Een Splunk MDR-oplossing voor 100+ onderwijsinstellingen

Meta description: *UMBRiO werd door deze klant gevraagd om een cybersecurity oplossing voor meer dan 100 Nederlandse onderwijsinstellingen bouwen. Het antwoord kwam in de vorm van een geavanceerde Managed Detection & Response (MDR) oplossing*

In een tijd waarin cyberdreigingen exponentieel toenemen, stond deze organisatie voor een enorme uitdaging: hoe bied je effectieve cyberbeveiliging aan meer dan 100 Nederlandse onderwijsinstellingen? Het antwoord kwam in de vorm van een geavanceerde Managed Detection & Response (MDR) oplossing, waarbij UMBRiO een cruciale rol speelde als technische partner.

De digitale ruggengraat van Nederlands onderwijs

Deze organisatie is uitgegroeid tot dé ICT-dienstverlener voor het Nederlandse onderwijs- en onderzoekslandschap. Vanuit het hoofdkantoor bedient zij een indrukwekkend netwerk van meer dan 100 aangesloten instellingen - van universiteiten tot HBO's, MBO's en diverse onderzoekscentra.

De missie is helder: innovatie in onderwijs en onderzoek mogelijk maken door middel van ICT, en geavanceerde, veilige IT-diensten aanbieden voor samenwerking, data en infrastructuur. Met honderduizenden studenten, onderzoekers en docenten die dagelijks afhankelijk zijn van haar diensten, is cyberbeveiliging niet alleen belangrijk - het is existentieel.

De uitdaging: Nationale cybersecurity op schaal

Toen deze organisatie besloot een eigen MDR-dienst te lanceren inclusief een Security Information and Event Management (SIEM) systeem voor al haar klanten, werd al snel duidelijk dat dit geen gewone implementatie zou worden. De scope was enorm: 83 individuele organisaties met elk hun eigen IT-infrastructuur, compliance-eisen en beveiligingsuitdagingen.

Toen de tender voor de MDR-dienstverlening werd gewonnen door een partner van UMBRiO, kwam zij automatisch bij ons terecht voor de hosting en het technische beheer van het SIEM-platform. Hier kwam de kennis en ervaring van UMBRiO goed van pas - niet alleen als hosting provider, maar als strategische partner die de complexe data-onboarding en -mapping voor zijn rekening zou nemen.

UMBRiO's oplossing: Multi-tenant Splunk op enterprise-niveau

De door UMBRiO ontwikkelde oplossing is een technisch hoogstandje: een multi-tenant Splunk-platform dat gegevens van 83 verschillende organisaties veilig scheidt en verwerkt. Deze architectuur brengt unieke uitdagingen met zich mee - van data-segregatie tot SAML-integraties en app-permissions - allemaal kritieke elementen die foutloos moeten functioneren om datalekken tussen klanten te voorkomen.

Technische innovaties en automatisering

UMBRiO heeft een uitgebreid monitoringsysteem geïmplementeerd dat constant toezicht houdt op de multi-tenant componenten. Daarnaast zijn geautomatiseerde processen ontwikkeld die foutieve configuraties automatisch detecteren en verwijderen - een essentiële veiligheidsmaatregel in een omgeving van deze omvang.

De onboarding van nieuwe klanten is volledig geautomatiseerd door middel van intelligente pipelines die server-classes, indexes, Technology Add-ons (TA's), apps, metadata-bestanden en SAML-configuraties automatisch aanmaken. Deze automatisering zorgt niet alleen voor consistentie, maar optimaliseert ook de snelheid waarmee nieuwe organisaties aangesloten kunnen worden.

Data-mapping naar Splunk CIM

Een cruciaal onderdeel van de oplossing is de mapping van alle inkomende data naar Splunk's Common Information Model (CIM) Data Models. UMBRiO's experts zorgen ervoor dat logbestanden van diverse bronnen correct worden gestructureerd, zodat de "Managed Detection Engine" van onze partner - een gespecialiseerde Splunk-app - optimaal kan functioneren bij het detecteren van dreigingen.

Klantgerichte transparantie en inzichten

Naast de technische backbone heeft UMBRiO meerdere klantgerichte applicaties ontwikkeld die zowel de opdrachtgever als de eindklanten volledige transparantie bieden in hun data-ingest en source forwarding. Deze apps tonen real-time welke bronnen correct zijn gemapped en welke hosts de juiste productiedata verzenden.

Alle individuele alerts worden gecorreleerd en omgezet naar "cases" die zichtbaar zijn voor zowel het SOC-team als de klant. Dit resulteert in een efficiënte response op alerts variërend van informatieve meldingen tot kritieke beveiligingsincidenten. Bij kritieke situaties wordt de klant direct gecontacteerd, waarbij de opdrachtgever en onze partner volledig op de hoogte blijven van de voortgang bij het leveren van de oplossing van het incident.

Resultaten: Een beveiligde digitale onderwijsomgeving

De samenwerking tussen UMBRiO, haar partner en de opdrachtgever heeft geresulteerd in een robuuste cybersecurity-oplossing die het complete Nederlandse onderwijs- en onderzoekslandschap beschermt. Met 83 aangesloten organisaties en meer dan 100 onderwijsinstellingen die profiteren van deze dienst, is dit project een van de grootste multi-tenant security-implementaties in Nederland.

De geautomatiseerde processen en geavanceerde monitoring zorgen voor een stabiele, schaalbare oplossing die meegroeit met de behoeften van de opdrachtgever en haar eindklanten. Tegelijkertijd biedt de transparante rapportage organisaties de inzichten die zij nodig hebben om hun eigen security posture te verbeteren.

Conclusie: Partnerships maken het verschil

Dit project illustreert de kracht van strategische partnerships in complexe ICT-implementaties. Door UMBRiO's technische expertise te combineren met de security-kennis van haar partner en de domeinexpertise van de opdrachtgever, ontstond een oplossing die geen van de partijen afzonderlijk had kunnen realiseren.

Voor organisaties die overwegen hun cybersecurity te professionaliseren, biedt dit project waardevolle lessen over de voordelen van managed security services en de mogelijkheden van moderne SIEM-platforms.

Neem contact op met de specialisten van UMBRiO en ontdek hoe UMBRiO ook uw kritieke Splunk-infrastructuur kan transformeren naar enterprise-grade betrouwbaarheid - met de operational excellence die deze klant dagelijks ervaart.

UMBRiO: Where Mission-Critical Infrastructure Meets Managed Service Excellence

Meer informatie:

Op verzoek van zowel de opdrachtgever als onze partner is deze referentie-case geanonimiseerd. Indien u meer informatie wenst over de door ons geleverde oplossing en de betreffende organisatie, kunt u uiteraard contact met ons opnemen.