

CASE STUDY POSTNL

PostNL: grip terug op securitydata



‘We wilden weer grip op onze eigen securitydata en dat is gelukt.’ - Koen Wackers, Team Lead Connectivity IT/OT bij PostNL

De uitdaging die iedereen herkent

Hoe ga je om met torenhoge ingestkosten, maandenlange onboarding van logbronnen en een gebrek aan inzicht in je eigen data? Het zijn uitdagingen waar niet alleen PostNL mee worstelt, maar vrijwel elke organisatie die afhankelijk is van een modern SOC.

Zonder grip op je securitydata loop je drie grote risico's:

- **Kosten lopen uit de hand.** Data die je niet nodig hebt, slokt budget op.
- **Security verliest snelheid.** Elke week vertraging bij nieuwe bronnen betekent langer risico.
- **Gebrek aan controle.** Zonder inzicht beslissen systemen in plaats van jijzelf.

Voor Koen Wackers waren dit geen theoretische vragen. Hij zag dagelijks hoe de bestaande constructie met Exabeam en Kafka zijn team afremde.

‘Het aansluiten van een nieuwe bron duurde soms tot wel twaalf weken, mét de bijbehorende kosten. Dan vraag je je af: doen we dit nog wel op de juiste manier?’

De aanpak samen met SMT

PostNL koos voor een fundamentele stap vooruit: Cribl Stream als nieuwe datalaag. Niet als geïsoleerde tool, maar als onderdeel van een doordachte strategie. Samen met SMT en Cybermeister werden vooraf eisen gesteld: lagere kosten, meer flexibiliteit, beter inzicht. Belangrijker nog: de oplossing moest passen binnen de serverless cloudomgeving van PostNL.

Wackers: ‘Onze infrastructuur is volledig serverless, dus Cribl moest als container draaien via infrastructure-as-code. Dat was even pionieren. Maar samen met SMT, Cribl en ons eigen team hebben we dat stap voor stap opgezet.’

Implementatie met impact

Binnen vier weken draaide Cribl in de dev-omgeving. Een wereld van verschil vergeleken met de twaalf weken die eerder nodig waren om nieuwe bronnen aan te sluiten.

De samenwerking gaf hierin de doorslag: 'SMT bracht structuur, dacht proactief mee en hielp bij het prioriteren. Dat maakte echt het verschil voor ons,' aldus Wackers.

Resultaten die ertoe doen:

- **Onboarding van bronnen teruggebracht van 12 naar 4 weken** (soms direct)
- **40% reductie in ingest-volume** bij AWS CloudTrail (verwachting: 30%)
- **Volledige controle** over welke data wel of niet naar Exabeam gaat
- **Containerized deployment** binnen bestaande serverless AWS-architectuur
- **Toekomstgericht:** uitbreiding met Cribl Edge op sorteerlocaties

'Onze eerste use case liet meteen resultaat zien: ruim 40% minder ingest. En belangrijker nog: we bepalen nu zelf wat we doorsturen, op basis van filtering en context. Dat scheelt niet alleen data, maar ook tijd.'

Waarom dit ook voor jou belangrijk is

Wat PostNL deed, gaat niet alleen over techniek. Het gaat over regie pakken op je eigen data. Wie dat niet doet, betaalt structureel te veel, heeft te weinig controle en verliest snelheid in securityprocessen.

Daar zit de crux: organisaties die nu investeren in een slimme datastrategie winnen aan wendbaarheid, kostenvoordeel en veiligheid. Organisaties die dat niet doen, zetten hun SOC op achterstand.

Waarom SMT?

De ervaring van PostNL laat zien waarom bedrijven SMT inschakelen:

- **Ervaring:** Meer dan 25 jaar bewezen oplossingen voor complexe datavraagstukken.
- **Kennis:** Volledig gecertificeerd in technologieën als Cribl en Exabeam.
- **Pragmatiek:** Geen eindeloze trajecten, maar concreet resultaat binnen een paar weken.
- **Visie:** Niet alleen de tool implementeren, maar organisaties helpen hun datastrategie te verscherpen.

Want grip op je securitydata is geen luxe. Het is een voorwaarde.

Over dit project

- Gebruikte oplossing: Cribl Stream
- Implementatiepartner: SMT
- SIEM-platform: Exabeam
- Strategisch advies: Cybermeister

Over SMT

SMT is al meer dan 25 jaar actief in het oplossen van complexe datavraagstukken. Dankzij diepgaande expertise in data-engineering, slimme tooling en een pragmatische benadering krijgen organisaties weer grip op hun datastromen.

De specialisten van SMT zijn volledig gecertificeerd in de technologieën die worden ingezet, waaronder Cribl. Er wordt uitsluitend gewerkt met bewezen oplossingen, met keuzes die aantoonbare waarde toevoegen. Met een bewezen trackrecord in uiteenlopende sectoren wordt consistent resultaat geleverd — betrouwbaar, schaalbaar en toekomstgericht.

