|  |
| --- |
| Richtlijn Logging en MonitoringTemplate |

|  |  |
| --- | --- |
| Auteur(s): |  |
| Versie: |  |
| Datum: | Kies of typ een datum |
| Kenmerk: |  |
|  |  |
|  |  |

**Documentinformatie**

Dit document maakt onderdeel uit van een complete set (beleidspiramide) met formeel vastgestelde documenten op strategisch, tactisch en operationeel niveau. Dit document heeft betrekking op de laag Richtlijn in de beleidspiramide.



**Versiebeheer**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Auteur** | **Verwerking** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Distributielijst**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Ontvanger** | **Doel** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Vaststelling**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Vastgesteld door** | **Vastgesteld op** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Samenhang met andere documenten**

|  |  |  |  |
| --- | --- | --- | --- |
| **Naam** | **Bovenliggend** | **Gelijk niveau** | **Onderliggend** |
| [INFORMATIEBEVEILIGINGSBELEID] | x |  |  |
| [STANDAARD LOGGING EN MONITORING] | x |  |  |
|  |  |  |  |

**Verwijzingen naar SURFaudit Toetsingskader en ISO27001**

|  |  |
| --- | --- |
| **Kader** | **Verwijzing (tags)** |
| SURFaudit Toetsingskader | SM.01, SM.02, SM.03, SM.04, SM.05, SM.06, SM.07, SM.08, SM.09, SM.10, SM.11, SM.12, SM.13  |
| ISO27001:2022 | A5.1, A8.1, A8.15, A8.16, A8.17, A8.18, A9.4, A8.19, A8.20, A8.21, A8.22, A5.3, A5.4, A8.23, A8.24, A9.3 |

**Creative Commons**

Dit template is een product van het SURF Security Expertise Centrum en beschikbaar onder de licentie Creative Commons Naamsvermelding 4.0 Internationaal. <https://creativecommons.org/licenses/by/4.0/deed.nl>

Inhoudsopgave

|  |
| --- |
| [Samenvatting 4](#_Toc199492431)[1 Inleiding 5](#_Toc199492432)[1.1 Doelstelling 5](#_Toc199492433)[1.2 Reikwijdte en Toepassingsgebied 5](#_Toc199492434)[2 Logbronnen 6](#_Toc199492435)[2.1 Verhoogde aandacht voor legacy 6](#_Toc199492436)[3 Soorten Logs en Gebeurtenissen 8](#_Toc199492437)[3.1 Functionele Logging 8](#_Toc199492438)[3.2 Technische Logging 8](#_Toc199492439)[3.3 Security Logging 8](#_Toc199492440)[3.4 Audit Logging 8](#_Toc199492441)[4 Loggingconfiguratie en opslag 9](#_Toc199492442)[4.1 Logformaat en gegevensvelden 9](#_Toc199492443)[4.2 Opslag en bewaarbeleid 9](#_Toc199492444)[5 Monitoring en detectie 10](#_Toc199492445)[5.1 Monitoringstrategie 10](#_Toc199492446)[5.2 Incident Detectie en Respons 10](#_Toc199492447)[6 Rapportage en Compliance 11](#_Toc199492448)[6.1 Standaardrapportages 11](#_Toc199492449)[6.2 Security en Compliance rapportages 11](#_Toc199492450)[6.3 Auditing en Controles 11](#_Toc199492451)[7 Evaluatie en Doorontwikkeling 12](#_Toc199492452)[7.1 Periodieke test van detectiecapaciteit 12](#_Toc199492453)[8 Vaststelling 13](#_Toc199492454)[Bijlage 1 Checklist Logging en Monitoring 14](#_Toc199492455)[1.1 Algemene Logging vereisten 14](#_Toc199492456)[1.2 Logging per IT-component 14](#_Toc199492457)[1.3 Monitoring & Detectie 16](#_Toc199492458)[1.4 Auditing, Compliance & Verbetering 17](#_Toc199492459)[Bijlage 2 Relevante bronnen 18](#_Toc199492460) |

Samenvatting

Hier komt een samenvatting, op zichzelf leesbaar, van de inhoud van dit document in max. 1 A4.

# Inleiding

Logging en monitoring zijn belangrijke onderdelen van ons informatiebeveiligingsbeleid. Deze richtlijn biedt een concrete uitwerking van onze ‘Standaard Logging en Monitoring’ en richt zich op de implementatie en operationele inrichting hiervan. Dit document definieert welke systemen loggegevens moeten genereren, welke gebeurtenissen minimaal gelogd moeten worden en hoe logs moeten worden beheerd en bewaakt.

De richtlijn volgt relevante wet- en regelgeving en is gebaseerd op internationaal erkende normen zoals CIS Controls v8, ISO 27001 en NIST 800-92.

## Doelstelling

Het doel van deze richtlijn is om een uniforme werkwijze vast te stellen voor logging en monitoring binnen onze instelling. Dit omvat:

* Het identificeren van logbronnen en te loggen gebeurtenissen.
* Het vaststellen van bewaartermijnen en beveiligingseisen voor logs.
* Het definiëren van monitoringmechanismen en rapportageverplichtingen.

## Reikwijdte en Toepassingsgebied

Deze richtlijn is van toepassing op alle IT-systemen, netwerken en applicaties die voor en/of door onze instellingen in gebruik zijn, inclusief on-premises en cloudgebaseerde omgevingen, en vereist dat deze systemen in staat zijn om loginformatie centraal aan te leveren. Systemen die deze functionaliteit niet bieden, kunnen niet worden opgenomen in het ICT-landschap van onze instelling, tenzij anders is gemotiveerd en goedgekeurd.

# Logbronnen

Een effectieve loggingstrategie vereist dat loggegevens afkomstig zijn van alle relevante IT-componenten binnen onze instelling. Hieronder volgt een overzicht van logbronnen die loggegevens moeten kunnen doorsturen naar het centrale logplatform (SIEM of Log Management Systeem). Dit stelt onze instelling in staat om afwijkingen te detecteren, beveiligingsincidenten te analyseren en naleving van regelgeving te controleren.

* **Authenticatie- en toegangsbeheer**

O.a. Active Directory, LDAP, Radius, MFA, Identity Providers, Proxies.

* **Netwerkinfrastructuur**

O.a. Firewalls, routers, switches, VPN-systemen, DNS-servers, DHCP.

* **IoT en OT apparaten**

O.a. Slimme apparaten, industriële besturingssystemen en beheersystemen hiervan.

* **Servers en werkstations**

O.a. Windows, Linux, Mac servers en werkstations, smartphones en andere ‘endpoint systemen’, hypervisors, database- en webservers.

* **Applicaties**

O.a. Bedrijfskritische applicaties, ERP-systemen, HRM-software, e-mailplatformen, hypervisors, ‘middleware’, databases en webservers, inclusief specifieke logging en monitoring van API-aanroepen en microservices.

* **Cloud-diensten**

O.a. SaaS-, PaaS- en IaaS-oplossingen, inclusief Office 365, AWS, Azure, Google Cloud.

* **Cloud-native**

Logging van serverloze en containerized workloads, zoals Kubernetes en AWS Lambda.

* **Security-componenten**

O.a. Endpoint Detection & Response (EDR), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), antivirusoplossingen.

Deze opsomming is niet limitatief.

## Verhoogde aandacht voor legacy

Binnen het ICT-landschap van onze instelling kunnen zich nog verouderde of niet meer actief ondersteunde systemen bevinden, aangeduid als legacy IT. Dergelijke systemen vormen een verhoogd risico op het gebied van informatiebeveiliging, mede vanwege beperkte ondersteuning voor actuele beveiligingsmaatregelen en beperktere mogelijkheden voor integratie met centrale logging- en monitoringsvoorzieningen.

Voor legacy IT geldt daarom een verhoogde eis tot logging en monitoring (verhoogde dijkbewaking). Zolang deze systemen onderdeel uitmaken van het ICT-landschap, is actieve bewaking vereist om afwijkend gedrag, mogelijke incidenten of misbruik vroegtijdig te signaleren. Dit omvat onder meer het zo veel mogelijk ontsluiten van relevante loginformatie naar de centrale logginginfrastructuur en het opnemen van deze systemen in de centrale monitoring.

Het onderbrengen van legacy systemen in een apart netwerksegment wordt niet als een afdoende maatregel beschouwd. Per systeem worden specifieke beheersmaatregelen en afspraken vastgelegd, gericht op het beperken van risico’s en het waarborgen van zicht op de activiteiten binnen deze systemen. Deze afspraken worden periodiek geëvalueerd en blijven van kracht tot het moment van volledige uitfasering van het betreffende systeem.

# Soorten Logs en Gebeurtenissen

Voor een gestructureerde aanpak worden logs gecategoriseerd op basis van hun doel en inhoud. Dit helpt bij het analyseren van logs en het instellen van juiste detectieregels. Elk type log moet voldoen aan specifieke registratieregels om de bruikbaarheid voor monitoring en forensisch onderzoek te garanderen.

## Functionele Logging

Functionele logs registreren applicatie- en gebruikersactiviteiten en prestaties binnen systemen. Dit type logging is belangrijk voor procesbewaking en foutopsporing binnen applicaties.

Activiteiten en prestaties die minimaal worden gelogd zijn o.a.:

* Toegang tot en gebruik van kernfunctionaliteiten.
* Foutmeldingen en herstelacties binnen applicaties.
* Release en deployment van nieuwe functionaliteiten.

## Technische Logging

Technische logs bevatten gedetailleerde informatie over de werking en status van systemen, netwerken en infrastructuurcomponenten. Deze logs vormen een belangrijke bron voor onder meer het analyseren van verstoringen en het optimaliseren van systeemprestaties. Daarnaast dienen technische logs als input voor security logging, waarbinnen verdacht gedrag en misbruik worden gesignaleerd.

Gebeurtenissen die minimaal worden gelogd zijn o.a.:

* Wijzigingen in systeemconfiguraties en instellingen.
* Starten, stoppen en herstarten van services en applicaties.
* Verbindingsproblemen en hardwarefouten.

## Security Logging

Security logging richt zich specifiek op het detecteren van afwijkingen, misbruik en andere beveiligingsrelevante gebeurtenissen. Hierbij wordt gebruikgemaakt van gegevens uit functionele en technische logging, gecombineerd met informatie uit beveiligingssystemen zoals firewalls, intrusion detection systems (IDS) en identity & access management (IAM).

Gebeurtenissen die minimaal worden gelogd zijn o.a.:

* Succesvolle en mislukte loginpogingen.
* Wijzigingen in accounts en toegangsrechten.
* Malwaredetecties, vulnerability-of poortscans en ongeautoriseerde firewallwijzigingen.

## Audit Logging

Audit logs worden gebruikt voor compliance-doeleinden en forensisch onderzoek. Ze bevatten een gedetailleerd overzicht van wijzigingen in toegangsrechten, kritieke systeeminstellingen en pogingen tot logwijzigingen.

Gebeurtenissen die minimaal worden gelogd zijn:

* Wijzigingen in toegangsbeheer en rechtenstructuren.
* Pogingen om logginginstellingen te wijzigen of uit te schakelen.
* Beheeracties door systeembeheerders.

# Loggingconfiguratie en opslag

Loggingconfiguratie en -opslag moeten worden ingericht volgens de principes van vertrouwelijkheid, integriteit en beschikbaarheid. Dit houdt in dat loggegevens beschermd zijn tegen ongeautoriseerde toegang en wijzigingen, beschikbaar blijven voor analyse en onderzoek, en op uniforme wijze worden vastgelegd. Daarbij worden onder meer afspraken gemaakt over logformaten, bewaartermijnen en toegangsrechten.

## Logformaat en gegevensvelden

Voor een consistente en betrouwbare verwerking van loggegevens moeten alle logbestanden een gestandaardiseerd formaat en een vaste set gegevensvelden bevatten. Dit zorgt ervoor dat loggegevens eenduidig kunnen worden geanalyseerd, gecorreleerd en doorzocht binnen het centrale logplatform.

* Logs worden opgeslagen in een gestandaardiseerd formaat (JSON, Syslog, CEF).
* Elke logregel bevat minimaal:
	+ Tijdstempel (UTC, NTP-gesynchroniseerd).
	+ Gebruikersnaam of systeem-ID.
	+ Bron- en bestemmingsadressen (IP-adressen, poorten, systeemnamen).
	+ Uitgevoerde actie en resultaat (geslaagd/mislukt).
	+ Betrokken systeemcomponent of applicatie.

## Opslag en bewaarbeleid

Om de integriteit en beschikbaarheid van loggegevens te waarborgen, worden logbestanden beheerd volgens vastgestelde bewaartermijnen en opslagrichtlijnen. Dit voorkomt informatieverlies en waarborgt dat logs beschikbaar blijven voor forensisch onderzoek, incidentanalyse en compliance-doeleinden.

De volgende bewaartermijnen zijn van toepassing:

* Standaard logging: minimaal 30 tot 90 dagen, afhankelijk van type systeem en de operationele noodzaak.
* Security logging: minimaal 180 dagen tot 1 jaar, afgestemd op de risicoanalyse en het detectievenster voor beveilgingsincidenten.
* Compliance logging: bewaartermijn wordt bepaald op basis van toepasselijke wet- en regelgeving of subsidievoorwaarden. Als geen wettelijke verplichtingen gelden, hanteren we een termijn van minimaal 1 jaar, mits onderbouwd.

Logbestanden worden initieel lokaal opgeslagen voor een minimumperiode van 28 dagen. Na deze periode mogen ze lokaal worden overschreven, mits de loggegevens succesvol zijn doorgestuurd naar het centrale logplatform en daar beschikbaar zijn voor verdere verwerking.

Alle loggegevens worden onveranderbaar opgeslagen met cryptografische technieken, zoals hashing en digitale handtekeningen, conform onze ‘Standaard Cryptografie’. Logrotatie en compressie worden toegepast om opslag efficiënt te beheren en gegevensverlies te voorkomen.

# Monitoring en detectie

Monitoring van loggegevens is belangrijk voor het tijdig detecteren van afwijkingen en beveiligingsincidenten. Door logs centraal te analyseren en correlaties toe te passen, kunnen dreigingen vroegtijdig worden gesignaleerd en mitigatiemaatregelen worden getroffen.

## Monitoringstrategie

Een effectieve monitoringstrategie combineert real-time detectie met periodieke controles om afwijkingen en bedreigingen tijdig te signaleren. Door middel van geautomatiseerde analyses en correlaties binnen SIEM-systemen (Security Incident & Event Management) kunnen verdachte activiteiten worden opgespoord en geëscaleerd. Monitoring moet afgestemd zijn op het risicoprofiel en het belang van systemen voor de continuïteit van de dienstverlening.

* Real-time monitoring via SIEM-systemen voor kritieke systemen en beveiligingslogs.
* Periodieke monitoring via handmatige of geautomatiseerde loganalyses.
* Gebruik van AI en correlatieregels om afwijkingen te detecteren.

## Incident Detectie en Respons

Snel en accuraat reageren op beveiligingsincidenten is essentieel om schade te beperken en risico's te beheersen. Incidentdetectie moet gebaseerd zijn op vooraf vastgestelde detectieregels en drempelwaarden. Bij afwijkend gedrag worden geautomatiseerde alerts gegenereerd en geëscaleerd naar het Security Operations Center (SOC) voor verdere analyse en opvolging.

* Detectieregels en drempelwaarden worden geconfigureerd op basis van risicoanalyses (afgestemd op MITRE ATT&CK en SIGMA-regels).
* Machine Learning wordt toegepast voor afwijkingsdetectie in SIEM-platformen.
* SIEM-systemen zijn in staat geautomatiseerde correlaties uit te voeren tussen verschillende logbronnen.
* Automatische alerting bij afwijkend gedrag met escalatie naar het Security Operations Center (SOC).
* Automatische triggers en playbooks zijn ingesteld voor verdachte activiteiten (bijv. blokkeren van verdachte IP-adressen).
* Logginggegevens moeten tijdig en volledig beschikbaar zijn voor forensisch onderzoek en compliance-audits.

# Rapportage en Compliance

Om een betrouwbare en controleerbare loggingomgeving te waarborgen, zijn periodieke rapportages over loggingactiviteiten, incidenten en afwijkingen verplicht. Deze rapportages dragen bij aan de transparantie van het logbeheerproces en vormen de basis voor sturing, verantwoording en continue verbetering. Daarnaast moeten compliance-controles structureel worden uitgevoerd om naleving van wet- en regelgeving, interne richtlijnen en externe normen aantoonbaar te maken. Logging- en monitoringprocessen worden aantoonbaar periodiek geëvalueerd, waarbij afwijkingen direct aanleiding geven tot corrigerende maatregelen.

## Standaardrapportages

Regelmatige rapportages over loggingactiviteiten bieden inzicht in trends, risico’s en naleving van beveiligingsbeleid. Door standaardrapportages in te stellen, kunnen afwijkingen sneller worden geïdentificeerd en kan tijdig worden bijgestuurd. Deze rapportages ondersteunen zowel operationele monitoring als strategische besluitvorming.

De volgende rapportages worden periodiek gegenereerd:

* **Beveiligingsincidenten**:

Trends in gedetecteerde beveiligingsgebeurtenissen.

* **Authenticatiegegevens**:

Trends in mislukte loginpogingen en verdachte inlogpatronen.

* **Gebruik van beheerrechten**:

Wie heeft toegang gehad tot welke systemen.

* **Wijzigingen in configuraties**:

Kritieke systeem- en firewallwijzigingen.

* **Bewaar- en retentiecontrole**:

Controle op naleving van logbewaartermijnen.

## Security en Compliance rapportages

Security en compliance-rapportages bevatten minimaal de volgende onderdelen:

* Overzicht van gedetecteerde aanvallen (gebaseerd op detectieregels).
* Geanalyseerde trends in verdachte activiteiten.
* Beheerderstoegang en kritieke systeemwijzigingen.

## Auditing en Controles

Auditing van loggingprocessen zorgt ervoor dat loggingconfiguraties correct zijn ingericht en effectief bijdragen aan beveiliging en compliance. Periodieke controles helpen bij het identificeren van misconfiguraties, ongeoorloofde toegangspogingen en afwijkingen van de vastgestelde beleidsregels. Audits moeten gedocumenteerd worden en leiden tot concrete verbetermaatregelen.

* Interne auditteams voeren periodieke controles uit op loggingconfiguraties en incidentdetectie.
* Systeemeigenaren zijn verantwoordelijk voor de juiste implementatie en naleving van loggingrichtlijnen.
* Leveranciersmanagement borgt dat externe partijen voldoen aan de loggingvereisten.

# Evaluatie en Doorontwikkeling

Logging- en monitoringsystemen worden periodiek geëvalueerd en verbeterd op basis van inzichten uit incidenten, audits en feedback van betrokken teams. Dit draagt bij aan een continue optimalisatie van detectie- en responsstrategieën.

* Logging- en monitoringsystemen worden jaarlijks geëvalueerd en geoptimaliseerd.
* Lessons learned uit incidenten worden verwerkt in verbeterplannen.
* Feedback van stakeholders wordt gebruikt voor de verdere doorontwikkeling van loggingstrategieën.

## Periodieke test van detectiecapaciteit

Om de effectiviteit van het Security Information and Event Management (SIEM) platform en de bijbehorende detectieprocessen te waarborgen, wordt op regelmatige basis een gecontroleerde test uitgevoerd. Deze test is gericht op het aantonen dat beveiligingsgebeurtenissen correct worden gedetecteerd, geanalyseerd en opgevolgd door het Security Operations Center (SOC).

De test kan de vorm aannemen van een white team-oefening (gecontroleerde injectie van logevents of simulatie van incidenten) of een red team-aanval (gesimuleerde aanval vanuit het perspectief van een aanvaller), waarbij wordt beoordeeld of het SIEM en SOC de aanvalssignalen tijdig en correct opmerken en afhandelen.

De resultaten van deze tests worden gedocumenteerd en geëvalueerd, en leiden waar nodig tot verbetering van de detectieregels, logconfiguraties of responsprocedures. Deze test wordt minimaal eenmaal per jaar uitgevoerd of bij significante wijzigingen in de SIEM-architectuur of gebruikte detectielogica.

# Vaststelling

Deze richtlijn is aldus vastgesteld.

[Plaats], [Datum].

[NAAM]

[FUNCTIE].

[Na (her)vaststelling, ook de tabel op p.2 bijwerken]

1. Checklist Logging en Monitoring
	1. Algemene Logging vereisten

|  |  |  |  |
| --- | --- | --- | --- |
| Onderdeel | Vereiste | Ingericht | Toelichting |
| Tijdssychronisatie | Alle logs bevatten UTC-tijdstempel en worden gesynchroniseerd via NTP |  |  |
| Formaat | Logs worden opgeslagen in een gestandaardiseerd formaat (JSON, Syslog, CEF, LEEF) |  |  |
| Beveiliging | Logs zijn versleuteld conform ‘Standaard Cryptografie’ |  |  |
| Retentie | Standaard logs: 1 jaarSecurity logs: 3 – 5 jaarCompliance logs: wettelijke termijn |  |  |
| Integriteit | Onveranderbare opslag (WORM, immutable storage) |  |  |

* 1. Logging per IT-component

Authenticatie & Toegang

|  |  |  |  |
| --- | --- | --- | --- |
| IT-Component | Aanbevolen logtypes | Ingericht | Toelichting |
| Active Directory (AD) / LDAP | Succesvolle/mislukte logins, aanmaak/verwijdering accounts, privilege wijzigingen |  |  |
| Single Sign-On (SSO) / MFA | Aanmeldpogingen, afwijzingen, 2FA-succes/mislukkingen |  |  |
| VPN / RDP / SSH | Inloggen, sessie start/stop, bron-IP, locatie |  |  |
| Privileged Access Management (PAM) | Beheeracties, privilege-escalatie, toegang tot gevoelige systemen |  |  |
|  |  |  |  |

Besturingssystemen & Servers

|  |  |  |  |
| --- | --- | --- | --- |
| IT-Component | Aanbevolen logtypes | Ingericht | Toelichting |
| Windows Servers / Clients | Event logs (ID 4624, 4625, 4720, 4732), service crashes, updates |  |  |
| Linux / Unix | Syslog, CLI-logging, sudo acties, failed logins, cron jobs, kernel messages |  |  |
| Hypervisors (VMware, Hyper-V) | VM-wijzigingen, snapshots, resource-uitputting, logins  |  |  |
|  |  |  |  |

Netwerk & Beveiligingsapparatuur

|  |  |  |  |
| --- | --- | --- | --- |
| IT-Component | Aanbevolen logtypes | Ingericht | Toelichting |
| Firewalls | Inkomend/uitgaand verkeer, policy changes, blokkades, scanning attempts |  |  |
| Switches / Routers | Config-wijzigingen, ARP spoofing, STP-fouten, BGP updates |  |  |
| IDS / IPS / WAF | Aanvallen gedetecteerd, valse positieven, updates signatures |  |  |
| Access Points | Authenticatiepogingen, client-verbindingen, roaming events, systeemstatus, WIPS-events |  |  |
|  |  |  |  |

Cloud & SaaS-diensten

|  |  |  |  |
| --- | --- | --- | --- |
| IT-Component | Aanbevolen logtypes | Ingericht | Toelichting |
| Azure / AWS / GCP | IAM events, API-calls, anomalieën in netwerkverkeer |  |  |
| Microsoft 365 / Google Workspace | Inlogpogingen, e-mail forwarding rules, externe sharing |  |  |
| Cloud Storage (OneDrive, S3, SharePoint) | Bestandsdownloads, wijzigingen, toegang vanaf onbekende apparaten |  |  |
|  |  |  |  |

Applicaties & Databases

|  |  |  |  |
| --- | --- | --- | --- |
| IT-Component | Aanbevolen logtypes | Ingericht | Toelichting |
| Webapplicaties | Login attempts, mislukte invoer, wijzigingen API-sleutels |  |  |
| Databases (SQL, NoSQL) | Failed logins, queries naar gevoelige data, tabelwijzigingen |  |  |
| ERP / HRM / CRM | Toegang tot PII-gegevens, wijzigingen records, export data |  |  |
|  |  |  |  |

IoT & OT-systemen

|  |  |  |  |
| --- | --- | --- | --- |
| IT-Component | Aanbevolen logtypes | Ingericht | Toelichting |
| IoT-systemen | Firmware updates, remote toegang, sensor data wijziging |  |  |
| SCADA / ICS-systemen | Wijzigingen PLC-configuraties, ongeautoriseerde commando’s |  |  |
|  |  |  |  |

* 1. Monitoring & Detectie

|  |  |  |  |
| --- | --- | --- | --- |
| Onderdeel | Vereiste | Ingericht | Toelichting |
| SIEM-platform | Logs worden gecentraliseerd in een SIEM (Splunk, ELK, Sentinel) |  |  |
| Threat Intelligence | Gebruik van MITRE ATT&CK en SIGMA detectieregels |  |  |
| Real-time monitoring | Monitoring van verdachte activiteiten (failed logins, privilege escalatie) |  |  |
| Incident response | Alerting en automatische escalatie van kritieke security-events |  |  |
|  |  |  |  |

* 1. Auditing, Compliance & Verbetering

|  |  |  |  |
| --- | --- | --- | --- |
| Onderdeel | Vereiste | Ingericht | Toelichting |
| Regelmatige audits | Jaarlijkse review van loggingbeleid en -configuratie |  |  |
| Logvalidatie | Controleren of logs volledig en correct worden vastgelegd |  |  |
| Beheerderstraining | Logging en monitoring team krijgt periodieke training |  |  |
|  |  |  |  |
|  |  |  |  |

1. Relevante bronnen

In deze bijlage zijn verwijzingen opgenomen naar relevante bronnen en publicaties met meer informatie over logging en monitoring. Deze bronnen bieden praktische handvatten, best practices en achtergrondinformatie om logging en monitoring effectief in te richten en toe te passen binnen de organisatie.

**NCSC – Detectie in cybersecurity**

<https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/detecteren/detectie-in-cybersecurity>

**Australian Cyber Security Centre – Best practices event logging en threat detection**

<https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-monitoring/best-practices-event-logging-threat-detection>

**MITRE ATT&CK – Datasources voor detectie**

<https://attack.mitre.org/datasources>

**AIVD – Loggen en dreigingen detecteren**

<https://www.aivd.nl/actueel/nieuws/2024/08/26/de-beste-manier-om-gebeurtenissen-te-loggen-en-dreigingen-te-detecteren>

**Australian Cyber Security Centre – System monitoring algemeen**

<https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-monitoring>