Geaggregeerd beeld IT-landschappen Deelnemers (op basis van inventarisatie)

Op basis van de beschikbare inventarisatie van securityproducten en -diensten ontstaat het volgende geaggregeerde beeld van de IT-landschappen van de Deelnemers.

De IT-omgevingen van de Deelnemers zijn overwegend Microsoft-georiënteerd en hybride van aard, waarbij zowel on-premises infrastructuur als cloudomgevingen (met name Microsoft Azure en Microsoft 365) worden toegepast. Vrijwel alle Deelnemers beschikken over Microsoft E5-licenties of vergelijkbare functionaliteit, waarmee reeds een belangrijk deel van de benodigde security- en loggingfunctionaliteit beschikbaar is.

De beveiligingsarchitectuur bestaat uit een combinatie van:

- Microsoft security-oplossingen (zoals Defender, Entra ID en Sentinel (in opbouw of reeds in gebruik));
- netwerkbeveiligingscomponenten (zoals firewalls en netwerksegmentatie-oplossingen);
- endpoint- en serverbeveiliging;
- aanvullende (deels legacy of best-of-breed) securitytools bij individuele Deelnemers.

De mate van volwassenheid verschilt per Deelnemer, maar kan in algemene zin als volgt worden getypeerd:

- Basis aanwezig: logging, identity & access management en endpoint security zijn in de meeste gevallen ingericht;
- SOC-volwassenheid variabel: van beperkte monitoring tot reeds ingerichte (of gedeeltelijk ingerichte) SIEM/SOC-capaciteit;
- Use case maturity nog in ontwikkeling: detectielogica en use case management zijn veelal nog beperkt ingericht of niet gestandaardiseerd;
- Procesmatige inbedding wisselend: incident response en security governance zijn aanwezig, maar niet overal uniform of volledig geïntegreerd.

Ten aanzien van datastromen en integraties geldt dat:

- een substantieel deel van de relevante logbronnen reeds technisch beschikbaar is binnen Microsoft-ecosystemen;
- aanvullende integraties nodig zijn voor netwerkcomponenten, on-premises systemen en specifieke applicaties;
- datakwaliteit, normalisatie en consistentie aandachtspunten zijn bij meerdere Deelnemers.

Voor OT-omgevingen geldt een afwijkend beeld:

- de aanwezigheid en volwassenheid van OT-monitoring is beperkt en sterk verschillend per Deelnemer;
- in de meeste gevallen is nog geen structurele logging of SIEM-integratie ingericht;
- implementatie van OT-monitoring vereist doorgaans aanvullende maatregelen, zoals de inzet van OT-specifieke sensoren en passieve monitoringtechnieken;
- één of enkele Deelnemers (waaronder Flevoland) hebben reeds eerste stappen gezet in OT-monitoring.

De omvang en complexiteit van de omgevingen variëren per Deelnemer, maar kenmerken zich in het algemeen door:

- middelgrote tot grote organisaties (orde grootte: duizenden gebruikers en honderden tot duizenden IT-assets);
- een mix van standaardplatformen en specifieke (beleids- en keten-)applicaties;
- een groeiende afhankelijkheid van cloud- en SaaS-diensten.

Dit geaggregeerde beeld dient door Inschrijvers te worden gebruikt als indicatief referentiekader voor de inrichting, dimensionering en prijsstelling van de SOC-dienstverlening. Hieraan kunnen geen rechten worden ontleend. Inschrijvers blijven zelf verantwoordelijk voor het vormen van een realistische inschatting van de benodigde inzet en complexiteit.