**Overzicht van een Ransomware Simulatie**

1. **Voorbereidingsfase**
	* **Analyse van Huidige Beveiligingsprotocollen**: De simulatie begint met een grondige analyse van de bestaande beveiligingsprotocollen en -procedures van de organisatie. Dit helpt bij het op maat maken van de simulatie.
	* **Ontwikkeling van Scenario's**: Er worden realistische ransomware-aanvalsscenario's ontwikkeld, rekening houdend met de specifieke kenmerken en behoeften van de organisatie.
2. **Uitvoeringsfase**
	* **Simulatie van Ransomware-aanval**: Een gecontroleerde, realistische cyberaanval wordt gesimuleerd. Dit test hoe het team reageert onder druk en identificeert potentiële zwakheden in de verdedigingsstrategie.
	* **Diverse Onderdelen van de Simulatie**: Dit kan onder meer inhouden:
		+ Stakeholderbetrokkenheid.
		+ SIEM (Security Information and Event Management) Threat Detection.
		+ Trainingstests voor medewerkers.
		+ Evaluatie van incidentrespons.
		+ Actieve monitoringtests.
		+ Oefeningen voor crisisteams.
		+ Real-time updates en plotwendingen.
		+ Oefeningen voor externe communicatie.
3. **Evaluatiefase**
	* **Debriefing en Evaluatie**: Na de simulatie volgt een uitgebreide debriefing waarbij de prestaties worden geanalyseerd.
	* **Identificatie van Verbeterpunten**: Zwakke punten en gebieden voor verbetering worden geïdentificeerd.
	* **Advies voor Aanpassingen**: Er worden aanbevelingen gedaan voor mogelijke aanpassingen aan beveiligingsprotocollen en trainingen.
4. **Rapportage en Follow-Up**
	* **Gedetailleerde Rapportage**: Een uitgebreid verslag van de simulatie en de bevindingen wordt verstrekt.
	* **Technische en Procedurele Evaluatie**: Een diepgaande evaluatie van zowel technische aspecten als procedures.
	* **Aanbevelingen voor de Toekomst**: Advies over hoe de organisatie zich verder kan ontwikkelen en verbeteren in cyberweerbaarheid.

 **Overwegingen voor "Make or Buy"**

* **Expertise en Resources**: Beschik je over de benodigde expertise en middelen om een dergelijke simulatie intern te ontwikkelen en uit te voeren?
* **Kosten**: Vergelijk de kosten van het zelf ontwikkelen van een simulatieprogramma met de kosten van het inkopen van deze dienst.
* **Tijd en Efficiëntie**: Het opzetten van een eigen simulatie kan tijdrovend zijn. Afwegen of de tijd die hierin geïnvesteerd wordt, opweegt tegen het direct inkopen van de dienst.
* **Maatwerk**: Overweeg of de simulaties die door externe partijen worden aangeboden, voldoende aanpasbaar zijn aan de specifieke behoeften van jouw klanten.

Het opnemen van ransomware simulaties in je dienstenpakket kan een waardevolle toevoeging zijn, gezien de toenemende dreiging van cyberaanvallen. Het biedt klanten een praktische manier om hun voorbereidingen op dergelijke incidenten te testen en te verbeteren.

**Kosten voor deze Simulatie al naar gelang de grote van het onderzoek:**

Klein is 5.000,-
Midden is 10.000,-
Groot is 15.000,-