	Variante „Startup “	Variante „Grownup“	Variante „Enterprise“
Zentrale Log-Ablage	90 Tage	90 Tage	90 Tage
Betriebsumgebung	Shared	Shared	Dediziert
DNS-Name	Kundenneutral (z.B. xdr099.secaas.it)	Kundenneutral (z.B. xdr099.secaas.it)	Kundenspezifisch
Dashboard Benutzer	bis zu 3	bis zu 6	bis zu 12
Bedrohungserkennung	Standard-Regeln	Standard-Regeln	Individuelle Regelanpassungen (siehe Angebot)
Automatisierte Alarmierungswege	Slack/Teams/E-Mail/PagerDuty	Slack/Teams/E-Mail/PagerDuty	Slack/Teams/E-Mail/PagerDuty
Inkludiert Server	bis 5	bis 15	Die im jeweiligen Angebot spezifizierte Anzahl zu überwachender Systeme
Inkludiert Clients	bis 15	bis 50	
Syslog (z.B. Netzwerkgeräte)	-	bis 5	
Zusätzliche Assets	Gegen Aufpreis gemäß Angebot möglich – max. 50	Gegen Aufpreis gemäß Angebot möglich – max. 200	Gegen Aufpreis gemäß Angebot möglich
Mindestvertragslaufzeit	12 Monate	12 Monate	12 Monate

Weitere optionale Erweiterungen			
Cloud Security (Office 365, Docker, AWS, Google, GitHub)	optional	optional	optional
Spezifische Benachrichtigungs-Workflows	-	optional	optional
SysMon Integration	-	optional	optional
...			

Initial-Setup-Unterstützung

Hilfe bei der Installation der Agenten auf zu überwachenden Servern. Ein Techniker des Service Providers führt einen Kundenvertreter im Rahmen einer Web-Session durch die notwendigen Schritte zur Installation der Agenten auf den zu überwachenden Servern. Die Systemzugriffe auf das jeweils zu überwachende System erfolgen dabei ausschließlich durch den Kunden.

Storage Extension Package
Erweiterung der Speicherdauer (Vorhaltezeit der Logs) auf 180, 270 oder 360 Tage.

Dedizierte Health-Check-Analyse
Durchführung einer monatlichen Detail-Analyse der Logs eines Kunden durch unser Spezialisten-Team und Besprechung mit einem Kundenvertreter.

Individual-Regelanpassung

Neuimplementierung oder Änderung einer Alarmierungsregel. Änderung derselben Regel in einem Abstand von größer 7 Werktagen werden als zwei Regeländerung betrachtet und verrechnet.

Sonstige Individual-Tasks
Alle anderen Tätigkeiten, wie z.B. Unterstützung bei der anlassbezogenen Datenanalyse (z.B. zur Nachverfolgung eines Informations-/IT-Sicherheitsvorfalls).

Service Level Agreement
Service-Nutzungszeit: 24 Stunden am Tag, 365 Tage im Jahr
Bedienter Betrieb/Servicezeiten: Montag bis Freitag von 9:00 bis 17 Uhr an Werktagen, bundeseinheitliche Feiertage sowie regionale Feiertage im Freistaat Bayern ausgenommen – Kontakt per E-Mail/Ticket-System
Angestrebte qualifizierte Reaktion auf Anfragen per E-Mail: innerhalb von 4 Stunden während der Servicezeiten
Regelmäßige Backups: 1 x pro Woche (RPO: 168 Stunden)