

**SURFcert**

# Dienstbeschrijving

**Document**

Dienstbeschrijving SURFcert

**Doelgroep**

Bij SURF aangesloten onderwijs- en onderzoeksinstituten

**Versie**

0.9, oktober 2026

**Contact SURFcert**

cert@surfcert.nl, 030 23 05 112

# 1. Wat is SURFcert

---

SURFcert is het Computer Security Incident Response Team (CSIRT) voor de Nederlandse onderwijs- en onderzoekssector. SURFcert bestaat al meer dan 30 jaar en is opgebouwd uit securityspecialisten van SURF en van aangesloten instellingen, die gezamenlijk zorgen voor een sterke, sectorbrede aanpak van cyberdreigingen.

SURFcert biedt 24 uur per dag, 7 dagen per week ondersteuning en advies bij beveiligingsincidenten. Daarnaast spoort SURFcert dreigingen en kwetsbaarheden proactief op, deelt deze met getroffen instellingen, en coördineert de aanpak zodra meerdere instellingen tegelijk worden geraakt. Tot slot deelt SURFcert kennis en helpt instellingen hun eigen incidentresponscapaciteit te versterken.

Heb je een vraag of vermoed je een beveiligingsincident binnen je organisatie? Neem contact op met SURFcert via 030 23 05 112 (24/7 bereikbaar) of [cert@surfcert.nl](mailto:cert@surfcert.nl). Voor vertrouwelijke berichten gebruikt SURFcert een PGP-sleutel, te vinden via de [OpenPGP-keyserver](#).

## 1.1. Voor wie is SURFcert

SURFcert levert diensten aan alle op het SURF-netwerk aangesloten organisaties. In beginsel wordt aan de hele doelgroep hetzelfde dienstenpakket geleverd. Daarnaast treedt SURFcert op als beoogd sectoraal CSIRT onder de [Cyberbeveiligingswet](#) (Cbw) voor alle bekostigde hogescholen en universiteiten in Nederland (ook de instellingen die nog geen SURF-netwerkaansluiting hebben).

Er worden geen additionele kosten in rekening gebracht voor diensten van SURFcert.

## 1.2. Over deze dienstbeschrijving

Dit document beschrijft de dienstverlening van SURFcert: de kerntaken die SURFcert uitvoert, de rol die SURFcert vervult voor de sector als geheel, en de verdeling van verantwoordelijkheden tussen SURFcert en de aangesloten instellingen. Het is een levend document, dat door SURFcert bijgewerkt wordt als de dienstverlening zich ontwikkelt.

# 2. Kerntaken van SURFcert

SURFcert voert de volgende kerntaken uit voor de bij SURF aangesloten instellingen:

## 2.1 Ondersteuning en advies bij incidenten

SURFcert is 24/7 telefonisch bereikbaar voor advies en ondersteuning bij een (vermoed) cyberincident: van de eerste beoordeling tot het indammen van de dreiging. SURFcert adviseert daarbij doorgaans op afstand, maar sluit bij grote incidenten ook aan bij het incidentteam van de instelling.

### 2.1.1 Triage en identificatie

Bij een melding beoordeelt SURFcert eerst wat er aan de hand is en hoe ernstig de situatie is (triage). Vervolgens ondersteunt SURFcert bij het identificeren van de oorzaak: SURFcert helpt het probleem te doorgronden, bekijkt de historie van netwerkverkeer en voert zo nodig forensische analyse uit op systemen of malware om de werkwijze van een aanvalleur te achterhalen. De inzichten hieruit, zoals

gevonden indicatoren (IoC's) of aanvalspatronen, gebruikt SURFcert ook om te bepalen of andere instellingen hetzelfde risico lopen en hen te waarschuwen (zie 2.2.2).

- Triage: inschatting en beoordeling van een gemeld incident.
- Ondersteuning bij identificatie van de oorzaak van een incident.
- Forensische analyse van systemen of malware.

### 2.1.2 Containment en DDoS-bescherming

Als ingrijpen nodig is om verdere schade van een incident te beperken, geeft SURFcert advies over de te nemen maatregelen (containment). Soms grijpt SURFcert ook zelf in. SURFcert kan bijvoorbeeld netwerkmaatregelen activeren, zoals een blokkade of filtering, of een IP-adres laten afsluiten om verdere schade te voorkomen.

Een specifieke, veelvoorkomende vorm hiervan is bescherming tegen DDoS-aanvallen. Met Netflow-analyse van verkeersgegevens van en naar de instelling detecteert SURFcert een netwerkaanval vroegtijdig. Om de impact van aanvallen op voorhand zo veel mogelijk te beperken, biedt SURFcert bovendien twee anti-DDoS-middelen aan als doorlopende, altijd actieve beschermingsvoorziening - niet alleen als reactie ná een gemeld incident.

Containment stopt de acute dreiging, maar is niet hetzelfde als het incident volledig oplossen. Voor eradication (het definitief verwijderen van de oorzaak, zoals malware of een kwetsbaarheid) en recovery (herstel van de normale dienstverlening) is de instelling zelf verantwoordelijk, eventueel met een externe partij - zie paragraaf 4.

- Netwerkmaatregelen, zoals blokkades of (DDoS)filtering, om een acute dreiging in te dammen.
- DDoS-filter
- DDoS-automitigatie

### 2.1.3 Advies bij meldplicht en aangifte

Heeft een incident mogelijk gevolgen die gemeld moeten worden, bijvoorbeeld vanwege de [meldplicht](#) onder de Cyberbeveiligingswet of in de vorm van een aangifte bij de politie, dan adviseert en begeleidt SURFcert de instelling hierbij.

Advies en begeleiding bij meldplicht en aangifte.

## 2.2 Threat intelligence en crisiscoördinatie

Waar paragraaf 2.1 gaat over het technisch afhandelen van één incident bij één instelling, gaat deze kerntaak over het proactieve werk: dreigingen en kwetsbaarheden opsporen, informatie daarover delen, en de coördinatie voeren zodra een dreiging of crisis meerdere instellingen tegelijk raakt.

### 2.2.1 Kwetsbaarheden opsporen

SURFcert detecteert kwetsbaarheden in het instellingsnetwerk die van buiten de instelling waarneembaar zijn, bijvoorbeeld applicaties die onbedoeld bereikbaar zijn, misconfiguraties, kwetsbare softwareversies, of meldingen die SURFcert van partners ontvangt. SURFcert meldt deze kwetsbaarheden aan de instelling voor opvolging (zie 2.2.3).

- Structureel en periodiek scannen van het instellingsnetwerk en bij SURFcert bekende assets vanaf de buitenkant, en het melden van kwetsbare systemen.
- Inzicht in het aanvalsoppervlak van de instelling via het Netwerk Dashboard.
- Op verzoek scannen van het instellingsnetwerk van buitenaf (in ontwikkeling).

### 2.2.2 Threat intelligence delen

SURFcert verzamelt dreigingsinformatie (threat intelligence) uit verschillende bronnen en doet ook zelf onderzoek. Daarnaast volgt SURFcert actuele, relevante kwetsbaarheden in software en systemen. Om deze informatie te delen, gebruikt SURFcert [MISP](#): een opensourceplatform voor het verzamelen en uitwisselen van informatie over cyberdreigingen. Via de [MISP-omgeving van SURFcert](#) kunnen aangesloten instellingen dreigingsinformatie raadplegen. Ook kunnen zij hun eigen systemen aansluiten op een door SURFcert samengestelde feed met dreigingsinformatie. Zo kunnen zij dreigingen sneller herkennen en passende beveiligingsmaatregelen nemen.

SURFcert combineert dreigingsinformatie ook met netwerkverkeersgegevens om relevante dreigingen te signaleren. Wanneer daar aanleiding toe is, informeert SURFcert instellingen hierover, zowel breed als gericht. Ook deelt SURFcert waar nodig adviezen met concrete handelingsperspectieven, toegesneden op de sector.

- Geautomatiseerde beschikbaarstelling van feeds met IoC's en threat intelligence via het Open Source Threat Intelligence Platform MISP, voor gebruik in systemen binnen de instelling.
- Detectie van bekende IoC's op netwerk- en DNS-niveau, met melding aan de instelling bij een hit.
- Adviezen over actuele dreigingen, waar relevant toegespitst op de sector.

### 2.2.3 Hoe bevindingen je bereiken: incidentmeldingen

De bovengenoemde detectie - kwetsbaarheden, DDoS-signalen, IoC-hits - resulteert in een incidentmelding aan de instelling. Elke instelling kan zo'n melding ontvangen, bijvoorbeeld over kwetsbare services, besmette machines of overlast die vanuit het eigen netwerk plaatsvindt. Dit kan zijn omdat SURFcert hierover meldingen van derden ontving, of omdat SURFcert zelf een incident in de IP-space van de instelling heeft waargenomen.

SURFcert stuurt deze meldingen naar het door de instelling geregistreerde Security Entry Point (SEP), of bij ontbreken daarvan naar het Site Security Contact (SSC). Meldingen kunnen ook machine-leesbaar (IODEF-formaat) worden aangeleverd.

Meldingen van SURFcert zijn niet vrijblijvend: SURFcert verwacht een tijdige en adequate reactie, zodat gemelde problemen snel worden opgelost. Zie paragraaf 4 voor de bijbehorende verantwoordelijkheid van de instelling.

### 2.2.4 Informatie delen via community SCIRT

Operationele securityexperts van aangesloten instellingen kunnen aansluiten bij [SCIRT](#), de besloten community van SURF waarin actuele securityuitdagingen worden besproken en tips worden uitgewisseld. Omdat binnen SCIRT ook gevoelige informatie wordt gedeeld (waaronder technische aanvalskennmerken), gelden hiervoor een code of conduct en een aanmeldingsprocedure.

SURFcert deelt algemene, niet instellings-specifieke adviezen en vertrouwelijke informatie via SCIRT.

### 2.2.5 Coördinatie bij incidenten en crises

De betrokkenheid van SURFcert bij een incident is nooit alleen gericht op de ene getroffen instelling, maar altijd ook op het beschermen van de hele sector. SURFcert fungeert daarbij als schakel: zodra gevonden indicatoren (IoC's) of aanvalspatronen erop wijzen dat andere instellingen hetzelfde risico lopen, coördineert SURFcert de aanpak en informeert de betreffende instellingen vertrouwelijk daarover. Hiervoor schakelt SURFcert indien relevant ook het (inter)nationale netwerk van experts en CSIRT's in, waaronder het NCSC, Z-CERT, School-CERT en internationale onderwijs-CERT's (zie ook paragraaf 3.3 over deze structurele samenwerking).

Treft een cybercrisis meerdere instellingen tegelijk, dan heeft SURFcert een bredere rol: SURFcert coördineert dan de informatievoorziening binnen de sector en naar de buitenwereld. SURFcert staat getroffen instellingen bij, maar informeert ook andere instellingen over wat voor hen relevant is om te weten, zodat een duidelijk en geverifieerd beeld van de situatie ontstaat. SURFcert vervult hiermee een cruciale rol in de centrale crisisstructuur binnen de sector.

- Coördinatie van het incident en fungeren als schakel naar de rest van de sector, opschalend naar sectorbrede crisiscoördinatie indien meerdere instellingen getroffen zijn.
- Inschakelen van en afstemmen met het (inter)nationale netwerk van experts en CSIRT's, waaronder het NCSC, Z-CERT, School-CERT en internationale onderwijs-CERT's.
- Vertrouwelijk waarschuwen en adviseren van collega-instellingen over een dreiging.

## 2.3 Kennisdeling en versterking van de sector

SURFcert is nadrukkelijk niet alleen een dienst voor individuele instellingen, maar vervult ook een sectorale rol: SURFcert bewaakt en versterkt de digitale weerbaarheid van het onderwijs en onderzoek in Nederland als geheel.

### 2.3.1 Kennisdeling

SURFcert publiceert regelmatig adviezen naar aanleiding van actuele ontwikkelingen, toegesneden op de organisaties, het IT-landschap en de manier van communiceren binnen de sector. Actuele trends komen ook terug in het dreigingsbeeld dat SURFcert voor de sector opstelt.

SURFcert brengt daarnaast experts van instellingen met elkaar in contact via de community SCIRT (SURF Community van Incident Response Teams) en tijdens de [jaarlijkse conferentie](#). SURFcert draagt actief bij aan securitytrainingen die SURF organiseert, zoals de TRANSITS-cursussen voor CSIRT-leden, en zorgt dat de kennis en ervaring van SURFcert ook terugkomt in aanverwante SURF-diensten, zoals crisisoefeningen en awarenesscampagnes. Ook beantwoordt SURFcert desgevraagd specifieke security-vragen van individuele instellingen, los van een concreet incident.

- Delen van sectorbrede adviezen over dreigingen en securitymaatregelen.
- Individueel advies: het beantwoorden van specifieke securityvragen binnen de instelling.
- Opstellen periodiek sectoraal dreigingsbeeld (in ontwikkeling).

### 2.3.2 Ondersteuning bij het opzetten van een eigen CSIRT

Een Computer Security Incident Response Team (CSIRT) handelt de beveiligingsincidenten binnen het eigen instellingsnetwerk af. Op verzoek kan SURFcert helpen bij het opzetten en professionaliseren van een eigen CSIRT en het versterken van de incidentrespons-capaciteit binnen de instelling. Alle bij SURF aangesloten instellingen ontvangen overigens ondersteuning van SURFcert, ongeacht of ze al een eigen CSIRT hebben opgericht.

### 3. Verdeling van verantwoordelijkheden

---

Informatiebeveiliging is een gedeelde verantwoordelijkheid. SURFcert ondersteunt, adviseert en coördineert, maar de instelling blijft te allen tijde zelf verantwoordelijk voor de eigen informatiebeveiliging. Onderstaand overzicht maakt duidelijke hoe de verantwoordelijkheden tussen SURFcert en de instellingen zijn verdeeld.

#### 3.1 Wat SURFcert doet

- 24/7 aanspreekpunt en ondersteuning bij beveiligingsincidenten, met name in de identificatiefase
- Deels ingrijpen (containment), bijvoorbeeld netwerkmaatregelen bij DDoS-aanvallen of het blokkeren van een IP-adres
- Waarschuwen voor kwetsbaarheden die van buiten de instelling waarneembaar zijn
- Leveren van dreigingsinformatie (threat intelligence) en IoC-feeds, onder andere via MISP
- Versturen van incidentmeldingen naar het geregistreerde SEP- of SSC-contact van de instelling, over kwetsbaarheden of incidenten die SURFcert van buitenaf heeft waargenomen
- Coördinatie van incidenten en crises richting de rest van de sector, waaronder het vertrouwelijk informeren en waarschuwen van andere instellingen bij relevante dreigingen
- Advies en begeleiding bij meldplicht en aangifte
- Ondersteuning bij het opzetten en professionaliseren van een eigen CSIRT
- Kennisdeling via adviezen, dreigingsbeelden, SCIRT

#### 3.2 Wat de instelling zelf doet

De instelling blijft altijd zelf verantwoordelijk voor de eigen informatiebeveiliging. Dat betekent onder meer:

- Het zelf ontwerpen, inrichten en beheren van het eigen instellings-IT-landschap, zodat dit zo veilig mogelijk is en weerbaar is tegen dreigingen.
- Zelf inrichten van monitoring van het interne instellingsnetwerk, logbestanden en clouddiensten - SURFcert monitort niet het interne instellingsnetwerk en de IT-omgeving; hiervoor kan ook een SOC-leverancier worden gecontracteerd
- Bij een incident: zelf de regie voeren en beslissen over te nemen maatregelen, en de maatregelen implementeren. SURFcert adviseert en ondersteunt vooral in de identificatie- en deels de containmentfase; voor de overige fases (eradication en recovery, en het resterende deel van containment) dient de instelling zelf voldoende kennis in huis te hebben of tijdig een externe incident response partij te betrekken
- Tijdig en adequaat reageren op incident- en kwetsbaarheidsmeldingen van SURFcert, en zich inspannen deze onverwijld op te lossen. De verantwoordelijkheid tot tijdig verhelpen is extra groot bij problemen die overlast of risico voor anderen veroorzaken (zoals actieve spam- of malwareverspreiding of een open DNS-resolver). De instelling richt het netwerk zo in dat systemen adequaat geïdentificeerd kunnen worden en meldingen opgevolgd kunnen worden.
- Het zo snel mogelijk inschakelen van SURFcert als een incident mogelijk gevolgen heeft voor andere instellingen of andere instellingen eenzelfde kwetsbaarheid kunnen hebben
- Het Security Entry Point (SEP) en/of Site Security Contact (SSC) registreren in Mijn SURF en up-to-date houden, zodat meldingen van SURFcert de juiste persoon of het juiste team bereiken

- Indien van toepassing: voldoen aan de zorgplicht, meldplicht en registratieplicht onder de Cyberbeveiligingswet

### 3.3 Samenwerking bij eigen verantwoordelijkheden

Voor een aantal taken die in principe bij de instelling zelf liggen, faciliteert SURF gezamenlijke dienstverlening om instellingen te ondersteunen:

- Voor structurele monitoring (SOC-dienstverlening) is er [SURFsoc](#). SURFcet werkt intensief samen met SURFsoc, zodat beide dienstverleningen elkaar versterken.
- Voor het tijdig inschakelen van een externe incident response-partij is er, via SURF, een gezamenlijk ingekocht incident response (retainer) raamcontract beschikbaar.

## 4. Samenvattend overzicht

Onderstaande tabel vat de belangrijkste verdeling van verantwoordelijkheden samen.

| Onderwerp                                     | SURFcet                                                  | Instelling                                                     |
|-----------------------------------------------|----------------------------------------------------------|----------------------------------------------------------------|
| Identificatie van een incident                | Advies en ondersteuning, 24/7                            | Incident (laten) onderzoeken en informatie aanleveren          |
| Containment (indammen dreiging)               | Deels: o.a. netwerkmaatregelen, DDoS-mitigatie           | Overige maatregelen; zelf de regie en eindverantwoordelijkheid |
| Eradication & recovery                        | Niet uitgevoerd door SURFcet                             | Zelf uitvoeren, of tijdig externe partij inschakelen           |
| Monitoring eigen netwerk, logbestanden, cloud | Niet uitgevoerd door SURFcet                             | Zelf inrichten, evt. via SURFsoc of eigen SOC-leverancier      |
| Kwetsbaarheden van buitenaf                   | Detecteren en melden                                     | Tijdig opvolgen en verhelpen                                   |
| Threat intelligence / IoC's                   | Verzamelen, delen (o.a. via MISP) en informeren bij hits | Verwerken in eigen systemen en opvolgen                        |
| Contactregistratie (SEP/SSC)                  | Meldingen sturen naar geregistreerd contact              | SEP en/of SSC registreren en actueel houden in Mijn SURF       |
| Coördinatie sector / crisis                   | Coördineert informatie binnen sector en naar buiten      | Meewerken en relevante informatie aanleveren                   |
| Cbw-meldplicht (indien van toepassing)        | Ontvangt verplichte meldingen, ondersteunt met advies    | Significante incidenten tijdig melden en registreren           |