Opleiden, trainen & oefenen

Security & Privacy

Februari 2026

Inhoud

Opeiden en Trainen

Thema Cybersecurity Incidentmanagement

- TRANSITS I, TRANSITS Extended, TRANSITS Essentials

Thema Governance, Risk & Compliance

- Toetsingskader Informatiebeveiliging, Toetsingskader Privacy , IT Risico beoordeling

Thema Awareness

- Training Awareness proces, Training Cybersecurity voor bestuurders

Oefenen

Crisis

- Crisisoefening OZON/NOZON

Hacken

- Hackwedstrijd HALON
- SURFcert Capture the Flag

Opleiden, trainen, oefenen

Binnen onze sector bieden we diverse bijeenkomsten om kennis op te op te doen, vaardigheden aan te leren en momenten om deze te oefenen.

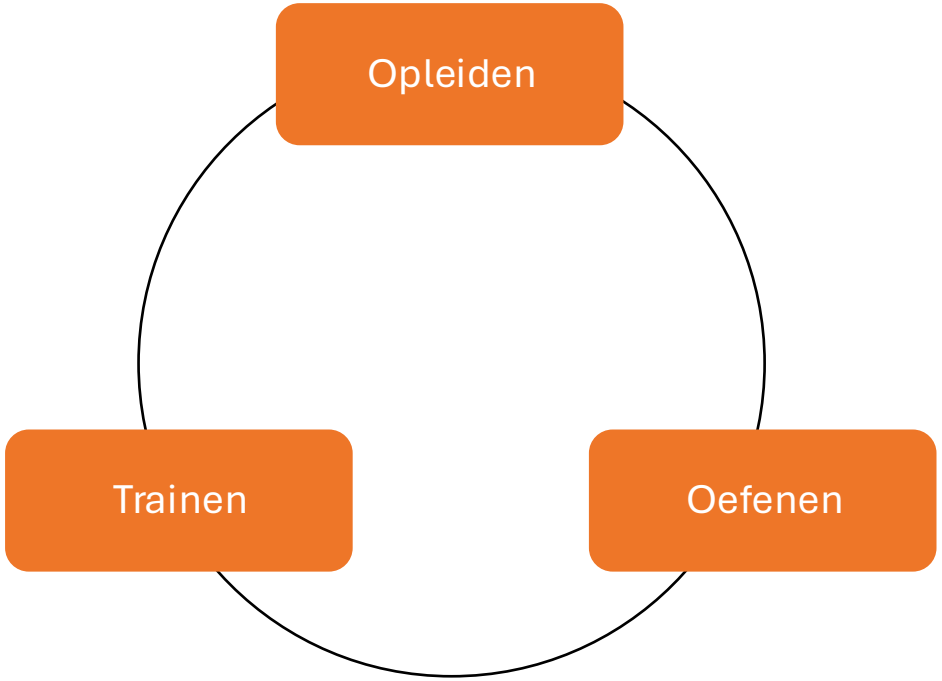
Deze cyclus borgt dat het kennisniveau bij de instellingen actueel blijft in een continue veranderend dreigingslandschap. Het centraal faciliteren van opleiden, trainen en oefenen bevordert samenwerking en kennisdeling.

Opleiden en trainen

Door het natuurlijk verloop van medewerkers kan kennis en ervaring verdwijnen.
Veel instellingen laten nieuwe medewerkers relevante security en privacy trainingen bij SURF doen. Zo krijgen zij snel inzicht in hoe zaken in de sector geregeld zijn, en krijgen zij actuele kennis over dreigingen.

Oefenen

Om geleerde vaardigheden te behouden en te testen hoe weerbaar een instelling is, zijn er diverse oefeningen waar instellingen of medewerkers van instellingen aan deel kunnen nemen. Deze oefeningen worden als zeer waardevol ervaren door de deelnemers.



Opleiden en trainen

Ons aanbod

SURF biedt diverse opleidingen en trainingen aan op het gebied van security en privacy in onderwijs en onderzoek. Deze organiseren we samen met de Nederlandse onderwijs- en onderzoeksinstellingen.

Voor wie?
Voor medewerkers die werken een bij SURF aangesloten instelling.

Waarom bij SURF?

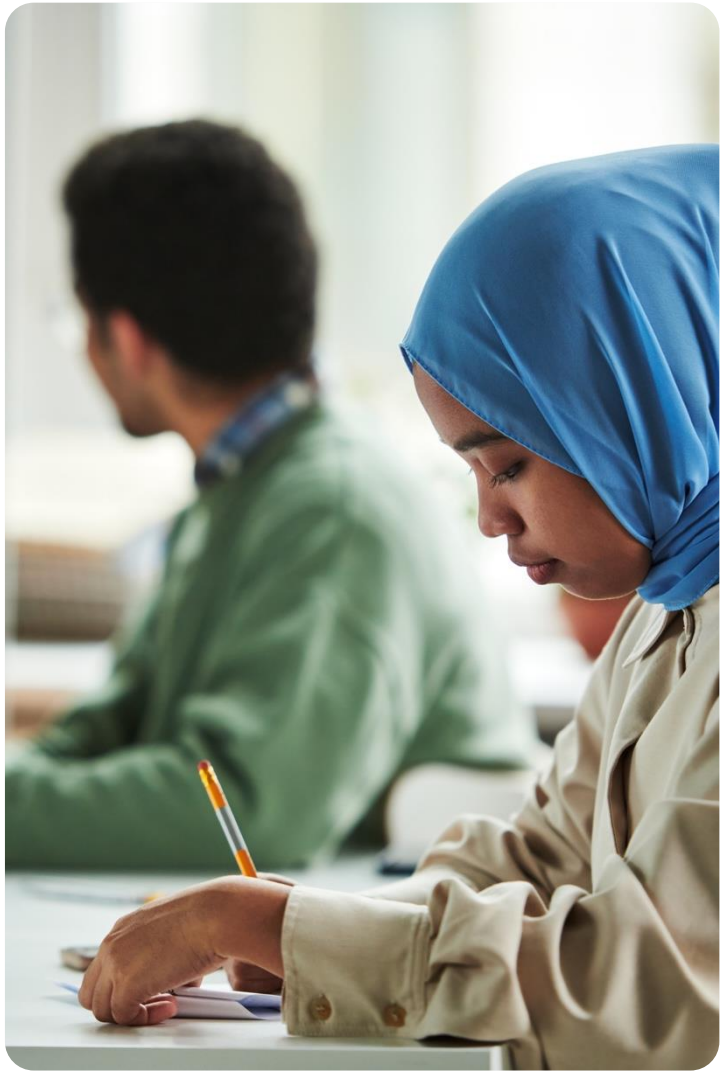
Uitwisseling van kennis en ervaring
Onze oplieidingen en trainingen zorgen voor nationale krachtenbundeling, het uitwisselen van kennis en ervaring in onderwijs en onderzoek.

Experts uit onderwijs en onderzoek
Experts binnen het onderwijs en onderzoek delen hun kennis en ervaringen over producten, diensten en projectresultaten.

Groot aanbod
Bij SURF kun je terecht voor diverse oplreidingen en trainingen op verschillende thema's binnen security en privacy.

Aantrekkelijk geprijsd
Aan het volgen van een SURF-training zijn kosten verbonden. We bieden onze trainingen aan tegen kostprijs en daarom aantrekkelijk geprijsd. We zijn geen commerciële organisatie.

Meer informatie en inschrijven
Wil je meer informatie over of je inschrijven voor een training? Kijk op SURF.nl



Overzicht trainingen per thema

SURF organiseert trainingen op verschillende inhoudelijke thema's. Meer over de thema's en de trainingen lees je de volgende pagina's.

Incidentmanagement

Cybersecurity incident management is het geheel van processen, procedures en maatregelen waarmee een organisatie cybersecurity-incidenten detecteert, analyseert, beheerst, oplost en ervan leert, om schade te beperken en herhaling te voorkomen.

- TRANSITS I
- TRANSITS Extended
- TRANSITS Essentials

Governance, Risk & Compliance

Governance, Risk & Compliance (GRC) is een geïntegreerde aanpak waarmee een organisatie haar besturing (governance), risicobeheersing (risk management) en naleving van wet- en regelgeving (compliance) op elkaar afstemt om doelstellingen verantwoord en gecontroleerd te behalen.

- Masterclass Toetsingskader Informatiebeveiliging
- Masterclass Toetsingskader Privacy
- Training IT risicobeoordeling

Awareness

Cybersecurity awareness is het bewustzijn en begrip van medewerkers (of gebruikers) over digitale dreigingen, veilige gedragingen en hun eigen rol in het beschermen van informatie en systemen.

- Training awareness proces*
- Training cybersecurity voor bestuurders*

*beschikbaar eind 2026

Cybersecurity incidentmanagement

In een wereld waarin digitale dreigingen steeds geavanceerder worden, is het niet langer de vraag óf een instelling te maken krijgt met een cybersecurity incident, maar wanneer. Een datalek, ransomware-aanval of phishing-campagne kan binnen enkele uren leiden tot het verstoren van onderwijs en onderzoek, reputatieschade en aanzienlijke financiële verliezen. Daarom organiseert SURF trainingen over hoe je deze incidenten managed.

TRANSITS I

In deze training leer je hoe je een Computer Security Incident Team (CSIRT) opzet en runt. Je leert meer over organisatie en oprationele aspecten, technische achtergrond, juridische aspecten en regelgeving rondom cybersecurity incidenten.

Voorkennis is niet noodzakelijk, maar een basiskennis van internettechnologie en beveiliging kan de leerervaring ten goede komen.

Voor wie? Security Officers, Security managers, (potentiële) leden van CSIRT,

3 dagen

Certificaat van deelname

TRANSITS Extended

In deze training leer je meer over een tal van onderwerpen rondom netwerkbeveiliging, zoals netflowanalyse, forensisch onderzoek en communicatievaardigheden.

Deze training gaat vooral in op technieken voor netwerkmonitoring en forensische analyse. Daarnaast reiken we een aantal tools aan om de (menselijke) communicatie te verbeteren

Voorkennis is niet noodzakelijk, maar enige basiskennis van Linux en command line kan je tijdens de training goed van pas komen.

Voor wie? Meer ervaren leden van CSIRTS

3 dagen

Certificaat van deelname

TRANSITS Essentials

Tijdens deze training leer je hoe cyberaanvallen werken, denk je samen na over veilige werkprocessen en ontdek je hoe je verschillende soorten bedreigingen kunt identificeren en gevoelige gegevens kunt beschermen.

Voorkennis is niet noodzakelijk.

Voor wie? Servicedesk medewerkers

1 dag

Kijk voor het actuele aanbod in de agenda op SURF.nl

25 February, 2026 | Published under cc-by licence

Governance, Risk & Compliance

Instellingen werken met steeds grotere hoeveelheden gevoelige data, van persoonsgegeven van klanten tot vertrouwelijke bedrijfsinformatie. Tegelijkertijd worden de wet- en regelgeving strenger en de verwachtingen van klanten en stakeholders hoger. Privacy en security toetsingskaders bieden organisaties een gestructureerde aanpak om deze uitdagingen het hoofd te bieden.

Effectief IT-risicomanagement identificeert kwetsbaarheden in systemen voordat kwaadwillenden ze kunnen misbruiken, en zorgt voor een gestructureerde aanpak van beveiligingsmaatregelen. IT-risicomanagement maakt organisaties weerbaarder, veiliger en succesvoller.

Masterclass Toetsingskader Informatiebeveiliging

Digitale weerbaarheid vraagt om actuele kennis en praktische vaardigheden. In de SURFaudit Masterclasses kunnen instellingen zich verdiepen in de thema's rond informatiebeveiliging, risicomanagement en compliance. Tijdens deze sessies delen experts hun inzichten, best practices en concrete handvatten, die direct toepasbaar zijn in de eigen instelling.

Deze training is onderdeel van de SURFaudit-dienstverlening.

Doelgroep: CISO's, security officers, auditors en andere professionals die verantwoordelijk zijn voor informatieveiligheid binnen hun organisatie

2 dagen

Masterclass Toetsingskader Privacy

Het Toetsingskader Privacy helpt je de juiste maatregelen te implementeren om persoonsgegevens adequaat te beschermen. Met het toetsingskader kun je alle zaken rondom privacy binnen de organisatie effectief inregelen, onderhouden, meten en evalueren.

Het Toetsingskader Privacy is ontwikkeld voor en door instellingen.

Doelgroep: Privacy Officers, CPO's, FG's en andere professionals die verantwoordelijk zijn voor privacy binnen hun organisatie

1 dag

Training IT Risicobeoordeling

In deze training maak je kennis met risicomanagement voor informatiebeveiliging en leer je over termen zoals enterprise risk management, ISO 31000 & ISO 27005, risicoleiderschap en governance. Je gaat ook praktisch aan de slag met een risicoregister en risicoscenario's.

Doelgroep: Voor iedereen die aan de slag gaat met risicobeheer voor informatiebeveiliging.

1 dag

Kijk voor het actuele aanbod in de agenda op SURF.nl

25 February, 2026 | Published under cc-by licence

Awareness

Mensen zijn steeds vaker het doelwit van cybercriminelen. Medewerkers en studenten zijn een belangrijk onderdeel van een digitaal weerbare instelling. Deze trainingen zijn gericht op specifieke doelgroepen: medewerkers die zich bezig houden met het verhogen van awareness bij een instelling, en bestuurders.

Deze trainingen zijn vanaf eind 2026 beschikbaar.

Training Awareness Proces

In deze training maak je kennis met de verschillende disciplines die nodig zijn voor effectieve awareness interventies, ontdek je hoe je met een procesaanpak stakeholders kunt overtuigen en hoe je dit binnen je instelling inricht. Na het volgen van deze training kun je de opgedane kennis meteen toepassen binnen je instelling.

Er is aanvullend awareness materiaal beschikbaar in de Cybersave Yourself Toolkit en templates en tools op SEC.SURF.nl

Voor wie? Medewerkers die zich bezighouden met security en privacy rawareness binnen instellingen.

2 dagen

Training cybersecurity voor bestuurders

Effectieve cyberveiligheid begint in de bestuurskamer. Cyberveiligheid raakt de continuïteit, reputatie en maatschappelijke functie van de instelling, en de sector als geheel.

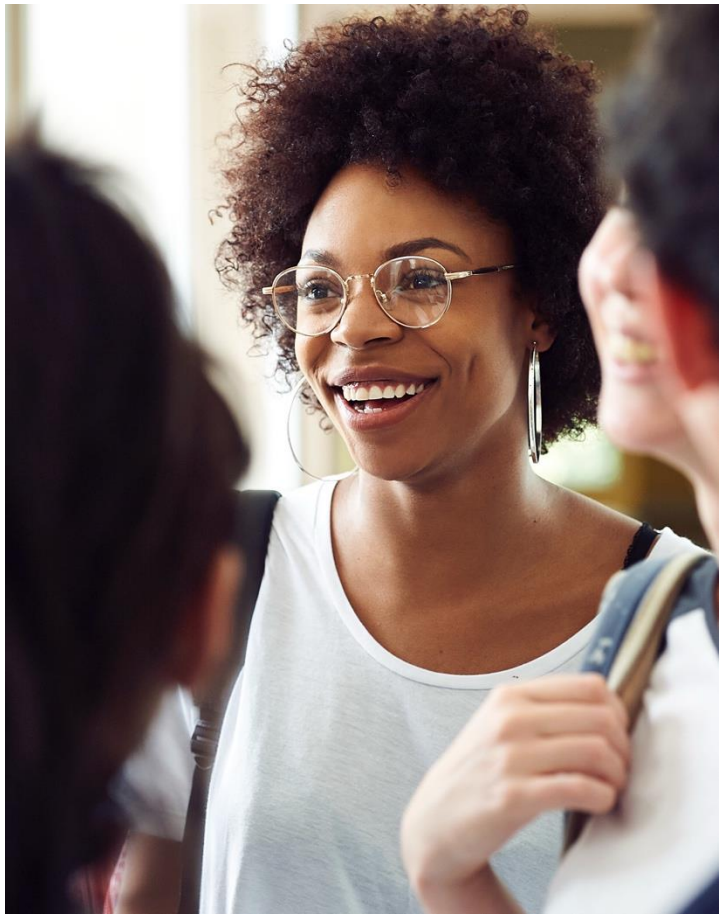
De Cyberbeveiligingswet (Cbw) verplicht bestuurders van instellingen die beoogd zijn aangewezen onder deze wet een training te volgen. Deze training omvat alle onderdelen die in de Cbw genoemd worden.

Deze training is toegankelijk voor alle leden van SURF: ook voor instellingen die niet vallen onder de Cbw.

Voor wie? Bestuurders van onderwijs- en onderzoeksinstellingen

NNTB

Kijk voor het actuele aanbod in de agenda op SURF.nl



25 February, 2026 | Published under cc-by licence

Oefenen

Ons aanbod

SURF biedt diverse oefeningen aan op het gebied van security en privacy in onderwijs en onderzoek. Ook deze organiseren we samen met de Nederlandse onderwijs- en onderzoeksinstellingen.

Een oefening:

- Is gericht op het oefenen van praktische vaardigheden
- Duur: ongeveer 1 dag (exclusief voorbereidingstijd)

Voor wie?
Voor medewerkers en studenten die verbonden zijn aan een bij SURF aangesloten instelling.

In dit overzicht vind je een omschrijving, de doelgroep en de duur per oefening.

Waarom meedoen aan een oefening bij SURF?

Uitwisseling van kennis en ervaring

Onze oefeningen bevorderen het uitwisselen van kennis en ervaring in onderwijs en onderzoek.

Inzicht in weerbaarheid

Een incident of crisis kan iedereen overkomen: door te oefenen met dergelijke situaties krijgt een instelling meer inzicht in de weerbaarheid.

Instellingsoverstijgend

Aan oefeningen bij SURF doen meestal meerdere instellingen mee. Zo krijg je meer inzicht in de dwarsverbanden tussen instellingen en leren instellingen van elkaar.

Oefening opmaat

De oefeningen zijn gemaakt op basis van realistische scenario's voor de sector onderwijs en onderzoek.

Meer informatie en inschrijven
Wil je meer informatie over of je inschrijven voor een oefening? Kijk op SURF.nl.

Crisisoefening

Opleiden en trainen verhogen de kennis en vaardigheden. Om deze kennis en vaardigheden te behouden, is het belangrijk om deze regelmatig te oefenen. Een oefening stelt instellingen in staat om hun cyberweerbaarheid te testen en hun vermogen om de impact te beperken wanneer er een incident of crisis is.

Niet alleen binnen de instelling, maar ook wanneer er sprake is van een crisis die de hele sector raakt.

OZON

OZON is dé sectorbrede cybercrisisoefening voor onderwijs en onderzoek die elke twee jaar plaatsvindt. Tijdens OZON oefen je hoe je moet reageren bij een cybercrisis en kom je erachter of je als instelling al goed bent voorbereid op een cybercrisis. In maart 2027 is de eerstvolgende editie.

In het jaar dat OZON niet plaatsvindt, kun je meedoen aan NOZON, een tabletop-cybercrisisoefening.

Aanmelding voor deze oefening is per instelling en niet op individueel niveau.

Voor wie? Instellingen aangesloten bij SURF.

1 dag (exclusief voorbereidingstijd)

NOZON

In het jaar dat OZON niet plaatsvindt, kun je meedoen aan NOZON, een tabletop-cybercrisisoefening.

Met behulp van de NOZON-handleiding kun je tussentijds ook zelf een tabletop-oefening organiseren.

Aanmelding voor deze oefening is per instelling en niet op individueel niveau.

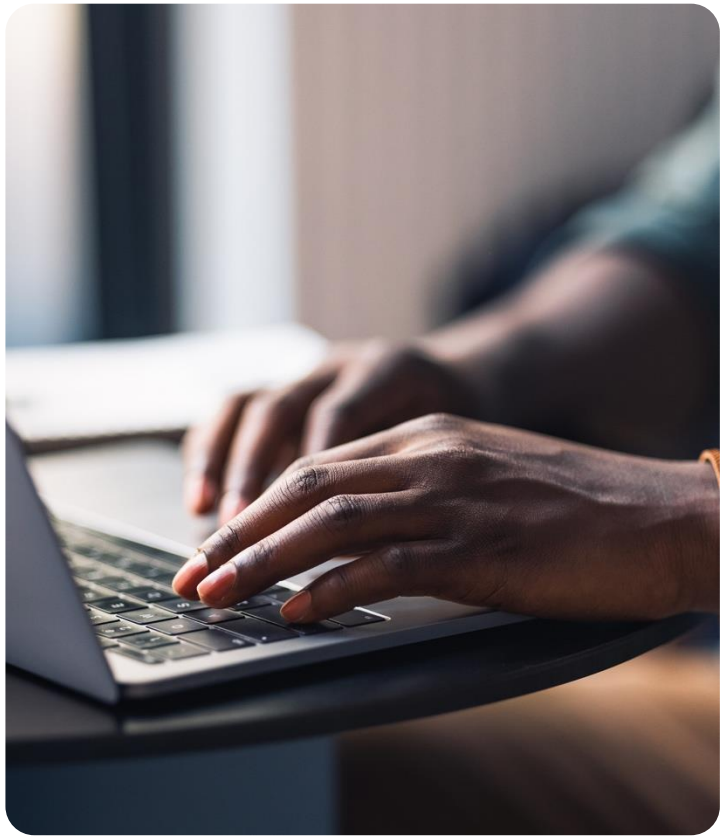
Voor wie? Instellingen aangesloten bij SURF.

halve dag (exclusief voorbereidingstijd)

Kijk voor meer informatie op SURF.nl

Hackoefeningen

Het ontwikkelen en behouden van kennis over hacken en hacktechnieken is een belangrijke schakel in de verdediging van onderwijs- en onderzoeksinstellingen. Voor medewerkers en studenten van instellingen organiseert SURF hackoefeningen. Aan deze oefeningen kun je als individu inschrijven. Bij deze evenementen zijn er opdrachten en doelwitten waar deelnemers mee kunnen oefenen.



HALON

HALON (Hack Al het Onderwijs in Nederland) is een hackevenement voor het onderwijs, door het onderwijs en onderzoek.

Met een team van maximaal drie personen ga je op zoek naar kwetsbaarheden in de open IP-reeksen en domeinnamen van diverse Nederlandse onderwijs- en onderzoeksinstellingen. Door het vinden van kwetsbaarheden draag je bij aan de cyberweerbaarheid van deze instellingen en de sector als geheel.

Aanmelden doe je op individueel niveau.

Voor wie? Studenten en medewerkers van universiteiten, hogescholen en mbo-instellingen.

1 dag

SURFcert Capture the Flag

De SURFcert (CTF) is een hack-event waarin je puzzels en technische security-uitdagingen oplost. Denk aan Web Hacking, Forensics, Cryptografie, Decoding, Binary en meer. Het doel van elke opdracht is het vinden van de verborgen 'vlag'. Per vlag zijn punten te verdienen. Het team dat aan het einde van de speeltijd de meeste punten heeft, wint.

Aanmelden doe je op individueel niveau, en je kunt je als team aanmelden.

Voor wie? Medewerkers en studenten van bij SURF aangesloten instellingen en collega-CERT's

1 dag

Kijk voor meer informatie op SURF.nl

Security & Privacy Trainingen

	Training	Inhoud	Duur
Incident Management	TRANSITS I	Leer hoe je een CSIRT opzet om security incidenten af te kunnen handelen.	3 dagen
	TRANSITS Extended	Leer meer over netwerkbeveiliging zoalsnetflowanalyse, forensisch onderzoek en communicatie technieken.	3 dagen
	TRANSITS Essentials	Leer hoe cyberaanvallen werken en ontdek je hoe je verschillende soorten bedreigingen kunt identificeren en gevoelige gegevens kunt beschermen.	1 dag
Governance, Risk, Compliance	Masterclass Toetsingskader IB	Leer het Toetsingskader Informatiebeveieliging toepassen zodat je zelf assessments kunt uitvoeren.	2 dagen
	Masterclass Privacy Toetsingskader	Leer het Toetsingskader privacy AVG/P toepassen, zodat je het zelf kunt toepassen in audits en zels assesments.	1 dag
	Training IT Risico Beoordeling	Maak kennis met risicomanagement voor informatiebeveiliging en leer meer over risicoleiderschap en governance.	1 dag
Awareness	Training Awareness Proces*	Maak je kennis met de verschillende disciplines die nodig zijn voor effectieve awareness interventies en leer hoe je awareness binnen je instelling inricht.	2 dagen
	Training Cybersecurity voor Bestuurders*	Over de rol van de bestuurder en cybersecurity en de strategische aanpak van cybersecurity	NNTB

*beschikbaar eind 2026

Oefeningen

	Oefening	Inhoud	Duur
Crisisoefening	OZON	Tijdens OZON oefen je hoe je moet reageren bij een cybercrisis en kom je erachter of je als instelling al goed bent voorbereid op een cybercrisis.	1 dag
	NOZON	Een tabletop-cybercrisisoefening die je bij je instelling kun tuitvoeren. Voor deze oefening wordt centraal een scenario voorbereid.	1/2 dag
Hackoefening	HALON	Een hack oefening op doelwitten bij onderwijs- en onderzoeksinstellingen. Met een team van maximaal drie personen ga je op zoek naar kwetsbaarheden in de open IP-reeksen en domeinnamen van diverse Nederlandse onderwijs- en onderzoeksinstellingen.	1 dag
	SURFcert Capture the Flag	Een hack-event waarin je puzzels en technische security-uitdagingen oplost. Denk aan Web Hacking, Forensics, Cryptografie, Decoding, Binary en meer. Het doel van elke opdracht is het vinden van de verborgen 'vlag'.	1 dag