Wat is SOC/SIEM?
SIEM/SOC is een voorziening die wordt ingezet voor monitoring en response. Een Security Information & Event Management Systeem (SIEM) is het gereedschap dat in staat is om (log)informatie vanuit verschillende bronnen te raadplegen, te interpreteren en te correleren naar wat zich binnen deICT-infrastructuur afspeelt op het gebied van digitale aanvallen en andere beveiligingsincidenten. Het beheer van het SIEM systeem en de analyse van meldingen vindt plaats vanuit een Security Operations Center (SOC). Dit SOC is decentrale plaats bij de externe leverancier van waaruit het monitoren van de digitale infrastructuur van de gemeente plaatsvindt op basis van verzamelde gebeurtenissen in logbestanden. Het soort applicaties en apparaten waar loginformatie vanverzameld wordt, kan zeer uiteenlopend zijn: van firewalls, IDS, routers en het netwerkverkeer tot aan bedrijfsapplicaties. Alle systemen die relevante informatie kunnen aanleveren om zicht te krijgen op het gebruik, de beveiliging of de status van het netwerk en de daarop aangesloten systemen, kunnen daarbij worden gebruikt.

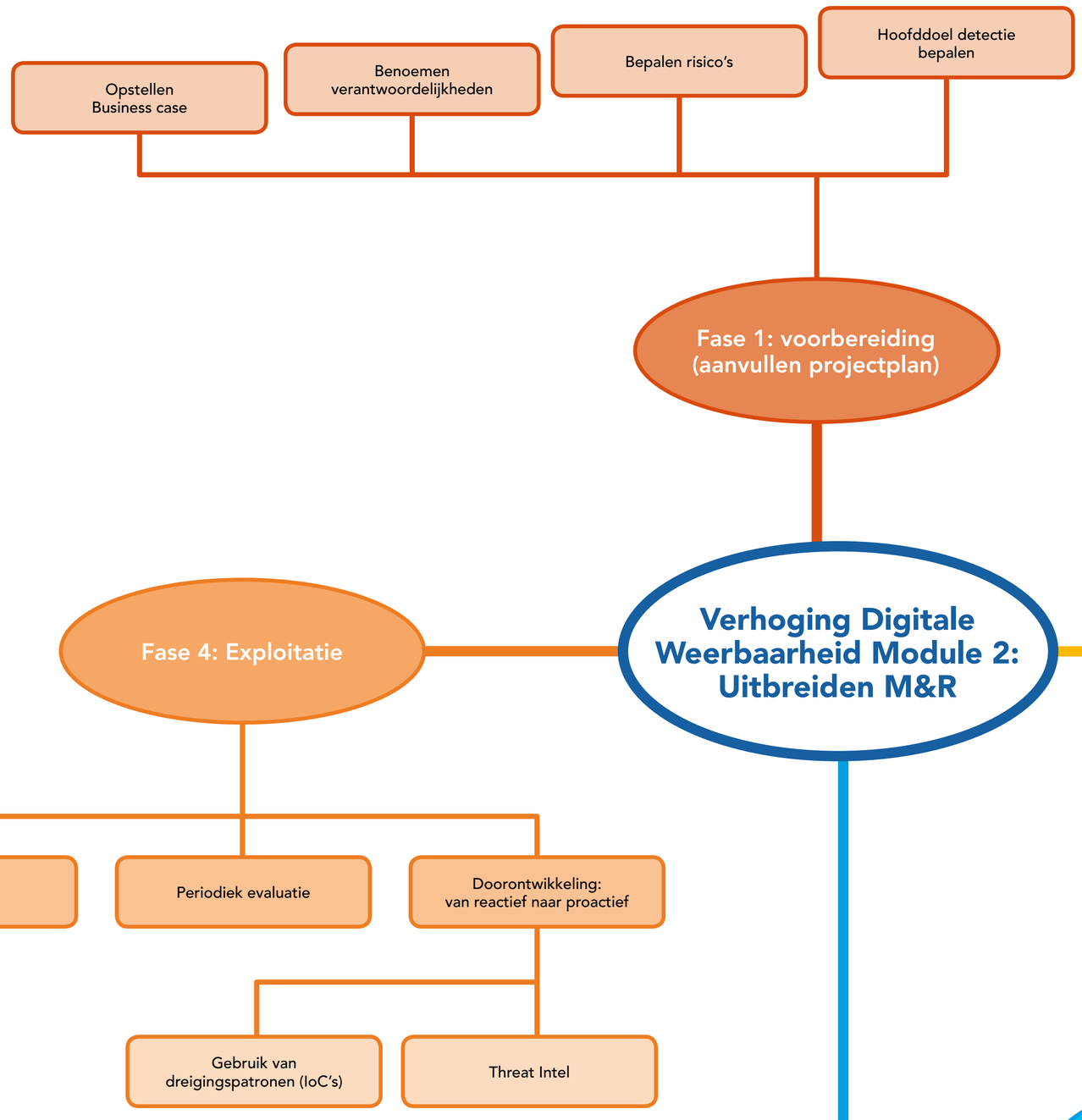
Uitgangspunt is dat SIEM/SOC wordt uitbesteed. Veel gemeenten hebben zich aangemeld voor GGI veilig en/of hebben aangegeven deze dienst bij een leverancier af te willen nemen.
Uitbreiden van M&R richt zich op het ontwikkelen en toevoegen van zowel Technische Use Cases alsook Business Use Cases.

Zie voor **nadere uitleg** de handreiking Uitbreiden van Monitoring en Response

Fase 1: Voorbereiding

Monitoring & Response kan effectief worden ingezet als de juiste voorbereidingen zijn getroffen. Een gedegen projectplan, met business case en een goede samenwerking tussen de CISO, FG, ICT & proceseigenaren is essentieel. Hieronder zijn enkele vragen opgesomd die richting geven om M&R goed voor te bereiden.

- ☐ Is er een business case opgesteld met daarin de meerwaarde om interne stakeholders te overtuigen?
- ☐ ZIjn de verantwoordelijkheden benoemd?
- ☐ Zijn de risico's in kaart gebracht?
- ☐ Zijn bedrijfskritische informatiesystemen (de kroonjuwelen) gedefinieerd?
- ☐ Is het hoofddoel voor detectie bepaald? (Technisch of gerelateerd aan de bedrijfsprocessen)



Fase 4: Exploitatie

Na overdracht naar de beheerorganisatie kan de dienst geleverd worden volgens de dienstverleningsovereenkomst. De signaleringen die hieruit voortvloeien kunnen nu opgevolgd worden. Er dient tevens een evaluatieproces te zijn om zowel de M&R leverancier als de interne samenwerking te evalueren. Nu kan er ook nagedacht worden over het doorontwikkelen naar een proactieve/preventieve dienstverlening. Hieronder zijn enkele vragen opgesomd die richting geven om de exploitatiefase van M&R in goede banen te leiden.

- ☐ Is er een periodiek evaluatieproces afgesproken met de M&R leverancier gebaseerd op specifieke indicatoren?
- ☐ Worden de signaleringen goed binnen incidentmanagement opgepakt?
- ☐ Wordt er geevalueerd hoe de interne beheerorganisatie met de meldingen van de M&R leverancier omgaat?

Doorontwikkeling:
- ☐ Wordt er gebruik gemaakt van dreigingspatronen/Threat Intel (IoC's)?
- ☐ Vindt er opvolging plaats op basis van deze patronen?

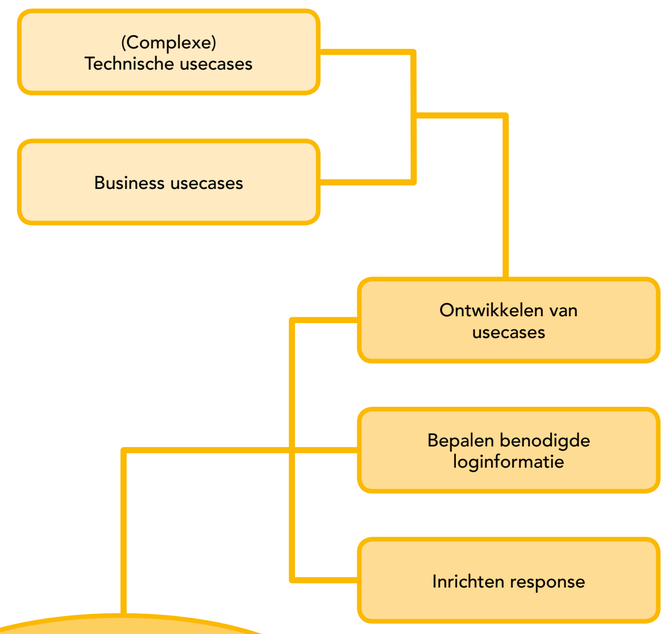
Fase 2: Ontwerp

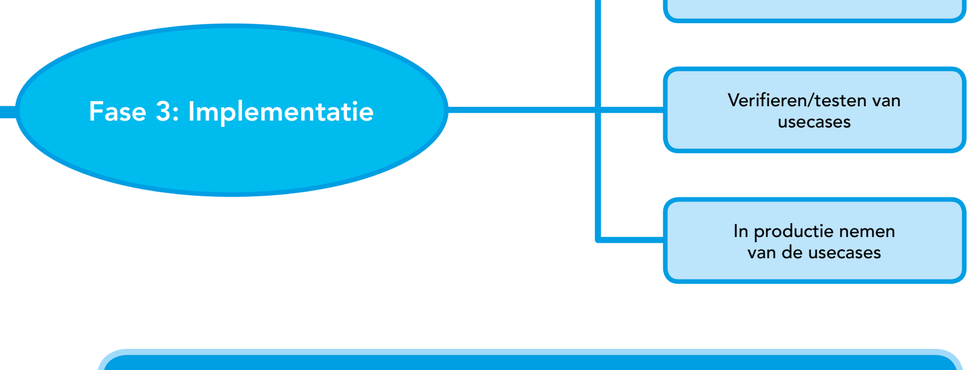
Tijdens deze fase dient er een ontwerp gemaakt te worden van de uitbreiding van de M&R omgeving. Bij starten met M&R is er al een goed begin gemaakt en daar kan nu op worden voort geborduurt. Als (een gedeelte van) de ICT is uitbesteed dan dienen de contracten met de leveranciers onderzocht te worden, met als doel om wijzigingen in het geval van een security incident snel op te kunnen lossen.
Hieronder zijn enkele vragen opgesomd die richting geven om de uitbreiding van M&R goed te ontwerpen.

- ☐ Is er capaciteit en kennis voor het ontwikkelen van additionele Use Cases? (Zowel technisch als business)
- ☐ Is er een samenwerking tussen proces eigenaren en technisch inhoudelijke mensen(bv beheerders) tbv het ontwikkelen van de Business Use Cases?
- ☐ Is er een ICT architect betrokken bij bovenstaande samenwerking?
- ☐ Zijn business use cases zo beschreven dat alle partijen het begrijpen?
- ☐ Is bepaald welke loginformatie nodig is?
- ☐ Zijn de logbronnen gekoppeld aan de SIEM omgeving?
- ☐ Zijn de alerts goed gedefinieerd?
- ☐ Is bepaald waarover gerapporteerd wordt?
- ☐ Is binnen de gemeente de 'response' op security incidenten ingericht?
- ☐ Is er een prioriteringsproces binnen de gemeente voor de alerts?

Let op!

Voor het ontwikkelen van Business Use Cases is een samenwerking noodzakelijk tussen technici en proces deskundigen. Deze partijen spreken niet dezelfde "taal", wat doorgaans additionele complexiteit oplevert.
Houd hier s.v.p. rekening mee.





Fase 3: Implementatie

De implementatie van Monitoring en Response is bij het uitbreiden van M&R een activiteit tussen technisch specialisten, beheerders en proceseigenaren. Zij implementeren de usecases. Als de technische implementatie klaar is, moet de opvolging van de signaleringen worden geïmplementeerd. Dit kent ook organisatorische aspecten en is daarmee een samenspel tussen technici en procesdeskundigen.

Hieronder zijn enkele vragen opgesomd die richting geven om M&R goed te implementeren.

- ☐ Zijn de bewaartermijnen van de loginformatie bepaald?
- ☐ Is de loginformatie van de nieuwe usecases correct geclassificeerd?
- ☐ Zijn de usecases getest en geverifieerd door de betreffende verantwoordelijken?
- ☐ Zijn de usecases correct in de tooling geconfigureerd?
- ☐ Is de opvolging (respons) geïmplementeerd en getest?

VNG Realisatie
INFORMATIE BEVEILIGINGS DIENST