WORKSHOP

Toolbox technische weerbaarheid

SAMENWERKEN AAN
CYBERVEILIGHEID
IN HET MBO

PROGRAMMA
Cyberveiligheid

NETWERK
Informatiebeveiliging
en Privacy

MBO Raad

mbo digitaal

mbodigitaal.nl/cyberveiligheid

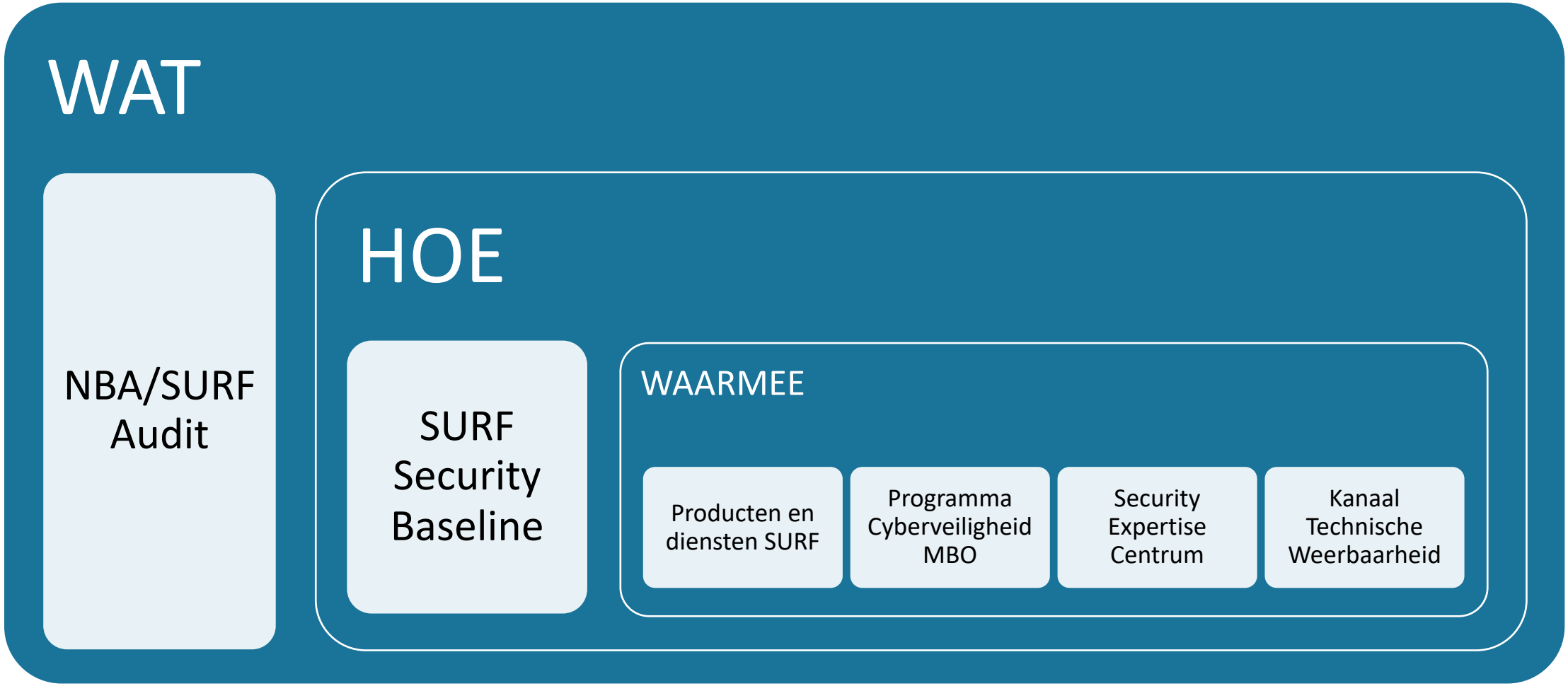
mbo digitaal

Focus

GOVERNANCE		PROCESSEN		TECHNISCHE WEERBAARHEID	
G01	Strategie	P08	Human Resources	T15	MFA - Thuiswerken
G02	Beleid	P09	ITIL	T16	SOC SIEM
G03	Architectuur	P10	Datamanagement	T17	Pentesten
G04	Eigenaarschap	P11	IAM	T18	Patchbeheer
G05	Risk Management	P12	Security Baselines	T19	Infrastructuur
G06	Roadmap	P13	Business Continuïteit	T20	Security Policy
G07	Toetsing	P14	Cloud Leveranciers	T21	Computer Operations

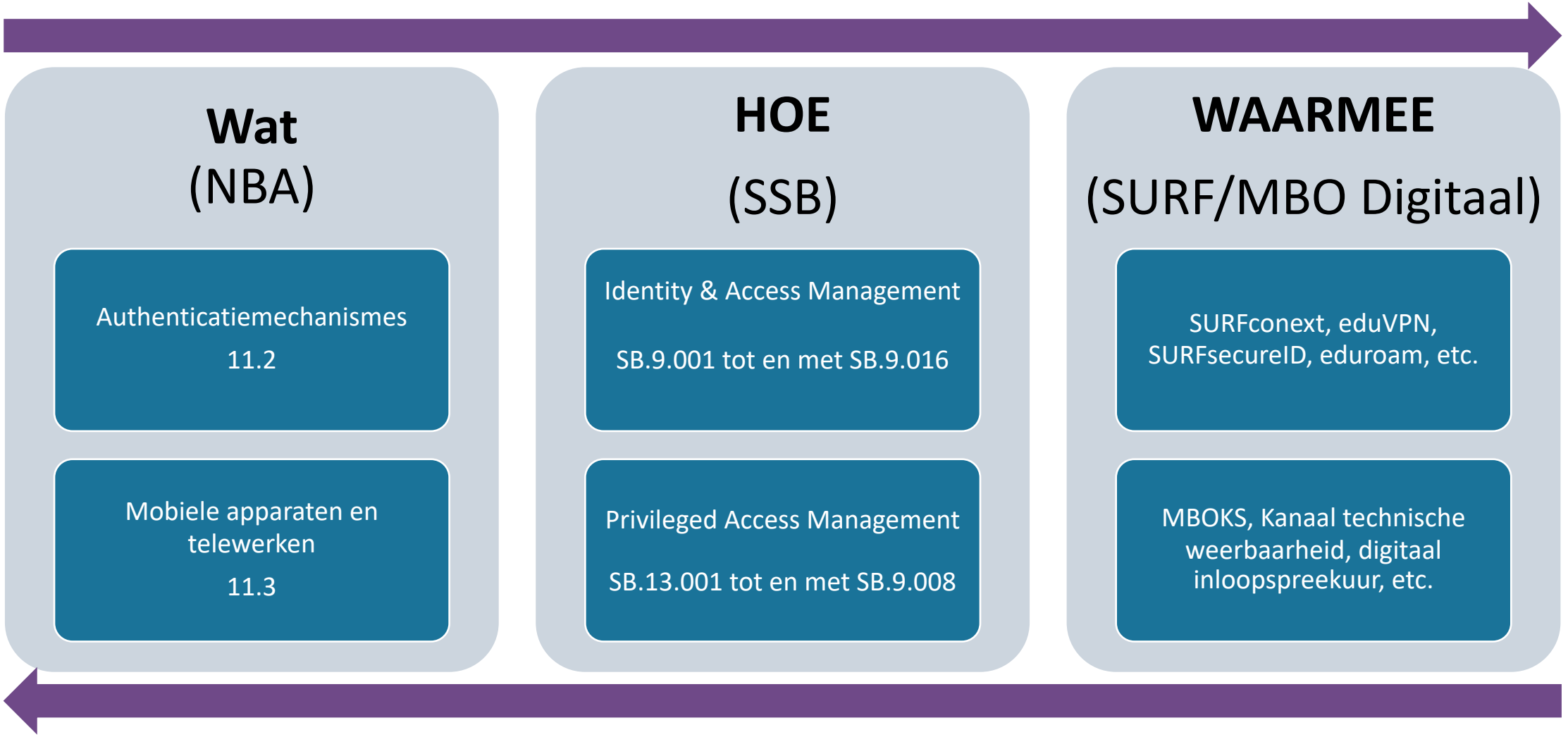
mbo digitaal

Verbanden



mbo digitaal

Voorbeeld



Security Expertise Centrum

Helpt instellingen weerbaar te maken en te houden tegen cybersecuritydreigingen en -aanvallen. Dit doen we door kennis te bundelen en beschikbaar te stellen op één platform voor alle instellingen.
Het Security Expertise Centrum (SEC) is een samenwerking tussen instellingen, externe partners en SURF.

Meer weten over het 'SEC'? Neem contact met me op!

Ed de Vries

+31 88 787 30 00

sec@surf.nl

Voordelen

- Schaalvoordeel
- Uitwisseling van kennis en producten
- Eén ingang voor al jouw security vragen
- Voor en door de instellingen
- Samen houden we onze sector veilig

Producten

- Portaal https://sec.surf.nl
- Actuele templates beleid, thema-beleid en andere
- Relevante artikelen en thema's
- Kennisproducten
- Overzicht van de SURF security-diensten

mbo digitaal

SURF Security Baseline

- 110 controls
- 16 domeinen
- Risico gebaseerd
- Eigenaarschap
- Werkgroep om SSB continu te verbeteren
- Relatie met NBA/SURFaudit
- Voor jezelf en leveranciers

- https://sec.surf.nl/controls/

mbo digitaal

Kanaal Technische Weerbaarheid

Technische weerbaarheid

Start | Nieuws | Aankomende events | Cybersecurity onderzoeken | Handige links | Prullenbak | Bewerken

+ Nieuw | Details voor de pagina | Analyse | Gepubliceerd op 28-11-2023 | Delen

- (Web)applicatie beveiliging
- Asset Management
- Backup & Restore
- Cloud Security
- Continuïteitsbeheer
- Cryptografie
- Cyberdreigingsbeeld
- Digitale inloopspreekuren cybersecurity
- DNS
- E-mail
- Fysieke beveiliging
- Hardening
- Identity & Access Management (IAM)
- Incident Response
- Internet of Things (IoT)
- Kwetsbaarheden Management
- Linux
- MBOKS
- Microsoft
- Mobiele apparaten
- Netwerkbeveiliging
- Operational Technology
- Printers
- Servers
- Software ontwikkeling
- Training

mbo digitaal

MBOKS

Geweest

1. Responsible disclosure
2. Incident Response
3. Monitoring & Detectie

Gepland

1. Vulnerability Management (18 december 2023)
2. Hardening (11 januari 2024)
3. Netwerksegmentatie & Logging (12 februari 2024)
4. Patchmanagement (14 maart 2024)

Heb je een suggestie of feedback? Laat het ons weten!

mbo digitaal

Digitaal inloopspreekuur cybersecurity

- Eerste maandag van de maand (10-11 uur)
- Derde vrijdag van de maand (10-11 uur)
- Tenzij anders aangegeven

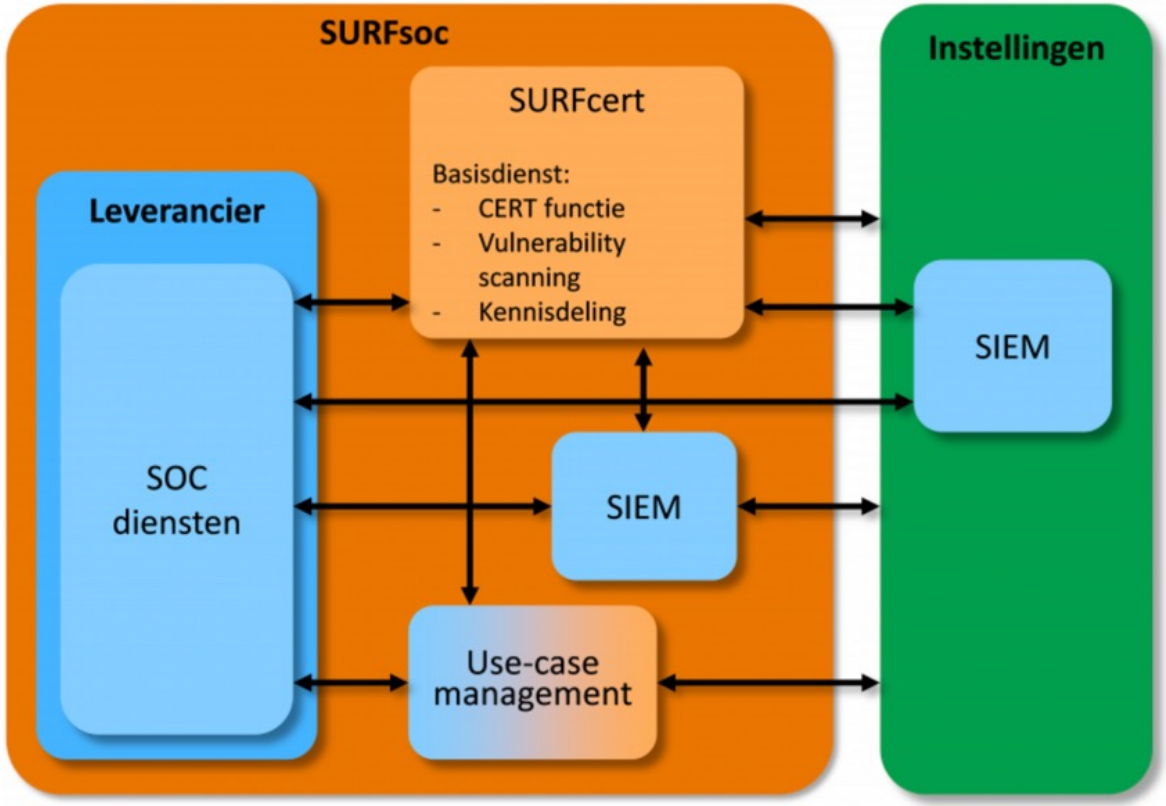
- Alle vragen/issues rondom IT-security/cybersecurity
- Jeffeny & Mick

Heb je een suggestie of feedback? Laat het ons weten!

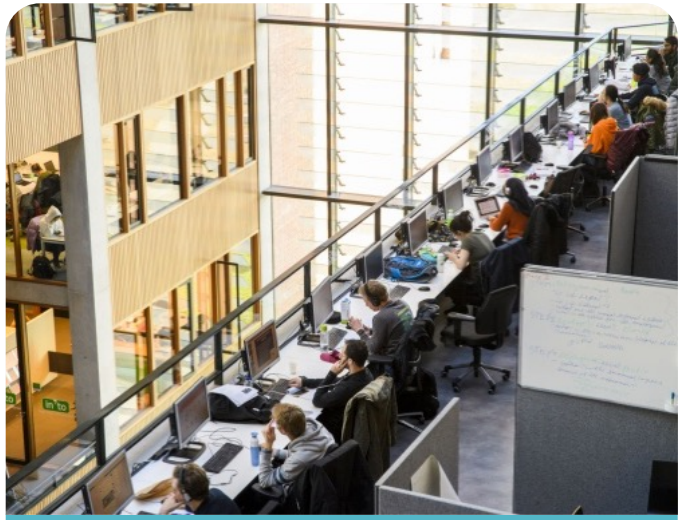
mbo digitaal

Extra ondersteuning SURFsoc

- Vergoeding aansluitkosten SURFsoc
- Implementatie ondersteuning
- SDM gesprekken
- Vragen & advies
- Hands-off SOC
- Microsoft Sentinel onderzoek

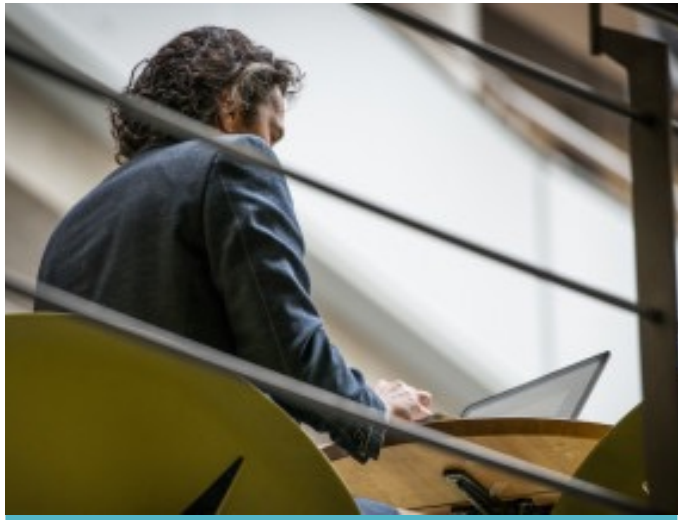


Diensten voor Security Techniek



Cyberweerbaarheids testen

Test de beveiliging van je systemen.



SURFcert

24/7 ondersteuning bij beveiligingsincidenten.

SURFsoc

Samen beveiliging verhogen met monitoring, vulnerability scanning en informatie.

Diensten voor Security Techniek

EduVPN

Overal veilig internetten en veilig toegang tot eigen infrastructuur.

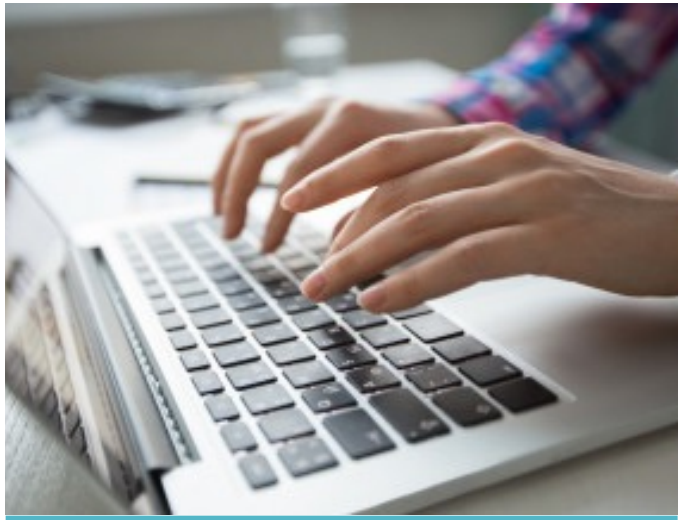
SURFmailfilter

Filter spam, phishing en virussen, behoud controle en waarborg aflevering

SURFcertificaten

Versleutel de verbindingen naar (onder andere) je webservers.

Diensten voor Security Techniek

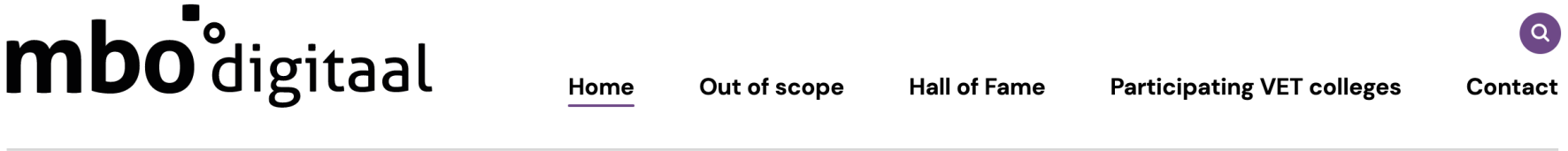


SURFdomeinen
Domeinregistratie en DNS-beheer voor de onderwijssector

SURFsecureID
Beveilig toegang tot diensten met 2-factorauthenticatie

mbo digitaal

Coordinated Vulnerability Disclosure



Responsible Vulnerability Disclosure

This page is part of **MBO Digitaal** and is a service for the participating secondary Vocational Education and Training (VET) in the Netherlands.

Despite our security efforts, a weakness could occur in one of the colleges systems. If you have found a weakness, we would like to hear about it so that we can take appropriate measures as quickly as possible. We are keen to cooperate with you to protect users and systems better. The Responsible disclosure procedure describes how to report a detected vulnerability. This statement applies to the **VET colleges** that participate in this.

A responsible disclosure can be reported using the email address **cvd@surfcert.nl**. In case of sensitive information, encrypt your findings with **our PGP key** to prevent the information from falling into the wrong hands. **SURFcert** is the sectoral CERT for the National Research and Educational Networks (NREN) in the Netherlands. Reports must be clear and contain the steps necessary to reproduce the vulnerability. The steps need to be in the body of the message. This Responsible Disclosure Policy is not an invitation to actively scan our network or our systems for weaknesses. We actively monitor our networks. Therefore, we are likely to pick up your scan, which our Computer Emergency Response Team (CERT) will investigate, and which will possibly lead to unnecessary costs.

mbo digitaal

Opzetten first responder training

- Eendaagse training
- De basis
- Praktisch

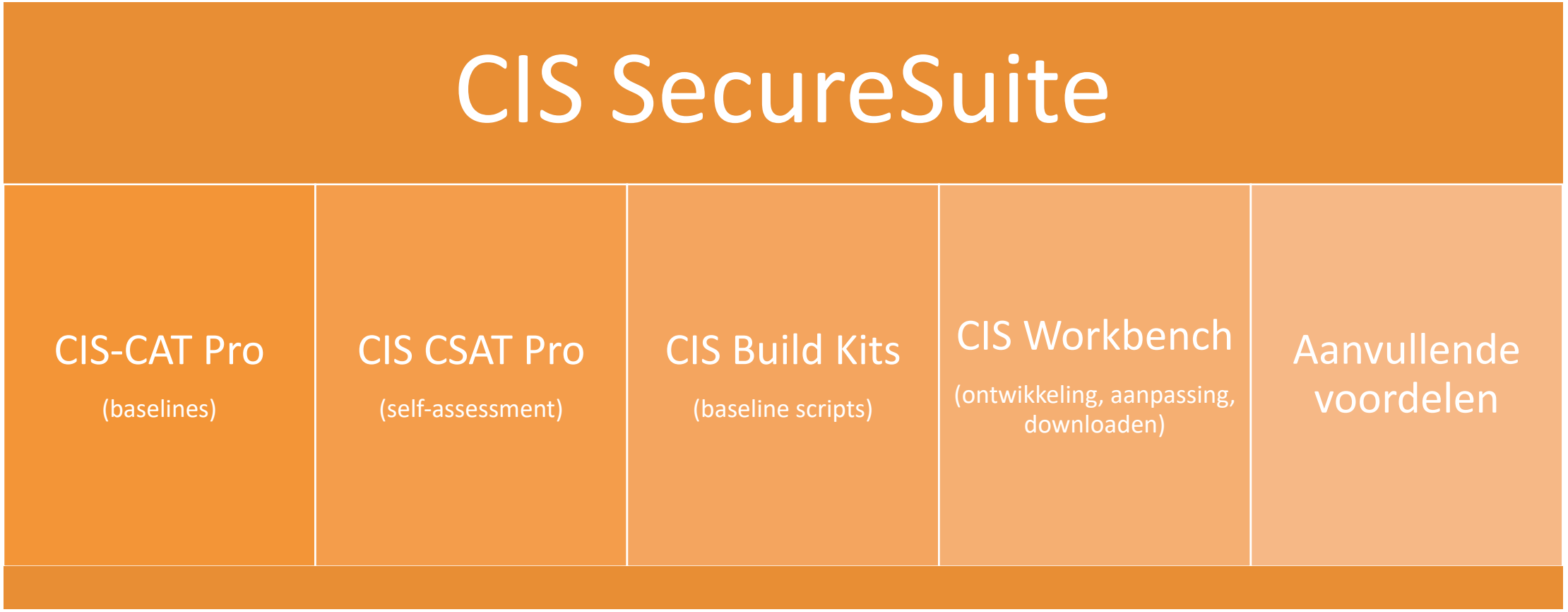
mbo digitaal

Handreikingen

- Transport Layer Security (TLS)
- Dataclassificatie Microsoft 365
- Top 10 misconfiguraties in netwerken
- AI chatbots

mbo digitaal

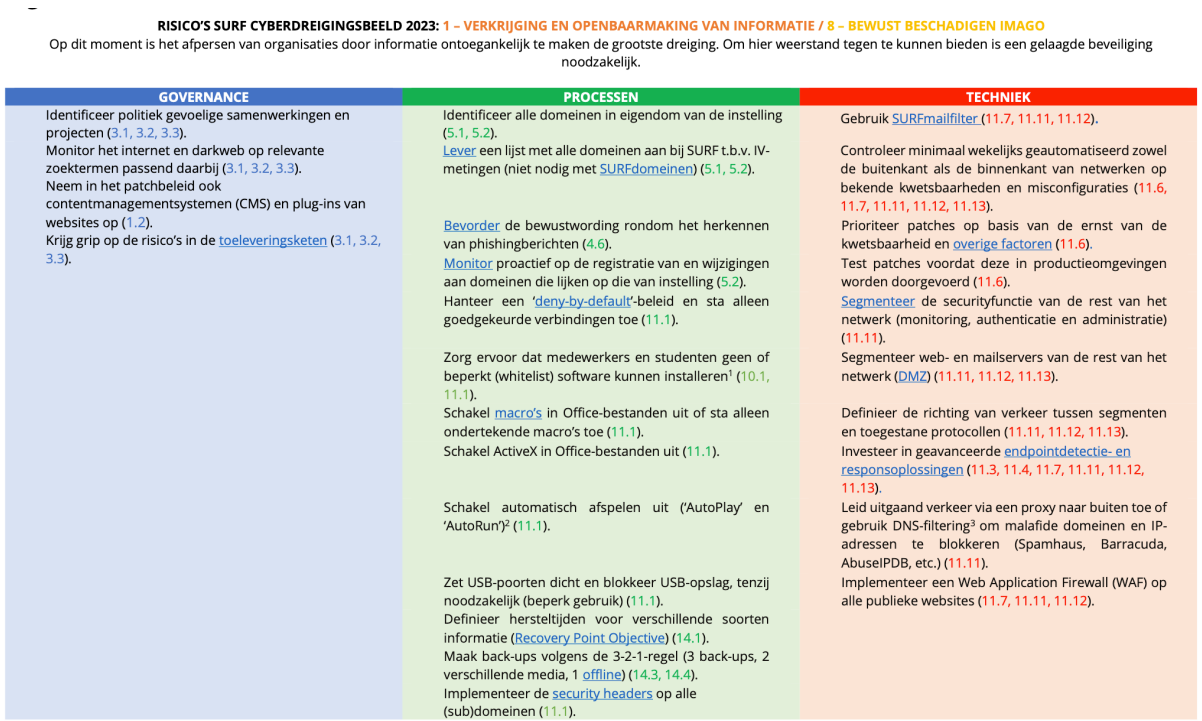
CIS SecureSuite Membership



mbo digitaal

Cyberdreigingsbeeld

- Praktische vertaling
- Visualisatie en doorklikbaar
- Werkgroep
- Hogere frequentie updates



RISICO'S SURF CYBERDREIGINGSBEELD 2023: 1 – VERKRIJGING EN OPENBAARMAKING VAN INFORMATIE / 8 – BEWUST BESCHADIGEN IMAGO

Op dit moment is het afpersen van organisaties door informatie ontoegankelijk te maken de grootste dreiging. Om hier weerstand tegen te kunnen bieden is een gelaagde beveiliging noodzakelijk.

GOVERNANCE	PROCESSEN	TECHNIEK
Identificeer politiek gevoelige samenwerkingen en projecten (3.1, 3.2, 3.3). Monitor het internet en darkweb op relevante zoektermen passend daarbij (3.1, 3.2, 3.3). Neem in het patchbeleid ook contentmanagementsystemen (CMS) en plug-ins van websites op (1.2). Krijg grip op de risico's in de toeleveringsketen (3.1, 3.2, 3.3).	Identificeer alle domeinen in eigendom van de instelling (5.1, 5.2). Lever een lijst met alle domeinen aan bij SURF t.b.v. IV-metingen (niet nodig met SURFdomeinen) (5.1, 5.2). Bevorder de bewustwording rondom het herkennen van phishingberichten (4.6). Monitor proactief op de registratie van en wijzigingen aan domeinen die lijken op die van instelling (5.2). Hanteer een 'deny-by-default'-beleid en sta alleen goedgekeurde verbindingen toe (11.1). Zorg ervoor dat medewerkers en studenten geen of beperkt (whitelist) software kunnen installeren[1] (10.1, 11.1). Schakel macro's in Office-bestanden uit of sta alleen ondertekende macro's toe (11.1). Schakel ActiveX in Office-bestanden uit (11.1). Schakel automatisch afspelen uit ('AutoPlay' en 'AutoRun')[2] (11.1). Zet USB-poorten dicht en blokkeer USB-opslag, tenzij noodzakelijk (beperk gebruik) (11.1). Definieer hersteltijden voor verschillende soorten informatie (Recovery Point Objective) (14.1). Maak back-ups volgens de 3-2-1-regel (3 back-ups, 2 verschillende media, 1 offline) (14.3, 14.4). Implementeer de security headers op alle (sub)domeinen (11.1).	Gebruik SURFmailfilter (11.7, 11.11, 11.12). Controleer minimaal wekelijks geautomatiseerd zowel de buitenkant als de binnenkant van netwerken op bekende kwetsbaarheden en misconfiguraties (11.6, 11.7, 11.11, 11.12, 11.13). Prioriteer patches op basis van de ernst van de kwetsbaarheid en overige factoren (11.6). Test patches voordat deze in productieomgevingen worden doorgevoerd (11.6). Segmenteer de securityfunctie van de rest van het netwerk (monitoring, authenticatie en administratie) (11.11). Segmenteer web- en mailservers van de rest van het netwerk (DMZ) (11.11, 11.12, 11.13). Definieer de richting van verkeer tussen segmenten en toegestane protocollen (11.11, 11.12, 11.13). Investeer in geavanceerde endpointdetectie- en responsoplossingen (11.3, 11.4, 11.7, 11.11, 11.12, 11.13). Leid uitgaand verkeer via een proxy naar buiten toe of gebruik DNS-filtering[3] om malafide domeinen en IP-adressen te blokkeren (Spamhaus, Barracuda, AbuseIPDB, etc.) (11.11). Implementeer een Web Application Firewall (WAF) op alle publieke websites (11.7, 11.11, 11.12).

mbo digitaal

Vragen?

m.deben@mbodigitaal.nl
jeffeny.hoogervorst@surf.nl