SMT
Data zonder gedoe

USE CASE

Van handwerk naar slagkracht - Versnel je security met Splunk SOAR

De situatie

Securityteams krijgen dagelijks een stortvloed aan meldingen binnen. Een deel vraagt directe actie, maar het grootste deel bestaat uit standaardchecks: IP-adressen nalopen, loggegevens verzamelen, incidenten beoordelen. Dat kost veel tijd. Tijd die vaak hard nodig is voor verdieping, analyse of beleidsontwikkeling.

Ook bij deze organisatie liep de druk op. De snelheid van incidentrespons bleef achter, fouten lagen op de loer en er was nauwelijks ruimte voor vernieuwing. Nieuwe specialisten waren bovendien lastig te vinden. Er moest iets gebeuren om het werk werkbaarder én effectiever te maken.

De uitdaging

De organisatie wilde haar securityprocessen versnellen, opschonen en structureel verbeteren.

Belangrijk daarbij was een oplossing die:

- **Repetitieve handelingen automatisch afhandelt**
- **Meer tijd vrijmaakt voor belangrijke taken**
- **Helpt om de security-aanpak naar een hoger volwassenheidsniveau te brengen**

Onze aanpak

SMT implementeerde Splunk SOAR: een platform dat slimme automatisering mogelijk maakt binnen securityteams. We werkten nauw samen met de klant om heldere workflows in te richten, waarbij terugkerende acties automatisch worden uitgevoerd. Denk aan:

- **Het verrijken van meldingen met extra informatie**
- **Het blokkeren van verdachte IP-adressen**
- **Het aanmaken en afsluiten van incidenttickets**

Door duidelijke afspraken en slimme playbooks werd SOAR een verlengstuk van het team. Niet als vervanging, maar als versneller.

De resultaten

De inzet van Splunk SOAR resulteerde in:

- ✓ **Snellere respons op incidenten dankzij geautomatiseerde standaardacties**
- ✓ **Minder handmatig werk waardoor er meer tijd overbleef voor verdieping en analyse**
- ✓ **Meer focus op strategisch werk en complexe dreigingsanalyse**
- ✓ **Hogere werktevredenheid en betere benutting van capaciteit**

De impact nu

Door te automatiseren, werkt het securityteam nu sneller én slimmer. Repetitieve handelingen kosten geen tijd meer, waardoor specialisten zich kunnen richten op wat echt telt: analyse, optimalisatie en samenwerking.

Automatisering met Splunk SOAR helpt niet alleen de werkdruk te verlagen, maar versterkt ook de veerkracht van het hele securityteam.

Waarom SMT

SMT loopt al meer dan 25 jaar voorop in data-engineering en introduceerde Splunk als eerste in de Benelux. Wij zijn de vertrouwde gids voor organisaties die maximale grip willen op hun data, met het hoogste aantal Splunk Core Certified Engineers in de regio én dagelijkse ervaring in omgevingen waar geen fout mag worden gemaakt.

Onze engineers combineren technische diepgang met discretie, compliance en een scherp oog voor samenwerking. Precies die mix maakt ons de logische partner voor wie maximale controle wil over data. Zonder concessies aan snelheid of betrouwbaarheid.

Geen ruis. Geen verspilling. Alleen data die werkt.

+31 (0)88 018 41 00 info@smtware.com www.smtware.com