PORTFOLIO IMPACT NIS2-SC10 BASIC CERTIFICAAT

Maatregelen	Klant	Partner	Samen	Project/ Consultancy	Portfolio
1.2 Beleidsvorming voor informatiebeveiliging en goedkeuring				V	Advisory
1.3 Toewijzing wie verantwoordelijk is bij informatiebeveiliging				V	Advisory
1.6.1 Overzicht van informatie				V	Advisory
1.6.2 Overzicht van ICT-bedrijfsmiddelen				V	Asset Inventory (vaak al onderdeel en de eerste stap van vulnerability management), Advisory
1.8 Het inleveren van bedrijfsmiddelen na gebruik				V	HR proces (code of conduct), advisory
1.14 Verlening en beheer van toegangsbevoegdheden				V	IAM
1.23 Voorbereiding en optimalisatie van de bedrijfscontinuïteit				V	Advisory - Business Continuity Planning: Risicoanalyse, BIA, strategie maatregelen + implementatie (waaronder backup), communicatieplan, IR-plan, crisisplan, testen en onderhouden
1.26 Samen de toeleveringsketen beveiligen				V	Third Party Risk Management. Advisory en Supply Chain risk tooling (bijv BitSight).
2.2 Educatie van bestuurders en medewerkers				V	Security Awareness Training, Cyber game
2.6 Thuis- of hybride werken op een veilige manier				V	Security Awareness, Advisory (beleid)
2.7 Registratie en rapportage van gebeurtenissen				V	ISMS, Vulnerability Management, Communicatieplan (zie BCP)

3.9 Beveiligingsmaatregelen voor toegang				V	IAM, MFA
4.1 Beveiliging en beheer gebruikersapparaten				V	EDR PW Managers Encryption EMM Vulnerability management Hardening
4.4 Bestrijding en preventie van malware				V	Antivirus, EDR E-mail security Security awareness Encryptie Firewalling
4.5 Informatiebehoud: back-up en herstel				V	Advisory (plannen) Backup (on premise) Backup (cloud)
4.7 Software op computers en apparaten up-to-date houden				V	Asset Inventory Vulnerability scanning Risico bepalen Patching, updates, hardening
4.10 Authenticatie op cruciale systemen				V	IAM Multi Factor Authenticatie Solutions

PORTFOLIO IMPACT NIS2-SC20 SUBSTANTIAL CERTIFICAAT

Maatregelen	Klant	Partner	Samen	Project/ Consultancy	Portfolio
1.2 Beleidsvorming voor informatiebeveiliging en goedkeuring				V	Advisory, ISMS
1.3 Toewijzing wie verantwoordelijk is bij informatiebeveiliging				V	Advisory
1.6.1 Overzicht van informatie				V	Advisory
1.6.2 Overzicht van ICT-bedrijfsmiddelen				V	Asset Inventory (vaak al onderdeel en de eerste stap van vulnerability management), Advisory
1.7 Informatie en aanverwante bedrijfsmiddelen acceptabel gebruiken				V	HR proces (code of conduct), advisory
1.8 Het inleveren van bedrijfsmiddelen na gebruik				V	Advisory
1.9 Informatie indelen van verschillende categorieën van bedrijfsinformatie die hetzelfde niveau van vertrouwelijkheid hebben				V	- Data classificatie (advisory en tooling zoals bijvoorbeeld Varonis) - DLP tools en/of dienstverlening - Compliance Management (voorbeeld is OneTrust)
1.13 Registratie en uitschrijving gebruikers				V	IAM
1.14 Verlening en beheer van toegangsbevoegdheden				V	IAM
1.15 Bescherming van informatie in samenwerking met leveranciers				V	Third Party Risk Management. Advisory + eventueel tooling bijv. Bitsight
1.20 Richtlijnen voor de aanpak van informatiebeveiligingsincidenten (cybersecurityincidenten)				V	Incident Response Plan (Advisory) CERT-dienstverlening/retainer
1.23 Voorbereiding en optimalisatie van de bedrijfscontinuïteit				V	Advisory - Business Continuity Planning: risicoanalyse, BIA,

					strategie maatregelen + implementatie (waaronder backup), communicatieplan, IR-plan, crisisplan, testen en onderhouden
1.26 Samen de toeleveringsketen beveiligen				V	Third Party Risk Management. Advisory en tooling zoals bijv BitSight.
1.27 Verzamelen bewijsmateriaal: bij welk type incidenten dient welk bewijsmateriaal verzameld en veilig gesteld te worden				V	Incident Response Plan (Advisory) CERT-dienstverlening, Forensics (retainer)
2.2 Educatie van bestuurders en medewerkers				V	Security Awareness Training, Cyber game
2.6 Thuis- of hybride werken op een veilige manier				V	Security Awareness, Advisory (beleid)
2.7 Registratie en rapportage van gebeurtenissen				V	ISMS, Vulnerability Management, Communicatieplan (zie BCP)
3.5 Regelgeving voor vertrouwelijke informatie achterlaten op bureau en scherm				V	Advisory: beleid, code of conduct Security Awareness & Behavior proces
3.8 Bedrijfsapparatuur veilig verwijderen of hergebruiken				V	Advisory: asset management, beleid
3.9 Beveiligingsmaatregelen voor toegang				V	IAM, MFA
4.1 Beveiliging en beheer gebruikersapparaten				V	EDR PW Managers Encryption EMM Vulnerability management Hardening
4.4 Bestrijding en preventie van malware				V	Antivirus, EDR E-mail security Security awareness Encryptie

					Firewalling
4.5 Informatiebehoud: back-up en herstel				V	Advisory (plannen) Backup (on premise) Backup (cloud)
4.7 Software op computers en apparaten up-to-date houden				V	Asset Inventory Vulnerability scanning Risico bepalen Patching, updates, hardening
4.9 Netwerksegmentatie: regels vast stellen en toepassen voor het segmenteren van groepen gebruikers, informatiesystemen en informatiediensten				V	Advisory: architectuur, Zero Trust Firewall, Microsegmentatie
4.10 Authenticatie op cruciale systemen				V	IAM Multi Factor Authenticatie Solutions
4.11 Logbestanden: logbestanden van relevante gebeurtenissen registreren en analyseren				V	Logmanagement SIEM NDR MDR, XDR SOAR SOC
5.1 Register van alle OT-bedrijfsmiddelen				V	Asset Management
5.2 Bepaal de afhankelijkheid van OT-systemen				V	Advisory: risicoanalyse, BIA
5.4 Back-ups van OT-systemen				V	Advisory: back up strategie Back up tooling
5.5 Recovery plan OT-systemen				V	Zie 1.23, maar dan specifiek voor OT
5.11 Overzicht van OT-systemen en aanvullende informatie				V	Asset & Configuration Management (Advisory en tooling zoals bijvoorbeeld Tenable)
6.1 Toegang tot broncode				V	Advies en implementatie van versiebeheer: gecentraliseerd versiebeheersysteem (bijv Git), betrouwbaar platform (bijv GitHub), toegangscontrole tot repositories, tags voor versie

					en releases, implementatie van continuous integration en -deployment tooling, Advies en Implementatie van rollen en rechten, authenticatie & autorisatie, auditlogging & monitoring, branchebescherming & pull requests Versleuteling van code in de cloud en in transit Bewustzijn/training ontwikkelaars Backup en disaster recovery Implementatie/gebruik van statische en dynamische analyse tools
6.3 Veilige software ontwikkelen				V	Awareness & training
6.9 Overzicht van geleverde software				V	Automatische versiecontrole via telemetrie en software agents Gebruik van software asset management tooling Versiebeheer in de cloud (SaaS) Informatie verzamelen via bijv API's Handmatige rapportage via bijv portals en rapportages
6.12 Afstemming met klanten over nieuwe software en updates				V	Advisory: procesinrichting voor communicatie en distributie

PORTFOLIO IMPACT NIS2-SC30 HIGH CERTIFICAAT

Maatregelen	Klant	Partner	Samen	Project/ Consultancy	Portfolio
1.2 Beleidsvorming voor informatiebeveiliging en goedkeuring				V	Advisory, ISMS
1.3 Toewijzing wie verantwoordelijk is bij informatiebeveiliging				V	Advisory
1.4 Aansturing door het management				V	- Governance - Opzet en implementatie van Asset & Configuration Management. - Awareness & behavior training
1.5 Beoordeling en inzicht van beveiligingsdreigingen				V	MDR-dienstverlening Threat Hunting CTI
1.6.1 Overzicht van informatie				V	Advisory
1.6.2 Overzicht van ICT-bedrijfsmiddelen				V	Asset Inventory (vaak al onderdeel en de eerste stap van vulnerability management), Advisory
1.7 Informatie en aanverwante bedrijfsmiddelen acceptabel gebruiken				V	HR proces (code of conduct), advisory
1.8 Het inleveren van bedrijfsmiddelen na gebruik				V	Advisory
1.9 Informatie indelen van verschillende categorieën van bedrijfsinformatie die hetzelfde niveau van vertrouwelijkheid hebben				V	- Data classificatie (advisory en tooling zoals bijvoorbeeld Varonis) - DLP tools en/of dienstverlening - Compliance Management (voorbeeld is OneTrust)
1.11 Het overbrengen van informatie binnen de organisatie en aan derden				V	Advisory: code of conduct, beleid, awareness/behavior training
1.13 Registratie en uitschrijving gebruikers				V	IAM

1.14 Verlening en beheer van toegangsbevoegdheden				V	IAM
1.15 Bescherming van informatie in samenwerking met leveranciers				V	Third Party Risk Management. Advisory + eventueel tooling bijv. Bitsight
1.16 Borgen van informatieveiligheid in overeenkomsten met leveranciers				V	Inrichten Third Party Risk Management- en Contract Management Proces
1.18 Toezicht, evaluatie en wijzigingsbeheer van leveranciersdiensten				V	Third Party Risk Management Questionnaires Pentesting Audit Contract Management
1.19 Informatie veilig houden bij het gebruik van cloudservices				V	Advisory: Contract Management
1.20 Richtlijnen voor de aanpak van informatiebeveiligingsincidenten (cybersecurityincidenten)				V	Incident Response Plan (Advisory) CERT-dienstverlening/retainer
1.21 Registratie, beoordeling en afhandeling van informatiebeveiligingsincidenten				V	Advisory: inrichting van risk management. Veel raakvlak met SOC en MDR en advies o.b.v. rapportages.
1.22 Incidenten melden aan externen				V	Advisory: zie ook Business Continuity Planning. CERT-retainer (uitbesteding van de activiteiten die hierbij horen).
1.23 Voorbereiding en optimalisatie van de bedrijfscontinuïteit				V	Advisory - Business Continuity Planning: risicoanalyse, BIA, strategie maatregelen + implementatie (waaronder backup), communicatieplan, IR-plan, DR-plan, crisisplan, testen en onderhouden

1.24 Objectieve toetsing van de aanpak van informatiebeveiliging				V	Audit of maturity assessment tegen een normenkader zoals ISO 27001 ISO 27k certificering
1.25 Handhaven van voorschriften, regelgeving en standaarden voor informatiebeveiliging				V	SOC-dienstverlening Vulnerability Management Advisory: inrichten van benodigde procedures en processen.
1.26 Samen de toeleveringsketen beveiligen				V	Third Party Risk Management. Advisory en tooling bijv BitSight.
1.27 Verzamelen bewijsmateriaal: bij welk type incidenten dient welk bewijsmateriaal verzameld en veilig gesteld te worden				V	Incident Response Plan (Advisory) CERT-dienstverlening, Forensics (retainer)
2.1 Geheimhoudingplicht in arbeidsovereenkomsten				V	HR-verantwoordelijkheid, eventueel advisory dienstverlening
2.2 Educatie van bestuurders en medewerkers				V	Security Awareness Training, Cyber game
2.4 Blijvende verantwoordelijkheden na vertrek of wijziging in de arbeidsrelatie				V	HR-verantwoordelijkheid, eventueel advisory dienstverlening
2.5 Overeenkomsten voor geheimhouding				V	HR-verantwoordelijkheid, eventueel advisory dienstverlening
2.6 Thuis- of hybride werken op een veilige manier				V	Security Awareness, Advisory (beleid)
2.7 Registratie en rapportage van gebeurtenissen				V	ISMS, Vulnerability Management, Communicatieplan (zie BCP)
2.8 Achtergrondcontroles bij kandidaten voor een dienstverband				V	HR-verantwoordelijkheid, eventueel advisory dienstverlening
3.1 Fysieke toegangsbeveiliging				V	Advisory ISMS
3.5 Regelgeving voor vertrouwelijke informatie achterlaten op bureau en scherm				V	Advisory: beleid, code of conduct Security Awareness & Behavior proces
3.8 Bedrijfsapparatuur veilig verwijderen of hergebruiken				V	Advisory: asset management, beleid

3.9 Beveiligingsmaatregelen voor toegang				V	IAM, MFA
4.1 Beveiliging en beheer gebruikersapparaten				V	EDR PW Managers Encryption EMM Vulnerability management Hardening
4.2 Bijzondere toegangsbevoegdheden				V	IAM tooling of -dienstverlening
4.4 Bestrijding en preventie van malware				V	Antivirus, EDR E-mail security Security awareness Encryptie Firewalling
4.5 Informatiebehoud: back-up en herstel				V	Advisory (plannen) Backup (on premise) Backup (cloud)
4.6 Redundantie van infrastructuur				V	Advisory: architectuur
4.7 Software op computers en apparaten up-to-date houden				V	Asset Inventory Vulnerability scanning Risico bepalen Patching, updates, hardening
4.8 Netwerken beheren en beveiligen				V	MSS Secure Networking SASE
4.9 Netwerksegmentatie: regels vast stellen en toepassen voor het segmenteren van groepen gebruikers, informatiesystemen en informatiediensten				V	Advisory: architectuur, Zero Trust Firewall, Microsegmentatie
4.10 Authenticatie op cruciale systemen				V	IAM Multi Factor Authenticatie Solutions
4.11 Logbestanden: logbestanden van relevante gebeurtenissen registreren en analyseren				V	Logmanagement SIEM NDR

					MDR, XDR SOAR SOC
4.12 Cryptografie en encryptie				V	Advisory HSM Certificaatbeheer
4.14 Technische kwetsbaarheden tijdig vinden en repareren				V	Vulnerability Management, hardening, patch management
4.15 Gecontroleerd doorvoeren van wijzigingen				V	Advisory: asset & configuration management
5.1 Register van alle OT-bedrijfsmiddelen				V	Asset Management
5.2 Bepaal de afhankelijkheid van OT-systemen				V	Advisory: risicoanalyse, BIA
5.4 Back-ups van OT-systemen				V	Advisory: back up strategie Back up tooling
5.5 Recovery plan OT-systemen				V	Zie 1.23, maar dan specifiek voor OT
5.6 Segmentatie van OT-netwerken				V	Advisory: architectuur netwerk Netwerk segmentatie: switching, firewalling, microsegmentatie NAC IAM/PRAM
5.8 Remote toegang tot kritieke OT-systemen				V	PRAM
5.9 OT-patches installeren				V	Vulnerability management en patch management
5.11 Overzicht van OT-systemen en aanvullende informatie				V	Asset & Configuration Management (Advisory en tooling zoals bijvoorbeeld Tenable)
6.1 Toegang tot broncode				V	- Advies en implementatie van versiebeheer: gecentraliseerd versiebeheersysteem (bijv Git), betrouwbaar platform (bijv GitHub), toegangscontrole tot repositories, tags voor versie en releases, implementatie van

					continuous integration en -deployment tooling, - Advies en Implementatie van rollen en rechten, authenticatie & autorisatie, auditlogging & monitoring, branchbescherming & pull requests - Versleuteling van code in de cloud en in transit - Bewustzijn/training ontwikkelaars - Backup en disaster recovery Implementatie/gebruik van statische en dynamische analyse tools
6.2 Actueel houden van de programmacode en externe componenten				V	
6.3 Veilige software ontwikkelen				V	Awareness & training
6.4 Bewustwording van informatiebeveiliging bij de ontwikkeling van applicaties				V	Awareness en secure coding
6.5 Testen van de beveiliging van applicaties				V	Pentesting, Red Teaming
6.6 Uitbestede softwareontwikkeling				V	Advisory, contract management
6.7 Scheiden van ontwikkel, test, acceptatie en productie				V	Architectuur advies
6.8 Procedures en methodes voor het deployen van software				V	Advisory
6.9 Overzicht van geleverde software				V	- Automatische versiecontrole via telemetrie en software agents - Gebruik van software asset management tooling - Versiebeheer in de cloud (SaaS) - Informatie verzamelen via bijv API's Handmatige rapportage via bijv portals en rapportages

6.10 Overzicht houden over geleverde apparatuur en programmatuur				V	Asset discovery Asset & configuration management Attack Surface Management Vulnerability Management
6.12 Afstemming met klanten over nieuwe software en updates				V	Advisory: procesinrichting voor communicatie en distributie
				V	