Samen aanjagen van vernieuwing

Bijlage 1 Opdrachtomschrijving

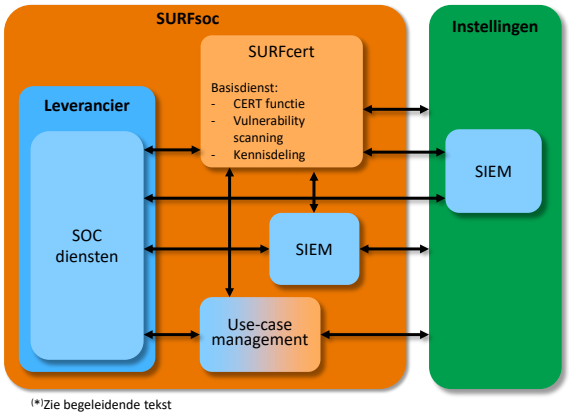
Inhoudsopgave

Inhoud

Inhoudsopgave 2
Nadere toelichting SURFsoc 3
Leveringsvormen SIEM 4
Toelichting begrippen binnen scope 6
Rolverdeling 7
Use-cases 8
Implementatie 10
Indicatie omvang Instellingen 11

Nadere toelichting SURFsoc

Instellingen willen de bestaande samenwerking op het gebied van informatiebeveiliging versterken door een gezamenlijk Security Operations Centre (SOC) te realiseren. Nadrukkelijk willen ze dit bij SURF positioneren, waar reeds meerdere jaren de gemeenschappelijke CERT-functie is belegd (SURFcert). Door te kiezen voor positionering bij SURF hebben instellingen één aanspreekpunt voor gezamenlijke diensten rondom het detecteren en voorkomen van beveiligingsincidenten. Een voordeel voor Instellingen is bovendien dat op deze wijze kennis makkelijker gedeeld kan worden tussen Instellingen. Zodoende is gekozen om vanuit SURF een nieuwe dienst aan te bieden aan Instellingen; SURFsoc.



(*)Zie begeleidende tekst

De visualisatie geeft aan op welke wijze SURFsoc gepositioneerd staat t.o.v. instellingen, SURF en de Opdrachtnemer die gezocht wordt voor ondersteuning bij SIEM. Zoals in de figuur duidelijk is opgenomen betreft de dienst SURFsoc een groter geheel dan hetgeen van de Opdrachtnemer gevraagd wordt. Van de Opdrachtnemer wordt het deel SIEM gevraagd met de daarbij behorende dienstverlening (blauwe blokken), zoals onder meer verderop beschreven onder “Toelichting begrippen binnen scope”. Zoals blijkt wordt de Opdrachtnemer een essentiële partner om de dienst SURFsoc goed aan te kunnen bieden aan Instellingen. Nadrukkelijk wordt gezocht naar een Opdrachtnemer die zich als partner opstelt en SURF en Instellingen helpt de informatiebeveiliging op een hoger niveau te krijgen. Hiertoe dient nauw samengewerkt te worden met medewerkers van SURFcert. Deze medewerkers dienen toegang te krijgen tot de gegevens, zoals geanalyseerde loggegevens en incidenten, van alle aangesloten instellingen, waarmee onder meer de CERT-functie versterkt wordt. Bij calamiteiten kunnen medewerkers van SURFcert meehelpen bij het oplossen/mitigeren van het probleem bij een instelling, op basis van gerichte adviezen vanuit de Opdrachtnemer.

Leveringsvormen SIEM

Instellingen kunnen straks bij SURFsoc aangeven welke dienstverlening zij wensen af te nemen, SURF zal dit vervolgens bij de via deze aanbesteding verkozen Opdrachtnemer afnemen. Verwacht wordt van de Opdrachtnemer dat twee leveringsvormen aangeboden worden:

1. SIEM in de infrastructuur van een individuele instelling; of
2. SIEM als multi-tenant omgeving welke bij SURF of de Opdrachtnemer is geplaatst.

Ad 1: Er zijn meerdere instellingen die nadrukkelijk hebben aangegeven enkel gebruik van SIEM-dienstverlening te kunnen en willen maken indien het SIEM binnen de eigen infrastructuur staat. Hierdoor blijven alle logbestanden binnen de infrastructuur van de instelling. Enkel de alerts uit dit SIEM worden naar het SOC van de Opdrachtnemer gestuurd. De instellingen die gebruik willen maken van deze leveringsvorm zijn met name de grotere instellingen. Die beschikken enerzijds veelal over een complexer IT-landschap en anderzijds veelal over meer security expertise dan kleinere instellingen. Deze expertise zullen deze instellingen inzetten om met het SIEM zo goed mogelijk de belangrijkste delen van hun complexe infrastructuur te bewaken en hierop door te ontwikkelen.

Ad 2: De meerderheid van de instellingen zal naar verwachting gebruik maken van een multi-tenant oplossing van het SIEM. Aan de Opdrachtnemer is de keuze of deze binnen de infrastructuur van SURF wordt gepositioneerd of bij de Opdrachtnemer zelf (SaaS-oplossing). Verwacht wordt dat u bij de aanbesteding aangeeft welke keuze u maakt en hoe deze keuze eruitziet (zie gunningscriterium K1). Een instelling die op deze wijze de dienst afneemt stuurt de logbestanden naar deze multi-tenant SIEM-omgeving. Vandaaruit worden de alerts naar het SOC van de Opdrachtnemer gestuurd.

Voor de duidelijkheid: beide leveringsvormen dienen door de Opdrachtnemer geboden te worden. Hierbij dient dezelfde techniek gebruikt te worden. Immers, de doelstelling is dat instellingen makkelijk kennis kunnen uitwisselen. Door gebruik te maken van dezelfde techniek wordt optimaal geborgd dat dit kan.

Graag merken wij nog het volgende op:

- SURF beheert de externe netwerkverbindingen van instellingen. Deze netwerkverbindingen zijn van hoge kwaliteit en capaciteit. Het verzenden van logbestanden van een instelling naar SURF gaat dan ook over eigen infrastructuur van SURF en Opdrachtnemers kunnen ervanuit gaan dat deze capaciteit ruim voldoende is. Mocht dit onverhoopt toch niet zo blijken te zijn, dan zorgen SURF en de instelling dat de capaciteit toereikend is;
- SURF is tevens in staat de verbinding te faciliteren tussen SURF en/of Instellingen en de omgeving van de Opdrachtnemer (zowel SIEM in geval van SaaS-oplossing als ook SOC in geval enkel doorsturen alerts). Hiertoe biedt SURF een peering netwerkkoppeling binnen één van de beschikbare locaties van SURF. Elke partij is verantwoordelijk voor de eigen kosten tot in de meet-me-room. De betreffende exchanges zijn: ams-ix, nl-ix, asteriod en lynx;
- Voor de multi-tenant omgeving dient Inschrijver de kosten voor servers en storage mee te rekenen in haar aanbieding. Zodoende is Opdrachtgever in staat een eerlijk vergelijk te maken tussen de aanbiedingen. Indien de winnende Inschrijver heeft aangeboden middels de multi-tenant variant binnen de infrastructuur van SURF dan wordt van de winnende Inschrijver verwacht dat hij na gunning in overleg met SURF treedt om te kijken of kostenbesparing

mogelijk is door gebruik te maken van serverruimte dan wel storage die SURF mogelijk kan bieden. Dit betekent dat inschrijver bij zijn inschrijving in beide varianten van Ad 2 - SaaS oplossing bij de Opdrachtnemer en plaatsing binnen de multitenant omgeving van SURF - de benodigde servers en storage dient te beprijzen. In de af te nemen situatie zal worden bekeken of de aangeboden servers en storage nodig zijn ; en

- SURF en Instellingen zien potentiële (kosten)voordelen door slim gebruik te maken van de via SURF aanwezige infrastructuur (waaronder de genoemde netwerkverbindingen). Bijvoorbeeld door netwerkverkeer van meerdere Instellingen door één netwerksensor te leiden om zodoende optimaal gebruik te maken van de capaciteit van die sensor. En bijvoorbeeld door gebruik te maken van licenties voor opslag door de totale benodigde opslagcapaciteit in de multi-tenant omgeving als uitgangspunt te nemen en niet de staffel per aangesloten Instelling. In de door Inschrijvers geboden oplossing kan hier slim gebruik van gemaakt worden om de kosten laag te houden met behoud van goede kwaliteit.

Toelichting begrippen binnen scope

De scope van de opdracht is beschreven in de paragrafen 1.2 en 1.3 van het Beschrijvend Document en de bijbehorende bijlagen 1 en 2 (waaronder deze bijlage)
Ter verduidelijking worden hieronder enkele begrippen toegelicht van hetgeen binnen deze scope afgedekt wordt en dus – naast de andere onderdelen die in de scope zijn opgenomen – door Opdrachtnemer geleverd dienen te worden:

- Security Monitoring: is het geautomatiseerde proces van het verzamelen en analyseren (inclusief filtering, correlatie en prioritering) van indicatoren van potentiële beveiligingsbedreigingen, en vervolgens het uitvoeren van de triage hierop om te komen tot passende acties. Om het verzamelen en analyseren van informatie over verdacht gedrag of ongeautoriseerde systeemwijzigingen in het netwerk te detecteren, is vooraf bepaald en in tooling geïmplementeerd welke soorten gedrag waarschuwingen moeten activeren inclusief passende acties hierop. De benodigde tooling dient door Opdrachtnemer verzorgd te worden;
- Security Incident Management: het proces van het realtime identificeren, beheren, vastleggen en analyseren van beveiligingsdreigingen of -incidenten. Het beoogt een robuust en uitgebreid beeld te geven van beveiligingsproblemen binnen het netwerk. In de gewenste situatie is het de bedoeling dat Opdrachtnemer de gevonden incidenten rapporteert aan SURF en de betreffende Instelling, zodat de Instelling hier vervolgens de passende maatregelen op kan nemen;
- Threat Intelligence: omvat het continue verzamelen van en periodiek rapporteren en adviseren over (niet) technische informatie ten aanzien van dreigingen, kwetsbaarheden en risico's relevant voor het netwerk, dienstverlening en sector waarbinnen de Instellingen opereren. Op basis van diverse bronnen, zowel commercieel als publiekelijk beschikbaar, met informatie over actuele dreigingen dient Opdrachtnemer automatisch informatie te aggregeren en correleren met aangesloten logbestanden/systemen;
- Security Analysis: is het specifieke proces van het realtime analyseren en beoordelen van beveiligingsdreigingen of -incidenten. Over het algemeen maakt Security Analysis integraal onderdeel uit van Security Incident Management. In de gewenste situatie is het de bedoeling dat Opdrachtnemer over de uitgevoerde analyses rapporteert aan SURF en Instellingen, zodat hier vervolgens de passende maatregelen genomen kunnen worden.

Met opmerkingen [SH1]: Aangepast n.a.v. ref. no. 144.

Rolverdeling

Rol Instellingen:

- Bepalen omvang van de gewenste dienstverlening:
    - Leveringsvorm;
    - Bepalen eigen bereikbaarheid (24/7 of beperkter);
    - Welke use-cases gebruikt worden voor de Instelling;
    - Welke delen van de infrastructuur afgedekt worden en het beschikbaar stellen van de betreffende logbestanden;
    - Bepalen wanneer welke doorgroei in aantal logbronnen/use-cases wordt gemaakt.
- Nemen van mitigerende maatregelen in de eigen infrastructuur naar aanleiding van meldingen/adviezen.

Rol SURF incl. SURFcert:

- Opdrachtgever richting Opdrachtnemer inclusief contractmanagement;
- Partner van Opdrachtnemer en Instellingen bij uitvoering van SIEM-dienstvelening;
- Analyse patronen van incidenten over Instellingen heen;
- Ondersteunen Instellingen bij vragen over toepassing SIEM en toepassing opvolgingsadviezen;
- 24/7 bereikbaar bij hoge prioriteit incidenten, ook voor Instellingen die zelf minder bereikbaar zijn.

Rol Opdrachtnemer:

- Leveren diensten zoals beschreven binnen Scope en in de Aanbestedingsstukken als partner van SURF en Instellingen.

Indien een instelling gebruik wenst te maken van het SIEM, inclusief de bijbehorende dienstverlening, dan wordt voor deze instelling een nadere overeenkomst gesloten tussen de Opdrachtnemer en het SURFsoc. Voor de betreffende instelling zal samen met de Opdrachtnemer worden gekeken hoe de instelling op een goede manier gebruik van de dienst kan gaan maken. Hierbij neemt Opdrachtnemer een actieve adviserende en (deels) uitvoerende rol in. Immers, instellingen verschillen onderling, zowel in IT-infrastructuur als in eigen expertise die beschikbaar is om te werken met de SIEM-oplossing. De instelling geeft aan welk deel van de dienstverlening gewenst is, en Opdrachtnemer onderzoekt of het bijvoorbeeld nodig is om netwerksensoren te leveren. Indien er al netwerksensoren zijn die ook gekoppeld kunnen worden aan het SIEM, dan hoeft de instelling deze niet bij de Opdrachtnemer af te nemen. Bij contact met een instelling kan de Opdrachtnemer direct schakelen met die instelling. Hierbij dient de Opdrachtnemer zich – indachtig het partnerschap met SURF – te presenteren als SURFsoc.

Use-cases

Voor use-case management is een samenwerking tussen de Opdrachtnemer en SURF voorzien. Vanuit SURF bestaat de behoefte om Instellingen te ondersteunen bij het prioriteren welke use-cases in ieder geval gebruikt zouden moeten worden (de uiteindelijke keus blijft echter bij een instelling). De rol van Opdrachtnemer is het (actief) adviseren bij het bepalen en inrichten van zinvolle use-cases die aansluiten bij de wensen van instellingen. SURF coördineert de bundeling van de wensen vanuit instellingen. Door de wensen te coördineren en bundelen, vindt standaardisatie plaats van gebruikte use-cases. Naar verwachting zullen de meeste Instellingen die starten met SIEM-dienstverlening tevens starten met deze gestandaardiseerde use-cases. Door standaardisatie verwerft SURF ook meer kennis over deze use-cases, kennis die door SURF mede ingezet kan worden om Instellingen te ondersteunen bij de opvolging van meldingen naar aanleiding van deze use-cases.

Met instellingen is een eerste set van 10 typen use-cases bepaald welke in ieder geval door de Opdrachtnemer geboden moeten worden. Dit betreft de volgende use-cases:

Nr	Categorie	Beschrijving
1	Identity and access	Veranderingen aan 'admin'-accounts (bijvoorbeeld wachtwoordwijziging) en afwijkend gebruik van admin accounts (bijv. tijdstip/locatie of vanaf niet logische plek inloggen, abnormaal gedrag). Inclusief Anomalous privilege escalation en wijzigingen van administratieve groepen, zowel op domein- als lokaal op serverniveau. Bronnen: Windows Event Logs/O365 op servers en logs van de domain controllers, AD-logging, logging Linux/Docker/etc.
2	Bewaken belangrijke servers	Veranderingen aan (belangrijke) systemen en programma's detecteren. Inclusief Installeren/stoppen/starten van niet standaard services/ daemons. Bronnen: Event log (windows/linux/mac)
3	Netwerkverkeer	Alerts genereren aan de hand van IOC's. Detecteren van het "raken van IOC's", inclusief netwerk intrusion Bronnen: firewall, DNS, Netflow
4	Netwerkverkeer	Detect lateral movement Bronnen: sensor en correlatie van andere use-cases
5	Netwerkverkeer	Onveilige diensten/software/protocollen detecteren. (Netwerkverkeer sniffen). Monitor Network devices - monitoring traffic over time and detecting unusual spikes, non-trusted communication sources, insecure protocols, and other signs of malicious behavior. Bronnen: sensor
6	Accountgebruik	Afwijkend gebruik van accounts over een tijdsbestek van 24 uur, bijvoorbeeld min of meer simultaan gebruik van een account vanuit bijvoorbeeld een Russisch en een Nederlands IP-adres. Bronnen: AD-logs, Webserverlogs (incl OWA), VPN-logs, O365.
7	Accountgebruik	Acties vanuit 1 account, vanuit 1 machine, of vanuit 1 IP-adres richting een hoop gemonitorde servers, bijvoorbeeld het benaderen van shares op vele verschillende servers vanuit 1 adres. Bronnen: Windows Event logs van allerlei gemonitorde servers, logs van de domaincontroller, netflowdata.

8	End points	Compromised End-points detecteren, inclusief servers/netwerk-componenten Bronnen: DNS/Netflow/End-point security software logs
9	Attacks	Detect Phishing en malware attacks, application intrusion attacks Bron: AV tooling
10	Audittrail	Manipulatie van audittrail: een aanvaller kan proberen eigen acties te verbergen door de audittrail van gemonitorde devices te wijzigen of te verwijderen Bron: alle aangesloten logbronnen

Een Instelling is en blijft zelf verantwoordelijk voor het bepalen welke use-cases ze daadwerkelijk willen gebruiken. Zodra een Instelling gebruik gaat maken van de SIEM-dienstverlening, dient de Instelling ook te bepalen welke logbronnen aangesloten gaan worden en welke use-cases gebruikt gaan worden. In eerste instantie zullen instellingen veelal met minder dan de bovengenoemde 10 use-cases starten. Doel is om na verloop van tijd te groeien in de af te nemen use-cases om zodoende de informatiebeveiliging telkens op een hoger niveau te krijgen.

Implementatie

De minimumeisen ten aanzien van implementatie zijn opgenomen in het Programma van Eisen. Hierbij wordt uitgegaan van een periode van maximaal 6 maanden na ingang van de Raamovereenkomst voor het bewezen op orde hebben van de dienst, inclusief het werkend opgeleverd hebben van bovengenoemde 10 use cases. Opdrachtnemer kan bij gunningscriterium K3 Implementatie aangeven op welke wijze deze implementatie wordt vormgegeven.

SURF is verantwoordelijk voor het aanleveren van voldoende Instellingen die binnen de initiële periode van 6 maanden aangesloten moeten worden. De eis voor de Opdrachtnemer betreft dat ten minste 10 Instellingen gebruik van de dienst maken via de multi-tenant omgeving en daarbij ten minste 5 Instellingen gebruik maken van de oplossing binnen de eigen infrastructuur. Indien Opdrachtnemer meer dan dit aantal Instellingen kan aansluiten binnen de genoemde periode, dan mag dat. Indien SURF te weinig Instellingen levert en/of wegens andere redenen buiten de schuld van Opdrachtnemer om het minimale aantal Instellingen niet wordt behaald, dan hoeft dit acceptatie van de geleverde oplossing niet in de weg te staan. Indien deze situatie zich voordoet, zal dit tot overleg tussen SURF en Opdrachtnemer leiden, met de intentie om te komen tot een waardevolle en zinvolle acceptatie van de geleverde oplossing.

Bij implementatie dienen de use-cases die Instellingen wensen aangeboden te worden. Dit betreft zowel de in dit document genoemde typen use-cases als specifieke use-cases die een Instelling zou willen toepassen. Opdrachtnemer is verantwoordelijk voor het goed uitwerken van de use-cases opdat deze zinvol toegepast kunnen worden door Instellingen.

In eis E3 is opgenomen dat de Opdrachtnemer in staat is om uiterlijk 6 maanden na ingang van de Raamovereenkomst ten minste 4 Instellingen per maand aan te sluiten op de dienstverlening. Opgemerkt wordt dat dit ook al eerder mag en dat het ook meer dan de genoemde 4 mogen zijn. Tevens wordt opgemerkt dat het mogelijk is dat zich minder dan 4 Instellingen per maand aanbieden om aan te sluiten. In dat laatste geval is de Opdrachtnemer uiteraard niet in gebrek.

Indien de Opdrachtnemer niet binnen de genoemde termijn van de eisen E1 en E2 voldoet aan het vereiste, dan behoud de Opdrachtgever zich het recht voor de Raamovereenkomst te ontbinden, dan wel om een verbetertraject af te spreken met Opdrachtnemer. Tijdens de periode van het verbetertraject behoud Opdrachtgever tevens het recht de boete-clause, zoals opgenomen in artikel 8 van de Raamovereenkomst, in te roepen.

Indicatie omvang Instellingen

Onderstaand is een indicatie gegeven van de omvang van verschillende Instellingen. Dit betreft de totale omvang van zo'n Instelling. Indien een Instelling gebruik gaat maken van de SIEM-dienstverlening, dan is het zeer wel denkbaar dat niet direct de hele infrastructuur van de Instelling ontsloten wordt in het SIEM. Er kan gekozen worden om slechts enkele logbronnen aan te sluiten en/of delen van het netwerk. De indicatie van de omvang is dan ook bedoeld om een overall beeld te geven van de omvang van een Instelling.

Indicatie omvang omgeving universiteit

Onderstaande indicatie is gebaseerd op ervaringscijfers van enkele universiteiten die reeds een pilot uitvoeren met SIEM-dienstverlening. Verschillende universiteiten kunnen onderling verschillen in complexiteit en omvang van hun infrastructuur. Een en ander is uiteraard erg afhankelijk van de inrichting van het SIEM en naar welke loginformatie op welke wijze wordt doorgestuurd.

Aantal users:

- +/- 25.000 studenten
- +/- 10.000 medewerkers

Indicatie verkeer:

- +/- 15.000 Mbps piek netwerkverkeer door netwerksensoren
- 150 tot 200 GB/dag logdata vanuit diverse logbronnen (AD/AV/DHCP/DNS/Firewall/IDS/Mail)
- +/- 50.000 concurrent ip-systemen op het netwerk (zowel gast als managed), waarvan:
    - +/- 4.000 servers
    - +/- 15.000 werkplekken
    - Rest BYOD

Opgemerkt wordt dat de indicatie per universiteit (sterk) kan afwijken, mede afhankelijk van de gekozen inrichting van het systeem.

Indicatie omvang omgeving hogeschool

Onderstaande indicatie is gebaseerd op cijfers van enkele gemiddelde HBO-instelling en een grotere HBO-instelling. Binnen het HBO is minder ervaring met SIEM-oplossingen dan binnen universiteiten, vandaar dat er nog geen ervaringscijfers beschikbaar zijn.

<u>Gemiddelde HBO-instelling:</u>

Aantal users:

- +/- 11.000 studenten
- +/- 1.100 medewerkers

Indicatie verkeer:

- +/- 5.000 Mbps piek netwerkverkeer door netwerksensoren

- +/- 5.000 concurrent ip-systemen op het netwerk (zowel gast als managed), waarvan:
    - +/- 150 servers
    - +/- 1.000 werkplekken
    - Rest BYOD

Grote HBO-instelling:

Aantal users:

- +/- 60.000 studenten
- +/- 6.500 medewerkers

Indicatie verkeer:

- +/- 10.000 concurrent ip-systemen op het netwerk (zowel gast als managed), waarvan:
    - +/- 93 fysieke servers
    - +/- 638 virtuele servers
    - +/- 6.000 werkplekken
    - Rest BYOD

Indicatie omvang omgeving MBO-instelling
Onderstaande indicatie is gebaseerd op cijfers van enkele gemiddelde MBO-instelling. Binnen het MBO is nagenoeg geen ervaring met SIEM-oplossingen, vandaar dat er nog geen ervaringscijfers beschikbaar zijn.

Gemiddelde MBO-instelling:
Aantal users:

- +/- 12.000 studenten
- +/- 1.500 medewerkers (1200 FTE)

Indicatie verkeer:

- +/- 2.000 Mbps piek netwerkverkeer door netwerksensoren
- +/- 3.500 concurrent ip-systemen op het netwerk (zowel gast als managed), waarvan:
    - +/- 110 servers (20 fysiek, de rest virtueel)
    - +/- 400 werkplekken volledig in beheer
    - +/- 800 werkplekken gedeeltelijk in beheer (security policies)
    - Rest BYOD

NB: de client inrichting verschilt sterk tussen instellingen, de ene heeft alles nog traditioneel in beheer, de andere heeft alles BYOD en natuurlijk alles daartussenin.