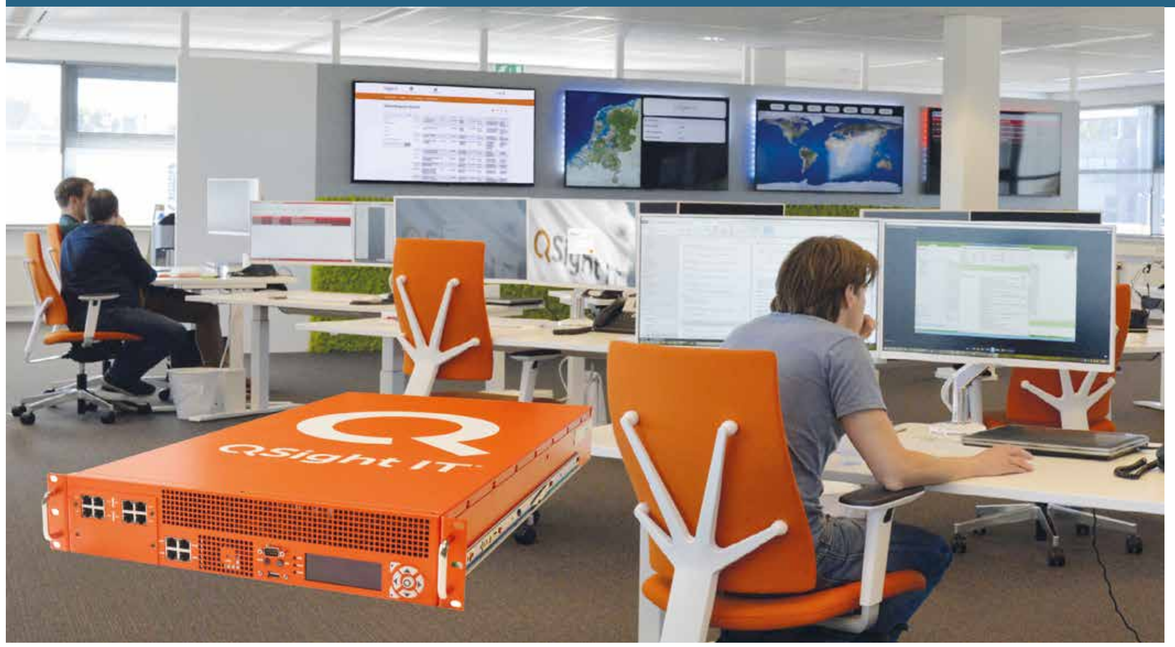


Door IoT en Industrie 4.0 is er een enorme toename aan apparaten die met internet verbonden zijn. Daarbij hebben veel bedrijven tegenwoordig een gedecentraliseerde IT omgeving waar zowel bedrijfsprocessen als informatie in de cloud worden opgeslagen. Dit biedt voor cybercriminelen mogelijkheden, voor bedrijven een groot risico en voor securitypartners een uitdaging, want de kans dat een organisatie in aanraking komt met een cyberaanval, neemt significant toe in een wereld waar elke 20 seconden een aanval plaatsvindt.

Wapenen tegen cybercrime

Met behulp van Open Source en Big Data

Industriële omgevingen zijn waar het cybersecurity aangaat niet anders dan de traditionele kantooromgevingen, met als verschil dat er andere IP-protocollen in gebruik zijn. Fabrikanten en dienstverleners moeten hier hun systemen op aanpassen. Deze specifieke protocollen kennen dan ook hun eigen aanvallen en kwetsbaarheden.
In industriële omgevingen is security vaak een nevenaandachtpunt. De prioriteit ligt bij het proces zelf waarbij beschikbaarheid van het hoogste belang is. Vaak kunnen computersystemen niet zelf onderhouden of geupdate worden, en heeft alleen de fabrikant van de productieapparatuur (letterlijk) de sleutel in handen. Hij wil het liefst vanuit zijn eigen kantoor toegang hebben en dat maakt dat niet alleen hij, maar ook de buitenwereld bij deze systemen kan komen, direct of indirect. De sterke toename van Internet of Things in de industriële wereld maakt dit gevaar nog groter. De industrie wordt hierdoor gevoelig voor spionage en sabotage.
Gelukkig is er de firewall of het intrusion prevention systeem dat een technische melding geeft bij onraad, maar dat zegt niets over de business impact. De crux zit 'm in het combineren van het signaleren van meldingen en het relateren van deze meldingen aan het bedrijfsrisico en eventueel de hele keten.

Meer dan een firewall

Het bedrijf QSight IT, met vestigingen in Delft, Arnhem en Veldhoven, gaat verder dan alleen de firewall en ziet IT-beveiliging als een totale dienstverlening. Zij hebben de QSight IT Probe ontwikkeld die een integraal onderdeel vormt (afbeelding 1). Dit apparaat verzamelt essentiële data in een netwerk en transporteert die data op veilige wijze naar het QSight IT Security Operations Centre (SOC). Uit deze grote hoeveelheid data word met behulp van Artificial Intelligence en Machine Learning zogenaamde Actionable Intelligence gehaald. Hieruit wordt een beeld gecreëerd van het dataverkeer in normale omstandigheden om zo afwijkend dataverkeer te kunnen herkennen. Hiermee hebben ze gegevens in handen waarmee zij hun klanten waarschuwen als er echt iets aan de hand is en adviseren ze hoe te handelen.
Big Data en Machine Learning blijken de meest effectieve verdediging te zijn tegen cyberinbraken. Betere, snellere en meer bruikbare informatie over de beveiliging vermindert immers de kritieke periode van detectie tot actie, en helpt securityspecialisten om proactief een organisatie te verdedigen en te beschermen. Met de inzet van Data Analytics op Big Data zijn zij in staat om informatiestromen real-time te analyseren en in een vroeg stadium indicatoren van cybercrime te signaleren.
Cybercrime aanvechten met behulp van Open Source en Big Data Efficiënte data- en analysemogelijkheden levert de best mogelijke organisatorische security en fraudepreventie. Het gebruik van statistische, netwerk-, pad- en big datamethodologieën kan helpen om voorspellende fraudedetectiemodellen te bouwen die op tijd waarschuwen om snel te kunnen ingrijpen. De data wordt gebruikt voor transparante rapportage van security incidenten, die zal resulteren in verbeterde risicomanagementprocessen voor de netwerken die op deze manier beveiligd worden. Verder kan de integratie en correlatie van gegevens van diverse klantomgevingen een compleet beeld geven van de fraude over verschillende branches, producten en transacties. Met het Security Enrichment Platform brengt QSight IT een aantal Open Source Big Data technologieën samen tot één security platform voor threat- en security monitoring streaming analytics. Het Security Enrichment Platform is hiermee een ideale analyse tool voor het security incident response proces.

QSight IT Probe

De QSight IT Probe wordt ingezet als monitoring- en analyse device in een netwerk ten behoeve van de IntelliDefense (security management) en IntelliGuard (security monitoring) dienstverlening. Door probes op strategische punten in een netwerk te plaatsen, wordt informatie verzameld waarmee een volledig beeld wordt verkregen van het securityniveau van een omgeving. Dit gebeurt enerzijds door het analyseren van netwerkdata die richting de probe wordt gestuurd door middel van tap- en spanpoorten, en anderzijds door het actief uitvoeren van beschikbaarheidsmonitoring en vulnerability scans (afbeelding 2)
Om de benodigde functionaliteit en snelheid voor het verzamelen van grote hoeveelheden data te kunnen leveren, is het device door QSight IT zelf ontwikkeld. Bij de ontwikkeling en revisie van het apparaat is nauw samengewerkt met de hardware specialisten van Arcobel.
Wanneer een probe in het netwerk wordt geplaatst, configureert de engineer op locatie eenvoudig de benodigde IP- en DNS informatie via een display aan de voorkant. Na het aansluiten van de managementinterface zet de probe een beveiligde verbinding op met het QSight IT datacenter. In het netwerk hoeven enkel een netwerkpoort, internetverbinding, DNS server en een aantal firewallregels te worden gefaciliteerd. Bij het onverhoopt wegvallen van de verbinding, wordt deze automatisch hersteld zodra dit mogelijk is. De data die in de tussentijd is verzameld, wordt gebufferd en alsnog richting het Security Enrichment Platform gestuurd.
Voor de IntelliGuard dienstverlening worden extra interfaces aan de probe toegevoegd waarop tap- en spanpoorten kunnen worden aangesloten. Per probe kan worden gekozen voor 1 Gbps koper of 10 Gbps fiberaansluitingen van respectievelijk 4 of 2 poorten. Ook combinaties van koper- en fiberaansluitingen zijn mogelijk.
Voor het leveren van de benodigde monitoring- en analyseservices wordt gebruik gemaakt van een aantal door QSight IT ontwikkelde virtuele probes. Per dienst kan worden bepaald welke virtuele probe wordt geïnstalleerd en mag inhaken op de tap- en spanpoorten van de probe. Het voordeel van deze virtuele laag is dat snel functionaliteit toegevoegd, vernieuwd of verwijderd kan worden zonder de probe te hoeven vervangen of opnieuw te hoeven installeren. Per virtuele probe kan bovendien worden bepaald hoeveel resources deze mag alloceren.
De probe biedt de volgende functionaliteit;

- **Beschikbaarheidsmonitoring**

Dit is een basisfunctionaliteit en wordt daarom standaard op elke probe uitgerold. Vanaf een virtuele probe worden onder andere ping, CPU en geheugengebruik, schijfruimte, netwerkverkeer en applicatiefunctionaliteit van managed devices gemonitord. Naast de managed devices in het klantnetwerk, wordt ook de probe zelf actief in de gaten gehouden. Problemen worden hierdoor vroegtijdig gesignaleerd en kunnen direct worden verholpen. Ook als de verbinding met de probe volledig wegvalt, wordt het Security Operating Center (SOC) hier direct van op de hoogte gesteld.

- **Remote management**

In de IntelliDefense dienstverlening kan de probe worden gebruikt voor het uitvoeren van beheertaken op managed devices. Hierbij kan worden gedacht aan het inloggen op Lights Out Management (LOM) interfaces van firewalls of het geautomatiseerd maken van configuratiebackups van managed devices.

- **Netwerk analyse**

Een belangrijke functie van de probe is het analyseren van netwerkdata die via de tap- en spanpoorten wordt aangeleverd. Hiervoor wordt een gespecialiseerde virtual probe geïnstalleerd die de netwerkdata oppakt en door verschillende tools laat analyseren om hier de benodigde beveiligingsinformatie uit te kunnen filteren. Er wordt gebruikgemaakt van een Intrusion Detection System (IDS) dat zinvolle informatie correleert uit de aangeleverde netwerkdata. Hierbij wordt gebruik gemaakt van diverse threat feeds die dagelijks automatisch worden vernieuwd. Ook wordt metadata zoals IP bron- en doelinformatie van alle pakketten opgeslagen en naar het Security Enrichment Platform in het QSight IT IntelliCenter gestuurd.

Bij QSight IT staan onderzoek en innovatie hoog in het vaandel. Met het IntelliCenter zorgt QSight IT voor een continue stroom van verbetering van bestaande en ontwikkeling van nieuwe producten en/of processen.

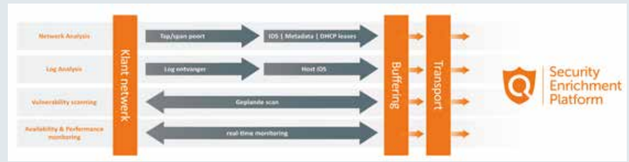
Arcobel Embedded Solutions

De probe die QSight IT (in oktober 2017 overgenomen door KPN) gebruikt voor hun Intelliguard dienstverlening heeft Arcobel Embedded Solutions een aantal jaar geleden volledig ontwikkeld samen met de technische afdeling van QSight IT. QSight IT klopte destijds bij Arcobel aan omdat zij een idee hadden om twee separate systemen samen te voegen tot één compacte oplossing.
Door dit te doen, konden zij een cybersecurity oplossing ontwikkelen in een computerbehuizing die bij een DDOS aanval of een andere cyber treat bij een klant direct inzetbaar was. Dit systeem diende flexibel te kunnen opschalen met LAN poorten en performance. Arcobel heeft daarbij de selectie gedaan voor de te gebruiken hardware maar ook unieke uitbreidbare LAN-modules ontwikkeld samen met hun zusterorganisatie Core Vision. QSight IT leunde daarbij tijdens de ontwikkeling volledig op de technische en mechanische hardware kennis van de specialisten bij Arcobel. Hierdoor konden zij zich richten op de applicatie en de snelle inzetbaarheid van het systeem. Inmiddels is er naast de initiële 1U variant ook een 2U variant ontwikkeld en hebben de aantallen een vlucht genomen. •

Voor meer informatie zie
www.etotaal.nl/achtergrond.
Artikel "Wapenen tegen cybercrime".

www.arcobel.com

Afbeelding 1. De Probe van QSight IT.



Afbeelding 2. De data-afhandeling in de probe.

Brancheorganisatie Cyberveilig Nederland

Acht cybersecurity dienstverleners zijn gekomen tot de oprichting van de brancheorganisatie Cyberveilig Nederland. Doel van de organisatie is de digitale weerbaarheid van Nederland te vergroten en daarnaast de kwaliteit en transparantie binnen de groeiende cybersecurity sector te verhogen. Computest, Fox-IT, Guardian360, Hoffmann, Motiv, Northwave, QSight IT en Zerocopter hebben daarvoor een overeenkomst gesloten en nodigen andere dienstverleners binnen de sector uit zich bij dit initiatief aan te sluiten.
97,1 procent van de Nederlandse bevolking heeft toegang tot internet. Nederland behoort daarmee tot de digitale voorhoede binnen Europa. Deze digitalisering brengt grote economische en maatschappelijke kansen met zich mee. Om die kansen te benutten, is het noodzakelijk om blijvend vertrouwen te kunnen hebben in onze informatie en informatiesystemen. Meer aandacht voor cybersecurity is daarom geen luxe, maar noodzaak.
Cyberveilig Nederland ziet voor zichzelf als rol om vanuit de sector deze onduidelijkheid weg te nemen en hoge kwaliteit van dienstverlening te stimuleren, bijvoorbeeld door het ontwikkelen van kwaliteitskeurmerken. Daarbij ontbreekt echter transparantie en een garantie voor kwaliteit. Beide zijn noodzakelijke elementen om het vertrouwen in de sector te waarborgen.