

SPL

ADVIESRAPPORT

**IT VEILIG
EN SOEPEL GEREgeld** 

SPL

Amsterdamseweg 54
6814 CP Arnhem

Email	info@spl.nl
Algemeen	085 - 40 14 280
Support	085 - 40 14 281

IN DIT RAPPORT VIND JE:

- De score van Voorbeeldklant op 18 cybersecurity-onderwerpen op basis van de CIS Critical Security Controls
- Een overzicht van de belangrijkste digitale risico's van Voorbeeldklant
- Concrete en geprioriteerde verbetermaatregelen voor Voorbeeldklant
- Een NIS2 compliance-check voor Voorbeeldklant
- Een geprioriteerd adviesvoorstel voor Voorbeeldklant met indicatieve investering

Contactpersoon

Matthijs van Yren
Commercieel Directeur
085-4014280
matthijs@spl.nl



VOORWOORD

Op 3 mei 2026 bezochten Glenn Mattheij en Matthijs van Yren Voorbeeldklant voor een uitgebreide cybersecurity-inventarisatie. In vier uur hebben we samen alles in kaart gebracht: het netwerk, alle hard- en software, toegangsbeheer, werkprocessen en het beleid rondom digitale veiligheid.

In dit rapport zie je precies waar je staat. Waar het goed gaat, waar de risico's zitten en, nog belangrijker, welke risico's als eerste opgepakt moeten worden. Aan het einde van het rapport vind je een concreet adviesvoorstel met indicatieve investeringsbedragen, zodat je weet waar je aan toe bent.

Dit traject omvatte:

- Digitale kennismaking (30 min.)
- Inventarisatie op locatie (4 uur)
- Verwerking en rapportage door SPL-consultants (5 werkdagen)
- Persoonlijke rapportbespreking op locatie (1,5 uur), nog in te plannen

Hartelijke groet,

Matthijs van Yren
Commercieel directeur

Glenn Mattheij
Senior Network Engineer

Geheimhouding en vrijwaring

SPL gaat vertrouwelijk om met alle informatie. We zijn verantwoordelijk voor de verwerking van de aangeleverde gegevens en de totstandkoming van dit advies. We kunnen niet aansprakelijk worden gesteld voor de juistheid en volledigheid van informatie die door Voorbeeldklant is aangeleverd.



INHOUD

VOORWOORD	2
INHOUD	3
SPL ESSENTIALS	4
<i>Governance</i>	4
<i>Beleid</i>	4
<i>Compliance</i>	4
<i>Bedrijfsrisico's</i>	4
CIS CRITICAL SECURITY CONTROLS	5
ANALYSE METHODIEK	6
<i>Inventarisatie</i>	6
SCORE TOTAAL EN SAMENVATTING	7
<i>Score totaal</i>	7
<i>Samenvatting</i>	7
SCORECARD	8
<i>Schematische weergave</i>	9
PRIORITEITEN	10
<i>Laagste scores op IG1</i>	10
ADVIES	11
<i>NIS2 compliance check</i>	13
VERVOLG	14
BIJLAGE 1 INVENTARISATIE	15
BIJLAGE 2 VERBETERPUNTEN IN DETAIL	18

SPL ESSENTIALS

Governance

Eindverantwoordelijke cybersecurity	Dhr. Voorbeeld
Functie eindverantwoordelijke cybersecurity	CISO
Naam van de CISO/ISO	Dhr. Voorbeeld

Beleid

Is er beleid rondom cybersecurity	Ja, zie ISMS
Wat is de frequentie voor revisie	Jaarlijks
Wat is de frequentie voor evaluatie	Jaarlijks

Compliance

Moet er worden voldaan aan wet/regelgeving	ja, NIS2
Welke zijn van toepassing	ISO27001 en NIS2
Wanneer was hiervoor de laatste audit	2 februari 2026

Bedrijfsrisico's

Is er een risico inventarisatie beschikbaar	Ja, zie ISMS
Wat is de frequentie voor evaluatie	6 maanden
Wanneer is deze voor het laatst uitgevoerd	2 februari 2026
Is er een incident response plan	Ja, zie ISMS
Is er afgelopen jaar een incident geweest	Nee

Belangrijkste risico's

Risico	Kans (1-10)	Continuïteitsplan
Datalek patiëntgegevens	6	Ja
Uitval datacenter	3	Nee – aandachtspunt
Ransomware	7	Ja

Kritieke bedrijfsprocessen

	Proceseigenaar	RTO	RPO	MTD
		X uur	X uur	X uur
		X uur	X uur	X uur
		X uur	X uur	X uur

CIS CRITICAL SECURITY CONTROLS

Wat zijn de CIS Critical Security Controls?

De CIS Critical Security Controls zijn ontwikkeld door het Center for Internet Security (CIS), een non-profitorganisatie die in 2000 is opgericht met als doel de digitale wereld veiliger te maken. De controls zijn wereldwijd erkend als best practices voor IT-beveiliging en worden gebruikt door organisaties van elke omvang.

De methodiek bestaat uit 18 aandachtsgebieden met in totaal 153 concrete maatregelen. Die zijn verdeeld over drie niveaus, zodat je stap voor stap kunt werken aan betere digitale veiligheid:

Niveau	Naam	Voor wie?
IG1	Essentieel	Elke organisatie; het is de basisbeveiliging die je op orde moet hebben
IG2	Gevorderd	Organisaties met complexere omgevingen en gevoelige data
IG3	Expert	Organisaties met een hoog risicoprofiel of specifieke compliance-eisen

Hieronder de schematische weergave van de CIS Controls. In deze weergave is te zien hoe de 153 maatregelen verdeeld zijn over de 18 onderwerpen.

1. Enterprise Assets	5	7. Vulnerability Management	7	13. Network Monitoring	11
2. Software Assets	7	8. Audit Log Management	12	14. Security Training	9
3. Data Protection	14	9. Email Web Protection	7	15. Service Provider Management	7
4. Secure Configuration	12	10. Malware Defenses	7	16. Application Security	14
5. Account Management	6	11. Data Recovery	4	17. Incident Response	9
6. Access Control	8	12. Network Infrastructure	8	18. Penetration Testing	7

IN TOTAAL 153 MAATREGELEN

ANALYSE METHODIEK

Inventarisatie

Tijdens de inventarisatie hebben we samen met jullie vastgesteld welke beveiligingsmaatregelen er al zijn en in hoeverre die zijn geïmplementeerd. Per maatregel kijken we hoe ver je bent: van ‘nog niet gestart’ tot ‘volledig ingericht’. Dat bepaalt de score.

Op basis van die scores berekenen we een totaalscore per beveiligingsonderwerp en per implementatieniveau. Zo zie je in één oogopslag waar je staat en waar de meeste winst te behalen is.

Elke organisatie en IT-omgeving is anders, dus het advies dat we op basis van deze inventarisatie opstellen is volledig afgestemd op de huidige situatie van Voorbeeldklant.




Wat kun je met deze uitkomsten?

Dit rapport is meer dan een momentopname. Het geeft je een onafhankelijk, extern beeld van waar Voorbeeldklant staat op het gebied van cybersecurity. Gebruik het als basis voor een verbeterplan, als input voor het ISMS en managementreview en als onderbouwing bij NIS2- of ISO 27001-trajecten. En als er vragen komen van auditors, partners of toezichthouders, laat je hiermee zien dat Voorbeeldklant aantoonbaar en gestructureerd bezig is met digitale veiligheid.

SCORE TOTAAL EN SAMENVATTING

Score totaal

Hieronder zie je de gemiddelde score van Voorbeeldklant over alle 18 onderwerpen, per implementatieniveau.

Niveau	Score	%
IG1		73%
IG2		59%
IG3		55%

Deze scores geven een goed beeld van waar Voorbeeldklant staat en waar de meeste winst te behalen is. Dat is een goede basis om verder op te bouwen.

Samenvatting

Voorbeeldklant heeft de afgelopen tijd flinke stappen gezet op het gebied van IT-beveiliging. Technisch zijn er al veel goede maatregelen en best practices ingericht. Procesmatig gaat er ook al veel goed van nature, alleen is nog niet alles formeel vastgelegd.

Het grootste verbeterpotentieel zit in overzicht en formalisering. Technische maatregelen zijn pas echt effectief als duidelijk is wat ze bewaken en hoe je hun werking kunt meten. Daarvoor is een compleet en actueel beeld van alle apparatuur, software en accounts essentieel. Dat overzicht is er op dit moment, maar het is te versnipperd.

Ons advies: begin met het stroomlijnen en ordenen van dat overzicht. Vanaf daar kun je stap voor stap verder bouwen aan een sterkere beveiliging.

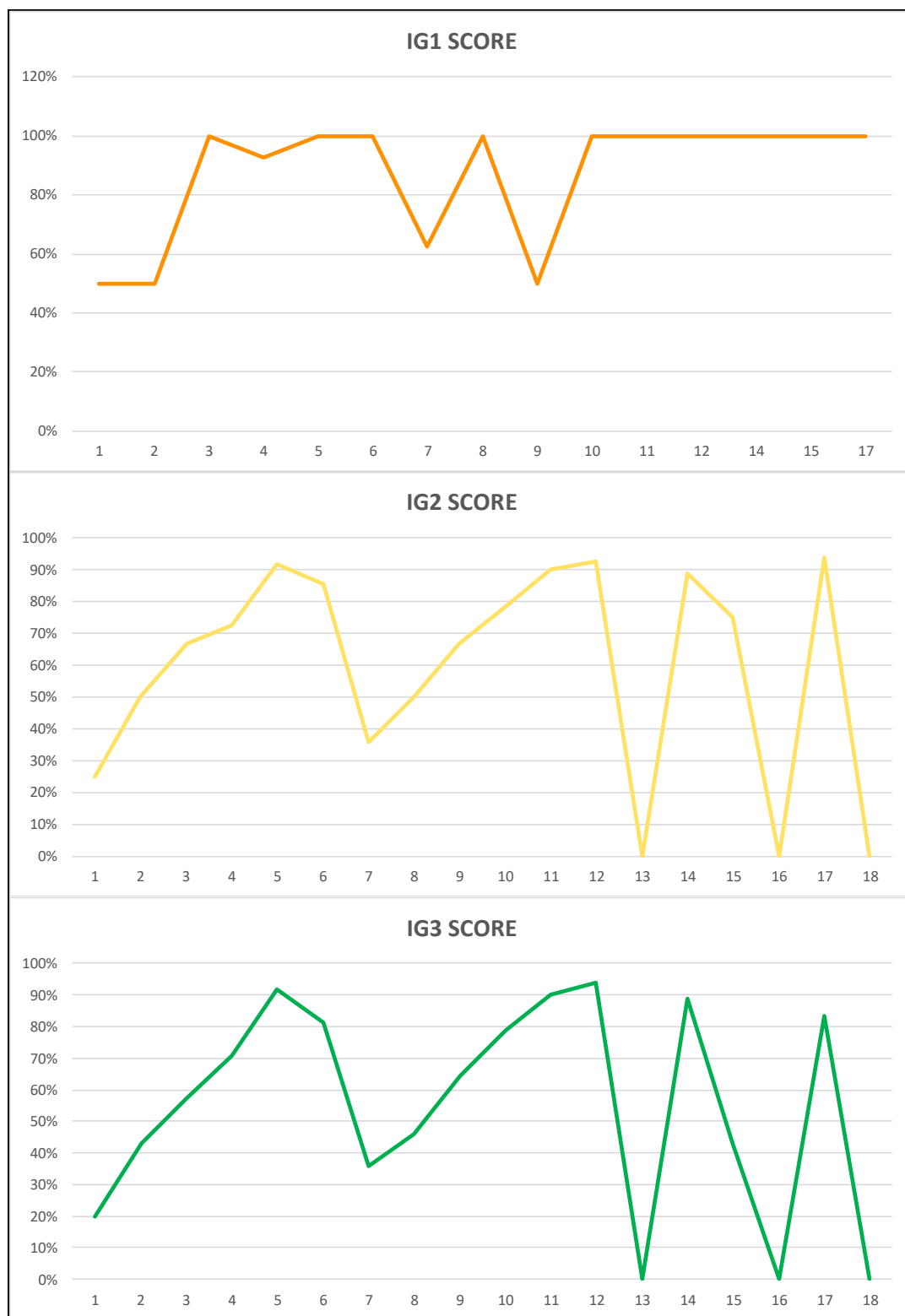
SCORECARD

Hieronder de score per onderwerp, uitgesplitst naar implementatieniveau.

HOOFDSTUK	CIS CONTROL	IG1 SCORE	IG2 SCORE	IG3 SCORE
1	Inventory and Control of Enterprise Assets Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and	50%	25%	20%
2	Inventory and Control of Software Assets Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.	50%	50%	43%
3	Data Protection Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.	100%	67%	57%
4	Secure Configuration of Enterprise Assets and Software Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non computing/IoT devices; and servers) and software (operating systems and applications).	93%	73%	71%
5	Account Management Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.	100%	92%	92%
6	Access Control Management Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.	100%	86%	81%
7	Continuous Vulnerability Management Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry	63%	36%	36%
8	Audit Log Management Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.	100%	50%	46%
9	Email and Web Browser Protections Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.	50%	67%	64%
10	Malware Defenses Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.	100%	79%	79%
11	Data Recovery Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.	100%	90%	90%
12	Network Infrastructure Management Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.	100%	93%	94%
13	Network Monitoring and Defense Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.	0%	0%	0%
14	Security Awareness and Skills Training Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.	100%	89%	89%
15	Service Provider Management Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.	100%	75%	43%
16	Application Software Security Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.	0%	0%	0%
17	Incident Response Management Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.	100%	94%	83%
18	Penetration Testing Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.	0%	0%	0%
GE M I D D E L D		73%	59%	55%

Schematische weergave

Hieronder de schematische weergave van de score per onderwerp op de verschillende niveaus.



PRIORITEITEN

Laagste scores op IG1

Dit zijn de drie onderwerpen waarop Voorbeeldklant het laagst scoort. Een lage score wil niet automatisch zeggen dat dit het grootste risico is. De weging van risico's is meegenomen in het adviesvoorstel verderop in dit rapport.

#	Onderwerp	Score	Risicoprioriteit
1	CIS Control 2: Software Asset Management	Laagst	Hoog
2	CIS Control 7: Vulnerability Management	Op 1 na laagst	Hoog
3	CIS Control 1: Enterprise Asset Management	Op 2 na laagst	Middel

ADVIES

De scores zijn de basis. Maar een advies op maat vraagt meer dan alleen kijken naar wat het laagst scoort. We kijken ook naar het risico als je niets doet, hoeveel een maatregel oplevert ten opzichte van de inspanning en of een oplossing invloed heeft op meerdere onderwerpen tegelijk. Dat zie je terug in de volgorde hieronder.

Stap 1: Realtime inzicht in huidige software (CIS Control 2)

Prioriteit: Hoog | Looptijd: X-X weken | Indicatieve investering: €X.XXX – €X.XXX

Goed weten welke software er in je organisatie draait, is de basis van alles. Zolang dat overzicht er niet is, kun je geen weloverwogen beslissingen nemen over beveiliging. Jullie hebben al een overzicht via Intune, maar daar wordt op dit moment nog te weinig mee gedaan.

Wat gebeurt er als je hier niets mee doet?

Verouderde of ongeautoriseerde software blijft onopgemerkt draaien. Dat vergroot de kans op ransomware en datalekken aanzienlijk.

Wat we adviseren:

- Software-inventarisatie opzetten en documenteren
- Controleren of alle software up-to-date en nog ondersteund is
- Ongeautoriseerde software in kaart brengen en opruimen
- Het bestaande Intune-overzicht als startpunt gebruiken en uitbreiden

Stap 2: Kwetsbaarheden bijhouden en oplossen (CIS Control 7)

Prioriteit: Hoog | Looptijd: X-X weken | Indicatieve investering: €X.XXX – €X.XXX

Zodra je weet welke software er draait, is de volgende stap zorgen dat die software automatisch wordt bijgewerkt. Dat is al gedeeltelijk geregeld via de Microsoft Intune app store, maar voor andere applicaties ontbreekt dit nog.

Wat gebeurt er als je hier niets mee doet?

Bekende kwetsbaarheden in software blijven open staan. Meer dan 60% van succesvolle cyberaanvallen maakt gebruik van kwetsbaarheden waarvoor al een patch beschikbaar was ¹.

Wat we adviseren:

- Automatisch patchen inrichten voor alle geautoriseerde software
- Een handmatig patchproces opzetten voor apps die buiten Intune vallen
- Vulnerability detection activeren via Microsoft Defender
- Maandelijks kwetsbaarheidsrapportage inrichten

Stap 3: Realtime inzicht in alle apparaten op je netwerk (CIS Control 1)

Prioriteit: Middel | Looptijd: X-X weken | Indicatieve investering: €X.XXX – €X.XXX

Tijdens het bezoek bleek dat er geen volledig overzicht is van alle apparaten die verbinding maken met jullie netwerk. Daardoor is het niet te controleren of er ongeautoriseerde apparaten aanwezig zijn.

Wat gebeurt er als je hier niets mee doet?

Onbekende apparaten kunnen onopgemerkt toegang krijgen tot het netwerk en gevoelige data bereiken. Dit is ook direct strijdig met de NIS2-eisen rondom netwerktoegang (Art. 21) en ISO A.8.18.

Wat we adviseren:

- Een volledig apparatenregister opstellen en bijhouden
- Een NAC-oplossing (Network Access Control) implementeren
- Automatische signalering instellen bij onbekende apparaten op het netwerk

¹ Bron: Verizon Data Breach Investigations Report 2025

NIS2 compliance check

Op basis van de inventarisatie zetten we jullie bevindingen af tegen de eisen van NIS2. Dit overzicht is indicatief en bedoeld als oriëntatie. Voor een formele toetsing of certificering heb je altijd een externe audit nodig.

Vereiste	Wat we hebben gezien	Status
Risicobeheer (NIS2 Art. 21)	ISMS aanwezig, risico-inventarisatie actueel	OK
Incident response plan (NIS2 Art. 21d)	Plan aanwezig, geen incidents het afgelopen jaar	OK
Asset management (NIS2 Art. 21b / ISO A.8)	Overzicht aanwezig maar versnipperd; geen volledig apparatenregister	Let op
Kwetsbaarheidsbeheer (NIS2 Art. 21b)	Gedeeltelijk via Intune; nog niet volledig ingericht	Let op

Een volledige mapping van alle CIS Controls naar NIS2 leveren we op verzoek aan.

VERVOLG

De bevindingen in dit rapport bespreken we graag persoonlijk met je. Samen kijken we naar de prioriteiten en bepalen we welke stap als eerste wordt opgepakt.



JOUW CONTACTPERSOON

Matthijs van Yren
Commercieel Directeur

Amsterdamseweg 54
6814 CP Arnhem

T: 085-4014280
E: matthijs@spl.nl

Bereikbaar op werkdagen van 08:00 tot 18:00 uur

WAT ANDEREN ZEGGEN

“SPL vertaalde onze IT-omgeving naar een overzichtelijk rapport met risicoscores en concrete vervolgstappen. Geen abstracte aanbevelingen, maar een plan dat aansloot op hoe wij als organisatie werken.”

- Bjorn Lentjes, Applicatiemanager bij Rentall



BIJLAGE 1 INVENTARISATIE

De volledige inventarisatie met scores per maatregel per CIS Control is opgenomen in deze bijlage.

1 Inventory and Control of Enterprise Assets								
Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; noncomputing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support								
Safeguard	CIS Controls and Safeguards	IG1	IG2	IG3	Ingericht	IG1	IG2	IG3
1,1	Establish and Maintain Detailed Enterprise Asset Inventory	1	1	1	Ja	2	4	5
1,2	Address Unauthorized Assets	1	1	1	Nee			
1,3	Utilize an Active Discovery Tool	1	1	1	Nee			
1,4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset	1	1		Nee			
1,5	Use a Passive Asset Discovery Tool			1	Nee	1	1	1
2 Inventory and Control of Software Assets						50%	25%	20%
Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.								
Safeguard	CIS Controls and Safeguards	IG1	IG2	IG3	Ingericht	IG1	IG2	IG3
2,1	Establish and Maintain a Software Inventory	1	1	1	Ja	3	6	7
2,2	Ensure Authorized Software is Currently Supported	1	1	1	Deels			
2,3	Address Unauthorized Software	1	1	1	Nee			
2,4	Utilize Automated Software Inventory Tools	1	1	1	Ja			
2,5	Allowlist Authorized Software	1	1		Deels			
2,6	Allowlist Authorized Libraries	1	1		Nee			
2,7	Allowlist Authorized Scripts			1	Nee	1,5	3	3
3 Data Protection						50%	50%	43%
Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.								
Safeguard	CIS Controls and Safeguards	IG1	IG2	IG3	Ingericht	IG1	IG2	IG3
3,1	Establish and Maintain a Data Management Process	1	1	1	Ja	6	12	14
3,2	Establish and Maintain a Data Inventory	1	1	1	Ja			
3,3	Configure Data Access Control Lists	1	1	1	Ja			
3,4	Enforce Data Retention	1	1	1	Ja			
3,5	Securely Dispose of Data	1	1	1	Ja			
3,6	Encrypt Data on End-User Devices	1	1	1	Ja			
3,7	Establish and Maintain a Data Classification Scheme	1	1	1	Deels			
3,8	Document Data Flows	1	1	1	Deels			
3,9	Encrypt Data on Removable Media	1	1		Nee			
3,10	Encrypt Sensitive Data in Transit	1	1		Nee			
3,11	Encrypt Sensitive Data at Rest	1	1	1	Nee			
3,12	Segment Data Processing and Storage Based on Sensitivity	1	1		Ja			
3,13	Deploy a Data Loss Prevention Solution	1			Nee			
3,14	Log Sensitive Data Access	1		1	Nee	6	8	8
4 Secure Configuration of Enterprise Assets and Software						100%	67%	57%
Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; noncomputing/IoT devices; and servers) and software (operating systems and applications).								
Safeguard	CIS Controls and Safeguards	IG1	IG2	IG3	Ingericht	IG1	IG2	IG3
4,1	Establish and Maintain a Secure Configuration Process	1	1	1	Ja	7	11	12
4,2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	1	1	1	Ja			
4,3	Configure Automatic Session Locking on Enterprise Assets	1	1	1	Ja			
4,4	Implement and Manage a Firewall on Servers	1	1	1	Ja			
4,5	Implement and Manage a Firewall on End-User Devices	1	1	1	Ja			
4,6	Securely Manage Enterprise Assets and Software	1	1	1	Ja			
4,7	Manage Default Accounts on Enterprise Assets and Software	1	1	1	Deels			
4,8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	1	1	1	Nee			
4,9	Configure Trusted DNS Servers on Enterprise Assets	1	1	1	Nee			
4,10	Enforce Automatic Device Lockout on Portable End-User Devices	1	1		Deels			
4,11	Enforce Remote Wipe Capability on Portable End-User Devices	1	1	1	Ja			
4,12	Separate Enterprise Workspaces on Mobile End-User Devices	1		1	Deels	6,5	8	8,5
5 Account Management						93%	73%	71%
Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service								
Safeguard	CIS Controls and Safeguards	IG1	IG2	IG3	Ingericht	IG1	IG2	IG3
5,1	Establish and Maintain an Inventory of Accounts	1	1	1	Ja	4	6	6
5,2	Use Unique Passwords	1	1	1	Ja			
5,3	Disable Dormant Accounts	1	1	1	Ja			
5,4	Restrict Administrator Privileges to Dedicated Administrator Accounts	1	1	1	Ja			
5,5	Establish and Maintain an Inventory of Service Accounts	1	1	1	Deels			
5,6	Centralize account management	1	1		Ja	4	5,5	5,5
6 Access Control Management						100%	92%	92%
Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.								
Safeguard	CIS Controls and Safeguards	IG1	IG2	IG3	Ingericht	IG1	IG2	IG3
6,1	Establish an Access Granting Process	1	1	1	Ja	5	7	8
6,2	Establish an Access Revoking Process	1	1	1	Ja			
6,3	Require MFA for Externally-Exposed Applications	1	1	1	Ja			
6,4	Require MFA for Remote Network Access	1	1	1	Ja			
6,5	Require MFA for Administrative Access	1	1	1	Ja			
6,6	Establish and Maintain an Inventory of Authentication and Authorization Systems	1	1	1	Nee			
6,7	Centralize Access Control	1	1		Ja			
6,8	Define and Maintain Role-Based Access Control	1		1	Deels	5	6	6,5

7	Continuous Vulnerability Management Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.	100%	86%	81%				
Safeguard	CIS Controls and Safeguards	IG1	IG2	IG3	Ingericht	IG1	IG2	IG3
7,1	Establish and Maintain a Vulnerability Management Process	1	1	1	Deels	4	7	7
7,2	Establish and Maintain a Remediation Process	1	1	1	Deels			
7,3	Perform Automated Operating System Patch Management	1	1	1	Ja			
7,4	Perform Automated Application Patch Management	1	1	1	Deels			
7,5	Perform Automated Vulnerability Scans of Internal Enterprise Assets		1	1	Nee			
7,6	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets	1	1		Nee			
7,7	Remediate Detected Vulnerabilities	1	1		Nee	2,5	2,5	2,5
8	Audit Log Management Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.	63%	36%	36%				
Safeguard	CIS Controls and Safeguards	IG1	IG2	IG3	Ingericht	IG1	IG2	IG3
8,1	Establish and Maintain an Audit Log Management Process	1	1	1	Ja	3	11	12
8,2	Collect Audit Logs	1	1	1	Ja			
8,3	Ensure Adequate Audit Log Storage	1	1	1	Ja			
8,4	Standardize Time Synchronization		1	1	Ja			
8,5	Collect Detailed Audit Logs	1	1	1	Deels			
8,6	Collect DNS Query Audit Logs	1	1		Nee			
8,7	Collect URL Request Audit Logs		1	1	Nee			
8,8	Collect Command-Line Audit Logs		1	1	Nee			
8,9	Centralize Audit Logs	1	1		Nee			
8,10	Retain Audit Logs		1	1	Nee			
8,11	Conduct Audit Log Reviews	1	1		Ja			
8,12	Collect Service Provider Logs			1	Nee	3	5,5	5,5
9	Email and Web Browser Protections Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.	100%	50%	46%				
Safeguard	CIS Controls and Safeguards	IG1	IG2	IG3	Ingericht	IG1	IG2	IG3
9,1	Ensure Use of Only Fully Supported Browsers and Email Clients	1	1	1	Ja	2	6	7
9,2	Use DNS Filtering Services	1	1	1	Onbekend			
9,3	Maintain and Enforce Network-Based URL Filters		1	1	Ja			
9,4	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions		1	1	Nee			
9,5	Implement DMARC		1	1	Ja			
9,6	Block Unnecessary File Types		1	1	Ja			
9,7	Deploy and Maintain Email Server Anti-Malware Protections			1	Deels	1	4	4,5
10	Malware Defenses Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.	50%	67%	64%				
Safeguard	CIS Controls and Safeguards	IG1	IG2	IG3	Ingericht	IG1	IG2	IG3
10,1	Deploy and Maintain Anti-Malware Software	1	1	1	Ja	3	7	7
10,2	Configure Automatic Anti-Malware Signature Updates	1	1	1	Ja			
10,3	Disable Autorun and Autoplay for Removable Media	1	1	1	Ja			
10,4	Configure Automatic Anti-Malware Scanning of Removable Media		1	1	Nee			
10,5	Enable Anti-Exploitation Features		1	1	Deels			
10,6	Centrally Manage Anti-Malware Software		1	1	Ja			
10,7	Use Behavior-Based Anti-Malware Software		1	1	Ja	3	5,5	5,5
11	Data Recovery Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.	100%	79%	79%				
Safeguard	CIS Controls and Safeguards	IG1	IG2	IG3	Ingericht	IG1	IG2	IG3
11,1	Establish and Maintain a Data Recovery Process	1	1	1	Ja	4	5	5
11,2	Perform Automated Backups	1	1	1	Ja			
11,3	Protect Recovery Data	1	1	1	Ja			
11,4	Establish and Maintain an Isolated Instance of Recovery Data	1	1	1	Ja			
11,5	Test Data Recovery		1	1	Deels	4	4,5	4,5
12	Network Infrastructure Management Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.	100%	90%	90%				
Safeguard	CIS Controls and Safeguards	IG1	IG2	IG3	Ingericht	IG1	IG2	IG3
12,1	Ensure Network Infrastructure is Up-to-Date	1	1	1	Ja	1	7	8
12,2	Establish and Maintain a Secure Network Architecture		1	1	Ja			
12,3	Securely Manage Network Infrastructure		1	1	Ja			
12,4	Establish and Maintain Architecture Diagram(s)	1	1	1	Ja			
12,5	Centralize Network Authentication, Authorization, and Auditing (AAA)	1	1		Deels			
12,6	Use of Secure Network Management and Communication Protocols		1	1	Ja			
12,7	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA		1	1	Ja			
12,8	Establish and Maintain Dedicated Computing Resources for All Administrative Work			1	Ja	1	6,5	7,5

13 Network Monitoring and Defense										
Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.						100%	93%	94%		
Safeguard	CIS Controls and Safeguards	IG1	IG2	IG3	Ingericht	IG1	IG2	IG3		
13,1	Centralize Security Event Alerting	1	1	1	Nee		6	11		
13,2	Deploy a Host-Based Intrusion Detection Solution	1	1	1	Onbekend					
13,3	Deploy a Network Intrusion Detection Solution	1	1	1	Onbekend					
13,4	Perform Traffic Filtering Between Network Segments	1	1	1	Onbekend					
13,5	Manage Access Control for Remote Assets	1	1	1	Onbekend					
13,6	Collect Network Traffic Flow Logs	1	1	1	Onbekend					
13,7	Deploy a Host-Based Intrusion Prevention Solution	1	1	1	Onbekend					
13,8	Deploy a Network Intrusion Prevention Solution	1	1	1	Onbekend					
13,9	Deploy Port-Level Access Control	1	1	1	Onbekend					
13,10	Perform Application Layer Filtering	1	1	1	Onbekend					
13,11	Tune Security Event Alerting Thresholds	1	1	1	Onbekend		0	0		
14 Security Awareness and Skills Training										
Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.							0%	0%		
Safeguard	CIS Controls and Safeguards	IG1	IG2	IG3	Ingericht	IG1	IG2	IG3		
14,1	Establish and Maintain a Security Awareness Program	1	1	1	Ja	8	9	9		
14,2	Train Workforce Members to Recognize Social Engineering Attacks	1	1	1	Ja					
14,3	Train Workforce Members on Authentication Best Practices	1	1	1	Ja					
14,4	Train Workforce on Data Handling Best Practices	1	1	1	Ja					
14,5	Train Workforce Members on Causes of Unintentional Data Exposure	1	1	1	Ja					
14,6	Train Workforce Members on Recognizing and Reporting Security Incidents	1	1	1	Ja					
14,7	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing	1	1	1	Ja					
14,8	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over	1	1	1	Ja					
14,9	Conduct Role-Specific Security Awareness and Skills Training	1	1	1	Nee	8	8	8		
15 Service Provider Management										
Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.						100%	89%	89%		
Safeguard	CIS Controls and Safeguards	IG1	IG2	IG3	Ingericht	IG1	IG2	IG3		
15,1	Establish and Maintain an Inventory of Service Providers	1	1	1	Ja	1	4	7		
15,2	Establish and Maintain a Service Provider Management Policy	1	1	1	Deels					
15,3	Classify Service Providers	1	1	1	Ja					
15,4	Ensure Service Provider Contracts Include Security Requirements	1	1	1	Deels					
15,5	Assess Service Providers	1	1	1	Nee					
15,6	Monitor Service Providers	1	1	1	Nee					
15,7	Securely Decommission Service Providers	1	1	1	Nee	1	3	3		
16 Application Software Security										
Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.						100%	75%	43%		
Safeguard	CIS Controls and Safeguards	IG1	IG2	IG3	Ingericht	IG1	IG2	IG3		
16,1	Establish and Maintain a Secure Application Development Process	1	1	1	Onbekend		11	14		
16,2	Establish and Maintain a Process to Accept and Address Software Vulnerabilities	1	1	1	Onbekend					
16,3	Perform Root Cause Analysis on Security Vulnerabilities	1	1	1	Onbekend					
16,4	Establish and Manage an Inventory of Third-Party Software Components	1	1	1	Onbekend					
16,5	Use Up-to-Date and Trusted Third-Party Software Components	1	1	1	Onbekend					
16,6	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities	1	1	1	Onbekend					
16,7	Use Standard Hardening Configuration Templates for Application Infrastructure	1	1	1	Onbekend					
16,8	Separate Production and Non-Production Systems	1	1	1	Onbekend					
16,9	Train Developers in Application Security Concepts and Secure Coding	1	1	1	Onbekend					
16,10	Apply Secure Design Principles in Application Architectures	1	1	1	Onbekend					
16,11	Leverage Vetted Modules or Services for Application Security Components	1	1	1	Onbekend					
16,12	Implement Code-Level Security Checks	1	1	1	Onbekend					
16,13	Conduct Application Penetration Testing	1	1	1	Onbekend					
16,14	Conduct Threat Modeling	1	1	1	Onbekend		0	0		
17 Incident Response Management										
Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.							0%	0%		
Safeguard	CIS Controls and Safeguards	IG1	IG2	IG3	Ingericht	IG1	IG2	IG3		
17,1	Designate Personnel to Manage Incident Handling	1	1	1	Ja	3	8	9		
17,2	Establish and Maintain Contact Information for Reporting Security Incidents	1	1	1	Ja					
17,3	Establish and Maintain an Enterprise Process for Reporting Incidents	1	1	1	Ja					
17,4	Establish and Maintain an Incident Response Process	1	1	1	Ja					
17,5	Assign Key Roles and Responsibilities	1	1	1	Ja					
17,6	Define Mechanisms for Communicating During Incident Response	1	1	1	Ja					
17,7	Conduct Routine Incident Response Exercises	1	1	1	Deels					
17,8	Conduct Post-Incident Reviews	1	1	1	Ja					
17,9	Establish and Maintain Security Incident Thresholds	1	1	1	Nee	3	7,5	7,5		
18 Penetration Testing										
Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.						100%	94%	83%		
Safeguard	CIS Controls and Safeguards	IG1	IG2	IG3	Ingericht	IG1	IG2	IG3		
18,1	Establish and Maintain a Penetration Testing Program	1	1	1	Nee		3	5		
18,2	Perform Periodic External Penetration Tests	1	1	1	Nee					
18,3	Remediate Penetration Test Findings	1	1	1	Nee					
18,4	Validate Security Measures	1	1	1	Nee					
18,5	Perform Periodic Internal Penetration Tests	1	1	1	Nee		0	0		

BIJLAGE 2 VERBETERPUNTEN IN DETAIL

De maatregelen hieronder brengen CIS Controls 1, 2 en 7 naar een 100% score op IG1-niveau als ze volledig zijn doorgevoerd.

CONTROL 01 Inventory and Control of Enterprise Assets

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
1.1	Establish and Maintain Detailed Enterprise Asset Inventory Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	Devices	Identify	●	●	●
1.2	Address Unauthorized Assets Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	Devices	Respond	●	●	●

CONTROL 02 Inventory and Control of Software Assets

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
2.1	Establish and Maintain a Software Inventory Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	Applications	Identify	●	●	●
2.2	Ensure Authorized Software is Currently Supported Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	Applications	Identify	●	●	●
2.3	Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	Applications	Respond	●	●	●

CONTROL
07**Continuous Vulnerability Management**

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
7.1	Establish and Maintain a Vulnerability Management Process Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Applications	Protect	●	●	●
7.2	Establish and Maintain a Remediation Process Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.	Applications	Respond	●	●	●
7.3	Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	Applications	Protect	●	●	●
7.4	Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	Applications	Protect	●	●	●