

Aansluiten op security monitoring

In onderstaande tabel worden de aansluitmogelijkheden voor interne (toepassingen binnen de Utrecht omgeving) en externe (SaaS en public cloud) weergegeven voor aansluiting op de Sentinel security monitoring omgeving.

Tabel 1 Aansluitmodel security monitoring

Nr.	Protocol	Intern	Toelichting	Extern	Toelichting
1	Rest API	Rest API gebaseerde bron middels Logs Ingestion API in Azure monitor ontsloten	Conform specificaties Log Ingestion API. Voorheen "HTTP data collector API"	Rest API gebaseerde bron middels Logs Ingestion API in Azure monitor ontsloten	Conform specificaties Log Ingestion . Voorheen "HTTP data collector API"
2	Azure Logic app, Azure Function	Alleen indien log ingestion niet functioneert	Alternatief voor log ingestion.	Alleen indien log ingestion niet functioneert	Alternatief voor log ingestion.
3	Azure Monitoring Agent	AMA Agent op IaaS resource	AMA agent levert de log data naar Azure monitor	Geen aansluiting	n.v.t.
4	Syslog	Via syslog collector Azure Monitor	Via een Azure Monitoring Agent met "Syslog NG"	Geen aansluiting	n.v.t.
5	Netflow	Bijv. netwerkkapparatuur	Alleen bij uitzondering	Geen aansluiting	