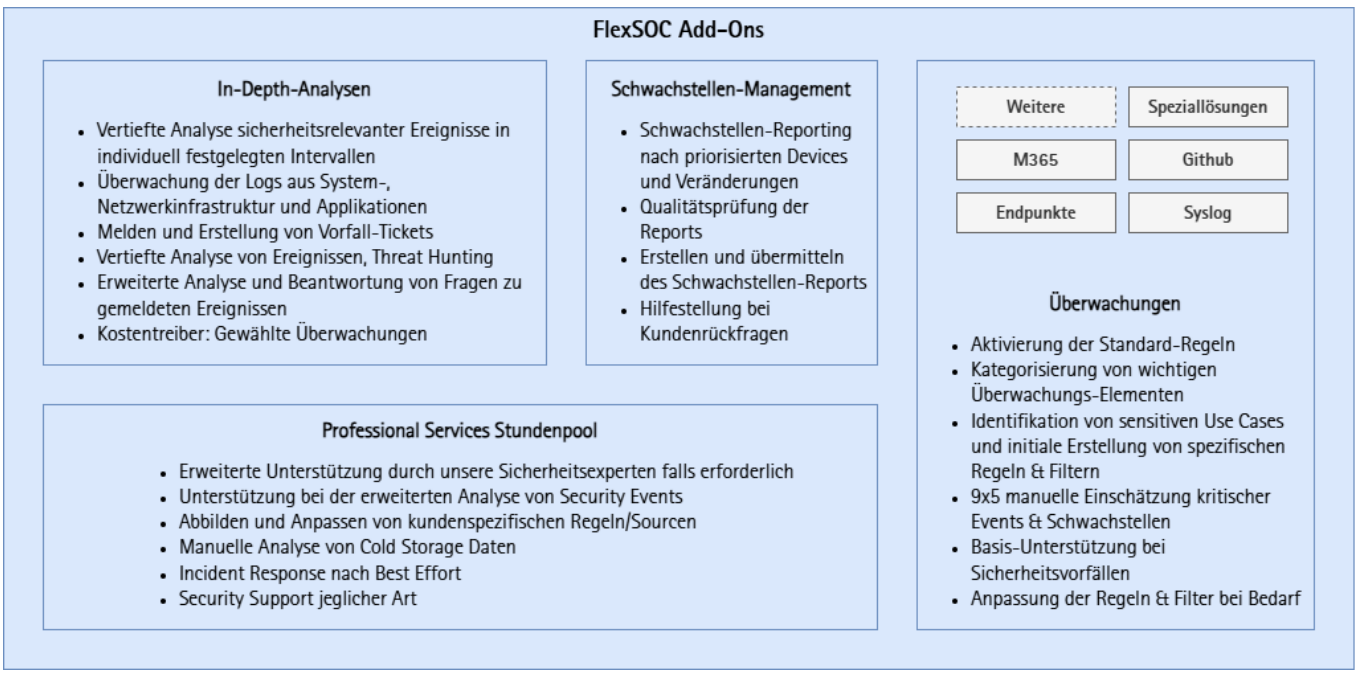
FlexSOC Essentials

Mit den Essentials sichern Sie sich den initialen Aufbau und Betrieb Ihrer Umgebung, inklusive Hosting und den grundlegenden Prozessen für einen professionellen und stabilen SOC-Betrieb.



FlexSOC Add-Ons

Sie wählen die für Ihr Unternehmen relevanten **Überwachungen**, zum Beispiel M365, aus, die wir für Sie vollständig managen. Schwachstellen-Management verschafft Ihnen mehr **Transparenz über bestehende Risiken**, während In-Depth-Analysen eine **frühere Erkennung** von Problemen ermöglichen.



MANAGED SERVICES

FlexSOC Preisbeispiel

Am Beispiel einer mittelständischen Firma mit rund 70 Mitarbeitenden und eigener IT-Infrastruktur zeigt sich, wie FlexSOC optimal eingesetzt werden kann. Für Unternehmen dieser Grösse reicht in der Regel die Dimensionierung „Small" aus, um bis zu 100 Endpunkte zuverlässig zu überwachen und die IT-Sicherheit professionell zu stärken.

Die **FlexSOC Essentials** umfassen das **Hosting** Ihrer Instanz sowie die **Basisprozesse**, um die Plattform stets **aktuell** zu halten. Sie beinhalten noch keine von uns verwalteten Überwachungen, bilden aber die solide Grundlage für eine flexible Auswahl an Add-Ons:

FlexSOC Essentials	Initialkosten	Mtl. Betriebskosten
Wazuh Cloud Subscription—Small		CHF 470.00
Basis-Service	CHF 340.00	CHF 85.00
Onboarding & Integrations-Projekt (nach Aufwand)	CHF 1'020.00	

Die meisten unserer Kunden entscheiden sich zu Beginn für die Überwachung der Endpunkte (PCs, Server etc.) sowie für die M365-Überwachung. Diese **FlexSOC Add-Ons** können dabei jederzeit monatlich aktiviert oder wieder gekündigt werden:

FlexSOC Add-Ons	Initialkosten	Mtl. Betriebskosten
Endpunkte-Überwachung (60 Büromitarbeiter, 10 Server)	CHF 680.00	CHF 170.00
M365-Überwachung (Mail, OneDrive, Sharepoint etc.)	CHF 340.00	CHF 255.00

Daraus ergibt sich folgende Summe:

FlexSOC	Initialkosten	Mtl. Betriebskosten
Endpunkte-Überwachung (60 Büromitarbeiter, 10 Server)	**CHF 2'380.00**	**CHF 980.00**

Die FlexSOC-Lösung bietet Unternehmen eine flexible und modulare Sicherheitsplattform: Essentials bilden die Basis, Add-Ons wie Endpunkt- oder M365-Überwachung lassen sich monatlich aktivieren oder kündigen. Mit einem Preis von rund CHF 14.– pro Endpunkt und Monat gem. Beispiel ist das Angebot wettbewerbsfähig und ideal für mittelständische Firmen bis 100 Endpunkte.

Weitere Highlights

- Möglichkeit zum kostenlosen 14-tägigen Test der Wazuh Plattform
- 5% Rabatt für eine Cyber-Versicherung bei exali (Incident Response, Forensik, Haftpflicht)
- Spezial-Lösungen und Überwachungen
- Professional Services Stundenpool mit 10% Rabatt bei Vorauszahlung
- Flexible monatliche Vertragsanpassungen (ausg. Wazuh Cloud Subscription mit Jahresvertrag)

Wir freuen uns auf Ihre Kontaktaufnahme und erstellen Ihnen gerne eine unverbindliche Offerte.

MANAGED SERVICES