Aanleiding voor het behoefte onderzoek (verder: de vragenlijst genoemd):

Met GGI-Veilig verhogen gemeenten en gemeentelijke samenwerkingsverbanden hun digitale weerbaarheid en maken zij hun ICT-infrastructuur veiliger. GGI-Veilig bestaat uit een portfolio van producten en diensten voor operationele informatiebeveiliging en is ingedeeld in drie percelen, die als afzonderlijke sets van producten/diensten kunnen worden gezien.

Na het wegvallen van **GGI-Veilig, perceel 1 SIEM/SOC-dienstverlening** is onderzocht of er behoefte is aan een opvolging hiervan.

- Anders dan bij de eerdere behoefte-inventarisatie werd niet uitgegaan van één geïntegreerde dienst voor zowel de monitoring, detectie en response als voor de SOC-dienstverlening. Beide aspecten zijn in de vragenlijst apart behandeld.

Doel van de vragenlijst: ophalen of er (nog) behoefte is aan een vorm van collectiviteit.
Vooraf hebben we aangegeven dat we resultaten na afloop (geanonimiseerd) delen. Daar geven we middels dit rapport gehoor aan.

Over de respondenten:

- De lijst is 86 keer ingevuld, echter 2 x door 1 gemeente. In totaal zijn er dus 85 unieke respondenten.
    - Een deel van de respondenten heeft dit ingevuld namens een samenwerkingsverband. Hierdoor hebben we van iets meer dan 155 van de 344 gemeenten een reactie ontvangen. Dit komt neer op ongeveer 45% van de hele doelgroep, daarmee beschouwen we dit onderzoek als representatief (red. hiervoor moet het percentage minimaal tussen de 35% en 50% liggen).
    - Voor het invullen van de vragenlijst is er telefonisch gevraagd aan gemeenten om dit te doen. Een veel gehoorde reactie was dat er nog interne afstemming moest plaatsvinden. De aanname die we hierop doen is dat een deel van de niet-respondenten wegbleef omdat zij nog geen antwoord op de vragen hebben. Dit sluit aan op een deel van de reacties die uit het behoefte onderzoek komen.
- De lijst is geanonimiseerd opgeleverd. Dit in verband met de privacy wetgeving (AVG) waarbij we niet meer informatie vragen dan wij inhoudelijk voor ons werk nodig hebben. In dit geval gebruiken we de contactgegevens alleen voor de terugkoppeling naar de deelnemers van de vragenlijst.

Wordt in of voor uw organisatie al gebruik gemaakt van een SIEM?

Van de respondenten die ‘ja’ invulden, hebben er 22 een toelichting gegeven. Waar men daadwerkelijk afneemt wisselt. Deze groep valt op te splitsen in *geen* deelnemers GGI-Veilig perceel 1 en *wel* deelnemers GGI-Veilig perceel 1. De eerste groep had de keuze om niet van de GGI-Veilig SIEM oplossing gebruik te gaan maken genomen voorafgaand aan de aanbesteding van GGI-Veilig. De gegeven toelichtingen van de tweede groep zijn als volgt samen te vatten:

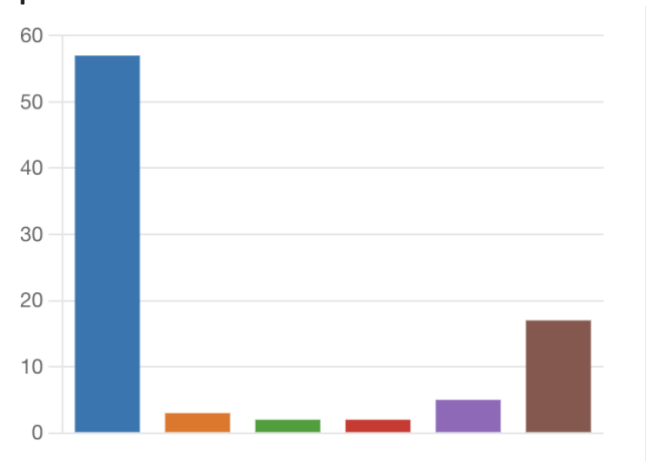
- Enkele hadden al een (soort) SIEM oplossing geïmplementeerd welke op termijn door de GGI-Veilig SIEM oplossing vervangen zou worden;
- Enkele hadden bij het traject van outsourcing/transitie naar de cloud de implementatie van een SIEM oplossing onderdeel van het traject gemaakt (mogelijkheid binnen de raamovereenkomst);
- Enkele hadden in overleg met de leverancier de overeenkomst eerder beëindigd voordat de raamoverkomst werd beëindigd en hebben aansluitend voor een andere oplossing gekozen;
- Enkele hebben de overeenkomst beëindigd nadat de raamoverkomst werd beëindigd en hebben aansluitend voor een andere oplossing gekozen.

Van de respondenten die ‘nee’ invulden, hebben er 23 een toelichting gegeven. De meest gegeven antwoorden:

- Dat men in afwachting was van GGI veilig en dit (nog) niet heeft opgepakt sinds ontbinding;
- Dat er een basis variant is die niet voldoet aan de formele vereisten;
- Dat men inmiddels zelf aan het aankopen of implementeren is;

.

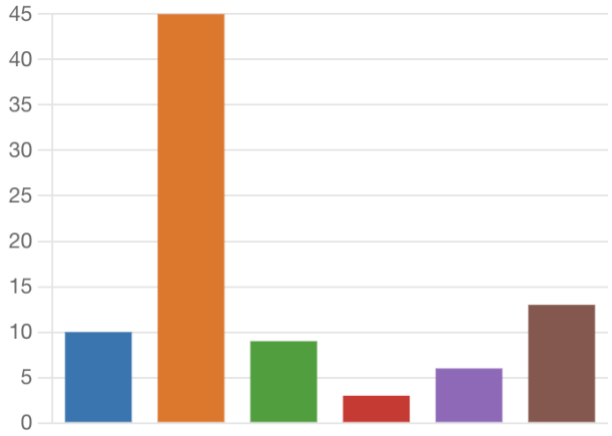
Is uw organisatie van plan om een dergelijke oplossing in de komende 2 jaar (opnieuw) in te kopen?



De antwoord categorieën (VLNR)

- **Blauw: ja > 57 respondenten**
- Oranje: nee; want we gaan over naar een Shared Service Center (SSC) > 3 respondenten
- Groen: nee; reorganisatie/samenwerking met andere gemeenten > 2 respondenten
- Rood: nee; andere prioriteiten > 2 respondenten
- Paars: nee; we wachten op de transitie naar de cloud > 5 respondenten
- Bruin: anders, namelijk kreeg 17 reacties met eigen toelichting. Deze zijn terug te lezen in de spreadsheet. De meest gegeven reacties waren:
    - **We zijn voorzien, al dan niet tijdelijk, en/of breiden dit uit.**
    - **Er is geen prioriteit voor (om diverse redenen)**

Gaat de voorkeur van uw organisatie bij de implementatie van de SIEM uit naar:



- Blauw: afname van Managed Service met volledig technisch en functioneel beheer door de leverancier waarbij organisatie zelf de feitelijke inzet van de SIEM-applicatie bepaalt en beheert
  > 10 respondenten
- **Oranje: afname van Managed Service met volledig technisch en functioneel beheer door de leverancier waarbij de organisatie door een leverancier ondersteund wordt bij de feitelijke inzet van de SIEM-applicatie**
  > 45 respondenten
- Groen: afname van product (de SIEM-applicatie) waarbij het technisch en functioneel beheer door de organisatie zelf wordt zelf gedaan, maar wel met opties voor ondersteuningsmogelijkheden (functioneel gericht)
  > 9 respondenten
- Rood: afname van product (de SIEM-applicatie) waarbij het technisch en functioneel beheer volledig door de organisatie zelf wordt zelf gedaan
  > 3 respondenten
- Paars: geen voorkeur
  > 6 respondenten
- Bruin: anders namelijk kreeg 13 reacties met eigen toelichting. Deze zijn terug te lezen in de spreadsheet. De meest gegeven reactie is: **we zijn nog in onderzoek.**

Wat opvalt is dat een Managed Service de voorkeur geniet.

Als u kiest voor een SIEM in eigen beheer, welke implementatie-vorm heeft dan de voorkeur van uw organisatie

- **Blauw: een volledig cloud based oplosing**
  > 27 respondenten
- Oranje: een hybride applicatie, tussen SaaS en On-Premise
  > 22 respondenten
- Groen: een On-Premise gehoste applicatie
  > 3 respondenten
- Rood: niet van toepassing
  > 23 respondenten
- Paars: Anders, namelijk kreeg 11 reactie met eigen toelichting. Deze zijn terug te lezen in de spreadsheet. De meest gegeven reacties zijn: **De keuze is nog niet gemaakt + we zijn nog in onderzoek.**

Maakt uw organisatie nu of in de komende 2 jaar gebruik van cloud-infrastructuurdiensten (IaaS) zoals Ms-Azure, Amazon-cloudservices, Google-cloudservices of van andere marktpartijen dan wel van uitbestede diensten (bijvoorbeeld door deelname aan een Shared Service Centrum)?

- Blauw: ja; grotendeels
  > 25 respondenten
- **Oranje: ja; een deel, namelijk ongeveer …%**
  > 36 respondenten
- Groen: nee; wel van plan binnen 2 jaar
  > 16 respondenten
- Rood: nee; niet van plan
  > 9 respondenten

  Van de 36 respondenten die Oranje antwoorden kwamen de volgende uitkomsten:
  - 3 x 5 %
  - 4 x 10 %
  - 3 x 15 %
  - 2 x 20 %
  - 4 x 25 %
  - 4 x 30 %
  - 2 x 40 %
  - 5 x 50 %
  - 1 x 60 %
  - 1 x 70 %
  - 6 x niet procentueel uit te drukken op dit punt

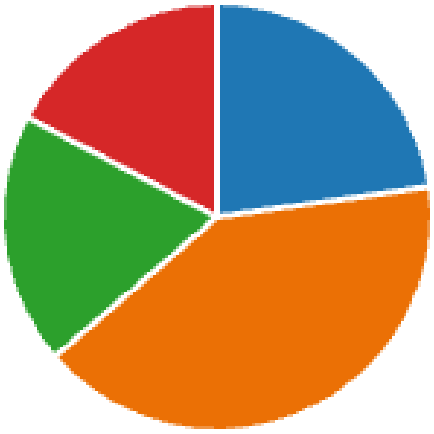
Gaat uw organisatie dan ook de SIEM van uw leverancier van clouddiensten gebruiken?

ja	16
nee	6
nog niet bekend	39

Ruimte om uw antwoord toe te lichten of (indien gewenst) aan te geven wie de gekozen/ voorgenomen leverancier cloudomgeving is:

Meest genoemd zijn: Azure, Microsoft Sentinel. Waar men geen leverancier benoemde hangt de keuze (veelal) af van het nog lopende onderzoek.
Nuttig om hier de excel sheet te raadplegen omdat er veel inhoudelijke terugkoppeling is gegeven.

Is uw organisatie voorstander van een collectieve aanpak t.a.v. de inkoop van SIEM-oplossing(en)? (Meerdere antwoorden zijn mogelijk)



- Blauw: ja; alleen als gekozen kan worden uit meerdere oplossingen voor SIEM
  > 25 respondenten
- **Oranje: ja; ervan uitgaande dat de geboden oplossing voldoende flexibiliteit biedt**
  > 45 respondenten
- Groen: nee; geen collectieve inkoop. Mijn organisatie organiseert zelf een aanbesteding
  > 21 respondenten
- Rood: anders werd door 19 respondenten ingevuld.

Respondenten konden meerdere antwoorden invullen. Dat is ook gedaan. Het is nuttig om hier de toelichting bij te raadplegen (zie excel sheet). **Het was ook voor iedereen mogelijk om een toelichting te geven op het antwoord. Dit werd door 45 respondenten gedaan.**

Veel gehoorde reacties:

- We kunnen niet wachten:
  - Aanbesteding traject loopt traag/ is omslachtig
- Meerdere marktpartijen want:
  - Het moet aansluiten bij de passende infrastructuur
  - Passend zijn voor kleine en grote gemeenten (ambities en wensen verschillen)

Dit zijn belangrijke aspecten om te erkennen in ons contact met de gemeenten. Er is **twijfel** over **de snelheid en voortgang**. En of een one-size-fits-all principe, zoals dat vaak gaat met collectieve inkoop, wel werkt voor iedere deelnemer. Deze punten moeten geadresseerd worden voor een vervolg opgestart kan worden.

In geval van collectieve inkoop, hebt u behoefte aan implementatie ondersteuning?

Bij het antwoord ‘anders’ zijn vooral reacties gegeven o.b.v. eerdere antwoorden (dat men het anders inricht bijvoorbeeld, dus dat de vraag niet van toepassing is). **Er is wel één (terugkerende) relevante reactie gegeven onder anders: dat er geen eenduidig ja of nee te geven is omdat het afhangt van de oplossing die gekozen wordt.**

Wordt in of voor uw organisatie al gebruik gemaakt van SOC-expertise voor de analyse en (advisering voor) opvolging van security meldingen door een SIEM?

ja	31
nee	55

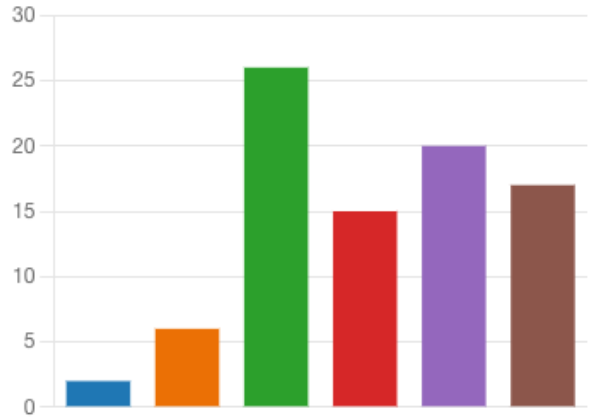
Hier kon men optioneel een toelichting geven op het ingevulde antwoord. Dit is door 29 respondenten gedaan. Een diverse reeks toelichtingen: het doornemen daarom zeker waard.
Grofweg is de reactie in 3 opties te verdelen:

1. **we doen het nu niet,**
2. **we hebben het half-half in huis,**
3. **het is uitbesteed.**

Voor de analyse en (advisering voor) opvolging van security meldingen door een SIEM: (Meerdere antwoorden mogelijk)

- Blauw: heeft mijn organisatie een eigen SOC-dienst, dan wel wordt mijn organisatie daarin door een derde partij (bijvoorbeeld SSC) reeds voorzien van 24/7-analyse, advisering en eventueel opvolging
  > 13 respondenten
- Oranje: heeft mijn organisatie een eigen SOC-dienst, dan wel wordt mijn organisatie daarin door een derde partij (bijvoorbeeld SSC) reeds voorzien van analyse en advisering gedurende kantoortijd en is geen behoefte aan SOC-dienstverlening buiten kantoortijd
  > 8 respondenten
- **Groen: wil mijn organisatie een SOC-dienst vanuit de markt afnemen voor een 24/7-dienstverlening.**
  > 63 respondenten
- Rood: anders werd door 13 respondenten gekozen en veelal onderbouwd met **“onbekend”.** Daarnaast hebben nog 20 andere respondenten een reactie gegeven, er waren geen opvallende opmerkingen. Lees hiervoor de excel sheet na.

Is uw organisatie voorstander van een collectieve inkoop van SOC-dienstverlening?



- Blauw: ja; alleen als de door mijn organisatie zelf verworven en ingezette SIEM op de collectieve SOC-dienstverlening kan worden aangesloten
  > 2 respondenten
- Oranje: ja, alleen als de door mijn organisatie zelf verworven en ingezette SIEM op de collectieve SOC-dienstverlening kan worden aangesloten en de SOC-dienstverlening tevens opties bevat voor het afnemen van advisering over en ondersteuning bij de inzet van de SIEM
  > 6 respondenten
- **Groen: ja; ervan uitgaande dat de collectief verworven SIEM-oplossing(en) op de collectieve SOC-dienstverlening kan/kunnen worden aangesloten en de SOC-dienstverlening tevens opties bevat voor het afnemen van advisering over en ondersteuning bij de inzet van de SIEM**
  > 26 respondenten
- Rood: ja, alleen als de collectief verworven SOC-dienstverlener tevens de SIEM levert, implementeert en functioneel en technisch beheert en daarmee een geïntegreerde SIEM/SOC dienst levert als managed service (vergelijkbaar met aanbesteding 2019)
  > 15 respondenten
- Paars: nee; geen collectieve inkoop. Mijn organisatie organiseert zelf een aanbesteding
  > 20 respondenten
- Bruin: Anders namelijk werd door 17 respondenten ingevuld en door 16 aangevuld met een toelichting. De meningen lopen daarin uiteen. Aan te raden om alle reacties te lezen.
  > 17 respondenten

Tot slot, wilt u ons nog iets meegeven dat niet aan bod is gekomen in de vragenlijst

Er is door 38 respondenten een inhoudelijke reactie gegeven, de meest in het oog spingende zaken waar wij met elkaar actie op kunnen nemen zijn hier opgenomen:

- Wij zullen zeker geen gebruik maken van de VNG, ik ben na de telefonie en siem/soc een beetje het vertrouwen kwijt.
- Vrijheid om te kiezen uit meer dan 1 leverancier is voor ons belangrijk.
- Operationeel in 2023; toekomst bestendige oplossing (meegroeien met de stand der techniek); ontzorging!
- Waarom komt er niet een siem/soc dienst vanuit de IBD? Zij verzorgen en bewaken al een deel, dus waarom niet opschalen en deze dienst aanbieden zoals een centrale meldkamer?
- (…) Daarnaast vraag ik mij serieus af hoeveel gemeenten daadwerkelijk al SIEM-SOC geïmplementeerd hebben.
- De te verwachten planning zal ook mede bepalend zijn voor deelname aan de collectieve Inkoop.
- De GT-aanbestedingen monden uit in complexe minicompetities. Dit geldt voor bv GT-veilig en GT-print waardoor het onaantrekkelijk wordt om deel te nemen. De benodigde tijd om een minicompetitie in te vullen, staat niet in verhouding tot de financiële voordelen die worden beoogd.

Conclusie en aanbevelingen

Uitkomst op de vraag of er (nog) behoefte is aan een vorm van collectiviteit?
Ja, er is overwegend interesse voor een collectieve inkoop met een aantal randvoorwaarden:

- De snelheid en de voortgang moet aansluiten op voor gemeenten gewenste wijze. Hierbij moet het niet werken van het 'one-size-fits-all' principe (zoals dat vaak toegepast wordt bij collectieve inkoop) worden geadresseerd voordat een vervolg kan worden opgestart.
- De ruimte voor meerdere aanbieders, zodat er keuze is.
- Wat de doorlooptijd zal zijn voor een collectieve inkoop: er is (enige) haast geboden en er is twijfel of een collectief snel (genoeg) is.
    - Het gaat hierbij zowel over het proces van aanbesteden als de tijd die nodig is voor implementatie.
- De complexiteit van het traject: loont het om de tijd te steken in het collectief (compact en simpel houden) of is het "net zo makkelijk en snel" om het zelf te doen?

Heeft u na het lezen van deze informatie vragen of bent u benieuwd of (en hoe) u kunt deelnemen aan het GGI-Veilig contract?
Lees dan verder op de webpagina GGI-Veilig. Aanvragen dient u in bij het *Servicecentrum Gemeenten* van VNG Realisatie. Let op, voorwaarde voor het gebruik van de verschillende percelen is dat u zich hebt aangemeld voor het betreffende perceel. Indien u dit niet heeft gedaan voor de aanbesteding van GGI-Veilig, maar alsnog wilt, kunt u contact opnemen met info@scgemeenten.nl.