Hoe UMBRiO een security gap veranderde in Enterprise SIEM Excellence

Meta description: *Ontdek hoe UMBRiO een volledig managed Splunk SIEM oplossing voor haar klant realiseerde, inclusief custom use cases en 24/7 security monitoring.*

Wanneer cybersecurity geen compromis meer toelaat

In het huidige dreigingslandschap kunnen universiteiten zich geen security gaps permitteren. Met duizenden gebruikers, gevoelige onderzoek data en een kritieke IT-infrastructuur vormen zij aantrekkelijke doelen voor cybercriminelen. Deze Universiteit besefte dit maar al te goed en stond voor een uitdaging die veel onderwijsinstellingen herkennen.

De klant beschikte niet over beveiligingsoplossingen die aansloten bij hun specifieke eisen en complexe omgeving. Daarom werd besloten een eigen, professionele SIEM-systeem te implementeren. Hoewel de keuze op Splunk viel, ontbrak de interne expertise voor implementatie, het inladen van data en het ontwikkelen van aangepaste gebruikssituaties. Hier begon de transformatie van een kwetsbare security posture naar een geavanceerd, proactief beveiligde omgeving - met UMBRiO als strategische managed SIEM partner.

De security uitdaging: Meer dan alleen technologie

De realiteit was dat de betreffende universiteit zich in een typische enterprise dilemma bevond. Er waren geen passende kant-en-klare oplossingen beschikbaar die voldeden aan de universitaire complexiteit en privacy-eisen. Daarnaast bestond er een kritieke lacune in de beveiligingszichtbaarheid binnen een omgeving met diverse gebruikersgroepen en systemen. De universiteit kampte ook met interne capaciteitsbeperkingen voor het implementeren van gespecialiseerde beveiligingstools, terwijl er wel urgentie bestond voor een eigen oplossing omdat andere oplossingen nog in ontwikkeling waren.

De keuze voor Splunk was strategisch doordacht. Het betrof een bewezen enterprise-platform met een solide trackrecord in complexe omgevingen. Splunk bood de flexibiliteit voor aangepaste gebruikssituaties die specifiek waren voor de onderwijssector, evenals de schaalbaarheid om groeiende datavolumes en gebruikersaantallen aan te kunnen. Bovendien beschikt het platform over geavanceerde analysemogelijkheden voor proactieve detectie van bedreigingen.

Maar een platform kiezen is één ding - het succesvol implementeren en operationeel houden is een ander verhaal.

UMBRiO's Managed SIEM benadering: Volledig partnership

UMBRiO ging verder dan traditionele consultancy. Voor deze universiteit werd een volledig beheerde SIEM-service opgezet die verschillende essentiële componenten omvatte.

Op het gebied van infrastructuurbeheer werd het complete Splunk-platform gehost door UMBRiO, inclusief 24/7 monitoring en prestatie-optimalisatie. Daarnaast wordt er voortdurend platformbeheer en updates verzorgd om de systemen optimaal te laten functioneren.

Voor de beveiligingsexpertise werd een Enterprise Security (ES) implementatie geoptimaliseerd voor de universitaire omgeving. UMBRiO bood ook dataonboarding consulting voor diverse bronnen, waaronder applicaties, systemen en gebruikersinteracties. Tot slot werden er aangepaste gebruikssituaties ontwikkeld die specifiek waren afgestemd op de beveiligingsvereisten van de klant.

De Vijf Pijlers van het SIEM

UMBRiO ontwikkelde een uitgebreid beveiligingskader rond vijf belangrijke use cases:

- Cybersecurity: Geavanceerde detectie van bedreigingen en reactie op incidenten
- IT Monitoring: Proactieve infrastructuurbewaking
- Application Management: Performance en security monitoring van kritieke apps
- Business Analytics: Datagedreven inzichten voor operationele optimalisatie
- Compliance: Automatische rapportages voor wettelijke vereisten

Technsche uitdaging: Collaborative Development

Er ontstond een unieke uitdaging toen beide teams - klant en UMBRiO - tegelijkertijd werkten aan dezelfde Enterprise Security-app vanuit verschillende GitHub-repositories. Repository-conflicten bedreigden de ontwikkelingsworkflow.

UMBRiO's Oplossing:

Voor een effectieve softwareontwikkeling is de implementatie van strikte, geautomatiseerde processen essentieel. Dit begint met het opzetten van version control workflows die collaborative development mogelijk maken, waardoor meerdere ontwikkelaars gelijktijdig kunnen werken aan dezelfde codebase zonder elkaar in de weg te zitten. Daarnaast zijn geautomatiseerde test- en implementatieprocedures essentieel om wijzigingen door te kunnen voeren zonder problemen in de huidige systemen te veroorzaken. Ten slotte garandeert een helder beheersmodel voor de gezamenlijke programmacode dat alle betrokkenen precies weten welke werkwijzen en verantwoordelijkheden van toepassing zijn bij het onderhouden van de gedeelde code.

Concluderend

Complexe technische uitdagingen vereisen niet alleen tools, maar ook proces aanpassingen. UMBRiO's workflow management werd later een beproefd template voor andere collaboratieve SIEM projecten.

Het belangrijkste resultaat? Van reactieve naar proactieve security

De nieuwe SIEM-omgeving leverde directe en langdurige voordelen:

Operational Excellence wordt bereikt door een uitgebreide ES-oplossing die volledig is aangepast aan de specifieke use cases binnen de universitaire context. Deze implementatie zorgt voor aanzienlijk snellere dreigingdetectie, waarbij de detectietijd voor kritieke incidenten is teruggebracht van uren naar slechts enkele minuten. De incident response is verder verbeterd door de inzet van geautomatiseerde workflows en alerting systemen. Om complete zichtbaarheid te garanderen, is er een gecentraliseerd Enterprise Logging Service opgezet dat alle activiteiten en gebeurtenissen binnen de organisatie monitort en registreert.

De technische mogelijkheden van het systeem zijn uitgebreid en veelzijdig. Integratie van meerdere gegevensbronnen maakt naadloze analyse mogelijk van applicaties, systemen én gebruikersinteracties, waardoor een compleet beeld ontstaat van alle activiteiten binnen de organisatie. Door aangepaste analyses toe te passen, zijn gebruikssituaties specifiek ontwikkeld voor het universitaire dreigingslandschap, wat zorgt voor meer gerichte en effectieve beveiligingsmaatregelen. De schaalbare architectuur garandeert dat het systeem klaar is voor toekomstige groei en nieuwe behoeften die kunnen ontstaan. Daarnaast faciliteren samenwerkende werkstromen een bewezen model voor klant-leverancier samenwerking, wat bijdraagt aan een efficiënte en transparante werkrelatie.

Succesvolle process innovatie

De GitHub repository uitdaging werd een ware showcase voor de capaciteiten van UMBRiO. Strikte automatisering en daaropvolgende governance creëerden een ‘collaborative development’-model dat:

- De snelheid van ontwikkeling toe liet nemen
- De kwaliteit verhoogde door geautomatiseerd testen
- Geoptimaliseerde kennisdeling tussen teams vanzelfsprekend maakte
- Schaalbaarheid liet toenemen door nieuwe mogelijkheden

Strategische lessen:

1. Managed Services = Strategisch voordeel

Het succes in deze klantcase toont dat managed SIEM oplossingen meer opleveren dan kostenbesparingen - ze bieden toegang tot gespecialiseerde expertise die intern onhaalbaar zou zijn.

2. Custom use-cases bieden extra waarde

Generieke SIEM implementaties missen sector-specifieke bedreigingen. Deze specifieke use cases creëerden security voordelen die voorheen onhaalbaar leken.

3. Samenwerken aan innovatie is mogelijk

Technische uitdagingen zoals conflicterende development workflows kunnen worden omgezet in innovatieve kansen met de juiste partner.

4. Proactief ia altijd beter dan Reactief

Van post-incident analyse naar voorspellende dreigings detectie -deze transformatie illustreert de kracht van geavanceerde SIEM oplossingen.

Klaar om uw beveiligingsbeleid te veranderen?

Deze reis naar een Enterprise SIEM toont wat mogelijk is met de juiste managed security partner. Bij UMBRiO combineren wij diepgaande technische expertise met innovative proces beheersing voor complexe security transformaties.

Herkent uw organisatie vergelijkbare security challenges? Of u nu een onderwijsinstelling, zorgorganisatie of enterprise organisatie bent - onze managed Splunk SIEM services kunnen uw beveiligingsbeleid fundamenteel versterken.

Complexe technische uitdagingen zoals gezamenlijke ontwikkeling, aangepaste use case-creatie en gegevensintegratie met meerdere bronnen? Dat zijn precies de uitdagingen waar UMBRiO in uitblinkt.

Start uw Security Assessment en ontdek hoe UMBRiO uw cybersecurity van reactief naar proactief kan transformeren - net zoals we voor deze universiteit realiseerden.

Neem contact op met de specialisten van UMBRiO en ontdek hoe wij ook uw kritieke Splunk-infrastructuur kunnen 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 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.