Krijg een compleet beeld van je securitystatus met een helder plan van aanpak

Cybersecurity assessment met CSAT

solutions

solutions

Specialist in veilig samenwerken:

- Met Microsoft technologie
- SI - samenwerkomgevingen volgens beproefde structuren in SharePoint Online en Teams
- ISV – ontwikkelaar van security en sovernance software
- Microsoft gebruikt QS solutions' eSAT software als geprefereerd Cybersecurity assessment middel

Online samenwerken – zo doe je dat veilig én gebruiksvriendelijk

Webinar: Hoe waarborg je security en governance in Microsoft Teams?

Hoe zorg je ervoor dat je basis security op orde is?

Als bedrijf kan je niet meer zonder aandacht voor cybersecurity. Het onderwerp is alleen zó veelomvattend dat het lastig is om concreet plan te maken en prioriteiten te stellen. Daarnaast ligt de lat sowieso hoog anno nu: niet alleen worden cybercriminelen steeds slimmer, ook het vele thuiswerken blijkt extra risico's met zich mee te brengen. Hoe dan ook, het start met het op orde brengen van een aantal basiszaken. Eén ding weet je zeker: als je niets doet gebeurt er niets.

Proactief werken aan je IT-security

Cybercriminaliteit is niet nieuw meer. We weten allemaal dat we 'iets' met digitale beveiliging moeten. Net zoals je je huis beveiligt met degelijke sloten om inbrekers buiten de deur te houden, geldt dit ook voor de veiligheid van bedrijfsdata. Hoe weet je wat de **kwetsbaarheden** zijn van *jouw organisatie*? Hoe besteed je het beschikbare **securitybudget** op de meest effectieve manier?

Iedere organisatie moet secure zijn

- Bewijs naar opdrachtgevers
- Branche-specifieke eisen
- Certificeringen
- Wetgeving

Essential Eight

CYBER ESSENTIALS

Information Security Management ISO 27001 Certified

NEN NEN 7510 | Informatiebeveiliging in de zorg

Normenkader informatiebeveiliging en privacy voor het onderwijs

NIS2 Directive

NIST Cybersecurity Framework

Iedere organisatie moet weten wat haar beveiligingssituatie is, en moet een plan hebben om te (blijven) verbeteren.

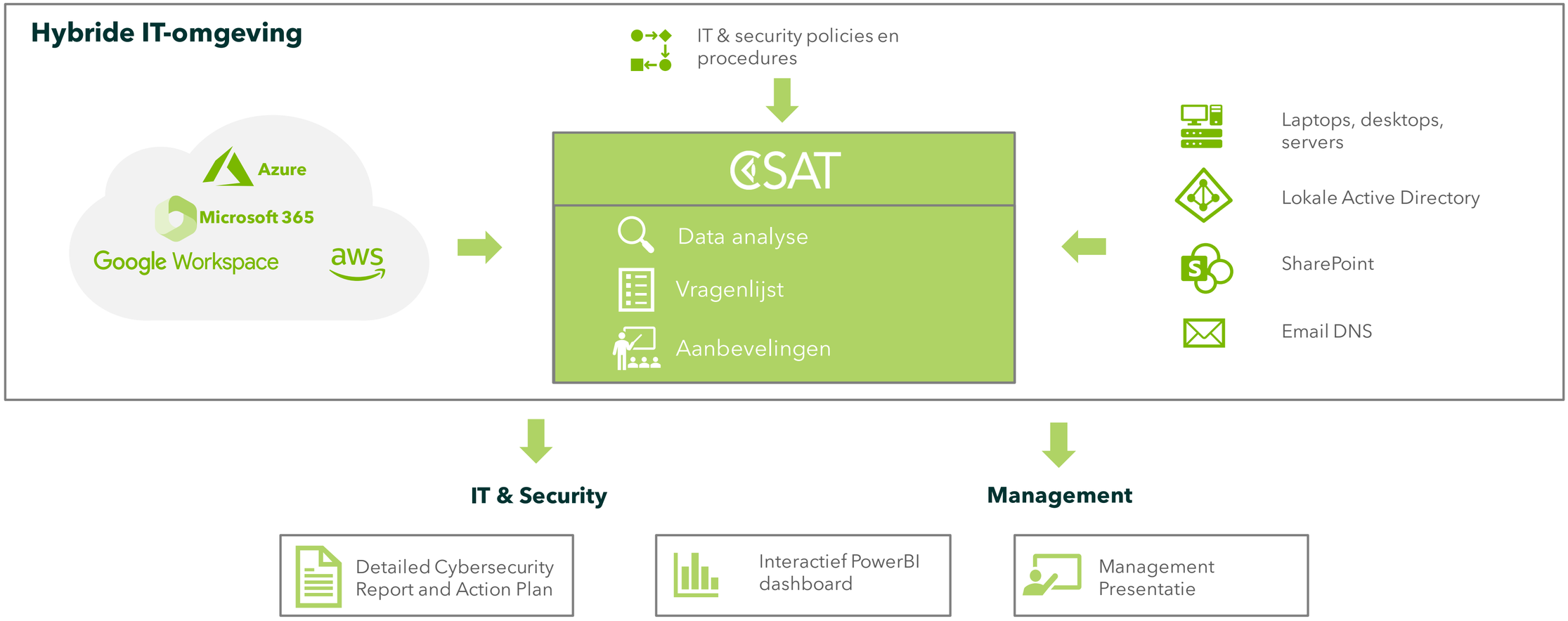
Voldoen aan het Normenkader IBP voor digitale veiligheid en privacy in het onderwijs is geen simpele opgave. Waar begin je als onderwijsinstelling en welke stappen moet je zetten?

Cybersecurity assessment met CSAT

Biedt een **holistisch beeld** van uw **cyberbeveiligingspositie** samen met **op feiten gebaseerde aanbevelingen** op basis van een internationaal erkend cyberbeveiligingskader.

CSAT **verzamelt** en analyseert **in korte tijd data** uit uw hybride IT-omgeving om datagedreven security aanbevelingen te doen.

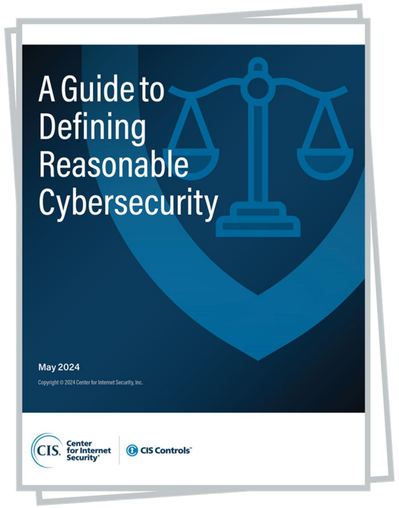
Data collectie en vragenlijst



CIS Controls

[CIS Critical Security Controls (cisecurity.org)]

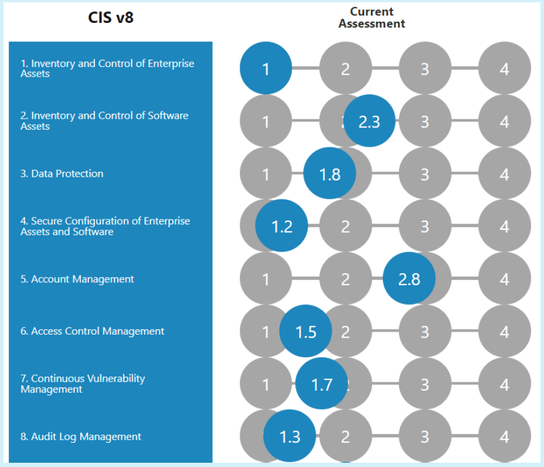
CONTROL 01 Inventory and Control of Enterprise Assets	5 Safeguards	IG1 2/5	IG2 4/5	IG3 5/5
CONTROL 02 Inventory and Control of Software Assets	7 Safeguards	IG1 3/7	IG2 6/7	IG3 7/7
CONTROL 03 Data Protection	14 Safeguards	IG1 6/14	IG2 12/14	IG3 14/14
CONTROL 04 Secure Configuration of Enterprise Assets and Software	12 Safeguards	IG1 7/12	IG2 11/12	IG3 12/12
CONTROL 05 Account Management	6 Safeguards	IG1 4/6	IG2 6/6	IG3 6/6
CONTROL 06 Access Control Management	8 Safeguards	IG1 5/8	IG2 7/8	IG3 8/8
CONTROL 07 Continuous Vulnerability Management	7 Safeguards	IG1 4/7	IG2 7/7	IG3 7/7
CONTROL 08 Audit Log Management	12 Safeguards	IG1 3/12	IG2 11/12	IG3 12/12
CONTROL 09 Email and Web Browser Protections	7 Safeguards	IG1 2/7	IG2 6/7	IG3 7/7
CONTROL 10 Malware Defenses	7 Safeguards	IG1 3/7	IG2 7/7	IG3 7/7
CONTROL 11 Data Recovery	5 Safeguards	IG1 4/5	IG2 5/5	IG3 5/5
CONTROL 12 Network Infrastructure Management	8 Safeguards	IG1 1/8	IG2 7/8	IG3 8/8
CONTROL 13 Network Monitoring and Defense	11 Safeguards	IG1 0/11	IG2 6/11	IG3 11/11
CONTROL 14 Security Awareness and Skills Training	9 Safeguards	IG1 8/9	IG2 9/9	IG3 9/9
CONTROL 15 Service Provider Management	7 Safeguards	IG1 1/7	IG2 4/7	IG3 7/7
CONTROL 16 Applications Software Security	14 Safeguards	IG1 0/14	IG2 11/14	IG3 14/14
CONTROL 17 Incident Response Management	9 Safeguards	IG1 3/9	IG2 8/9	IG3 9/9
CONTROL 18 Penetration Testing	5 Safeguards	IG1 0/5	IG2 3/5	IG3 5/5



[Reasonable Cybersecurity Guide (cisecurity.org)]

CSAT rapportage

Gedetailleerd rapport

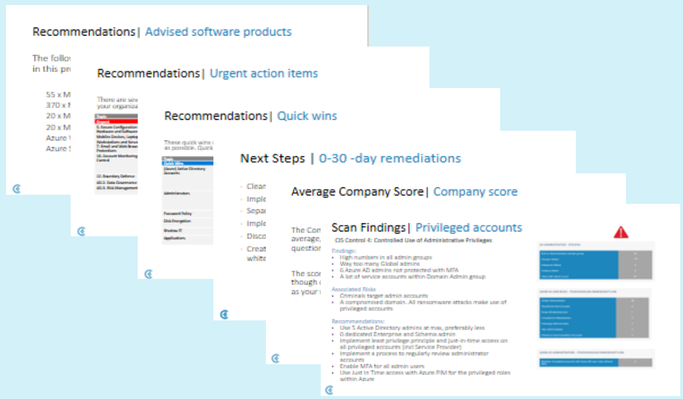


4.1 Urgent Actions (assembled)

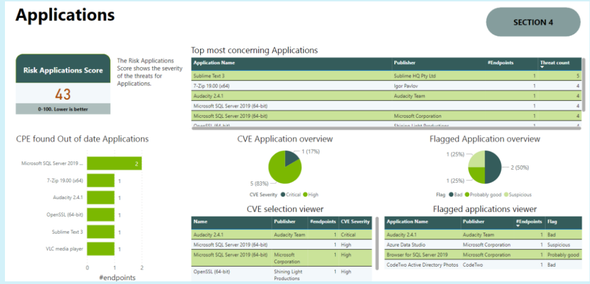
To provide you with a condensed overview of most urgent findings, we assembled them here. For detailed information, refer to the respective controls in chapter 5. We recommend reviewing the items and, depending on your risk appetite and budget priorities, to add your choices to the beforementioned plan of approach or roadmap/project plan.

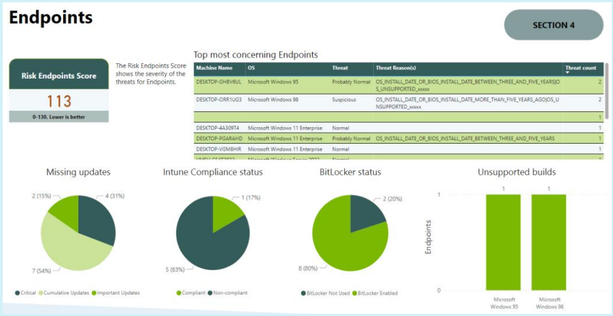
Topic	Action	Associated Software Products	ZTA Zone	RCA mitigation
Urgent				
3. Continuous Vulnerability Management	• implement a patch management process and tooling. Gain insights on the patch status of all systems • Gain continues insight on your specific regulatory requirements	• Microsoft Endpoint Manager • Windows Server Update Services (WSUS) • Azure Security Center • Azure Sentinel • Azure AD identity Protection	3	0-30
4. Controlled Use of Administrative Privileges	• Setup personal admin accounts and enable multi-factor authentication for all external administrative access with just in time permissions	• Azure AD Privileged Identity Management (PIM) • Privileged Access Management (PAM) • Azure AD Multi-Factor Authentication (MFA) • Azure AD Conditional Access	1	0-30

Management samenvatting



Power BI dashboards





Demo

Assessment aanpak

Stap 1

Kick-off met een cybersecurity specialist:
- Introductie
- Bespreek de doelen van het assessment

Systeemvereisten delen
Bereid de omgeving voor en plan de vervolgactiviteiten

2 uur

Stap 2

Teams afspraken met een cybersecurity-specialist om de scans op te zetten om data te verzamelen

Beantwoorden van de vragenlijst in een interview

8 uur

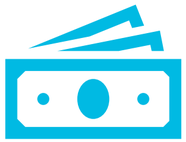
Stap 3

Eindpresentatie maken van bevindingen, conclusies en aanbevelingen.

Eindrapport en presentatie

1.5 uur

CSAT maakt op begrijpelijke wijze duidelijk hoe security ervoor staat



Slimme en verantwoorde investeringen in beveiliging die gericht zijn op zwakheden van de organisatie

Bespaar tijd, moeite en budget door te focussen op wat urgent en relevant is

Afstemming tussen IT/Security en ‘anderen’

Bewijs van vooruitgang op het gebied van beveiliging en werken aan verbetering

Volledig op de hoogte van de huidige veiligheidsstatus en controle over de zwakke plekken

Word cyberweerbaar via een geprioriteerde actielijst

Succes met een vliegende start naar Normenkader IBP!

Bedankt!