Unsere SIEM-Pakete im Vergleich

PAKETINHALTE	SIEM ONE ESSENTIALS PROTECT STANDARD	SIEM ONE	SIEM 100 ab 03/2022
Automatisierte Berichte nach vereinbarten Intervallen	✔	✔	✔
Prüfung der SIEM-Meldungen, Ereignisse (Skripte, Executables & Detections) durch CyberSec24 IT-Security Spezialisten	monatlich	täglich	täglich
Durchsprache der SIEM-Meldungen | Dauer: 1 Stunde	monatlich	wöchentlich	wöchentlich
Aufbewahrungszeit der Raw-Events (Datastore) | Dauer: 1 Woche	✔	✔	✔
Konzeptionelle Betreuung und Besprechung, Fragen (außerhalb des 60 Minuten-Slots)	nicht verfügbar	✔	✔
Einsatz im medizinischen Umfeld		✔	✔
Detection und automatisierte Response hinsichtlich der Top 100 Bedrohungen & Angriffsszenarien			✔
Monatliche Aktualisierung der Angriffsliste auf den aktuellen Stand der weltweiten Angriffsszenarien			✔
Automatisierter Bot-Net-Schutz (voraussichtlich ab Ende 2022)	monatlich	wöchentlich	wöchentlich
Empfehlungen zum weiteren Umgang mit aufgetretenen Bedrohungen auf den Endgeräten			✔
Wissenstransfer und Sensibilisierung zu IT-Security Themen	✔	✔	✔

Einmalige Einrichtungspauschale zur Konfiguration | entfällt bei Laufzeiten ab 3 Jahren

Grundvoraussetzung zum Betrieb: Jedes zu überwachende Endgerät benötigt eine ESET PROTECT Essentials bzw. ESET PROTECT Advanced Installation, die auf Wunsch als Service (Add-On) gebucht werden kann. Der Betrieb von ESET durch den Kunden ist auf eigenes Risiko möglich.

ADD-ON			
ESET PROTECT Essentials bzw. ESET PROTECT Advanced as a Service Abrechnung nach Endgerätestaffel pro Gerät und Monat	✔	✔	✔
Beratung bei der Umsetzung neuer IT-Projekte, im eigenen Hause (Assessments, Pentests, Netzwerkanalyse | Berechnung nach Aufwand	✔	✔	✔
Verlängerung der Aufbewahrungszeit der Raw-Events (Datastore) pro zusätzliche Woche, 1 Euro / Endgerät und Monat	✔	✔	✔
Auf Wunsch kundenspezifische Schulung und Fortbildung für IT und non-IT Mitarbeiter Angebot anfordern	✔	✔	✔
SIEM WEEKEND – tägliche Prüfung auch an Wochenenden und Feiertagen Abrechnung nach Endgerätestaffel pro Gerät und Monat.	nicht verfügbar	✔	✔

ADD-ON ZU SIEM ONE / SIEM 100: SECURITY OPERATION CENTER (SOC) AS A SERVICE			
SOC LITE 8x5 (verfügbar voraussichtlich ab März 2022): Permanent fortlaufende Prüfung von Ereignissen im Unternehmen | 8x5 Betrieb durch Fachpersonal Abrechnung nach Endgerätestaffel pro Gerät und Monat	nicht verfügbar	✔	✔
SOC Complete 24x7 (verfügbar voraussichtlich ab März 2022: Permanent fortlaufende Prüfung von Ereignissen im Unternehmen | 24x7 Betrieb durch Fachpersonal Abrechnung nach Endgerätestaffel pro Gerät und Monat	nicht verfügbar	✔	✔

Makro Factory GmbH & Co. KG / An der RaumFabrik 30 / 76227 Karlsruhe / Tel +49 721 97 003 100 / Fax +49 721 97 003 199 / info@makrofactory.com / www.makrofactory.com