Bijlage J Onderwerpen en casussen voor de presentatie Aanbesteding SOC/SIEM

Naar aanleiding van de inschrijving zal de aanbestedende dienst u mogelijk vragen voorleggen, die u in de presentatie kunt beantwoorden.

Punt	Minuten	eind	Omschrijving
1.	5	5	Geef aan wie de presentatie verzorgt, met korte info over de leverancier.
2.	15	20	Licht het Plan van Aanpak toe, waarbij u de vragen van de aanbestedende dienst beantwoordt (gunningscriterium 1)
3.	10	30	Laat een handleiding voor het configureren van de FortigateFirewall en/of FortiAnalyzer zien, waarbij u aantoont dat de benodigde informatie voor het detecteren van use cases wordt geleverd. (gunningscriterium 2)
4.	30	60	U licht toe hoe en op basis van welke (log-)informatie u de volgende use cases detecteert (zowel met de huidige als de mogelijke toekomstige EDR oplossingen): - Geweigerde toegang (Access denied na sudo, cat /etc/shadow etc.) op Linux-systemen - IP-discovery en portscans op interne netwerksegmenten - Online brute force password aanvallen, inclusief password spraying, zowel extern als intern - Dump van passwordhashes - Aanmaken van een DomainAdmin account - Toevoegen van accounts aan groepen met beheerdersrechten (AD/Windows en Linux) - Login vanuit ongebruikelijke locaties/verplaatsingen - E-mails met kwaadaardige bijlagen of links - Versleuteling van gegevens (ihkv Ransomware Aanval) - Extractie van data (gunningscriterum 2/3)
5.	10	70	Licht toe hoe u naar uw mening met uw afdekking van de detectie van aanvalstechnieken uit het Mitre Att&ck framework een adequate detectie biedt, met specifieke aandacht voor Log4J en printnightmare. (Gunningscriterium 3)
6.	10	80	Licht een (geanonimiseerd) real-life voorbeeld van een complexe high/critical casus toe van het proces van detectie en de opvolging daarvan, inclusief communicatie met en acties genomen door de klant.
7.	5	85	Idem voor een low/medium casus
8.	5	90	Idem voor een threat hunting casus
9.	15	105	Beantwoording van overige vragen van de aanbestedende dienst
Totaal	105		