



Uitvoeringsorganisatie
Bedrijfsvoering Rijk
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

SIEM/SOC huidige situatie Logius

UBR|HIS

Bezoekadres

Rijkskantoor Beatrixpark
Wilhelmina van Pruisenweg 52
2595 AN Den Haag

Postbus 20011
2500 EA Den Haag

Bijlage A3 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
2 Dienstverlening.....	4
2.1 Doel en resultaat van de dienst.....	4
2.2 Werking van de dienst	4
2.3 Use Case Management.....	5
2.4 Expert analyse.....	5
2.5 Wijze van ontsluiting	5
3 Kentallen	6
3.1 De gemonitorde omgeving.....	6
3.1.1 Managed environment.....	6
3.1.2 Flow.....	6
3.1.3 Capaciteit	6
3.2 SIEM + SOC activiteiten.....	6
3.2.1 Use case monitoring.....	6
3.2.2 Use case ontwikkeling	6
3.2.3 Incidentafhandeling	6
3.2.4 Analyse	6
4 Architectuur.....	7
5 Bronnen	8

1 Inleiding

Dit document is onderdeel van de achtergrondinformatie verstrekt door Logius in de gecombineerde aanbestedingsprocedure voor infrastructuur- en SIEM/SOC-diensten. Het document bevat uitleg over de bestaande SIEM/SOC dienstverlening. Deze is niet gelijk aan de gewenste dienstverlening, zie daarvoor Bijlage A4 SIEMSOC Visie Logius.

2 Dienstverlening

2.1 Doel en resultaat van de dienst

De SIEM dienst geeft invulling aan de informatiebeveiligingsfunctie Logging en Monitoring op de Logius Voorzieningen. De SIEM dienst draagt hiermee bij aan de invulling van de BIR eisen en de Logging en Monitoring functionele eisen. De SIEM dienst draagt bij aan het inzichtelijk maken van risicovolle gebeurtenissen voor de Logius Voorzieningen en dient een bijdrage te leveren aan de digitale weerbaarheid van de Logius Voorzieningen.

De SIEM dienst is ingericht als centrale voorziening binnen het Managed Services platform. Het Managed Services platform bestaat uit infrastructurele diensten, aangevuld met platformdiensten. Deze worden gebruikt als bouwstenen in de Voorzieningen die Logius ontwikkelt en beheert voor zijn afnemers.

2.2 Werking van de dienst

De SIEM dienst is er om de aan informatiebeveiliging gerelateerde gebeurtenissen die aandacht vereisen te detecteren, technisch te correleren, te signaleren, te analyseren en daarover te rapporteren en adviseren. SIEM maakt gebeurtenissen zichtbaar en maakt het proces van opsporen vele malen efficiënter en betrouwbaarder. Het repeterende deel van de SIEM dienst verzamelt, analyseert en correleert logregels en detecteert de afwijkingen en mogelijke incidenten in near real-time (op basis van functionele use cases) en maakt daarmee zichtbaar waar potentiële risico's zich voordoen. Naast deze repeterende analyses vindt er ook expertanalyse plaats van signalen, logregels en actuele dreigingsinformatie om nieuwe potentiële risico's inzichtelijk te maken. Na beoordeling van de output van deze potentiële risico's worden de relevante risico's gemeld in tickets. Verdere afhandeling van deze tickets vindt plaats in de reguliere incident, change en overige processen.

2.3 Use Case Management

De dienst SIEM werkt op basis van scenario's die beschrijven op welke activiteiten, afwijkend gedrag of afwijkende gebeurtenissen meldingen in het SIEM systeem triggeren. Een scenario bevat o.a. de risico classificering van het scenario en de benodigde actie(s) welke uitgevoerd dienen te worden mocht het scenario zich materialiseren. De scenario's zijn gegroepeerd in een use case. Een use case is een generieke functionele omschrijving van een situatie waarvan gewenst is om te weten dat hij zich voordoet en hoe vervolgens op die situatie gereageerd moet worden.

Use Case management is essentieel voor een effectieve inzet van de SIEM dienst. Het bepaalt wat de dienst rapporteert en geeft de mogelijkheid om te sturen op de meldingen en draagt daarmee bij aan de IB doelstellingen. Logius en de Managed Services leverancier werken samen aan de wenselijke use cases. De Managed Services leverancier implementeert en beheert de use cases, Logius voert de regie.

2.4 Expert analyse

De SIEM dienst werkt deels reactief op basis van Use Case Management zoals hierboven beschreven. Echter is er voor het doel en de beoogde resultaten van de dienst ook de noodzaak aanwezig om proactief risicovolle gebeurtenissen zichtbaar te maken. Dit onderdeel van de SIEM dienst dat intelligentie aan de dienst toevoegt, wordt Expert Analyse genoemd.

2.5 Wijze van ontsluiting

De SIEM dienst wordt als volgt ontsloten.

De input is:

- Logregels
- Use Cases
- Threat Intelligence

De output is:

- Rapportages over de dienst
- Incidenten
- Meldingen
- Adviezen uit Expert Analyse & Incidenten
- Threat Intelligence uit Expert Analyse & Incidenten

3 Kentallen

De hieronder genoemde kentallen geven nader inzicht in de bestaande SIEM/SOC dienstverlening.

3.1 De gemonitorde omgeving

3.1.1 *Managed environment*

De middels SIEM gemonitorde omgeving bestaat uit:
2.500 VM's (exclusief redundantie).

3.1.2 *Flow*

Het aantal events per seconde voor de gemonitorde omgeving is:
rond de 10.000 EPS, met voorspelde groei naar rond de 20.000 EPS.

De hoeveelheid nieuw verwerkte data door het SIEM platform is:
300 GB/dag.

3.1.3 *Capaciteit*

De huidige SIEM omgeving heeft een totale opslagcapaciteit van:
100 TB. Een deel daarvan bestaat uit het bewaren van historie, deze opslag zal op termijn verschuiven naar het analyseplatform.

Het analyseplatform heeft een totale opslagcapaciteit van:
10 TB. De benodigde capaciteit zal groeien vanwege het bewaren van historie in het analyseplatform, hetgeen dan zal leiden tot parallelle vermindering van de capaciteitsbehoefte in de SIEM omgeving.

3.2 SIEM + SOC activiteiten

3.2.1 *Use case monitoring*

Aantal te monitoren functionele use cases:
20 use cases.

Aantal te monitoren generieke rules:
150 rules.

3.2.2 *Use case ontwikkeling*

10 nieuwe rules per maand.

3.2.3 *Incidentafhandeling*

Aantal incidenten:
709 incidenten per jaar (2018).

3.2.4 *Analyse*

Bij de analyse wordt gebruik gemaakt van specifieke tools. Deze worden momenteel beheerd door de analisten zelf. Naar schatting besteden zij +/- 1 FTE aan werktijd aan het applicatiebeheer op deze tools.

4 Architectuur

De bestaande architectuur van SIEM/SOC zal vanwege vertrouwelijkheid niet gedeeld worden in de selectiefase.

5 Bronnen

Nr	Titel, Auteur	Versie	Datum
1	SIEM + SOC Visie Logius	0.7	2 mei 2019
2			
3			
4			
5			