Nederlandse gemeente versterkt informatiebeveiliging met **hybride SOC** van PuurData

Nederlandse gemeente versterkt informatiebeveiliging met **hybride SOC** van PuurData

Een Nederlandse gemeente wilde haar informatiebeveiliging toekomstbestendig maken en tegelijkertijd grip houden op de eigen IT-omgeving. In samenwerking met PuurData en REQON implementeerde de organisatie een hybride SOC-oplossing op basis van Elastic SIEM. Dankzij de juiste balans tussen eigen regie en de externe expertise van PuurData en REQON beschikt de gemeente nu over meer overzicht, grip en vertrouwen in haar IT-omgeving.

Van verplichting naar praktische oplossing

De aanleiding voor het project lag in de toenemende eisen vanuit wet- en regelgeving, waaronder de Baseline Informatiebeveiliging Overheid (BIO). De BIO is het landelijke kader dat overheden verplicht om informatiebeveiliging aantoonbaar op orde te hebben. Tegelijkertijd wilde de gemeente de stap maken van reactieve naar proactieve monitoring.

Over de gemeente

Een middelgrote Nederlandse gemeente met een eigen IT-afdeling die verantwoordelijk is voor infrastructuur, informatievoorziening en gegevensbeheer. De organisatie werkt met een compacte IT-omgeving waarin efficiëntie, betrouwbaarheid en datasoevereiniteit belangrijke uitgangspunten zijn.

Over REQON

REQON is gespecialiseerd in 24/7 SOC-dienstverlening en ondersteunt organisaties bij het continu bewaken en opvolgen van beveiligingsmeldingen. Met hun managed SOC helpen ze dreigingen vroegtijdig te signaleren en snel te handelen.

“We zijn een kleine organisatie met een sterk eigen IT-team,” vertelt de strategisch informatiemanager. “We wilden niet alles uitbesteden, maar wel 24/7 zekerheid dat onze omgeving bewaakt wordt. Die balans vonden we in de samenwerking met PuurData en REQON.” PuurData ondersteunt organisaties bij data-analyse, monitoring en security op basis van Elastic-technologie. REQON vult dit aan met 24/7 SOC-dienstverlening voor continue bewaking.

Eerdere centrale SOC-initiatieven bleken voor kleinere gemeenten te omvangrijk en kostbaar. De gemeente koos daarom bewust voor een oplossing die beter aansloot bij de eigen schaal en infrastructuur.

Hybride SOC met Elastic SIEM

Samen met PuurData en REQON werd een hybride SOC-oplossing ingericht op basis van Elastic SIEM. De aanpak brengt eigen beheer samen met externe monitoring en ondersteuning.

De implementatie begon met een Minimal Viable Product (MVP) waarin drie Elastic-nodes werden gekoppeld aan de belangrijkste databronnen, zoals firewalls, Active Directory en Microsoft Defender. Deze pragmatische start bood een solide basis voor verdere uitbouw.

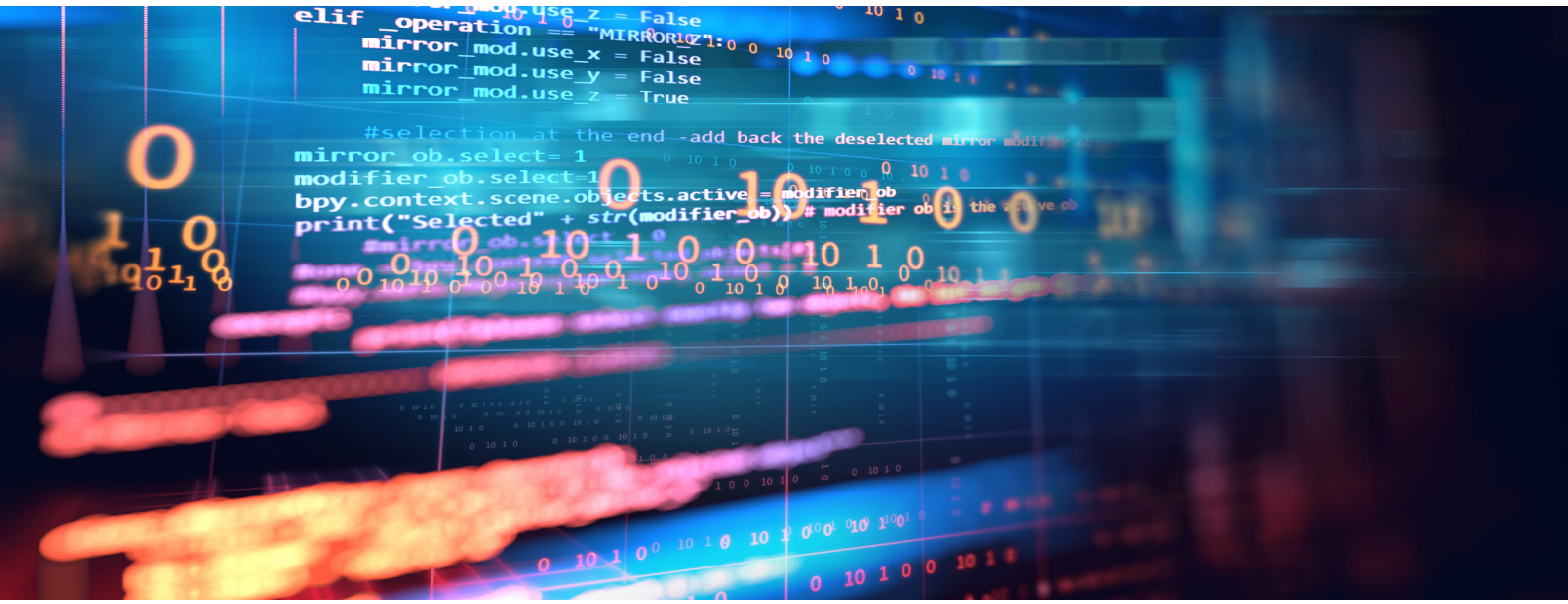
“Het voelde behapbaar,” aldus de informatiemanager. “We konden klein beginnen, leren en doorgroeien. Dat past bij onze organisatie. Onze systeembeheerders konden bovendien zelf meewerken aan de inrichting, waardoor kennis behouden blijft binnen de organisatie.”

Implementatie in samenwerking

De onboarding en technische configuratie verliepen in korte, overzichtelijke sessies. PuurData richtte zich op de installatie, dashboards en alerting, terwijl REQON het 24/7 SOC-gedeelte verzorgde.

“De samenwerking met PuurData was heel prettig,” vertelt de informatiemanager. “Korte lijnen, duidelijke communicatie en de juiste mensen aan tafel. Onze systeembeheerders waren enthousiast over de manier van werken.”

Hoewel het SOC-deel iets meer tijd vergde dan verwacht, bleef de begeleiding transparant en persoonlijk. “Je moet beseffen dat zo’n implementatie tijd kost,” vervolgt de informatiemanager. “Het is geen kwestie van ‘morgen draaien’. Maar de begeleiding was goed en flexibel. Daardoor bleef iedereen aangehaakt.”



Meer inzicht en rust

De nieuwe SIEM-omgeving biedt de organisatie nu beter inzicht in wat er binnen het netwerk gebeurt. “We waren extern al goed beschermd, maar intern hadden we minder overzicht. Nu zien we afwijkingen en mogelijke dreigingen veel sneller. Dat geeft letterlijk rust, je slaapt beter als je weet dat alles bewaakt wordt.”

De komende periode gebruikt de gemeente om de omgeving verder te optimaliseren en te evalueren. Het doel is om de oplossing structureel onderdeel te laten worden van de IT-strategie.

Waarom PuurData?

- **Pragmatische aanpak:** geen standaardpakket, maar een oplossing die past bij de schaal van de organisatie.
- **Technische expertise:** diepgaande kennis van Elastic SIEM en security-monitoring.
- **Sterke samenwerking:** één geïntegreerd team met REQON voor implementatie en 24/7-bewaking.

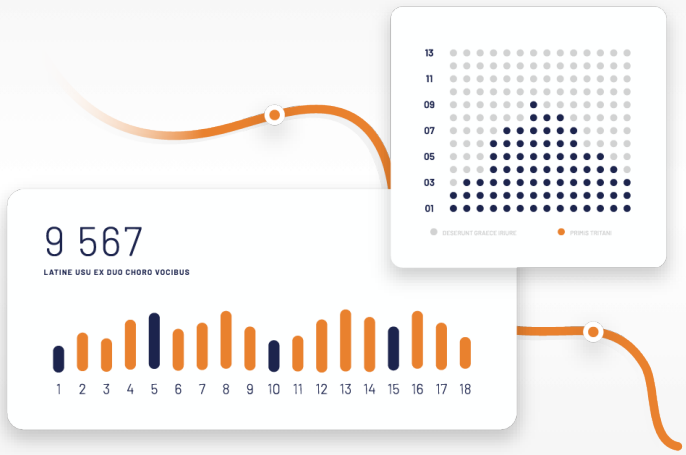
"Wat prettig is aan PuurData, is dat ze niet alleen implementeren, maar ook meedenken," zegt de informatiemanager. "Ze helpen je om zelf grip te houden op de techniek. Dat past perfect bij hoe wij willen werken."

Verder bouwen aan een veilig IT-landschap

Met de succesvolle implementatie van het hybride SOC heeft de gemeente een stevige basis gelegd voor toekomstbestendige informatiebeveiliging. De volgende stap is verdere integratie van databronnen, verfijning van alerting en het uitbreiden van dashboards.

"We zien dit als een leertraject," besluit de informatiemanager. "Klein beginnen, stap voor stap uitbreiden en leren wat voor ons werkt. De combinatie van PuurData en REQON helpt ons daarbij elke dag verder."

Meer weten? Bezoek PuurData (www.puurdata.nl) en REQON (www.reqon.nl).

PuurData
Argonstraat 28, 6718 WT, Ede

T +31 (0)88 7887328
E info@puurdata.nl