BIJLAGE 2 Behoeftebeschrijving SOC-diensten

Onze organisatie – Z-CERT - heeft behoefte aan een Security Operations Center (SOC) dat 24/7 toezicht houdt op de digitale weerbaarheid van onze IT-omgeving. Het SOC ondersteunt ons bij het tijdig signaleren, analyseren en mitigeren van dreigingen, zodat de continuïteit, integriteit en vertrouwelijkheid van onze bedrijfsprocessen worden gewaarborgd.

De beoogde dienstverlening omvat in ieder geval de volgende **vijf kerncompetenties**:

- **Kerncompetentie 1: Monitoring & detectie**
  - Real-time bewaking van relevante logbronnen (zoals netwerk, endpoints, cloud, applicaties en overige relevante bronnen).
  - Gebruik van geavanceerde detectiemechanismen (bijvoorbeeld SIEM, XDR, SOAR of gelijkwaardige oplossingen).

- **Kerncompetentie 2: Incidentrespons**
  - Analyse, triage en opvolging van beveiligingsmeldingen.
  - Ondersteuning bij het treffen van mitigerende maatregelen en herstel na incidenten.

- **Kerncompetentie 3: Threat intelligence & analyse**
  - Integratie van actuele dreigingsinformatie in de monitoring.
  - Correlatie van dreigingen met gebeurtenissen in onze omgeving.
  - Periodieke dreigings- en trendanalyses.

- **Kerncompetentie 4: Rapportage & compliance**
  - Periodieke operationele en tactische rapportages over incidenten, trends en verbeterpunten.
  - Ondersteuning bij het kunnen aantonen van naleving van relevante wet- en regelgeving en normen (zoals AVG en ISO 27001).

- **Kerncompetentie 5: Samenwerking & dienstverlening**
  - Heldere dienstafspraken (zoals SLA/DAP) en periodieke overleggen op operationeel, tactisch en strategisch niveau.
  - Inzicht in monitoring- en alarmeringsinformatie (bijvoorbeeld via een portal of SIEM-omgeving) en de mogelijkheid om gezamenlijk monitoring- en alertingscenario's op te stellen en te verfijnen.

De beoogde oplossing moet schaalbaar zijn en kunnen meebewegen met de verdere ontwikkeling van onze IT-omgeving en informatiebeveiliging. In de vervolgfase van de procedure wordt de scope van de dienstverlening nader uitgewerkt.