

SMT



Cribl®

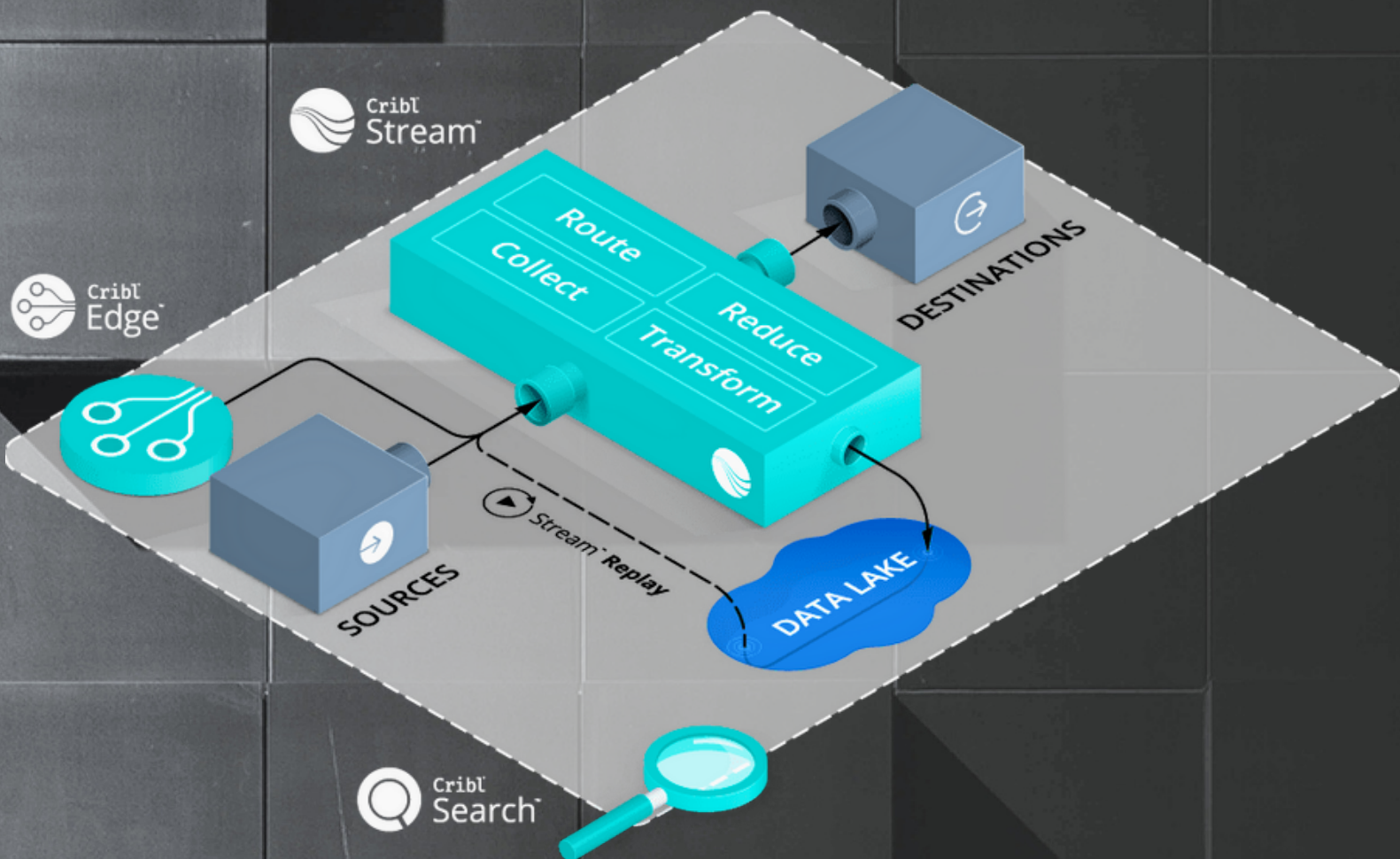
Klantencases





Volledige Controle Over:
 Security | Observability | Telemetry

DATA



Met Cribl verzamel, verrijk, normaliseer, anonimiseer en routeer je moeiteloos **alle** vormen van data van **elke** bron naar **elke** bestemming.

Controle
over data

Observability

Compliance

Kostenbesparing

Geen
vendor lock-in

Security

Introductie

Welke waarde heeft data voor jou? Ter inspiratie hier een selectie van SMT Cribl klantencases. De successen in de praktijk laten de waarde van de combinatie SMT en Cribl zien.

Doel

De klantencases laten zien hoe waardevol het integreren van Cribl in data-infrastructuur is. Enkele voorbeelden samengevat:

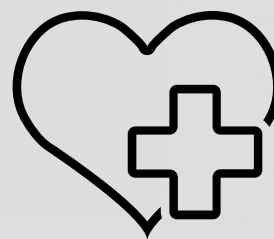
- SMT heeft bij een *financiële instelling* Cribl geïmplementeerd om databeheer en beveiliging te verbeteren. Het resultaat is een **sterk verbeterde compliance en risicobeheersing**.
- SMT heeft Cribl geïmplementeerd bij een *medische organisatie* om datastromen inzichtelijk te maken. Hierdoor kunnen **beslissingen sneller en nauwkeuriger** genomen worden.
- SMT heeft bij een *technologiebedrijf* Cribl geadopteerd om dataverwerking eenvoudig te maken. Het resultaat is een **sterk verbeterde operationele efficiëntie**.

Zo wordt per sector inzichtelijk wat de kracht van Cribl is.

Neem contact met ons op en laat je inspireren.

De klant

- Onderzoeksorganisatie gezondheid en milieu
- Werknemers: 1730



Het probleem

- Kosten verbonden aan het doorsturen van deze logdata naar SURFsoc. Deze kosten nemen toe naarmate de hoeveelheid data groter wordt.
- Geen budget beschikbaar voor het onboarding van extra data.
- De organisatie is wettelijk verplicht om al hun IT-logdata naar SURFsoc te sturen.

De oplossing

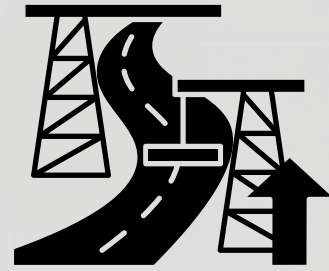
- SMT heeft in nauwe samenwerking met de IT-afdeling een diepgaande analyse uitgevoerd van het data-probleem.
- Vanaf implementatie in de productieomgeving heeft SMT het beheer van de Cribl omgeving bij deze organisatie op zich genomen (managed services).
- SMT en de onderzoeksorganisatie kozen samen voor Cribl om gegevens te filteren. We hebben een passende Cribl-architectuur ontwikkeld, eerst in een testomgeving opgezet, daarna in de productieomgeving geïmplementeerd en een gedetailleerde roadmap opgesteld.

Het resultaat

- Volledig inzicht in, en controle over, alle datastromen
- Aanzienlijke kostenbesparing
- 100% van de data wordt gefilterd
- 30% van de data gaat naar SURFsoc
- 70% van de data wordt opgeslagen

De klant

- Toezichthouder infrastructuur
- 9200 werknemers



Het probleem

- De koppeling tussen de software die de verkeerscentrale gebruikt en het incident registratiesysteem.
- Hulpdiensten konden niet goed en tijdig worden aangestuurd door het ontbreken van de juiste informatie.

De oplossing

- SMT en de toezichthouder hebben samen besloten om Cribl te gebruiken voor het converteren van verkeersdata naar de juiste informatie voor hulpdiensten.
- We hebben een geschikte Cribl-architectuur ontwikkeld, getest, geïmplementeerd in de productieomgeving en een gedetailleerde roadmap opgesteld.

Het resultaat

- Optimale koppeling tussen de software van de verkeerscentrale en het incident registratiesysteem.
- Data flexibiliteit, de toezichthouder verkeer kan vanaf nu, ongeacht de bron, elk type output genereren.
- Betere aansturing van hulpdiensten door juiste informatie.
- Hulpdiensten krijgen sneller de juiste informatie.
- Tijdswinst, dit was voorheen een handmatige actie.
- Medewerkers hebben meer tijd vrij voor andere taken.

De klant

- Toezichthouder verkeer
- 1800 werknemers

Het probleem

- Onoverzichtelijk beheer in de drie datacentra van de toezichthouder.
- Hoge software kosten door geïmplementeerde architectuur.



De oplossing

- SMT en de toezichthouder hebben samen besloten om in alle drie de datacentra Cribl Stream Workers te implementeren.
- SMT heeft een implementatieplan voor Cribl Stream Workers ontwikkeld, getest, in productie uitgerold en een gedetailleerde roadmap vastgesteld.
- SMT voert het onderhoud uit op de Cribl omgeving.

Het resultaat

- Verbeterde inzage in datastromen.
- Besparing op software kosten.
- Geen zorgen om onderhoud Cribl omgeving.

De klant

- Transportbedrijf
- 260 werknemers
- Omzet 2022: €230 miljoen



Het probleem

- Verouderde, inefficiënte en onveilige manier van datatransport naar externe partijen.
- Het transportbedrijf is verplicht om specifieke data aan te leveren.

De oplossing

- SMT en het transportbedrijf hebben samen besloten om Cribl te gebruiken zodat de data vanuit de Splunk universal forwarder direct kan worden doorgestuurd.
- SMT voert het onderhoud uit op de Cribl omgeving.
- SMT heeft Cribl geïmplementeerd na een succesvolle testomgeving, en een gedetailleerde roadmap opgesteld voor verdere optimalisatie.

Het resultaat

- Het transportbedrijf kan op een efficiënte en veilige manier aan de verplichting voldoen om specifieke data aan te leveren (aan externe partijen).
- Geen zorgen om onderhoud Cribl omgeving.

De klant

- Energieleverancier
- 4300 werknemers
- Omzet 2022: €1,3 miljard

Het probleem

- Overbodige syslog data van de firewalls werd naar Splunk gestuurd.

De oplossing

- SMT en de energieleverancier hebben samen besloten Cribl te gebruiken om overbodige data te filteren.

Het resultaat

- Beter inzicht in datastromen.
- Overbodige data wordt gefilterd.
- Besparing op Splunk licentie kosten.

- Splunk licentie.

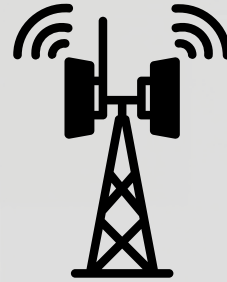
- SMT heeft een passende Cribl architectuur gekozen, deze in een testomgeving opgezet, de implementatie van Cribl in de productieomgeving uitgevoerd en vervolgens een gedetailleerde roadmap vastgesteld.

- Vervolgproject waarin SMT met de Energieleverancier de IT en OT Splunk omgeving gaan samenvoegen met behulp van Cribl.



De klant

- Telecommunicatie provider
- 47000 werknemers
- Omzet 2022: €7,2 miljard



Het probleem

- Veel overbodige data werd naar Splunk gestuurd.
- Splunk licentie.

De oplossing

- SMT en de telecommunicatie provider hebben samen besloten Cribl te gebruiken om overbodige data te filteren.
- SMT heeft een passende Cribl oplossing gekozen, deze in een testomgeving opgezet, de implementatie van Cribl in de productieomgeving uitgevoerd en vervolgens een gedetailleerde roadmap vastgesteld.

Het resultaat

- Beter inzicht in datastromen.
- Besparing op Splunk licentie kosten.
- Overbodige data wordt gefilterd.
- Vervolgproject waarin Cribl breder wordt ingezet.

De klant

- Online winkel
- 1500 werknemers
- Omzet 2022: €800 miljoen



Het probleem

- Naarmate de online winkel groeide, werd het in stand houden van hun open-source dataplatform arbeidsintensief en kostbaar.
- Het ontwikkelen van een in-house observability-pijplijn voor real-time stream processing resulteerde in aanzienlijke technische problemen.
- Het verwerken van dagelijks 2-3 TB aan weblogs leidde tot uitdagingen bij het configureren van bronnen, het up-to-date houden van systemen en het verbruiken van waardevolle engineeringtijd.

De oplossing

- Cribl Stream werd ingezet voor het verbergen van gevoelige patronen met behulp van redactie, hashing of randomisatie. Het introduceerde ook de Replay-functie voor het selectief opnieuw inlezen van data vanuit S3 naar analyseplatforms.
- Cribl Stream werd gebruikt voor het opvragen en aggregeren van logdata en statistieken
- Cribl Edge werd geïmplementeerd om duizenden edge nodes te beheren.

Het resultaat

- Aanzienlijke kostenbesparing op het gebied van infrastructuur, prestaties, engineeringtijd en downtime.
- Maskeren van gevoelige patronen en data waardoor de beveiliging van gevoelige data werd verhoogd.
- Verbeterde efficiëntie en mogelijkheden voor het datateam, zelfs toen het dagelijkse datavolume verdubbelde.
- Gebruikersvriendelijke en intuïtieve dashboards konden worden gecreëerd voor waardevolle inzichten in systeemprestaties.
- Snellere zoekopdrachten in Splunk met lagere infrastructuurvereisten.

De klant

- Reisorganisatie
- 1200 werknemers
- Omzet 2022: €700 miljoen



Het probleem

- De implementatie van CrowdStrike Falcon Data Replicator (FDR).
- Dit dwong de reisorganisatie om prioriteiten te stellen bij het onboarden van data voor hun SIEM.
- De reisorganisatie stuitte op een onverwacht hoog volume logs, dat de beschikbare licentieruimte en infrastructuurcapaciteit van hun Splunk SIEM-oplossing overschreed.

De oplossing

- Implementatie van Cribl om logs te optimaliseren, waardoor het logvolume daalde tot het verwachte niveau zonder de context te verliezen die nodig is voor detectie.
- Gebruik van Cribl CrowdStrike Pack, wat resulteerde in een onmiddellijke vermindering van het logvolume.
- Cribl Stream werd gebruikt om gegevens naadloos naar verschillende bestemmingen te routeren.

Het resultaat

- Snelle waarde realiseren uit CrowdStrike FDR en binnen datalimieten blijven.
- Vermindering van 50% in logdata, na verdere optimalisatie bereikte de reisorganisatie een totale data vermindering van 72%.
- Minder tijd kwijt aan het beheren van dataonboarding, configuraties, normalisatie en licentiebeperkingen, waardoor meer tijd vrij kwam voor andere taken.
- Het team kon de waarde van de tools in hun beveiligingsstack verhogen door Cribl Stream op een eenvoudige manier te integreren.

De klant

- Cyber Security bedrijf
- 250 werknemers
- Omzet 2022: €400 miljoen

Het probleem

- Security experts ervaren een overvloed aan data, afkomstig uit diverse bronnen en in verschillende formaten.
- Uitdagingen bij het detecteren van inbreuken, opsporen van nieuwe bedreigingen en efficiënt reageren op security incidenten.
- Gebrek aan mogelijkheden om data te delen tussen ingezette security tools.
- Het datalandschap is versnipperd en vormt een uitdaging voor effectief security beheer.



De oplossing

- Implementatie van Cribl Stream's datafiltering om de kwaliteit te verbeteren, van en naar elke gewenste bron en bestemming.
- Verrijk security data met externe bronnen zoals GeoIP en bekende dreigingsdatabases voordat ze in logging- en/of SIEM-platforms terecht komen.
- Verhoog de waarde van (opgeslagen) securitydata door automatische en real-time verrijking met context uit externe bronnen.
- Filter security events voor dynamische sampling, of zet loggegevens om in metrics voor aanzienlijke volumevermindering.

Het resultaat

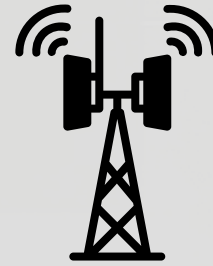
- De mogelijkheid om gevoelige data te kunnen verbergen en daarmee voldoen aan wettelijke naleving.
- Verbeterde operationele efficiëntie door een gestroomlijnde en intelligente aanpak van security databeheer en -analyse.
- Verhoging van de waarde van de tools in de security-stack door naadloze integratie met Cribl Stream.
- Effectieve filtering van overbodige data uit security analytics platforms.
- Verbeterde security context door verrijking van data van externe bronnen.

De klant

- Telecommunicatie provider
- 95.000 werknemers
- Omzet 2022: €4.1 miljard

Het probleem

- Het verwerken van veel operationele data, toepassingen, infrastructuur en services vormde aanzienlijke uitdagingen.
- Het beheren van diverse databronnen leidde tot operationele uitdagingen in dataverwerking.
- De syslog-data van firewalls en DNS-servers voegden complexiteit toe, inclusief redundante data die speciale verwerking vereiste.
- Het onboarden van nieuwe databronnen bracht uitdagingen met zich mee op het gebied van complexiteit en tijdsbesteding.



De oplossing

- Implementatie van Cribl Stream voor end-to-end dataverwerking, inclusief importeren, voorbereiden, opschonen en transporteren van data als dienst aan interne klanten.
- Gebruik van Cribl Stream om data aan te passen aan specifieke structuren voor dashboards.
- Met Cribl Stream werden ontwerp patronen en regelsets vooraf gemaakt en beschikbaar gesteld aan klanten, waardoor het onboardingproces voor nieuwe databronnen werd vereenvoudigd en versneld.

Het resultaat

- Aanzienlijke verbeterde efficiëntie en mogelijkheden voor het data engineering team.
- Verbeterde serviceverlening naar klanten door data in een specifieke structuur voor dashboards aan te kunnen leveren.
- Het onboardingproces voor nieuwe databronnen werd vereenvoudigd en versneld.
- Kan nu context worden toegevoegd en onnodige data kan worden verwijderd uit binnenkomende databronnen.
- Een verhoogde mate van Observability, waardoor het team beter zicht kreeg op hun infrastructuur data.

De klant

- Financiële instelling
- 9000 werknemers
- Omzet 2022: €1.2 miljard



Het probleem

- Veel moeite met het analyseren van een brede dataset om de veiligheid, prestaties en algehele gezondheid van hun systemen te begrijpen (Observability).
- Geïmplementeerde observability-oplossingen beperken de financiële instelling in mogelijkheden om data naar externe analysetools te sturen, waardoor de flexibiliteit beperkt is.
- De beperkingen in datatoegang leidt tot suboptimale analyses, verminderde inzichten en een beperkt vermogen om snel te reageren op veranderende behoeften in de financiële sector.

De oplossing

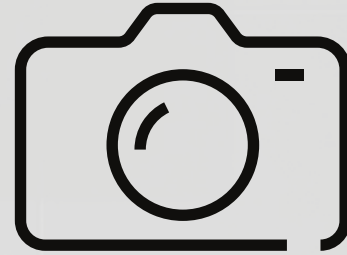
- Implementatie van Cribl Stream om dataflexibiliteit te bieden aan de financiële instelling, waarbij het mogelijk wordt om elke soort data van elke bron naar elk analysesysteem te sturen.
- Inzet van Cribl Stream voor het integreren (verrijken) van databronnen zoals financiële transacties, interne (security) systemen, en externe marktgegevens naar verschillende analysesystemen.

Het resultaat

- Benodigde financiële data naar de meest geschikte locatie worden verzonden, in het vereiste formaat.
- De vrijheid om de meest geschikte tools te kiezen, zonder beperkingen van de huidige leveranciersstack.
- Data kan flexibel worden verzonden naar elk gewenst analysesysteem, ongeacht de bestaande leveranciersstack.
- Toegang tot cruciale informatie voor betere strategische beslissingen.

De klant

- Online beeld en fotografisch leverancier
- 1300 werknemers
- Omzet 2022: €828 miljoen



Het probleem

- Het verwerken van een extreem hoog volume aan diverse data van verschillende bronnen en het routeren naar diverse bestemmingen.
- De noodzaak om data te optimaliseren en normaliseren voor indexering, wat tijdrovend is.
- Uitdagingen bij het aanpassen van dataformats en het routeren naar de juiste bestemmingen bij groei en verandering in de data-architectuur.
- Beheer van piekdatastromen tijdens drukke periodes.

De oplossing

- Gebruik van Stream's dynamische routeringsfunctionaliteit om de juiste bestemmingen te bereiken, zelfs bij veranderingen in de data-architectuur.
- Centralisatie van zichtbaarheid en controle over de datastroom via Stream als een centraal beheerpunt voor operationeel gemak.
- Beheer van piekdatastromen door middel van Stream's controle over wat wordt geïndexeerd, met event payload-reductie en dynamische sampling voor efficiënt gebruik van licentiebandbreedte.
- Implementatie van Cribl Stream voor het opschonen van data vóór indexering.

Het resultaat

- Verbeterde datakwaliteit door voorafgaande opschoning met Cribl Stream, waardoor gebruikers betere resultaten krijgen.
- Operationeel gemak en betere probleemoplossing dankzij de centralisatie van zichtbaarheid en controle met Cribl Stream als centraal beheerpunt.
- Flexibiliteit en veerkracht in dataroutering.
- Efficiënt gebruik van licentiebandbreedte tijdens piekuren.

De klant

- IT Managed Service Provider
- 3800 werknemers
- Omzet 2022: €2.9 miljard

Het probleem

- Overweldigende hoeveelheid data van verschillende bronnen voor Managed Detection and Response (MDR) activiteiten.
- Beperkingen van klassieke oplossingen (vaak open source) vanwege overhead of diepgaande technische expertise.
- Uitdagingen bij het sturen van data naar de juiste bestemming in het juiste formaat, vooral bij groei en complexiteit.
- Verbeterde mogelijkheid om aan opslagcompliance-eisen te voldoen.



De oplossing

- Implementatie van Cribl Stream ter verzameling van logdata voor MDR-cliënten.
- Gebruik van Cribl Stream voor reductie, standaardisatie en normalisatie van diverse soorten data.
- Dynamische routing in Cribl Stream om data automatisch naar de juiste bestemming te sturen, zelfs bij veranderende dataarchitectuur.
- Snelle en eenvoudige configuratie van Cribl Stream voor doorsturen, optimaliseren en transformeren van data.

Het resultaat

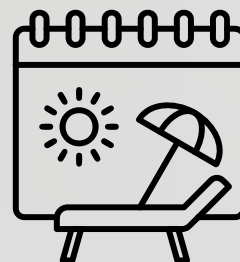
- Verbeterde prestaties van SIEM door schonere, genormaliseerde data.
- Snellere onboarding van klanten met Cribl Packs, waardoor de onboardingtijd met 60-90% wordt verminderd.
- Schaalbaarheid en herbruikbaarheid van configuraties met Cribl Packs, wat leidt tot enorme tijdswinst.
- Halvering van de werklast voor het engineeringteam.
- Aanzienlijke kostenbesparingen op engineeringresources dankzij de flexibiliteit en efficiëntie van Cribl Stream.
- Verlaagde gemiddelde onboardingtijd voor nieuwe klanten met 70%.

De klant

- Vakantie- en conferentiecentrum
- 400 werknemers
- Omzet 2022: €200 miljoen

Het probleem

- Overgang van een volledig uitbestede SOC naar een hybride SOC om kosten te besparen.
- Noodzaak om high-value data te scheiden van high-volume data voor naleving van regelgeving.
- Vereiste om de SIEM-uitgaven te verminderen en toch uitgebreide dekking te behouden.



De oplossing

- Implementatie van Cribl Stream om logs te filteren, data te normaliseren en routeren naar een nieuwe SIEM.
- Gebruik van Cribl Packs voor snelle onboarding en configuratiebeheer.
- Dynamische aanpassing van logconfiguraties voor optimale prestaties en kostenbesparingen.

Het resultaat

- Probleemloze overgang naar nieuwe MSSP zonder verlies van cyber security dekking.
- Volledige operationele SOC binnen 60 dagen opgebouwd.
- SIEM-licentie- en infrastructuurkosten met 60% verminderd.
- Terugwinnen van verloren engineeringtijd door automatisering van herhalende taken.
- Verhoogde detectie en reactie snelheid.

De klant

- Softwareontwikkelaar
- 13.000 werknemers
- Omzet 2022: €900 miljoen



Het probleem

- Uitdagingen met real-time toegang tot logdata en complexe licentie modellen voor logging services.
- Omvangrijke, gegroeide data-infrastructuur met complexe logging.
- Overmatige ondersteuning van de data-infrastructuur, waardoor weinig tijd overblijft voor strategische planning en activiteiten.

De oplossing

- Gebruik van Cribl Stream om de complexiteit van de bestaande data-infrastructuur te verminderen.
- Implementatie van Cribl Stream als observability pipeline.
- Snelle en probleemloze overgang naar een modernere, eenvoudigere en weerbaardere data-infrastructuur.

Het resultaat

- Modernisering van de data-infrastructuur en verlaging van kosten voor gebruikte analytics tools.
- Vermindering van 166% in de import van redundante logging data.
- Vereenvoudigde onboarding van nieuwe databronnen, wat resulteert in een snellere stijging in de waarde van de data.

SMT



Cribl®

Klantencases

**Klaar om
geïnspireerd te worden?
Neem contact met ons op.**

sales@smtware.com

+31 (0)88 018 41 00