



Uitvoeringsorganisatie
Bedrijfsvoering Rijk
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

SIEM/SOC visie Logius

UBR|HIS

Bezoekadres

Rijkskantoor Beatrixpark
Wilhelmina van Pruisenweg 52
2595 AN Den Haag

Postbus 20011
2500 EA Den Haag

Bijlage A4 Behorend bij

Europese aanbesteding Uitbesteden Infrastructuurdiensten en SIEM/SOC diensten

ten behoeve van het

ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Datum	08 juli 2019
Kenmerk	201850054.011.018

Inhoud

Inhoud	2
1 Inleiding	3
1.1 Doel en doelgroep	3
1.2 Terminologie.....	3
1.3 Nut en noodzaak van SIEM/SOC in cybersecurity context	3
2 De Security Operations Functie.....	5
2.1 Beleid & Sturing.....	5
2.2 Ontwikkeling & Deployment.....	5
2.3 Service Operations	5
2.4 Security Operations	5
2.5 Raakvlakken en samenwerking in Security Operations	6
3 Security Operations dienstverlening	7
3.1 Threat Intelligence diensten.....	7
3.2 Monitoring & Response diensten.....	7
3.3 Baseline Security diensten.....	7
3.4 Penetratietestdiensten	8
3.5 Forensische diensten	8
3.6 Beschikbaarheidsmonitoring	8
3.7 SIEM platform.....	9
3.8 Analyseplatform.....	10
3.9 Algemene zaken.....	10

1 Inleiding

1.1 Doel en doelgroep

Dit document is opgesteld in het kader van de Europese aanbesteding door Logius van SIEM/SOC diensten. Het document dient tot informatie aan kandidaten ten behoeve van een inschrijving of hun oriëntatie daarop.

1.2 Terminologie

In dit document worden de volgende termen gebruikt.

- **SIEM** – Security Information and Event Management. Hiermee wordt in dit document bedoeld: het detectie- en analysesysteem op security incidenten, alsmede de bijbehorende taken (diensten) van gespecialiseerde medewerkers.
- **SOC** – Security Operations Center. Hiermee wordt het organisatie onderdeel bedoeld, dat de toebedeelde security operations functies uitvoert. Een SOC beschermt proactief de IT-omgeving en draagt bij aan mitigatie van alle dreigingen voor de IT-dienstverlening van de Rijksoverheid binnen de eigen organisatie. Door tijdige signalering van kwetsbaarheden en controle van oplossingen heeft Logius zijn ICT-systemen op orde en worden de operationele risico's beperkt.
- **Security Operations** – De integrale bedrijfsfunctie die zich richt op IT beveiliging, en waaraan SIEM en SOC bijdragen.

1.3 Nut en noodzaak van SIEM/SOC in cybersecurity context

De Digitale Overheid is een interessant target voor cyber crime en spionage. Het dreigingsbeeld voor onze kritieke en vitale voorzieningen is hoog.

Daarnaast is het niet langer de vraag of een organisatie met een cyber incident te maken krijgt, maar wanneer en of het incident wordt opgemerkt.

De gevolgen van een cyber incident zullen dus moeten worden vermeden en beperkt. Dat alleen door een gelaagde beveiliging van de voorzieningen en een combinatie van preventie-, detectie- en responsmaatregelen.

Voor de inrichting van die beveiligingsvoorzieningen hanteert Logius de volgende uitgangspunten:

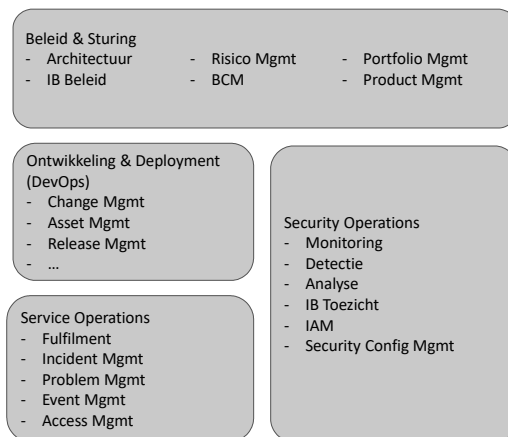
- Snelle detectie is noodzakelijk om de effectieve duur van cyber dreigingen te voorkomen of te beperken.
- Continue monitoring van applicaties en netwerken zorgt voor structurele bewaking van kritische beheerprocessen (capaciteit, beschikbaarheid, toegang, wijzigingen).
- Centrale aanpak vereenvoudigt de aansturing van leveranciers door middel van standaardisatie van monitoring en detectie componenten
- We hebben een integrale blik op de compliance eisen en het voldoen aan relevante wet- en regelgeving kost minder tijd

Een ingericht SIEM-platform en SIEM/SOC-diensten vullen een belangrijk deel van voornoemde uitgangspunten in. Gerichte doelen van Logius voor SIEM/SOC zijn:

- Vroegtijdige detectie van onbeschikbaarheid, cyberdreigingen en afwijkend gedrag;
- Een integraal cybersecurity beeld van Logius;
- Uitwisseling van intelligence met ketenpartners.

Dit document bevat in hoofdstuk 2 een beknopte visie op de Security Operations functie in relatie tot overige relevante bedrijfsfuncties. Hoofdstuk 3 bevat Logius' visie op de SIEM/SOC dienstverlening die Logius uit de markt wenst te betrekken.

2 De Security Operations Functie



Figuur 1 Functionele positionering van Security Operations

Figuur 1 toont vanuit een functionele insteek het Security Operations aandachtsgebied in relatie tot overige aandachtsgebieden binnen Logius. Deze aandachtsgebieden worden hieronder kort toegelicht. Aansluitend volgt een korte toelichting op de voorziene raakvlakken en samenwerking tussen de aandachtsgebieden.

2.1 Beleid & Sturing

Onder beleid en sturing vallen functies die sturend en/of kaderstellend zijn aan andere functies. Hieronder vallen architectuur, informatiebeveiliging, business continuity management, portfolio management, risico management en product management. Deze functies ontvangen informatie uit – en werken samen met – de overige functies.

2.2 Ontwikkeling & Deployment

Onder ontwikkeling en deployment vallen functies die zorgdragen voor alle soorten wijzigingen op de operationele omgeving en de beheersing van die wijzigingen, zoals change management, asset management, release management.

2.3 Service Operations

Met service operations worden bedoeld: de functies die zorgen voor het operationeel zijn en blijven van de operationele omgeving, alsmede de ondersteuning van het reguliere gebruik van die omgeving. Hieronder worden bijvoorbeeld verstaan: request fulfilment, incident management, problem management, event management, access management.

2.4 Security Operations

Onder security operations vallen functies die zich richten op beveiliging van de operationele omgeving. Hieronder worden onder andere verstaan: monitoring op kwetsbaarheden en detectie van events in de operationele omgeving, (historische) analyse van gelogde informatie op achterliggende oorzaken en verbanden, controle op de effectiviteit van security maatregelen, IAM werkzaamheden, security configuratiebeheer, coördinatie op security incidenten.

2.5 Raakvlakken en samenwerking in Security Operations

De scheidslijn tussen de Service Operations functie enerzijds en de Security Operations functie vertaalt zich niet naar een hard organisatorisch onderscheid: de service operations organisaties (van de platform- en infrastructuurdiensten en van de Voorzieningen) vullen niet alleen de Service Operations functie in, maar ook een deel van de Security Operations functie. Zo dragen zij zelf zorg voor monitoring, bewaking, en afhandeling van security incidenten van diensten waarvoor zij verantwoordelijk zijn. De security operations organisatie voedt op haar beurt de service operations organisaties door ze dashboards en analyses te verstrekken ten behoeve van bewaking en inzichten, nadere analyse te doen, en adviezen te verstrekken. Uitgangspunt is de gezamenlijke, transparante werkelijkheid uit de logs en de SIEM-omgeving. Er wordt samengewerkt aan de analyse en opvolging van incidenten, en aan het verbeteren van de inzichten in cq. de verbetering van de werking van de informatiebeveiliging.

Uiteraard zijn essentiële verantwoordelijkheden gescheiden waar dat noodzakelijk is: de rol om onafhankelijk toezicht te houden ligt bij de security operations organisatie, buiten de service operations organisaties.

Het inzicht en werkgebied van de security operations organisatie is breder dan van de service operations organisaties afzonderlijk: de security operations organisatie heeft een organisatiebrede, soms zelfs ketenbrede/overheidsbrede blik. Zij hebben ook de taak om gedrag breder te duiden en daarop te acteren, bijvoorbeeld door crisismangement in te schakelen.

3 Security Operations dienstverlening

Logius voorziet onderstaande dienstverlening door SIEM/SOC Leverancier. Onderstaand betreft een verduidelijking op de scope, zoals neergelegd in de overeenkomst. De opsomming dient gelezen te worden inclusief de randvoorwaarden van organisatorische samenwerking en gezamenlijke inzichten zoals die zijn verwoord in 2.5.

3.1 Threat Intelligence diensten

Onder Threat Intelligence diensten worden in algemene zin verstaan:

- Het verzamelen van informatie over mogelijke dreigingen;
- Het verrijken en correleren van informatie tot analytisch betrouwbare aannames over toekomstige dreigingen;
- Het definiëren van preventieve maatregelen.

De door Logius beoogde dienstverlening van SIEM/SOC Leverancier bestaat uit:

- Zorgen voor actuele threat intelligence/technische dreigingskennis op de bewaakte assets;
- Adviseren over adequate bewaking en respons bij onmiddellijke dreigingen en anderszins.

3.2 Monitoring & Response diensten

Onder Monitoring & Response diensten worden in algemene zin verstaan:

- Het definiëren van intrusion management rules en filters;
- Log management: beheer van centrale en/of generieke logging componenten conform het logbeleid;
- Security event management: het tunen van SIEM filters en het herkennen van ongewoon gedrag uit log events;
- Het behandelen van security incidenten;
- Security incident response: het leveren van informatie ten behoeve van het oplossen van een incident.

De door Logius beoogde dienstverlening van SIEM/SOC Leverancier bestaat uit:

- Monitoring van assets, inclusief IAM en beveiligingsoplossingen op incidenten en potentiële bedreigingen;
- Monitoring van assets op proces- of ketenniveau ten behoeve van algehele beschikbaarheid van diensten van Logius. Deze dienstverlening is nader uitgewerkt in 3.6;
- Bij onmiddellijke dreigingen: te ondernemen acties organiseren en Logius-calamiteitenorganisatie inschakelen;
- Deelname aan het testen van respons en recovery op security incidenten;
- Het detecteren en analyseren van events, bepalen van impact;
- Het (doorlopend) configureren van SIEM (regels, correlatiepatronen, overig);
- Het behandelen van security incidenten, inclusief regie over Leveranciers;
- Security incident response: het leveren van informatie ten behoeve van het oplossen van een incident.

Hierbij geldt voor de monitoring, detectie en responsactiviteiten een 24x7 dienstverlening.

3.3 Baseline Security diensten

Onder Baseline Security diensten worden in algemene zin verstaan :

- Vulnerability handling: op basis van assetinformatie vaststellen of er kwetsbare

- componenten gebruikt worden in de infrastructuur;
- Configuration monitoring: afwijkingen van de configuratie t.o.v. de technische security baseline vaststellen en rapporteren. Monitoring op BIR2017 compliance valt ook onder Configuration monitoring.
- Vulnerability scanning: het uitvoeren van security scans om publiek bekende kwetsbaarheden in de infrastructuur te detecteren.

De door Logius beoogde dienstverlening van SIEM/SOC Leverancier bestaat uit:

- Het inrichten van assets, rules en overige configuraties (use cases) in de SIEM omgeving. Het relateren daarvan aan (het onderhoud van) de diensten van Logius. Het classificeren van kwetsbaarheden;
- Intake van nieuwe diensten in de SIEM omgeving;
- Bewaken van vulnerability scanning resultaten, advisering over opvolging;
- Uitvoeren van vulnerability monitoring;
- Uitvoeren van controle op beveiligingsoplossingen, waaronder:
 - configuratie monitoring,
 - intrusion & detection management,
 - nationaal detectienetwerk,
 - misbruik detectie tools,
 - NCSC foto,
 - vulnerability scanning,
 - database activity monitoring,
 - DDoS mitigatie,
 - threat intelligence.
- Controleren op afwijkingen van onderhoudsafspraken.

3.4 Penetratietestdiensten

Onder Penetratietest diensten worden in algemene zin verstaan :

- Penetratietesten uitvoeren;
- Regievoering: organiseren, scope bepalen, opvolgen van bevindingen.

De door Logius beoogde dienstverlening van SIEM/SOC Leverancier bestaat uit:

- Geen. Buiten scope.

3.5 Forensische diensten

Onder Forensische diensten worden in algemene zin verstaan :

- Waarheidsvinding: het veiligstellen, onderzoeken en analyseren van digitale sporen;
- Diepgaand onderzoek bij aanvallen en incidenten, waaronder integriteitsschendingen;
- Aansturing overige SOC functies op basis van kennis en expertise;
- Training & awareness organiseren.

De door Logius beoogde dienstverlening van SIEM/SOC Leverancier bestaat uit:

- Verzorgen van specialistische kennissessies op cybersecurity, threat intelligence, emerging response patterns, et cetera;
- Het leveren en technisch beheren van een analyseplatform;
- Ad hoc bijdragen aan forensische analyse;
- Bijdragen aan cq. ongevraagd adviseren in het verbeteren van monitoring & respons.

3.6 Beschikbaarheidsmonitoring

Logius verwacht functioneel van beschikbaarheidsmonitoring [7]:

- Alerting. De mogelijkheid tot het (vroegtijdig) bieden van waarschuwingen rondom

- de werking en beschikbaarheid van (een keten van) applicaties aan alle belanghebbenden;
- Trends. De mogelijkheid tot genereren van dashboards en rapportages van de werking (ook vanuit gebruikersperspectief) en beschikbaarheid van Logius-brede voorzieningen over een bepaalde tijdsperiode;
- Kwaliteit. De controle of een geleverde dienst ook conform de eerder afgesproken (technische) specificaties is geleverd.

De door Logius beoogde dienstverlening van SIEM/SOC Leverancier bestaat uit:

- Inrichten van de door alle belanghebbenden te gebruiken dashboards;
- Inrichten van de geautomatiseerde waarschuwingen rondom de werking en beschikbaarheid van diensten en/of applicaties, aan alle belanghebbenden;
- Het maken en leveren van trendanalyses op werking en beschikbaarheid van diensten en/of applicaties;
- Mogelijkheden bieden aan belanghebbenden om vanuit dashboards, waarschuwingen, en analyses interactieve nadere analyse (bijvoorbeeld drill-down) te kunnen doen;
- Bijdragen aan de ontwikkeling van inzichten op ketenniveau in overheidsketens met componenten buiten de Logius omgeving.

3.7 SIEM platform

De van de SOC organisatie verwachte diensten zullen in belangrijke mate worden ondersteund met een SIEM platform. De SIEM/SOC leverancier dient dit SIEM platform te leveren en te implementeren op Logius' IT-infrastructuur. Het is voor de inpassing van dat platform van belang om de Logius IT-context te kennen:

- De te monitoren platforms betreffen multi-tenant applicatieomgevingen die enerzijds zijn gerealiseerd als 'virtual private cloud' (VPC) omgevingen en anderzijds als gegroepeerde container deployments;
- De VPC omgevingen zullen de komende jaren afnemen in aantal ten gunste van containergebaseerde omgevingen;
- De applicatieomgevingen verzorgen eigen logging en operationele monitoring;
- De log bestanden uit de applicatieomgevingen voeden centrale log servers, die op hun beurt mede de bron voor SIEM vormen;
- De huidige SIEM/SOC dienstverlening is gecombineerd met de infrastructuurdienstverlening ten behoeve van Logius' applicatieomgevingen;
- De toekomstige SIEM/SOC dienstverlening zal ontvlochten worden van de infrastructuurdienstverlening, waardoor het noodzakelijk zal worden explicietere normen en richtlijnen te stellen aan de infrastructuurdienstverlening ten behoeve van security operations. Het belangrijkste uitgangspunt daarbij is, dat de omgevingen van leveranciers van infrastructuurdiensten voor Logius *in volledige transparantie* beschikbaar zijn voor SIEM/SOC dienstverlening.

Aan het SIEM platform verbindt Logius, aanvullend op voornoemde diensten, de volgende beoogde dienstverlening:

- Borgen van beschikbaarheid, integriteit, vertrouwelijkheid;
- Inrichting van het SIEM platform binnen de Logius IT-context:
 - o Het SIEM platform zelf;
 - o Logging en monitoring van SIEM zelf;
 - o De koppelingen met de log servers;
 - o De koppeling met het analyseplatform;
 - o Toegang tot het platform aan Logius en zijn leveranciers, logisch gescheiden per beheerdomein.
- Technisch onderhoud;
- Aanvullend functioneel onderhoud, voor zo ver niet in voornoemde diensten benoemd.

3.8 Analyseplatform

Onder andere de forensische diensten benoemd in 3.5 zullen worden ondersteund met een analyseplatform. Dit analyseplatform biedt de (forensisch) analisten mogelijkheden tot nadere analyse van events uit SIEM, onderliggende log data uit SIEM, en eventuele aanvullende bronnen. De SIEM/SOC Leverancier dient dit platform te leveren en te implementeren op de Logius infrastructuur.

Aan het analyseplatform verbindt Logius, aanvullend op voornoemde diensten, de volgende beoogde dienstverlening:

- Borgen van beschikbaarheid, integriteit, vertrouwelijkheid;
- Inrichting van het analyseplatform binnen de Logius IT-context:
 - o Het analyseplatform zelf;
 - o Logging en monitoring van het analyseplatform zelf;
 - o Toegang en inrichtingsmogelijkheden van de door alle belanghebbenden te gebruiken dashboards;
 - o De koppeling met de SIEM omgeving;
 - o Toegang tot het platform, met daarbij het strikt scheiden van bevoegdheden met het analyseplatform;
- Technisch onderhoud.

3.9 Algemene zaken

Er zullen diverse, gebruikelijke raakvlakken met Logius zijn in de samenwerking:

- Informatie-uitwisseling tussen SIEM/SOC Leverancier, overige leveranciers van Logius en Logius zelf;
- Afstemmingsmomenten en werkwijzen;
- Documenteren;
- Rapporteren.

Logius voorziet een 'purple teaming' samenwerkingsvorm tussen SOC en overige stakeholders, waarbij de beveiliging van diensten op een doorlopende, agile en interactieve manier wordt verbeterd met behulp van de kennis van de Leveranciers (blue teams), het SOC + Logius (red teams). De 'purple team' rol ligt daarin primair bij Logius, van SOC is daarin actieve medewerking, kennis- en expertise-inbreng en bijdrage vereist.