SMT
Data zonder gedoe

USE CASE

SOC-werkdruk omlaag met Splunk Attack Analyzer

De situatie

Een middelgroot Security Operations Center (SOC) had dagelijks te maken met een groeiende stroom aan verdachte phishingmails en malwaremeldingen. Het team werkte grotendeels handmatig: bestanden openen, links onderzoeken, signalen combineren.

Dat zorgde voor vertraging, frustratie en risico's:

- Incidenten werden laat opgepakt
- Analisten maakten fouten door hoge werkdruk
- Escalaties naar Tier 3 namen toe
- De capaciteit stond continu onder druk

De uitdaging

Wat dit SOC ervaart, speelt breder in de markt. Veel teams hebben:

- Te weinig tijd voor elke melding
- Geen geautomatiseerde context bij phishingdreigingen
- Een versnipperd proces rond dreigingsanalyse
- Te veel escalaties die te voorkomen zijn

Zelfs organisaties met een goed SIEM-platform missen vaak een oplossing voor gestroomlijnde analyse van verdachte bestanden en links.

Onze aanpak

SMT adviseerde de inzet van Splunk Attack Analyzer.

Met SAA wordt:

- De analyse van verdachte bestanden en links volledig geautomatiseerd
- Realtime inzicht gegeven in payloads, scripts en webcontent
- De werkdruk verlaagd doordat analisten zich minder met routine hoeven bezig te houden
- De responstijd drastisch verkort door snelle en consistente rapportage

De resultaten

Binnen enkele maanden na implementatie:

- ✓ 50% snellere triage van phishingmeldingen
- ✓ 40% snellere incidentrespons
- ✓ 20% minder escalaties naar Tier 3
- ✓ Meer ruimte voor focus op complexe dreigingen

En na zes maanden:

- Lagere operationele kosten (minder tijd kwijt aan handmatige triage)
- Snellere detectie én afhandeling van dreigingen
- Tevredenheid en retentie onder SOC-analisten verbeterd

De impact nu

Met Splunk Attack Analyzer beschikt het SOC over een geautomatiseerd, betrouwbaar proces voor dreigingsanalyse.

Tijdrovend handwerk is vervangen door realtime inzicht.

De werkdruk is afgenomen, escalaties zijn teruggedrongen en analisten kunnen zich richten op waar ze echt voor nodig zijn:

het beschermen van de organisatie.

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