Leverandør:		Løsning:		Kontakt Christian Schmidt, chr@dediko.dk med spørgsmål
Dediko A/S Your Security is our Passion	**SIEM Modenhedsmåling/Checkliste**		Under "Måling" skrives 0 for Nej, 1 for delvist og 2 for Ja. Kommentar feltet udfyldes for alle punkter	
Spørgsmål	**Beskrivelse**	**Måling**	**Kommentar**	**12%**
	Generelle krav			
SPG: 01	Agentløs logindsamling	✓		**86%**
SPG: 02	Agentbaseret logindsamling på Windows	✓		
SPG: 03	Nem introduktion a nye logkilder	✓		
SPG: 04	Out-of-the-box analyse for ønskede logkilder	✓		
SPG: 05	Producnt support for nye ukendt logkilder	!		
SPG: 06	Workflow for håndtering af incidents i LMS	!		
SPG: 07	Out-of-the-box compliance rapportering	✗		
	Arkitektur og skalerbarhed			
SPG: 08	Båndbredde håndterig	✗		**0%**
SPG: 09	Sikring af logoverførsel. Ingen logs må gå tabt	✗		
SPG: 10	Filtrering af logs - både ved kilden og i LMS	✗		
SPG: 11	Failover på LMS	✗		
SPG: 12	Fleksibilitet på valg af storage til LMS	✗		
SPG: 13	Skalerbar LMS	✗		
	Indhentning af logs			
SPG: 14	Understøttelse af forskellige systemer og noder/devices	✗		**0%**
SPG: 15	Distribueret behandling af logs	✗		
SPG: 16	Normalisering af logdata (NIST 800-92)	✗		
SPG: 17	Oversættelse af logs til nemt læsbart format	✗		
SPG: 18	Reduktion af "støj" og irrelevante events	✗		
SPG: 19	Sikring af logs mod tampering og kryptering af logs	✗		
SPG: 20	Helbredsovervågning af LMS	✗		
SPG: 21	Håndtering af inkorekte tidsstempler	✗		
	Log Management, Storage og opbevaring (Retention)			
SPG: 22	Centraliseret opbevaring af logs	✗		**0%**
SPG: 23	Håndtering af peak EPS	✗		
SPG: 24	Indeksering af gemte logs	✗		
SPG: 25	Adgang til logs baeret på roller	✗		
SPG: 26	Håndtering af specifikke retention perioder	✗		
SPG: 27	Log data integritet	✗		
SPG: 28	Nemt interface for at søge i logs (ingen scripting sprog)	✗		
SPG: 29	Drilldown i den enkelte søgning	✗		
SPG: 30	Ultra hurtig søgningi specifikke logs	✗		
SPG: 31	Søgning i både strukturerede logs og ustrukturerede logs	✗		
SPG: 32	Fleksibel prædefineret søgning	✗		
SPG: 33	Søgning i specifikke tidsrammer	✗		
SPG: 34	Søgning efter boolean logik	✗		
SPG: 35	Søgning efter RegEx	✗		
	Analyse og workflow			
SPG: 35	Robuste og dækkende korrelerings regler	✗		**0%**
SPG: 36	Mulighed for at korrelere på tværs af logkilder	✗		
SPG: 37	Statistisk/anormalitets korrelering	✗		
SPG: 38	Historisk korrelering	✗		
SPG: 39	Session Korrelering	✗		
SPG: 40	Korrelering mod lister	✗		
SPG: 41	Inddeling af logkilder i logiske grupper	✗		
SPG: 42	Reduktions af falske positiver / støj. Hvordan?	✗		
SPG: 43	Genkendelse af bestemte "mønstre" i logs	✗		
SPG: 44	Kæder af korreleringsregler	✗		
SPG: 45	Alarmering på basis af korrelering	✗		
SPG: 46	Genbrug af filtre og objekter	✗		
SPG: 47	Integration til andre IT Sikkerhedsværktøjer	✗		
SPG: 48	Incident response og administration og rapportering	✗		
SPG: 49	Intern audit af brugen af LMS	✗		
	SIEM Rapportering og visualisering			
SPG: 50	Færdige rapporter til compliance og andre formål	✗		**0%**
SPG: 51	Mulighed for at lave egne rapporter helt fra grunden	✗		
SPG: 52	Rapporter over tendenser i LMS	✗		
SPG: 53	Logiske diagrammer og dashboards	✗		
SPG: 54	Mulighed for at lave egne dashboards helt fra grunden	✗		
SPG: 55	Visualisering af angreb	✗		
	Avanceret brug			
SPG: 56	Automatisering af compliance arbejdet	✗		**0%**
SPG: 57	Visualisering 6 Alarmering på udbrud af angreb (fx virus/orm) i organisationen	✗		
SPG: 58	Definition af brugeradgang på rolle basis	✗		
SPG: 59	Overvågning af aktivitet på brugerniveau	✗		
SPG: 60	Overvågning af specifikke konti - fx service konti	✗		
SPG: 61	Visualisering & alarmering på insider trusler	✗		
SPG: 62	Mulighed for at lave en forentic undersøgelse af et forløb/incident	✗		
SPG: 63	Aktiv mitigering af trusler på server og endpoints	✗		