Succesvolle samenwerking tussen Pinewood en Puur Data

Van SIEM-implementatie tot SOC-diensten

pinewood
THE INTERSTELLAR COLLECTION

PUUR DATA

Ontdek hoe Pinewood en Puur Data gezamenlijk een flexibele en efficiënte SIEM-oplossing hebben geïmplementeerd met Elastic, en hoe dit partnerschap nu ook geavanceerde Security Operations Center (SOC)-diensten levert.

Over Pinewood

Pinewood is een managed security service provider (MSSP) die diensten levert aan verschillende sectoren op de Nederlandse markt zoals financiën, gezondheidszorg, retail en overheid. De klanten van Pinewood variëren van 250 tot 10.000 werkplekken, met een focus op het midden- en lagere topsegment.

Pinewood biedt een breed scala aan diensten, verdeeld over vier pijlers: Predict, Prevent, Detect en Respond. Het bedrijf houdt zich bezig met het inzichtelijk maken van kwetsbaarheden en risico's op technisch, tactisch en strategisch gebied door middel van pen-testers en securityconsultants. Daarnaast heeft Pinewood een engineeringteam dat advies en producten levert, vaak resulterend in installaties of implementaties van security-oplossingen. De kern van Pinewood's activiteiten is echter de detectie- en responsafdeling, met een Security Operations Center (SOC) dat 24/7 de infrastructuren van hun klanten monitort.

pinewood
THE INTERSTELLAR COLLECTION

De uitdagingen

Voordat Pinewood met Puur Data samenwerkte, hadden ze te maken met diverse uitdagingen die hun operationele efficiëntie en veiligheid in gevaar brachten:

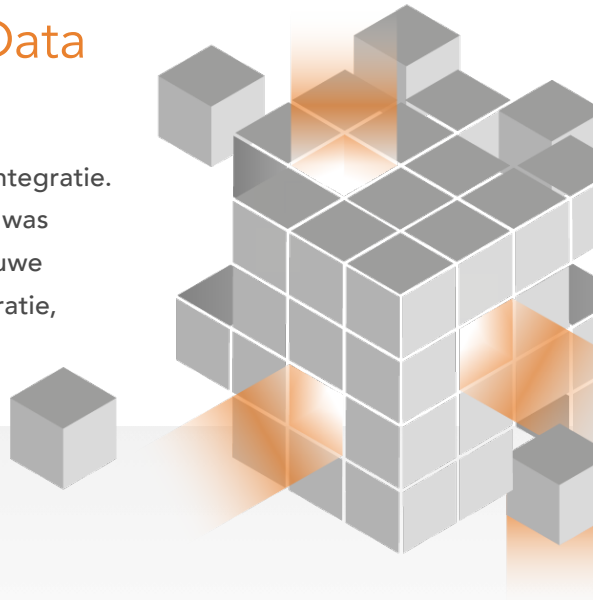
- **Verscheidenheid aan cyberdreigingen:** Pinewood moest omgaan met een groot aantal en een verscheidenheid aan cyberdreigingen van verschillende klanten, waarbij de applicaties, netwerken en systemen veilig en veerkrachtig moesten blijven.

- **Functionaliteiten:** Behoefte aan een platform dat schaalbaarheid, multi-tenancy, verbeterde rapportage, vermindering van valspositieve resultaten en gebruiksvriendelijkheid bood. En daarnaast ook future proof is met onder andere een sterke ondersteuning voor AI-functies.

Sebastiaan Kors, CEO van Pinewood, vertelt: “Ons bestaande SIEM-platform was simpelweg niet toereikend om de groeiende behoeften van onze klanten en de toenemende complexiteit van cyberdreigingen aan te pakken. We hadden een flexibele, schaalbare en gebruiksvriendelijke oplossing nodig die ons kon helpen om proactief bedreigingen te detecteren en te reageren.”

De oplossing: Elastic SIEM en Puur Data

Pinewood besloot om Elastic SIEM te implementeren, met Puur Data als hun implementatiepartner. Puur Data heeft uitgebreide kennis van Elastic-producten en -diensten en biedt expertise in data-analyse en integratie. Marco van den Brandhof, directeur van Puur Data, licht toe: “Onze rol was om Pinewood te helpen bij het opzetten en optimaliseren van hun nieuwe SIEM-omgeving. We zorgden voor een snelle onboarding en klantmigratie, ondersteund door een breed scala aan gegevensbronnen.”



Elastic SIEM bood de volgende voordelen en functies die aan de behoeften van Pinewood voldeden:

- **Kosteneffectieve en schaalbare licenties:**
  Elastic biedt licenties zonder gebruiksbeperkingen, geschikt voor on-premises, cloud of hybride infrastructuren.
- **Eenvoudige implementatie en gegevenskoppeling:**
  Puur Data zorgde voor snelle onboarding en klantmigratie, met ondersteuning voor een breed scala aan gegevensbronnen via Beats, Logstash en Elastic Agents.
- **Gebruiksvriendelijke interface:**
  Moderne en intuïtieve gebruikersinterface met ondersteuning voor Kibana voor gegevensvisualisatie, dashboarding en rapportage.
- **Geavanceerde data-analyse:**
  Gedistribueerde en veerkrachtige architectuur die real-time en historische zoekopdrachten en analyses ondersteunt.
- **Naadloze integratie:**
  Ondersteuning voor integratie met tools en technologieën zoals dreigingsinformatie, orkestratie en automatisering.

Sebastiaan Kors vult aan: *“De keuze voor Elastic werd ook beïnvloed door de flexibiliteit van het systeem om maatwerk use cases te bouwen. Dit was cruciaal voor ons, omdat we niet alleen standaard use cases wilden monitoren, maar ook bedrijfsspecifieke risico’s.”*

Implementatieproces

Het implementatieproces verliep soepel dankzij de nauwe samenwerking tussen Pinewood, Puur Data en Elastic. Marco van den Brandhof legt uit: “We waren vanaf het begin betrokken en werkten nauw samen met zowel Pinewood als Elastic. We combineerden de informatie van beide kanten om de business case op papier te zetten. Vervolgens hebben we de omgeving bij Fundaments opgezet en Elastic geïmplementeerd.”

De analisten van Pinewood koppelden de data sources en maakten gebruik van de ondersteuning van Puur Data bij het opzetten van functionaliteiten en detectieregels. Puur Data beheert de omgeving technisch, monitort de informatie-invoer en fungeert als vraagbaak bij problemen. “Het formele pad van samenwerking is vaak niet nodig; we communiceren veel via informele kanalen zoals Teams, wat prima werkt,” aldus Van den Brandhof.

Resultaten en voordelen

Elastic SIEM bood de volgende voordelen en functies die aan de behoeften van Pinewood voldeden:

- **Verhoogde gegevensdekking:**
  De gegevensdekking is met 20% vergroot door gegevens uit verschillende bronnen te normaliseren en te verrijken.
- **Verbeterde datakwaliteit:**
  De datakwaliteit is met 60% verbeterd door consistentie en gebruik van het Elastic Common Schema (ECS).
- **Verbeterde datavisibiliteit:**
  De datavisibiliteit is met 30% verbeterd door gebruik van interactieve en aanpasbare dashboards.
- **Versnelde gegevenszoekopdrachten:**
  De snelheid van gegevenszoekopdrachten en respons is met 400% verhoogd, wat resulteerde in snellere detectie en reactie op beveiligingsincidenten.

Sebastiaan Kors benadrukt: “We merken nu al een verbeterde stabiliteit en snelheid. Rapportages en queries die voorheen uren duurden, zijn nu veel sneller. De mogelijkheden van Elastic zorgen voor een stabieler platform met meer functionaliteiten dan we voorheen hadden.”

Puur Data en SOC-dienstverlening

Een belangrijk aspect van deze samenwerking is dat Puur Data, door samen te werken met Pinewood, nu ook in staat is om SOC-dienstverlening te leveren. Dit betekent dat Puur Data niet alleen de implementatie van dergelijke omgevingen kan verzorgen, maar ook kan ondersteunen bij het leveren van continue beveiligingsmonitoring en responsdiensten.

Marco van den Brandhof legt uit: “Met onze uitgebreide kennis en ervaring zijn we in staat om onze klanten een complete oplossing te bieden. Dit omvat zowel de technische implementatie als de operationele ondersteuning in de vorm van SOC-diensten. We fungeren als een verlengstuk van Pinewood en zorgen ervoor dat onze klanten altijd beschermd zijn.”

> “Door onze uitgebreide kennis van Elastic-producten kunnen wij Pinewood snel en efficiënt ondersteunen bij de implementatie van hun nieuwe SIEM-platform.”
>
> Marco van den Brandhof,
> Directeur Puur Data

Tevredenheid en toekomstige samenwerking

De samenwerking tussen Pinewood en Puur Data heeft niet alleen geleid tot technische verbeteringen, maar ook tot een versterking van de onderlinge relatie. Sebastiaan Kors is zeer tevreden over de samenwerking: “Wat ik het meest waardeer aan Puur Data is hun expertise en de flexibiliteit in hun aanpak. Ze begrijpen onze specifieke behoeften en spelen daar perfect op in.”

Op de vraag of hij Puur Data zou aanbevelen aan andere bedrijven, antwoordt Sebastiaan zonder aarzelen: “Zeker. Puur Data heeft bewezen een betrouwbare partner te zijn met diepgaande kennis van Elastic-producten en -diensten. Ze zijn in staat om complexe uitdagingen aan te pakken en oplossingen op maat te bieden.”

Marco van den Brandhof ziet de toekomstige samenwerking positief tegemoet: “We blijven Pinewood ondersteunen in hun groei en ontwikkeling. Onze focus ligt op het continu verbeteren van hun SIEM-omgeving en het aanbieden van aanvullende diensten die hun beveiligingsoperaties verder kunnen versterken.”

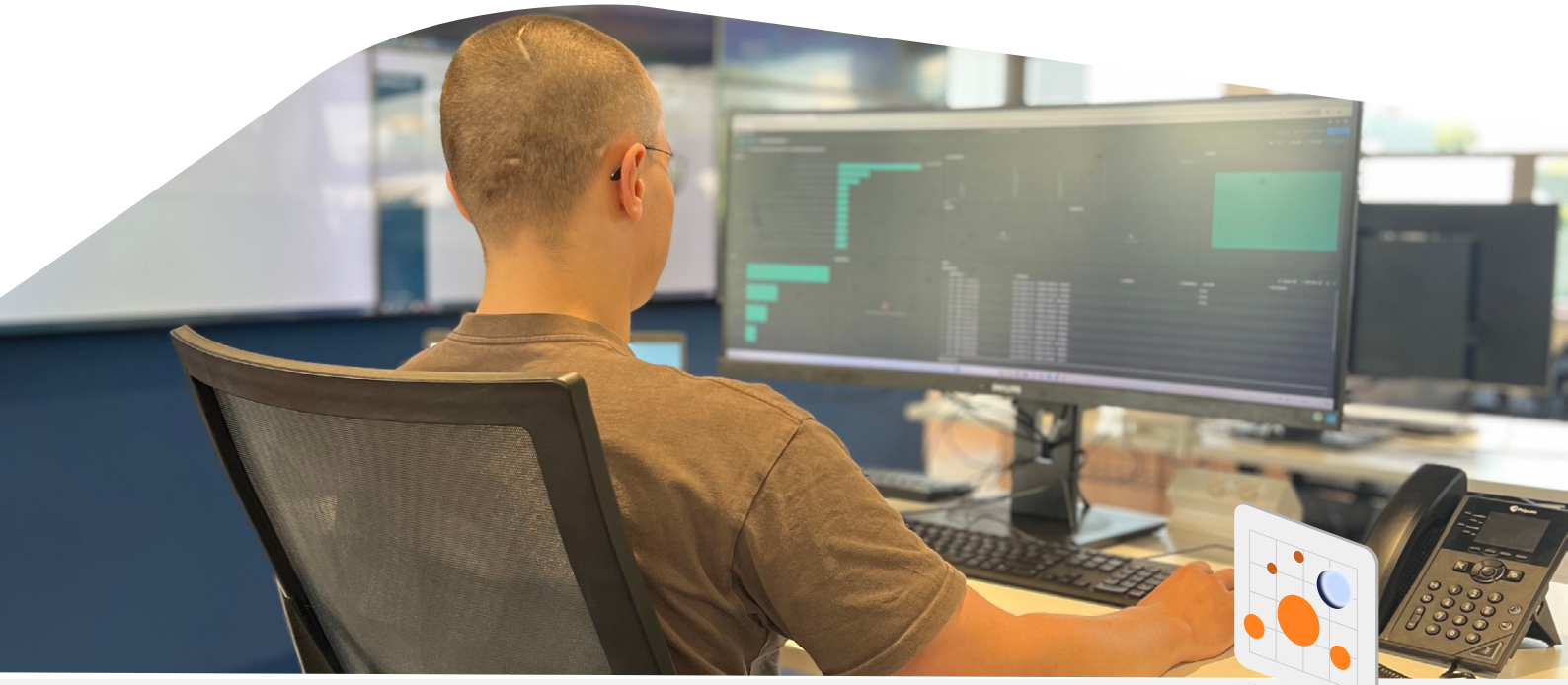
Sebastiaan voegt toe: “We beschikken met Elastic over een state-of-the art platform wat heel goed aansluit bij de dynamische markt van cybersecurity. De samenwerking met Puur Data verloopt soepel en zij blijven een cruciale rol spelen in het technisch beheer en de ondersteuning.”

> “Dankzij Puur Data hebben we nu een robuuste en flexibele SIEM-oplossing die ons in staat stelt om cyberdreigingen effectiever te monitoren en aan te pakken.”
>
> Sebastiaan Kors,
> CEO Pinewood

Conclusie

De samenwerking tussen Pinewood en Puur Data heeft geleid tot de succesvolle implementatie van Elastic SIEM, wat resulteerde in verbeterde beveiligingsmonitoring en operationele efficiëntie. Door de expertise van Puur Data en de krachtige functionaliteiten van Elastic, heeft Pinewood een flexibeler en effectiever platform kunnen creëren voor hun beveiligingsoperaties.

Deze samenwerking illustreert bovendien hoe belangrijk het is voor MSSP's om te investeren in geavanceerde technologieën en betrouwbare partnerships waarmee ze klanten de best mogelijke beveiliging kunnen bieden.



Puur Data
Argonstraat 28, 6718 WT, Ede

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