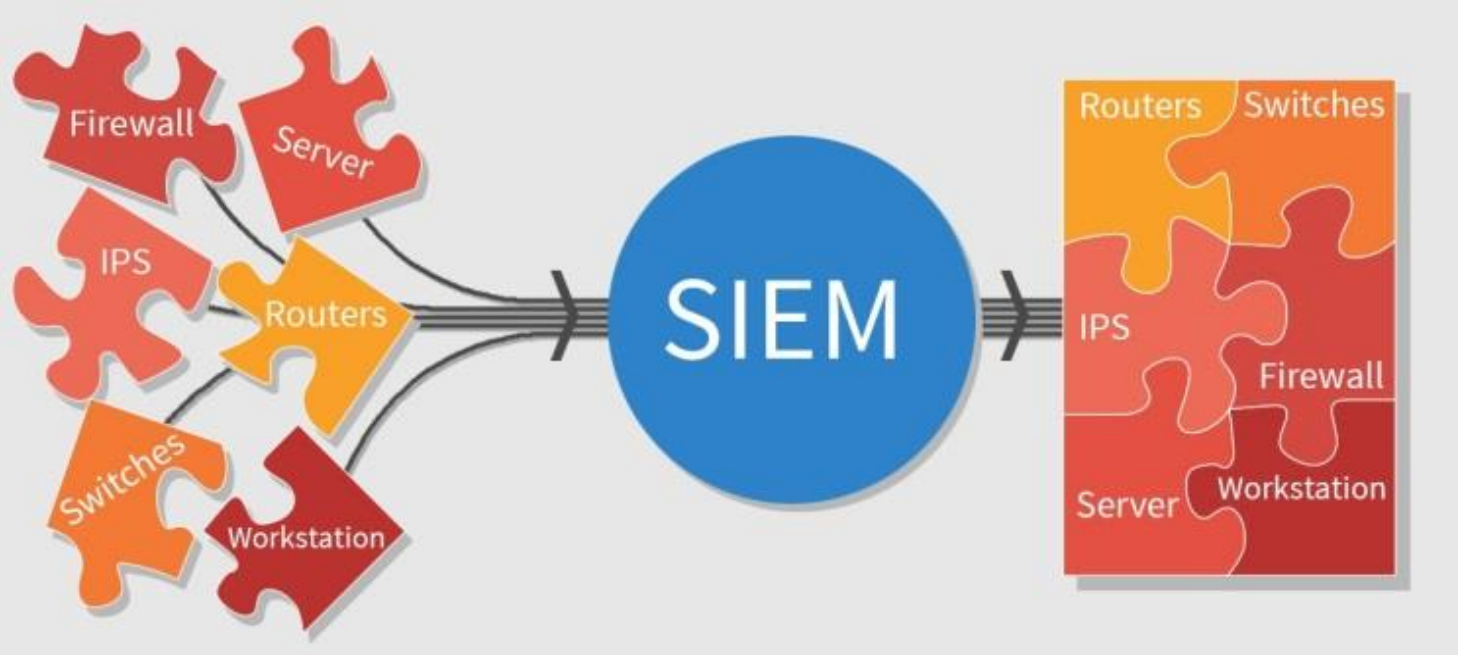

Data
Cyber Attack

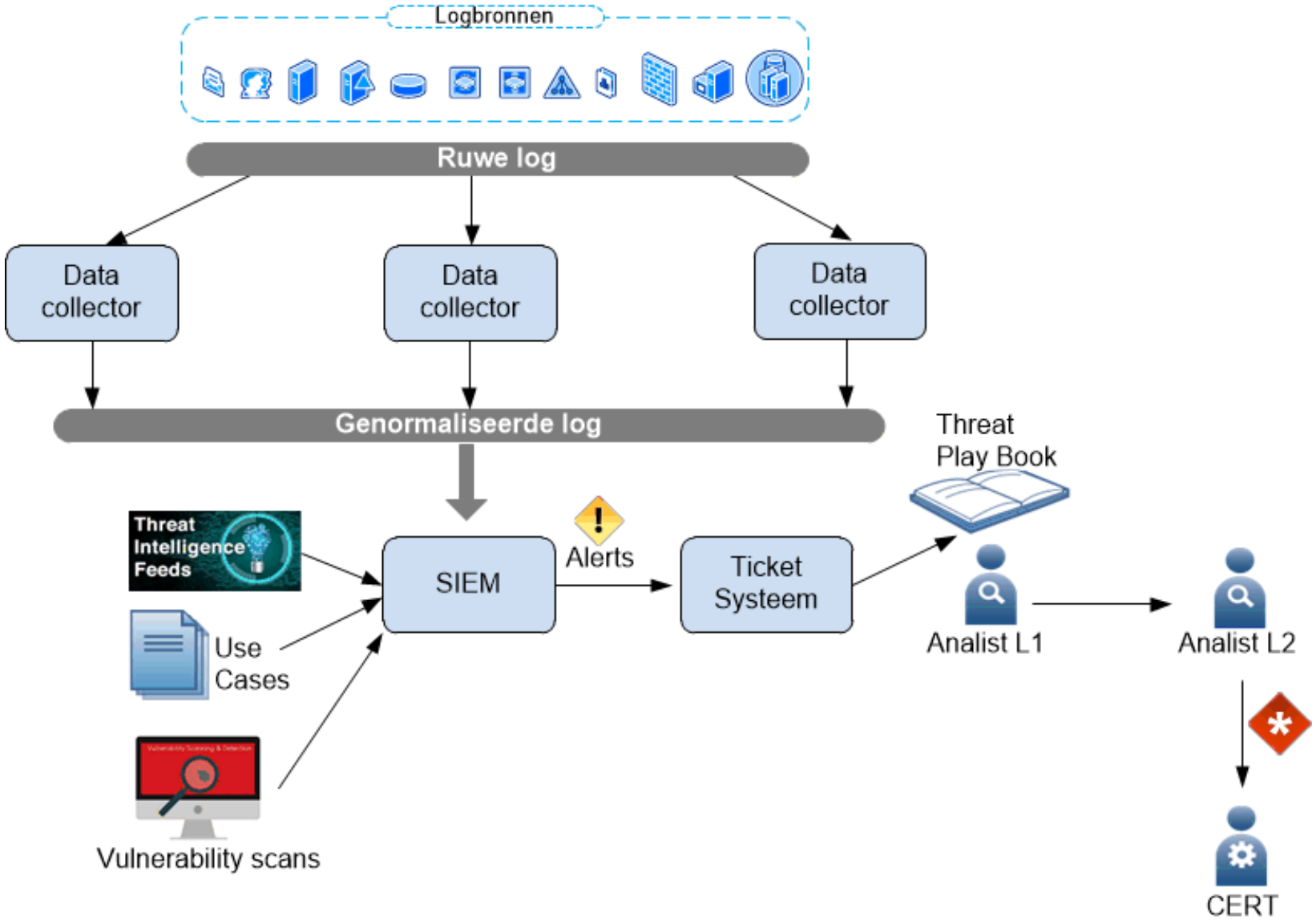
Wat is een SIEM ?

Een SIEM

Een SIEM normaliseert log data en kan d.m.v. correlaties en logica alarmen laten triggeren



Van logbron tot alarm



To SIEM or **not to SIEM**

- Een SIEM is geen oplossing voor een probleem maar een hulpmiddel om een doel te bereiken.
- Er bestaat geen standard SIEM content voor een IT infrastructuur
- Een SIEM is bedoeld voor het (near) realtime detecteren van vooraf gedefinieerde scenario's en eventueel afwijkingen op normaal gedrag. (Use cases)
- Het inrichten van een SIEM kost tijd en resources en is nooit af.
- Goede normalisatie van data is key voor een juiste werking van een SIEM
- De output van een SIEM is afhankelijk van de input, garbage in = garbage out

De output van een SIEM is afhankelijk van de input

"Garbage in, garbage out"

Your analysis is as good as your data.

To SIEM or not to SIEM

- Centraal system waar alle IT systemen en security maatregelen security logging naar toe kunnen sturen.
- Alle logdata wordt genormaliseerd tot een uniform formaat
- Correlatie mogelijk tussen verschillende typen en formaten log
- Faciliteert situational awareness
- Reduceert veel informatie tot alleen die informatie die relevant is voor security monitoring
- Heeft een running context (hoe vaak is iets gebeurd in X tijd)
- Kan real time aanvallen en afwijkend gedrag detecteren
- Maakt integratie met Threat intelligence en Ticketing mogelijk

Een veel gehoorde klacht met een SIEM is:

- We halen er niet genoeg meerwaarde uit
- Het kost te veel tijd en resources om te onderhouden / in te richten
- Het is te complex om goed in te richten
- Het is niet mogelijk om onbekende aanvallen te detecteren
- We krijgen te veel false positives
- Het sluit onvoldoende aan bij de business

Standaard dreigings scenarios

- Misbruik van autorisaties
- Verdachte authenticaties
- Ongeautoriseerde toegang
- Misbruiken van kwetsbaarheden op systemen
- Netwerk aanvallen
- Ongeautoriseerd toegang tot data
- Ongeautoriseerd Manipuleren van data en/of system instellingen
- Uitvoeren van verdachte commando’s
- Detecteren van afwijkend gedrag

We hebben een SIEM gekocht, wat nu ?

We sturen alle log data er naar toe

We zien nu wat er gebeurd op het het network

We maken rules of gebruiken standard rules/content.

Zijn we gehacked of is het een puinhoop op het netwerk?

Tijd voor housekeeping, er moet opgeruimd worden

Welke changes moeten we hiervoor aanvragen ?

Wat moet ik doen als een alarm af gaat?

HELP ik loop vast .....

We hebben een SIEM gekocht, wat nu ?

Wat betekent de informatie in de logs ?

Zijn het false positives of gaan alarmen terecht af ?

Moeten er condities uit gefilterd worden en wie weet welke ….

Wat moeten we met de output van een alarm doen ?

Welke systemen zijn kritisch ?

Is de log compleet?

- Wordt alle relevante log wel aangeleverd door het systeem?
- Loggen alle systemen naar SIEM ?

Bij wie moet ik zijn als log niet meer wordt gestuurd?


LOST
CONFUSED
UNSURE
UNCLEAR
PERPLEXED
DISORIENTED
BEWILDERED


WHAT
NOW?

Security monitoring op basis van use cases

Pak de implementatie van een SIEM gestructureerd aan en implementeer een use case methodology.

Doel van de use case methodology:

- **Gestructureerde aanpak van logmonitoring.**

  Je wilt niet alles zien, maar de slechts de belangrijke dingen.

- **Business alignement.**

  Security monitoring als meerwaarde voor de bedrijfsvoering en dienstverlening.

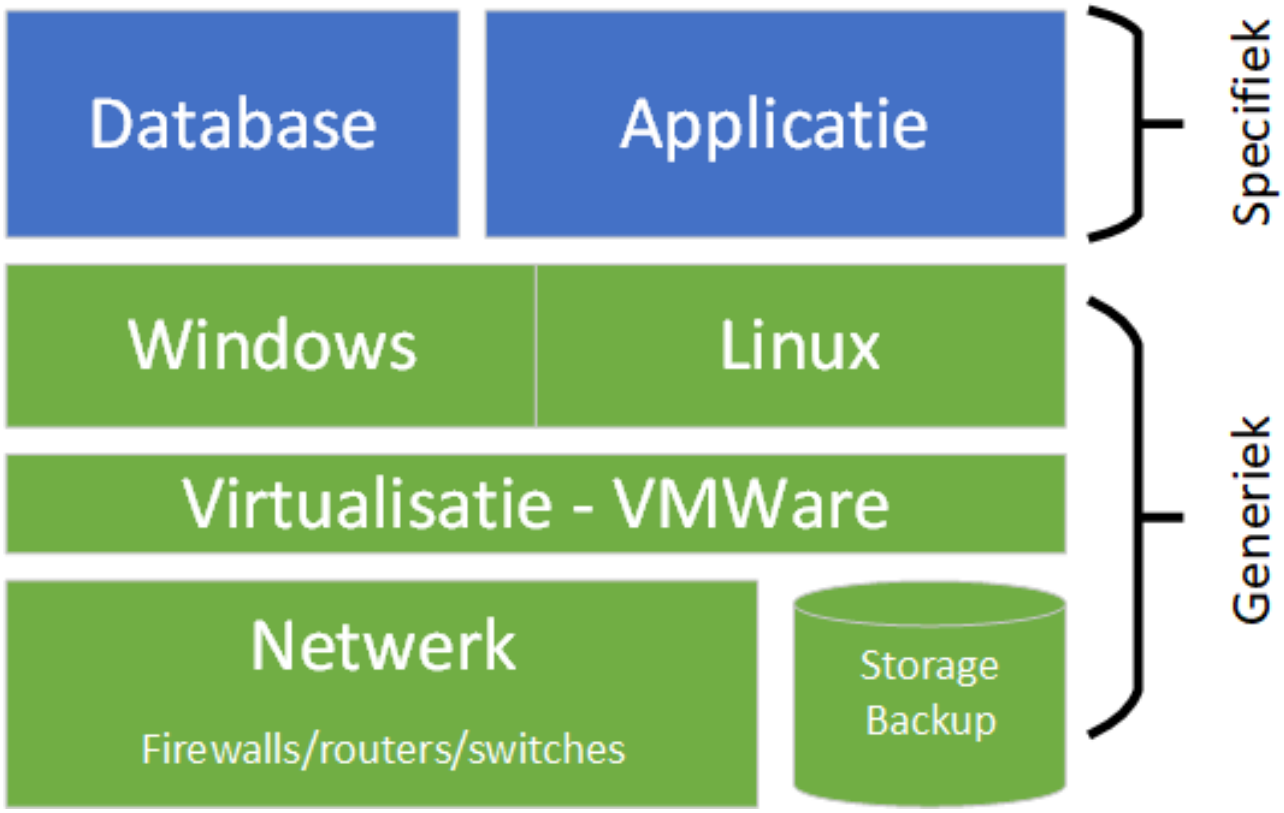
- **Het betrekken en betrokken houden van de organisatie.**

  Stakeholders geven aan wat belangrijk is en prioriteit moet krijgen en krijgen terugkoppeling over resultaten.

Definitie Use case

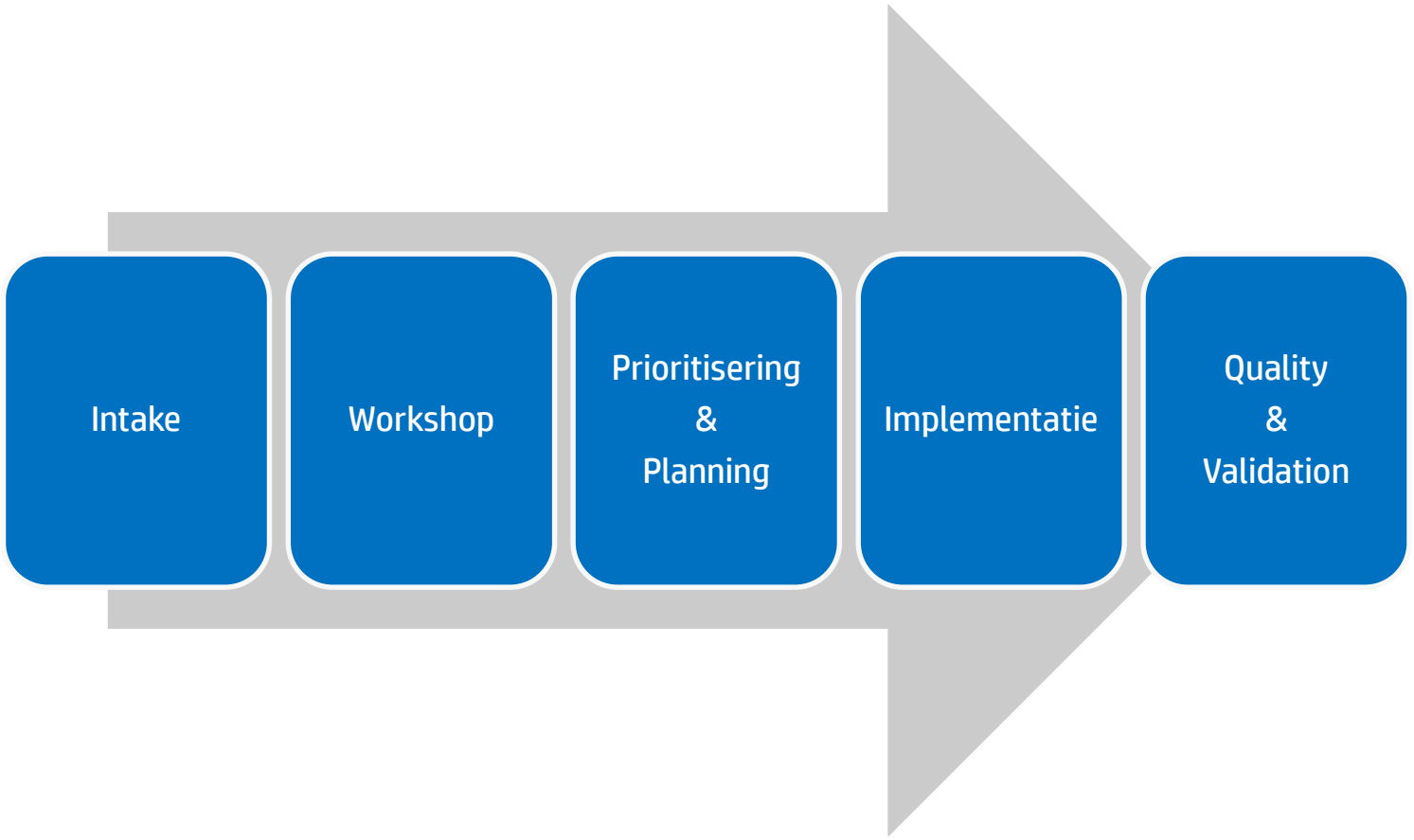
In software and systems engineering, a use case is a list of actions or event steps typically defining the interactions between a **role** (actor) and a **system** to achieve a **goal**. The actor can be a human or other external system.

En wat dan met de standaard content ??



Licht de standard use cases / content toe aan stakeholders maak een selectie en werk het Threat playbook uit.

Voorbeeld Use Case methodology



Ingrediënten Use Case

- Een overzicht met stake holder(s)
- Mandaat van stakeholders om de use case te implementeren
- Een te detecteren scenario
- Een overzicht met de logbronnen waar dit op van toepassing is
  - Overzicht met IP adressen en type logbronnen
  - De benodigde log voor het triggeren van het scenario
- Een Threat Play Book; Wat te doen als het alarm af gaat
  - Instructies voor 1e triage
  - Contact personen en instructies voor escalatie

Uitdagingen bij de implementatie

- **Onvoldoende mandaat t.b.v. implementatie.**
- **Het ontsluiten van logs**
  - **systemen loggen niet de juiste informatie**
  - **Firewalls blokkeren de log aanvoer**
  - **netwerk toegang tussen logbron en SIEM collector niet altijd mogelijk**
- **Hoe kan ik rules maken voor log die er nog niet is.**
  - **Er moeten aanvullende maatregelen worden genomen op de logbron**
  - **Er moeten audit polices gewijzigd worden wat mogelijk impact heeft op de werking**
- **Uitvoeren testplan**
  - **Testen moeten uitgevoerd worden op een acceptatie omgeving**
  - **Eenmalig genereren van test events en hergebruiken tijdens content ontwikkeling**

Definition - What does *Threat Intelligence* mean?
Threat intelligence is the analysis of internal and external threats to an organization in a systematic way. The treats that threat intelligence attempts to defend against include zero-day threats, exploits and advanced persistent threats (APTs). Threat intelligence involves in-depth analysis of both internal and external threats.
Threat intelligence is also known as cyber threat intelligence (CTI).

Threat Intelligence

- Er is een standaard formaat voor het opslaan van Threat intelligence (STIX)
- Er is ook een standaard protocol voor het uitwisselen van STIX berichten; TAXI

Deze worden gebruikt door verschillende Threat Intel Platforms. Een TIP kan interfacen met verschillende SIEM systemen en informatie uitwisselen met verschillende protocollen waaronder TAXI.

Voor de overheid wordt hier gebruik gemaakt van Eclectic IQ die gehost wordt door NCSC.

We hebben threat intelligence nodig

Maar wat is dan concreet van waarde voor een SIEM?

- IP adressen (van actors)
- Domein namen (die gebruikt worden als C&C)
- File hashes (van bestanden met bekende malware)
- URL's (die gebruikt worden voor explotatie van malware)

We hebben meer data nodig

Maar we willen ook de werkplek log analyseren, processen die worden opgestart, powershell commando's, netflow data, en meer sensors in het network.

Meer data, meer data en nog meer data

Maar dat kan allemaal niet meer in een SIEM .....

Wat nu ?

Big data

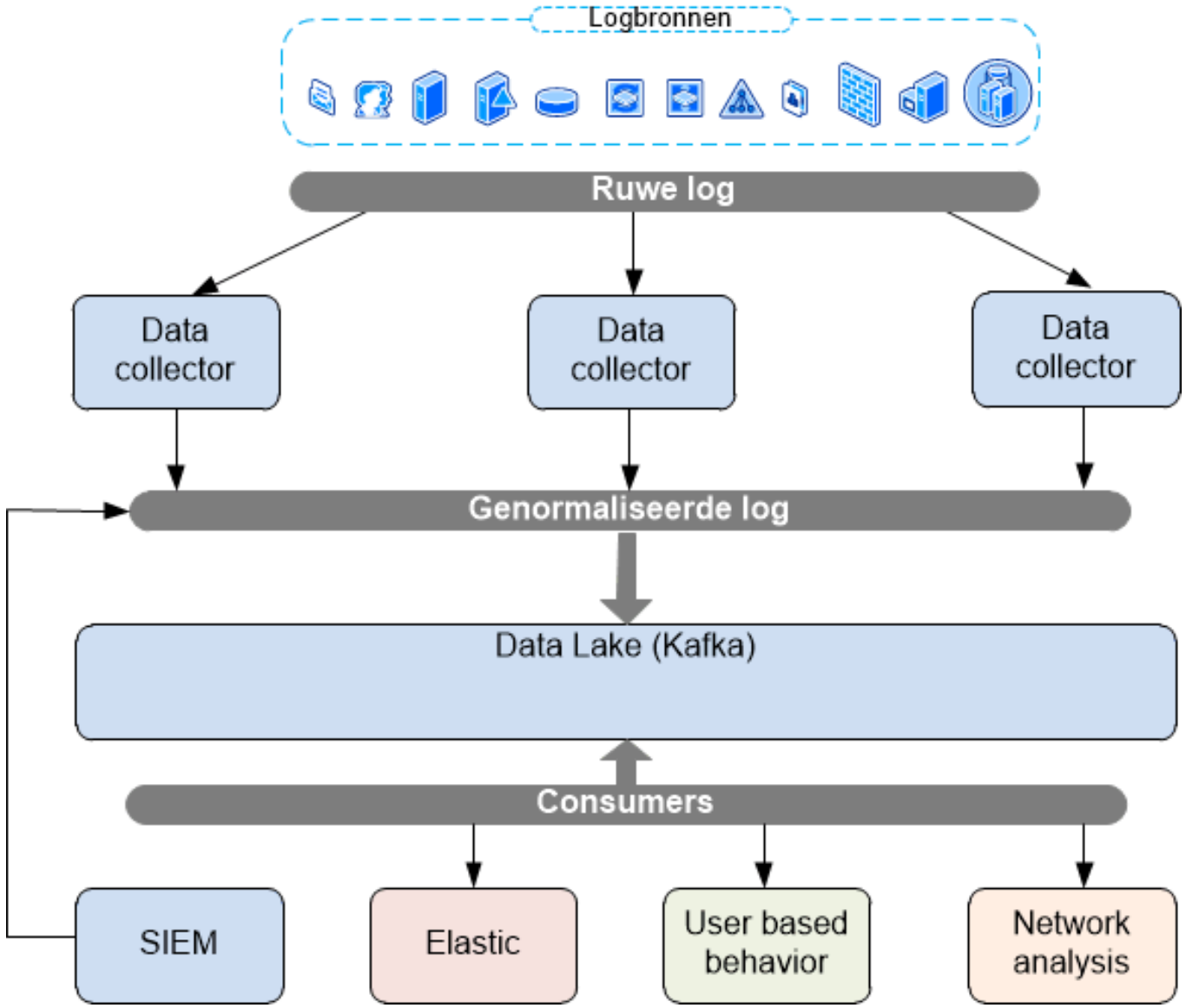
Alle data op een hoop, en nu ?

Nieuwe trend Security monitoring

Verschillende tools willen gebruik maken van dezelfde data sets.

- **SIEM**
- **Log management**
- **Netwerk analyse**
- **User based behavior**
- **Threat hunting**
- **Anomali detection / Machine Learning**
- **Forensics**

Data lake


Logbronnen
Ruwe log
Data collector
Data collector
Data collector
Genormaliseerde log
Data Lake (Kafka)
Consumers
SIEM
Elastic
User based behavior
Network analysis

Nieuwe trend Security monitoring

Data wordt meer en meer en er is behoefte aan oplossingen die beter schaalbaar zijn en waarmee het mogelijk wordt te zoeken op grotere datasets.

Ook is er naast detectie op basis van use cases (knowns) behoefte aan het detecteren van de unknowns, dit laatste wordt o.a. threat hunting genoemd waarbij gezocht wordt naar afwijkingen of verdachte activiteit op log informatie uit het verleden.

We willen dus snel kunnen zoeken

Normalisatie van log data

Om te zoeken in data is een data model nodig, dus normalisatie van log data is van essentieel belang bij het gebruik van

Zorg voor een goede normalisatie van log data die door verschillende afnemers gebruikt kan worden.

Voorbeelden hiervan zijn:

- **Common Event Format (ArcSight, Mikrofocus)**
- **Log Event Extended Format (Qradar, IBM)**
- **Custom mapping**