Guardian360 Lighthouse features

Feature	Hoe Guardian360 hier invulling aan geeft	Voordelen voor IT-afdelingen	Voordelen voor compliance afdelingen	Voordelen voor management
24x7 beschikbaar	SAAS platform met een SLA voor uptime van 99,999%	Doorlopend inzicht in actuele technische details	Doorlopend inzicht in compliance aanbevelingen. Voor auditors bewijs dat er een continu dienst is geïmplementeerd	Doorlopend inzicht in de belangrijkste KPI's
Mobiele app	App voor Android en iOS gebruikers	Ook inzicht in technische informatie als er geen laptop of PC beschikbaar is	Ook inzicht in compliance aanbevelingen als er geen laptop of PC beschikbaar is	Efficiënte manier om op de hoogte te blijven van de belangrijkste KPI's
Sterke wachtwoorden, multi Factor authentication	De password policy van Guardian360 vereist wachtwoorden van minimaal 15 karakters. MFA is verplicht, gebruikers kunnen niet inloggen met username en password alleen	Wachtwoorden kunnen niet eenvoudig geraden of gekraakt worden. MFA is een best practice die door Guardian360 wordt gehandhaafd, IT-afdelingen hoeven hier geen tijd in te steken	Met sterke wachtwoorden wordt voldaan aan normeringen. Doordat MFA verplicht is, hoeven er geen controls ingeregeld te worden om MFA te toetsen.	MFA is een van de belangrijkste verdedigingsmechanismen tegen ransomware. De standaard implementatie door Guardian360 vermindert de kans op ransomware en datalekken via het Lighthouse platform aanzienlijk
Named accounts	We dwingen named accounts af, het is niet mogelijk om generieke accounts te maken	Gebruikers zijn altijd herkenbaar in het platform, altijd is duidelijk wie een comment heeft geplaatst,	Gebruikers zijn altijd herkenbaar in het platform, dus ook wanneer een issue geaccepteerd of gedeeld is	Doordat er geen anonieme accounts mogelijk zijn, is de kans op misbruik verlaagd
Eigen identity provider gebruiken	We bieden mogelijkheden met integratie met AzureAD en The Identity Hub aan.	Gebruikersaccounts zijn eenvoudiger te beheren, geen onnodig dubbel werk en minder kans op het vergeten van deactiveren van user accounts	Audits zijn eenvoudiger omdat toegang tot het Lighthouse platform via de eigen identity provider geregeld kan worden	Medewerkers die uit dienst gaan kunnen automatisch niet meer inloggen als er een eigen identity provider gebruikt wordt. De kans op misbruik en datalekken neemt hierdoor af.
Integration possibilities	Guardian360 Lighthouse biedt een API die alle mogelijkheden biedt die gebruikers ook via de GUI kunnen benutten	Lighthouse kan gekoppeld worden aan een ticketingsysteem, waardoor bepaalde issues via het normale ticket proces afgehandeld kunnen worden	Lighthouse kan gekoppeld worden aan ISMS en GRC tools, waardoor deze systemen ook bewijs bevatten van hoe de controls geïmplementeerd zijn	Doordat Lighthouse data ook in andere dashboards en rapporten opgenomen kan worden, ontstaat er een beter beeld
Meertaligheid	Guardian360 Lighthouse is beschikbaar in Nederlands, Duits en Engels	Engineers kunnen de applicaties gebruiken in het Engels, wat de voertaal binnen de IT is	Relevante compliance inzichten zijn vertaald naar de locale markt	Niet technische gebruikers krijgen informatie in begrijpelijke taal
Inzichten in plaats van data	Lighthouse toont dashboards met actual information in plaats van een overload aan data	Engineers kunnen focussen op het oplossen van issues, in plaats van dat ze tijd kwijt raken aan het ordenen van data.	Per wet en norm zijn de KPI's eenvoudig te volgen en te rapporteren.	Door een dashboard te gebruiken is alle data ontdaan van ruis en kunnen er betere management beslissingen genomen worden.
Voldoen aan Europese wetgeving	Lighthouse wordt gehost in een Nederlands datacenter dat eigendom is van een Nederlandse serviceprovider, data blijft altijd binnen de EU.	Geen zorgen over waar de data van de organisatie wordt gehost.	Geen zorgen over waar de data van de organisatie wordt gehost.	Geen zorgen over waar de data van de organisatie wordt gehost.

Vulnerability scanning IP-adressen, IP-reeksen en web applicaties

Feature	Hoe Guardian360 hier invulling aan geeft	Voordelen voor IT-afdelingen	Voordelen voor compliance afdelingen	Voordelen voor management
Up to date inzicht in kwetsbaarheden	Dagelijkse scan	Je kunt er vanuit gaan dat we altijd de meest actuele informatie tonen en dat je tijd investeert in het oplossen van echte issues.	Altijd inzicht in de meest actuele aanbevelingen om beter te voldoen aan normeringen	Altijd inzicht in de compliance status m.b.t. wet- en regelgeving
Zo min mogelijk false positives	Ons platform maakt gebruik van meerdere scanners, die elkaar cross-checken	Engineers hebben meer zekerheid dat ze naar echte issues kijken, in plaats van false positives	Doordat we minder false positives tonen in vergelijking met andere systemen, is er meer zekerheid dat we de juiste compliance inzichten tonen	De organisatie is bezig met de juiste kwetsbaarheden.
Geen overbodig werk	Lighthouse sluit verholpen issues automatisch en het is mogelijk om issues te accepteren.	Bewijs dat je daadwerkelijk moeite doet om veiliger te worden, dat je hard gewerkt hebt. Alleen de issues in beeld die de moeite waard zijn	Door issues te accepteren bieden we bewijslast voor auditors over hoe er gehandeld is, dat de organisatie in control is. Gesloten issues bewijzen dat er daadwerkelijk moeite is gedaan om te verbeteren	Resources worden efficiënt ingezet doordat er een goede business case gemaakt kan worden
Moderne technieken	Binnen het Lighthouse platform wordt gebruik gemaakt van Machine Learning, Kubernetes en andere moderne technieken om de stabiliteit, schaalbaarheid en veiligheid zoveel mogelijk te garanderen	Als engineer werk je met cutting edge technologie die je werk makkelijker maakt.	Er wordt geen verouderde software gebruikt, waardoor er geen non-conformities ontstaan bij het gebruik van Guardian360.	De organisatie zet de modernste technologie denkbaar in om haar beveiliging op orde te houden.
Geen issues over het hoofd zien	Lighthouse is een gesloten systeem waardoor er geen issues verwijderd kunnen worden. De database met kwetsbaarheden wordt elke dag geüpdatet.	Vertrouwen dat de lijst met issues niet is aangetast en dat Lighthouse alle issues kan vinden die met haar scanners te vinden zijn	Bewijs dat er niet geknoeid kan worden met scanresultaten, vertrouwen dat de lijst met issues zo volledig mogelijk is.	Vertrouwen dat de volledige scope in beeld is
Inzicht in assets	Lighthouse geeft een apart overzicht met gevonden assets dat dagelijks wordt geactualiseerd.	Na elke scan een actueel inzicht in de assets in de scope. BYOD wordt snel ontdekt, devices van kwaadwillenden ook	Compliance inzichten in nieuwe assets zijn binnen een dag zichtbaar	De volledige scope wordt gescand, daardoor binnen een dag inzicht in uitbreidingen
Agentless	We scannen met een probe in het netwerk, niet met agents op systemen.	Lage beheerlast voor IT-administrators, geen dubbele informatie	Minder applicaties om controls voor te verzinnen	Vertrouwen dat Lighthouse issues vindt op een manier dat een crimineel dat ook zou doen.
Scan uitsluitingen	We bieden de mogelijkheid om bepaalde scanners of volledige scanobjecten uit te sluiten van de scan scope.	Beheerders kunnen complete IP-reeksen opvoeren en hoeven niet ip-adressen een voor een op te voeren. Het uitsluiten van een ip-adres, een scanner of zelfs de scanning op een bepaalde poort is mogelijk	Altijd inzicht in de scan scope en welke scan objecten met welke motivatie een uitsluiting hebben	Garantie dat de volledige scan scope gescand wordt en dat altijd duidelijk is waarom er uitzonderingen gemaakt zijn.
Dashboards	Het Lighthouse platform biedt meerdere dashboards en overzichtspagina's	Engineers kunnen via verschillende overzichtspagina's doorklikken naar het door hen gewenste detailniveau	Het is mogelijk om op verschillende manieren compliance trends in te zien en vervolgens naar de onderliggende data te kijken	Ook niet technische bestuurders kunnen inzicht krijgen in de belangrijkste informatiebeveiligingsrisico's en zich een mening vormen
Reports	Het Lighthouse platform biedt mailrapporten en de mogelijkheid om te exporteren naar csv, pdf en documenten te printen	Op de door hen gewenste manier en op het door hen gewenste moment geïnformeerd worden	Op de door hen gewenste manier en op het door hen gewenste moment geïnformeerd worden	Managers hoeven niet in te loggen op het dashboard om toch inzichten te krijgen.
Alerting	Het Lighthouse platform stuurt alerts via sms en email als er urgente zaken zijn	Engineers kunnen erop vertrouwen dat ze essentiële alerts direct krijgen	De organisatie kan snel acteren op een datalek en daardoor beter voldoen aan bijvoorbeeld de AVG	Vertrouwen dat de organisatie snel acteert als er wat mis is, de kans dat een datalek na 3 maanden via een klant, leverancier of de media bekend wordt is daardoor minimaal.

Compliance module

Feature	Hoe Guardian360 hier invulling aan geeft	Voordelen voor IT-afdelingen	Voordelen voor compliance afdelingen	Voordelen voor management
Inzicht in aanbevelingen om beter aan wetgeving te voldoen	In onze compliance module hebben we de AVG en NIS2 geïmplementeerd	Engineers worden ondersteund met inzichten om beter te voldoen aan deze wetgeving	Het Lighthouse platform biedt een aantal inzichten om beter te voldoen aan wetgeving, daardoor is eenvoudig aan te tonen dat de organisatie haar best gedaan heeft te voldoen aan een toezichthouder, rechter of overheidsinstelling	Lagere kans op boetes, het beter voldoen aan de AVG en NIS2 kan commerciële kansen bieden omdat klanten en leveranciers meer vertrouwen in de organisatie hebben.
Inzicht in afwijkingen van normeringen om beter aan deze normen te voldoen	De compliance module bevat diverse normeringen: ISO 27001:2013, ISO 27001:2017, ISO 27001:2022, NEN7510, BSI IT-Grundschutz, TISAX, OWASP, NBA:2019, NOREA/ DigiD, NCSC, ISO 27017:2015, BIG, BIO, BIR, BIWA, BIC, PCI-DSS, saMBO-ICT, IBP FO	Doordat compliance inzichten automatisch worden gegenereerd, hoeven IT-afdelingen hier geen handmatige acties voor uit te voeren	Vulnerability management is een van de eisen in veel normen, met Guardian360 Lighthouse is eenvoudig aan te tonen dat men voldoet. Daarnaast worden audits eenvoudiger.	Management kan eenvoudig aantonen dat zij aan normeringen voldoet, audits worden eenvoudiger.
De bevindingen van Guardian360 kunnen opheffen	Ons platform biedt geen mogelijkheid om bevindingen op te heffen, wel kunnen bevindingen gemotiveerd geaccepteerd worden, waardoor ze niet meer in de lijst met actuele aandachtspunten zijn opgenomen	Engineers hoeven alleen tijd te steken in die issues die daadwerkelijk een aanbeveling of afwijking vormen	Als de organisatie een andere interpretatie van wetten en normen heeft dan Guardian360 heeft, kunnen deze in het platform zichtbaar gemaakt worden. Hierdoor kan weer aangetoond worden dat men haar best gedaan heeft om te voldoen.	Mensen steken tijd in de juiste werkzaamheden, resources worden op de juiste manier ingezet.

Detectie van criminelen

Feature	Hoe Guardian360 hier invulling aan geeft	Voordelen voor IT-afdelingen	Voordelen voor compliance afdelingen	Voordelen voor management
Zo min mogelijk false positives	De Guardian360 Lighthouse hacker alert reageert alleen als er echt iets aan de hand is	Je hoeft alleen te acteren als er daadwerkelijk wat aan de hand is	Minder onjuiste meldingen van datalekken	Mensen steken tijd in de juiste werkzaamheden, resources worden op de juiste manier ingezet.
Eenvoudige installatie	De Guardian360 Hacker Alert kan eenvoudig in het netwerk geplaatst worden en draait daarna volledig automatisch	Eenvoudige deployment en minimale beheertijd; Guardian360 zorgt voor de monitoring, updates en dergelijke/	Doordat Guardian360 een SLA afgeeft hoeft de compliance afdeling minder controls te implementeren.	Mensen steken tijd in de juiste werkzaamheden, resources worden op de juiste manier ingezet.
Vertrouwelijke data moet niet voor iedereen zichtbaar zijn	Afgevangen wachtwoorden worden standaard niet getoond, pas na het wegnemen van die afscherming worden deze getoond	Wanneer een van de beheerders per ongeluk de hacker alert triggert, dan is het wachtwoord niet gelijk voor iedereen zichtbaar	Ook hier wordt voldaan aan de eisen van wetten en normeringen om zorgvuldig met wachtwoorden om te gaan	Wanneer een van de bestuurders of managers per ongeluk de hacker alert triggert, dan is het wachtwoord niet gelijk voor iedereen zichtbaar
Aantonen dat meldingen juist zijn opgevolgd	Lighthouse biedt de mogelijkheid om meldingen te accepteren, waardoor duidelijk is wie dat gedaan heeft op welk moment	Bewijs dat er snel gehandeld is en voorkomen van dubbel werk	Bewijs dat er voor de wet en normeringen tijdig gehandeld is.	Vertrouwen dat de organisatie juist handelt en dat er geen boetes komen door te laat handelen.
Alerting	Het Lighthouse platform stuurt alerts via sms en email als er een crimineel in het netwerk gedetecteerd is	Engineers kunnen erop vertrouwen dat ze hacker alerts direct krijgen	De organisatie kan snel acteren op een datalek en daardoor beter voldoen aan bijvoorbeeld de AVG	Vertrouwen dat de organisatie snel acteert als er wat mis is, de kans dat een datalek na 3 maanden via een klant, leverancier of de media bekend wordt is daardoor minimaal.