SIEM

Wel of niet nuttig of slimmer

7 februari 2019 – Van der Valk Utrecht

PvIB Platform voor InformatieBeveiliging

Huishoudelijke Mededelingen

Uw telefoon op stil (flightmode)

Uw evaluatie graag aanleveren via de QR-code

Uw badge aan het eind inleveren

Registratie bij binnenkomst en na afloop (voor o.a. (C)PE punten)

Volgende bijeenkomst: 12 maart ‘Hoe blijf ik goed in mijn vak’

PvIB Platform voor InformatieBeveiliging

Agenda

18:00	Ontvangst met broodjes
19:00	Opening door de dagvoorzitter
19:10	Roeland Braam, de valkuilen en best practices van SIEM
19:55	Pauze
20:25	Rob van Os, Volksbank, het MaGMa model
21:10	Paneldiscussie, SIEM wel of niet nuttig of slimmer o.l.v. Hans Teffer m.m.v. Roeland Braam, Rob van Os, Ernst Mellink en Marc de Groot
21:30	Afsluiting en borrel

PvIB Platform voor InformatieBeveiliging

Waarom een SIEM?

PvIB Platform voor InformatieBeveiliging

SIEM Taken

- Log management
- Logfile analyse
- Analyses op netwerk informatie

SIEM Nuttig?

- Helaas vaak niet!

SIEM Nuttig?

- Helaas vaak niet!
- Waarom?

SIEM Nuttig?

- Helaas vaak niet!
- Waarom?
- Out of the box functionaliteit, het moet slimmer!

PvIB Platform voor InformatieBeveiliging


BOSCH

PvIB Platform voor InformatieBeveiliging

SIEM Slimmer?

- Informatie beveiligingsbeleid is nodig !

SIEM Slimmer?

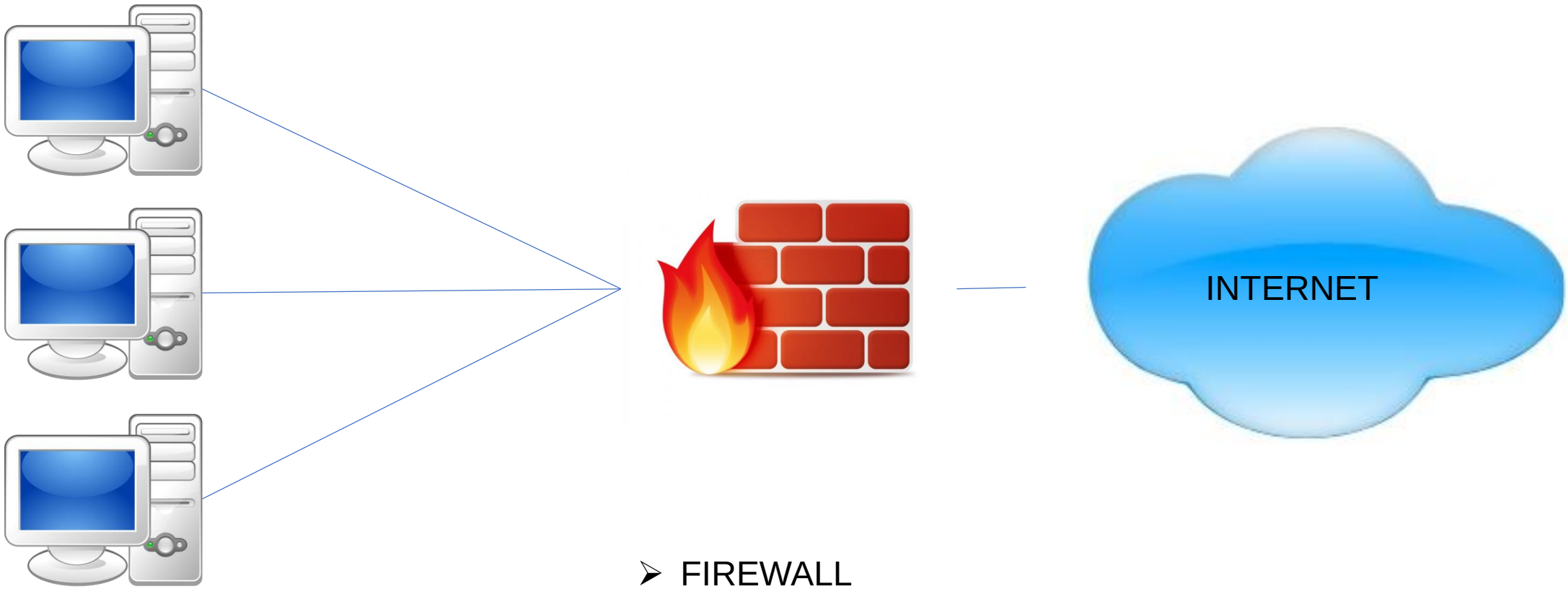
- Informatie beveiligingsbeleid is nodig !
- SIEM moet beleid ondersteunen

SIEM Slimmer?

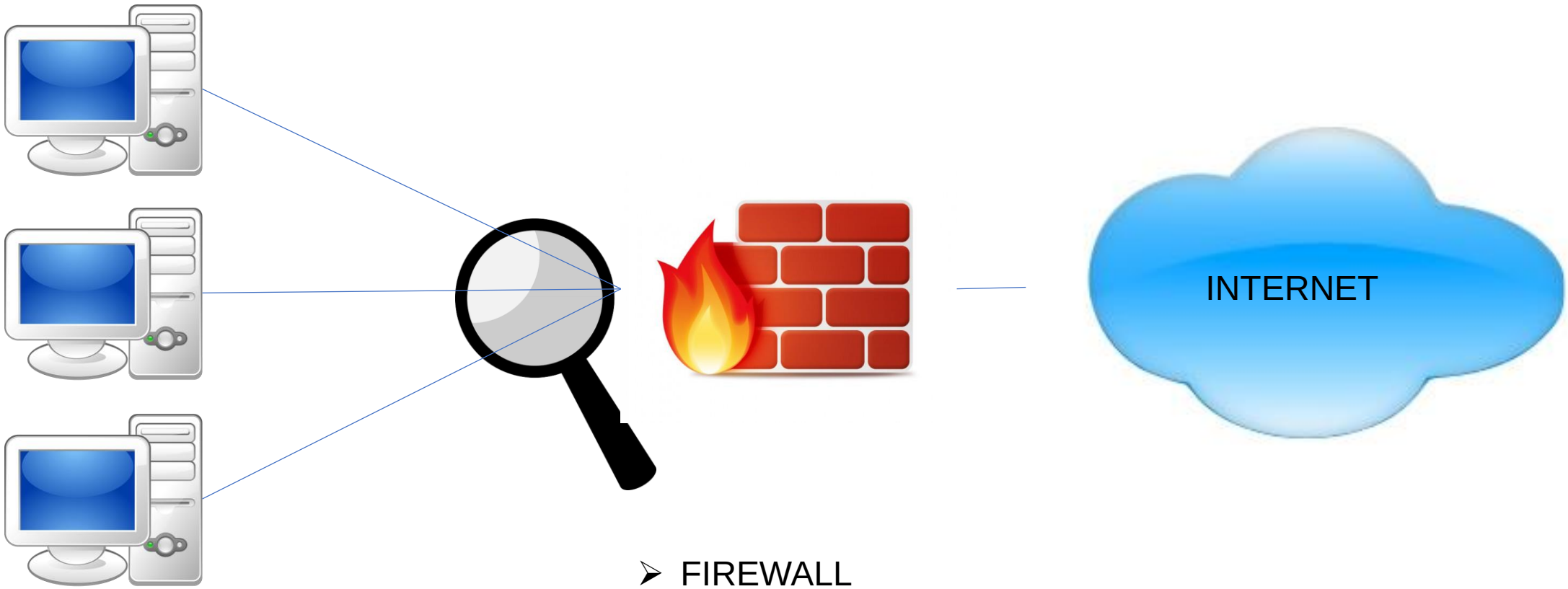
- Informatie beveiligingsbeleid is nodig !
- SIEM moet beleid ondersteunen
- Wat ga je monitoren?

SIEM Slimmer?

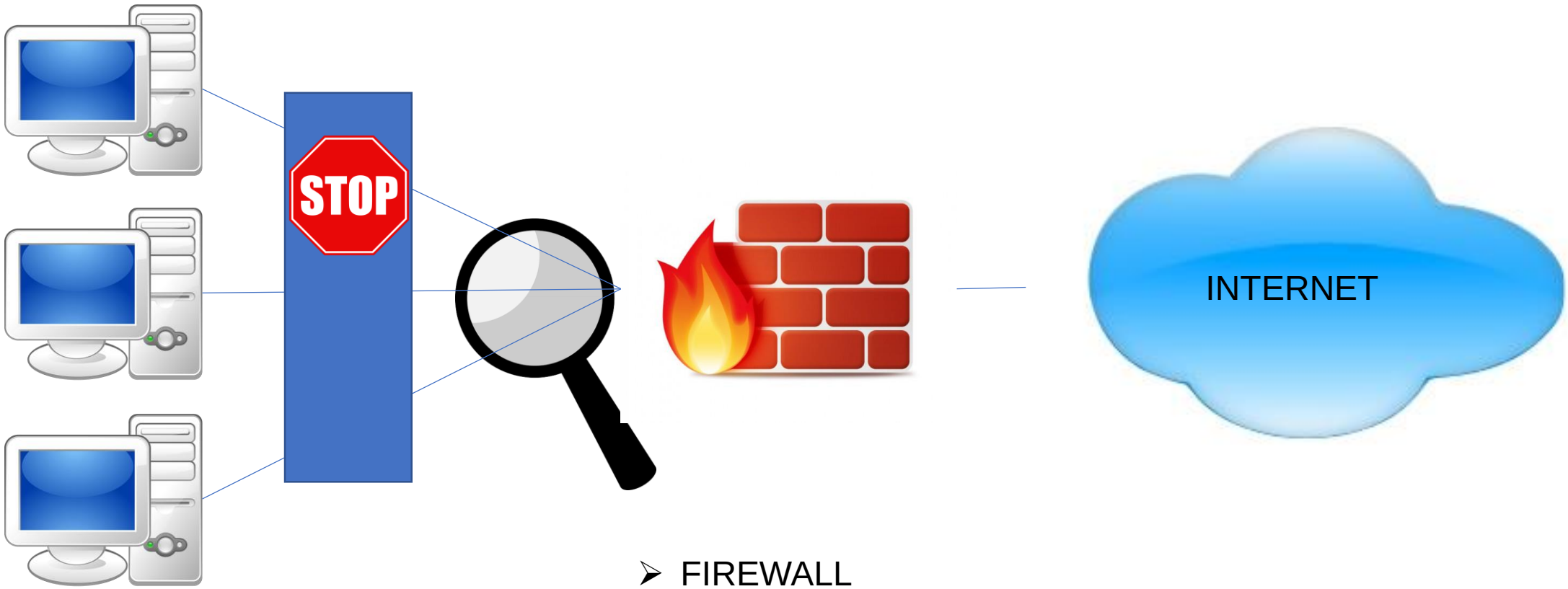
- Informatie beveiligingsbeleid is nodig !
- SIEM moet beleid ondersteunen
- Wat ga je monitoren?
- Configuration Management Database



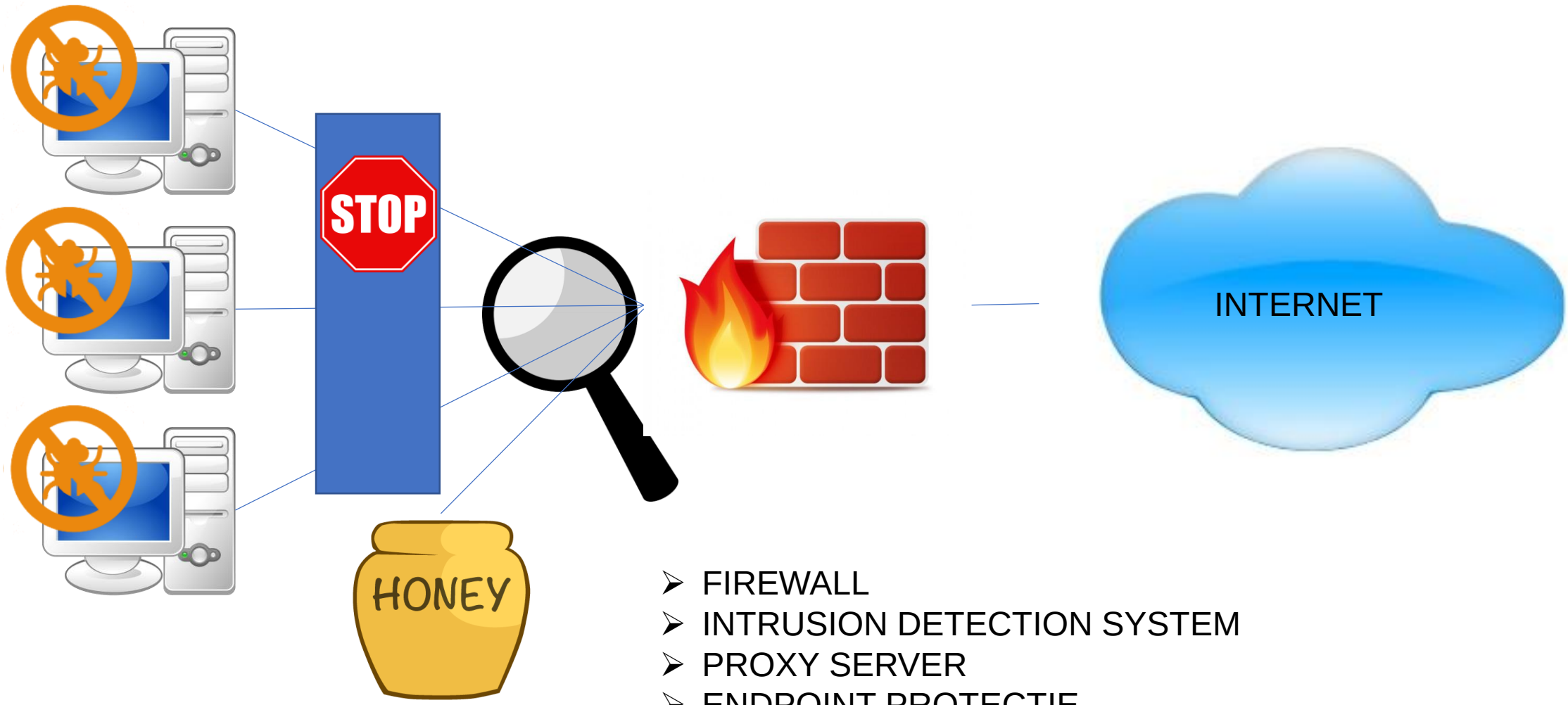
- FIREWALL



- FIREWALL
- INTRUSION DETECTION SYSTEM



- FIREWALL
- INTRUSION DETECTION SYSTEM
- PROXY SERVER



- FIREWALL
- INTRUSION DETECTION SYSTEM
- PROXY SERVER
- ENDPOINT PROTECTIE
- HONEY POT

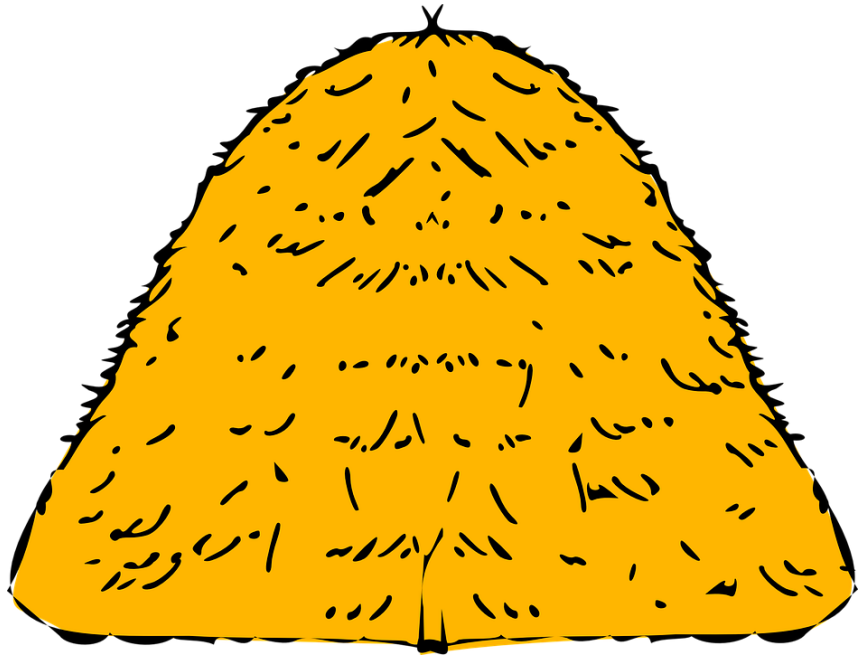
- FIREWALL
- INTRUSION DETECTION SYSTEM
- PROXY SERVER
- ENDPOINT PROTECTIE
- HONEY POT
- SIEM

PvIB Platform voor InformatieBeveiliging


© PAWS

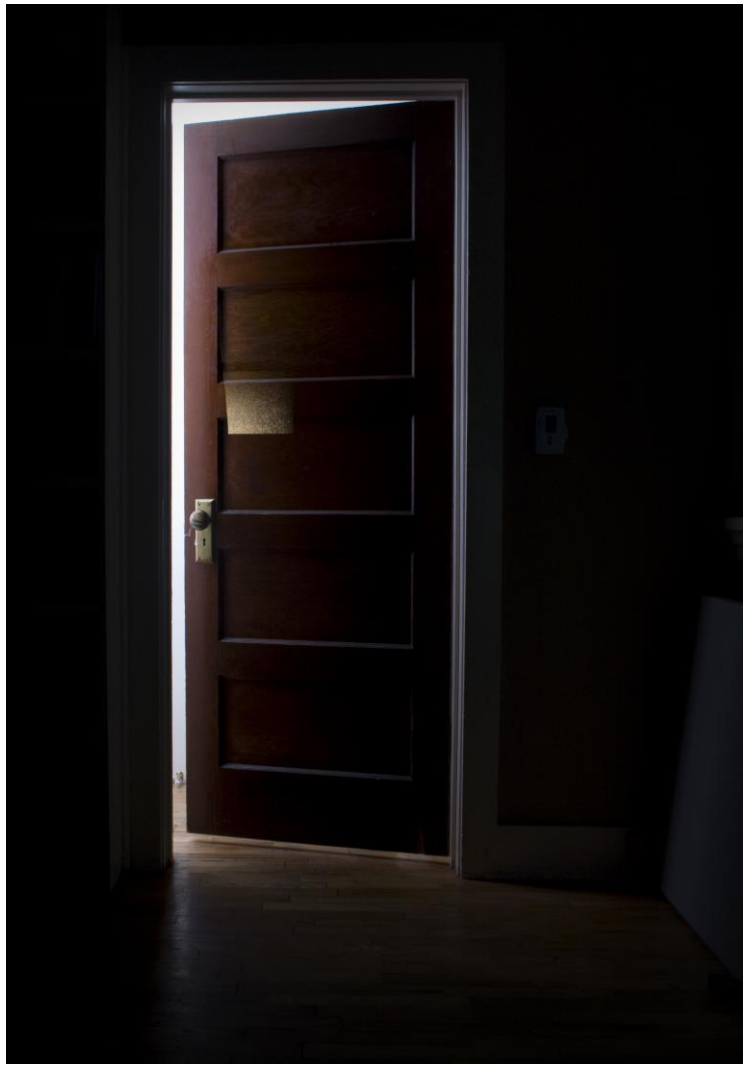
De Praktijk

- Veel false positives



De Praktijk

- Veel false positives
- Verlagen marges van detectie



PvIB Platform voor InformatieBeveiliging

De Praktijk

- Veel false positives
- Verlagen marges van detectie
- Intelligente malware / Zero day exploits

De Praktijk

- Veel false positives
- Verlagen marges van detectie
- Intelligente malware / Zero day exploits
- Management : Waarom hebben we een SIEM!

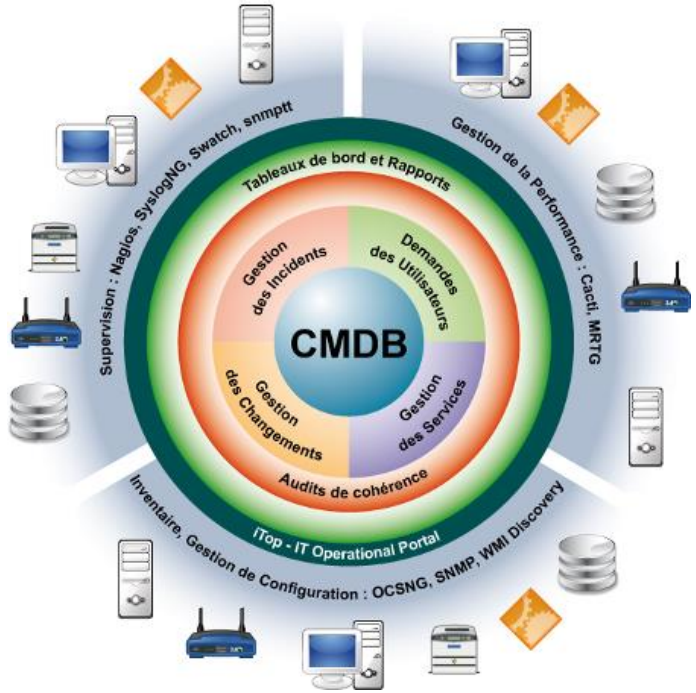
Welke aanpak?

- Risico inventarisatie

PvIB Platform voor InformatieBeveiliging

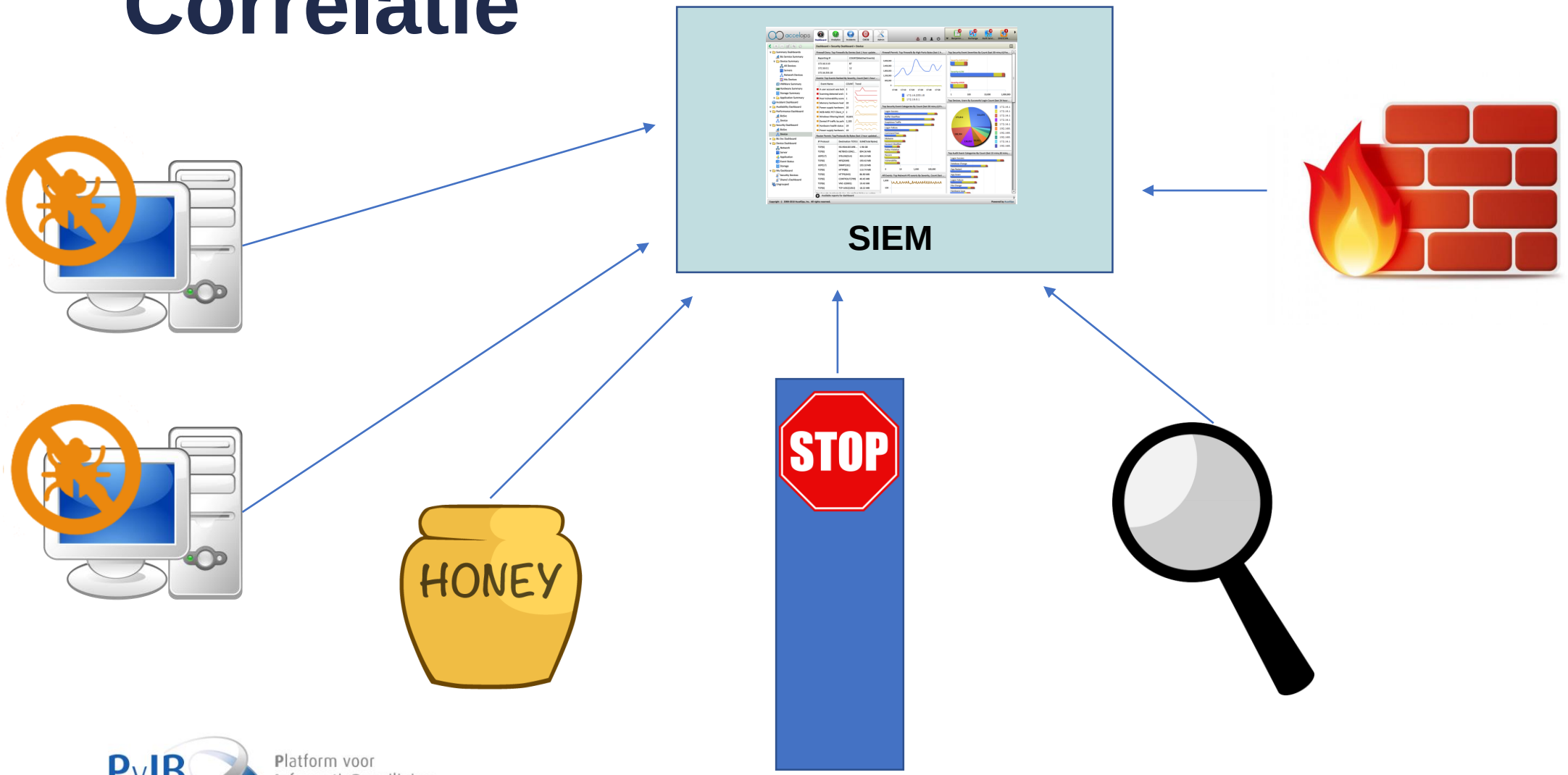
Welke aanpak?

- Risico inventarisatie
- Inventarisatie infrastructuur



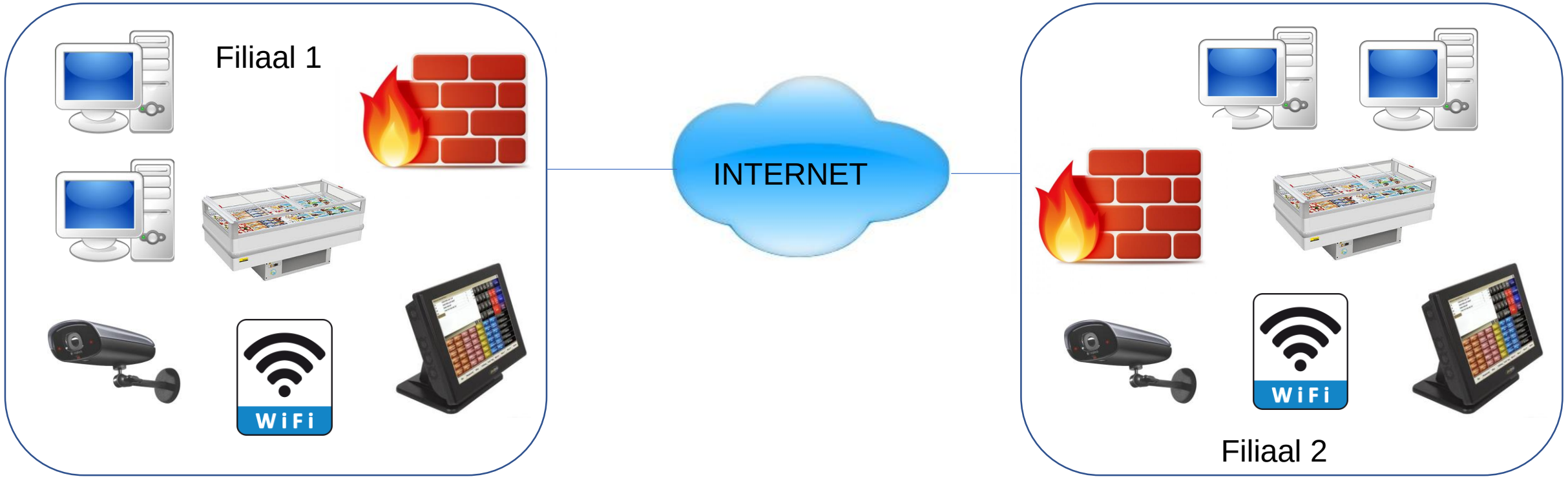
PvIB Platform voor InformatieBeveiliging

Correlatie



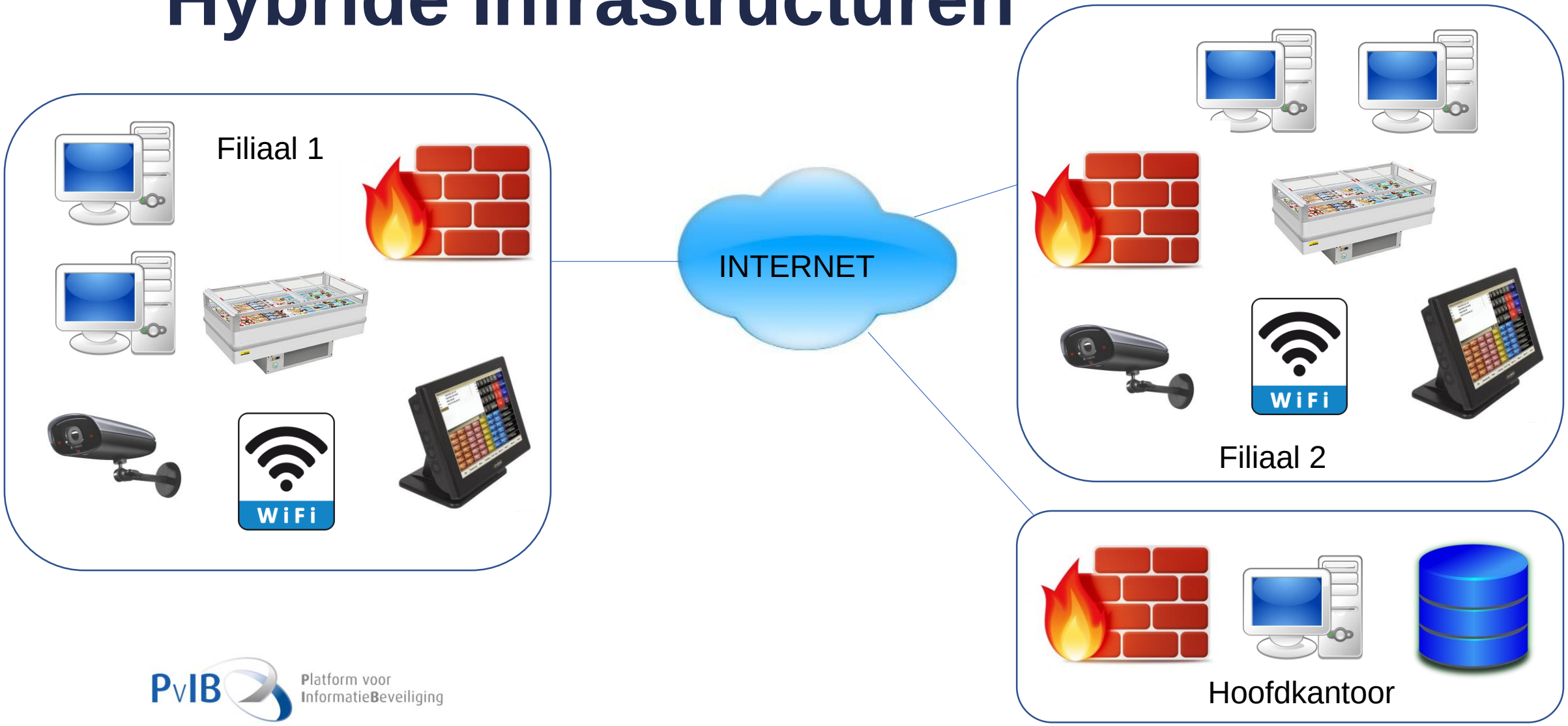
PvIB Platform voor InformatieBeveiliging

Hybride Infrastructuren



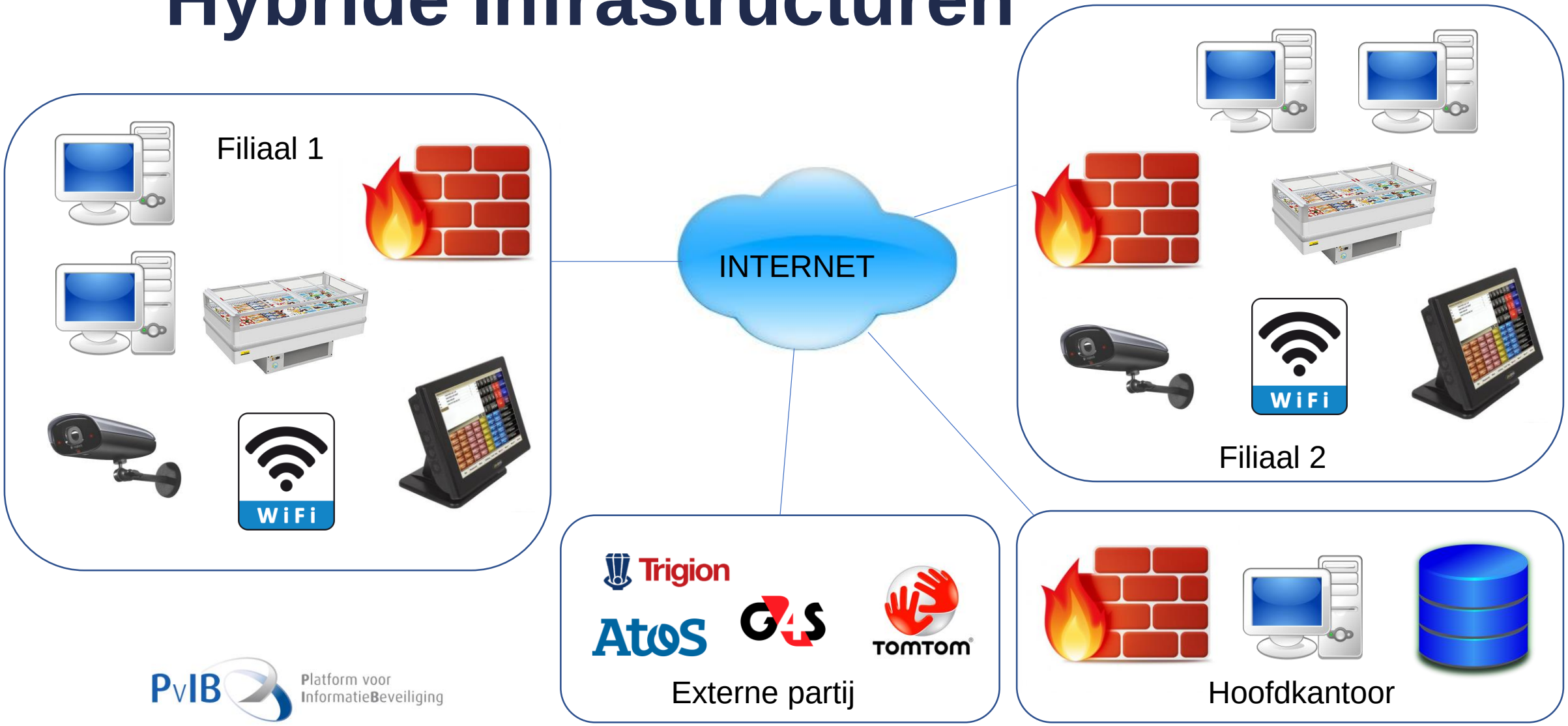
PvIB Platform voor InformatieBeveiliging

Hybride Infrastructuren



PvIB Platform voor InformatieBeveiliging

Hybride Infrastructuren



PvIB Platform voor InformatieBeveiliging

Cloud en outsourcing

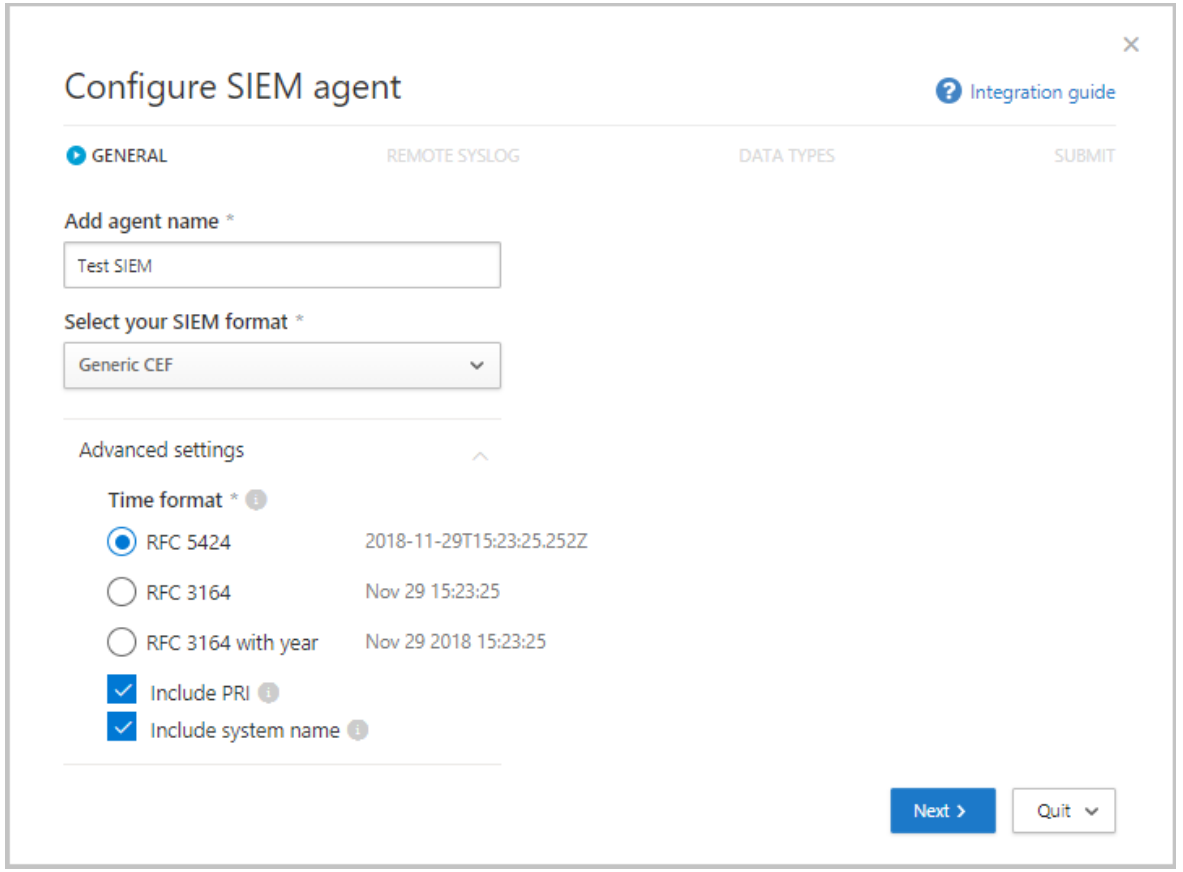
Dropbox

PeopleSoft

SAP®

PvIB Platform voor InformatieBeveiliging

Office 365 – Cloud App Security



PvIB Platform voor InformatieBeveiliging

Azure SIEM integratie

SELECT

records.ArrayValue.[Properties you want to track]

INTO

[OutputSourceName – the Power BI source]

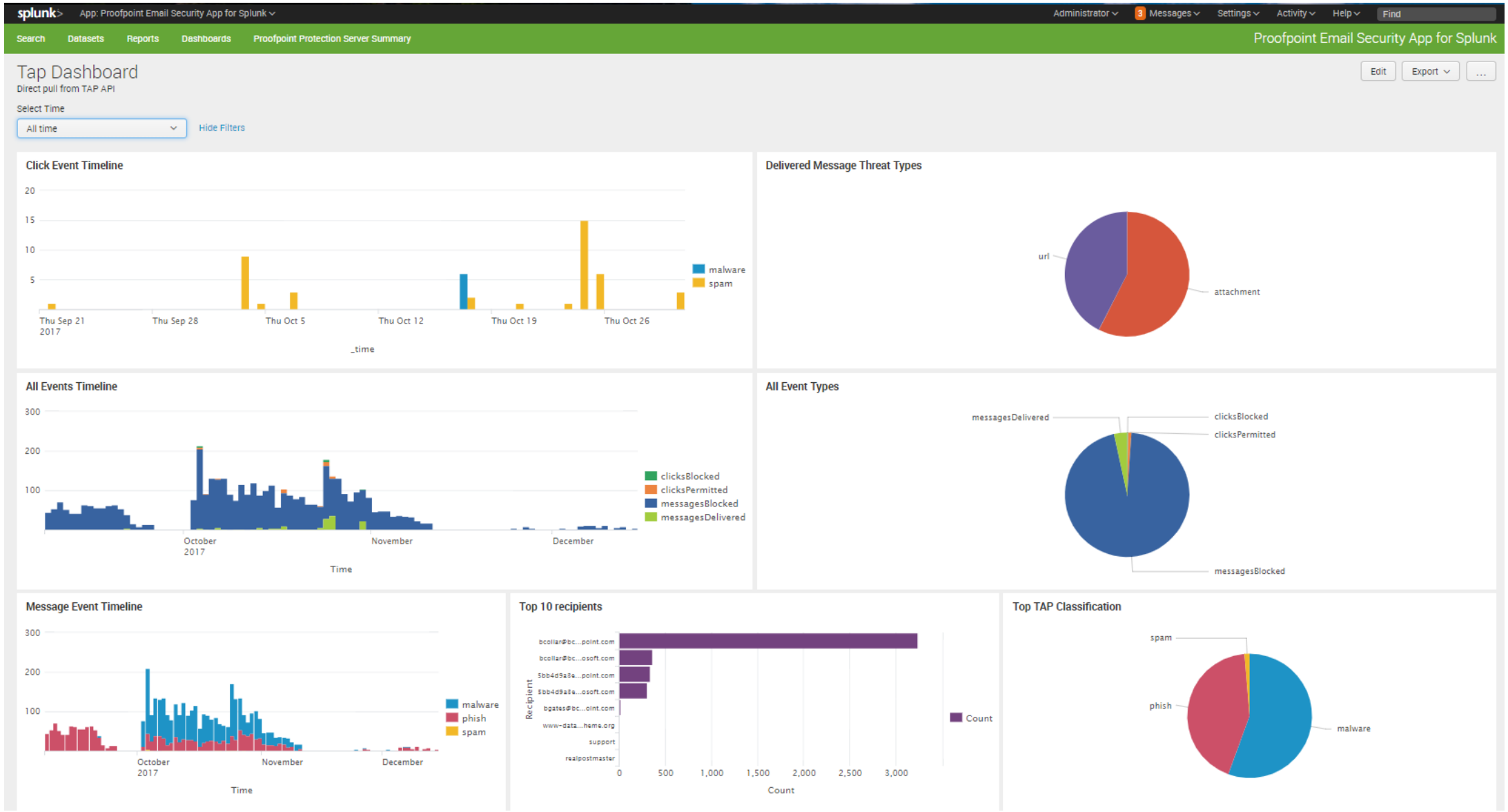
FROM

[InputSourceName] AS e

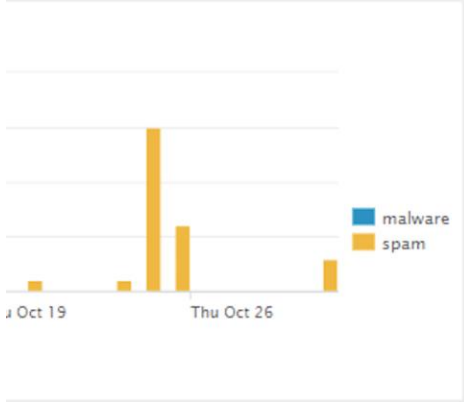
CROSS APPLY GetArrayElements(e.records) AS records

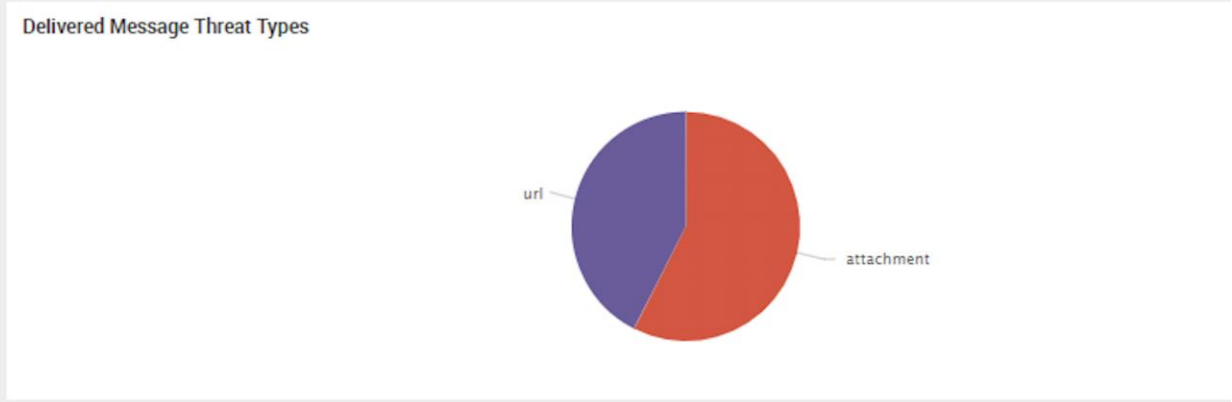
E-Mail protectie en SIEM

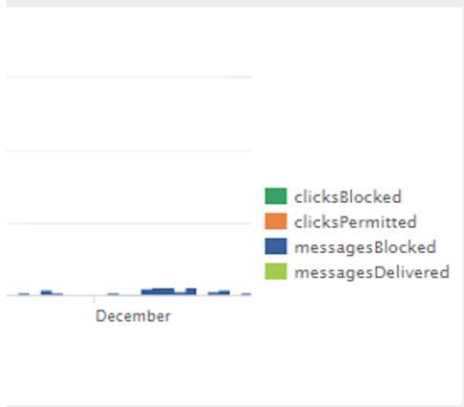
PvIB Platform voor InformatieBeveiliging

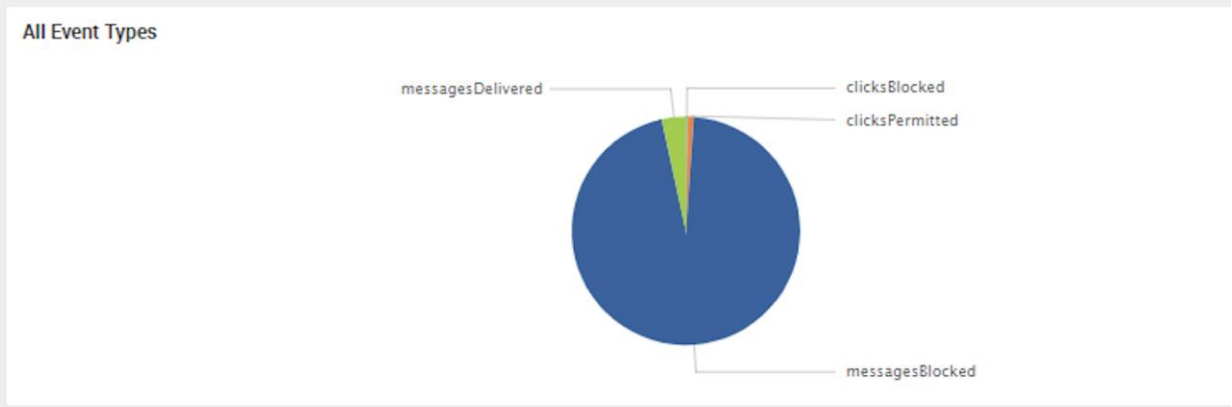


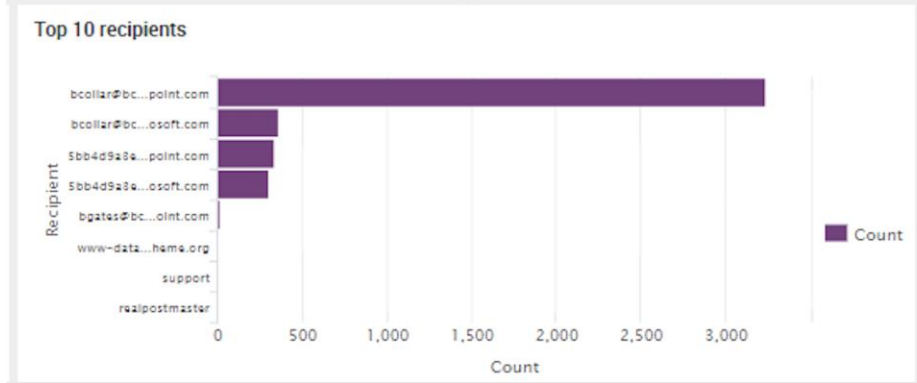
PvIB Platform voor InformatieBeveiliging

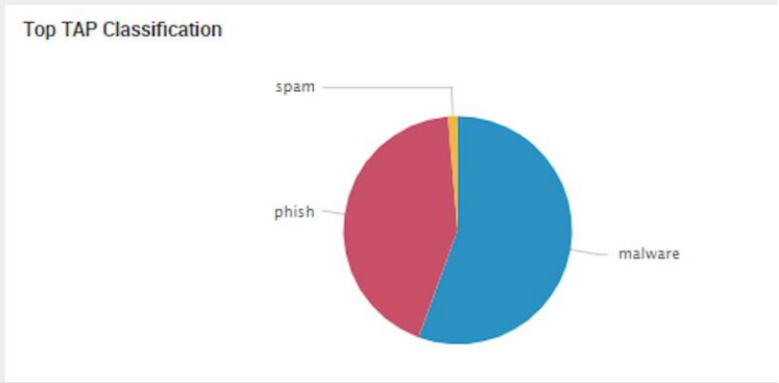






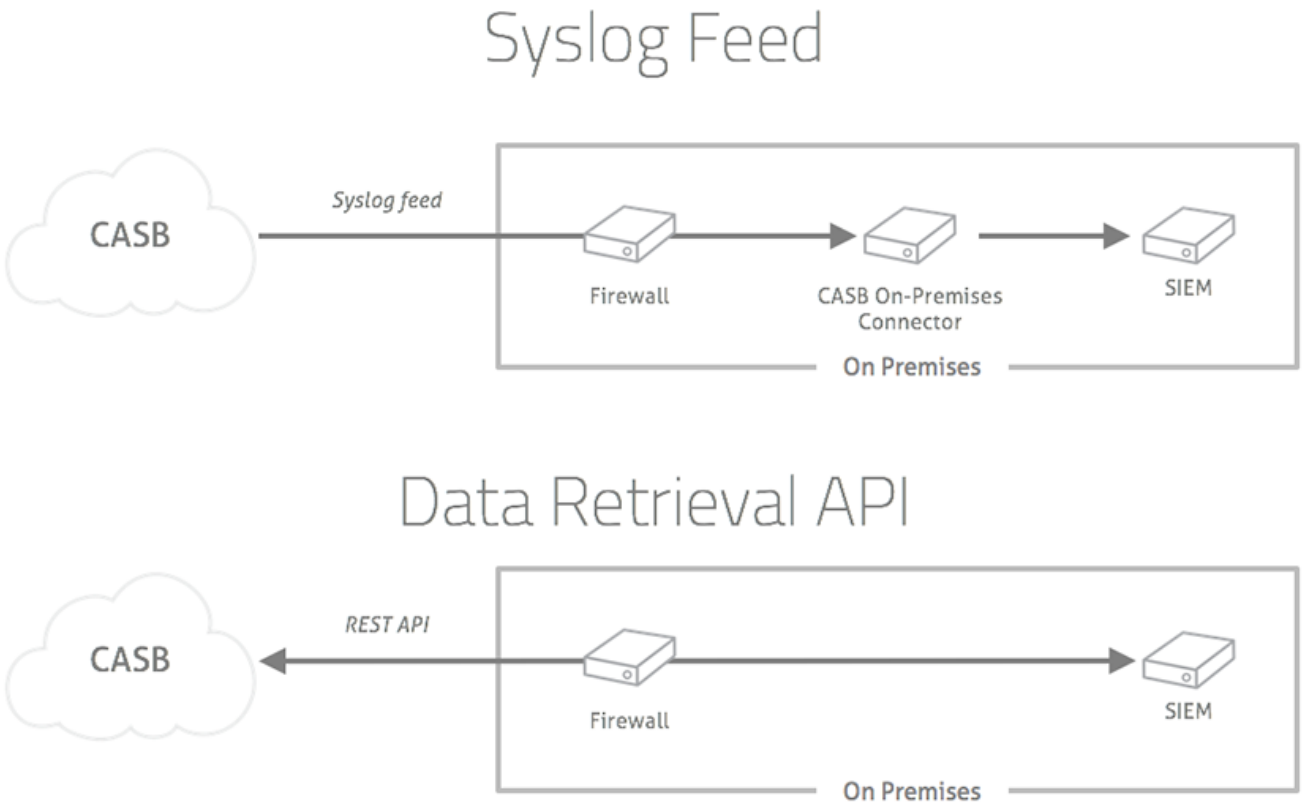






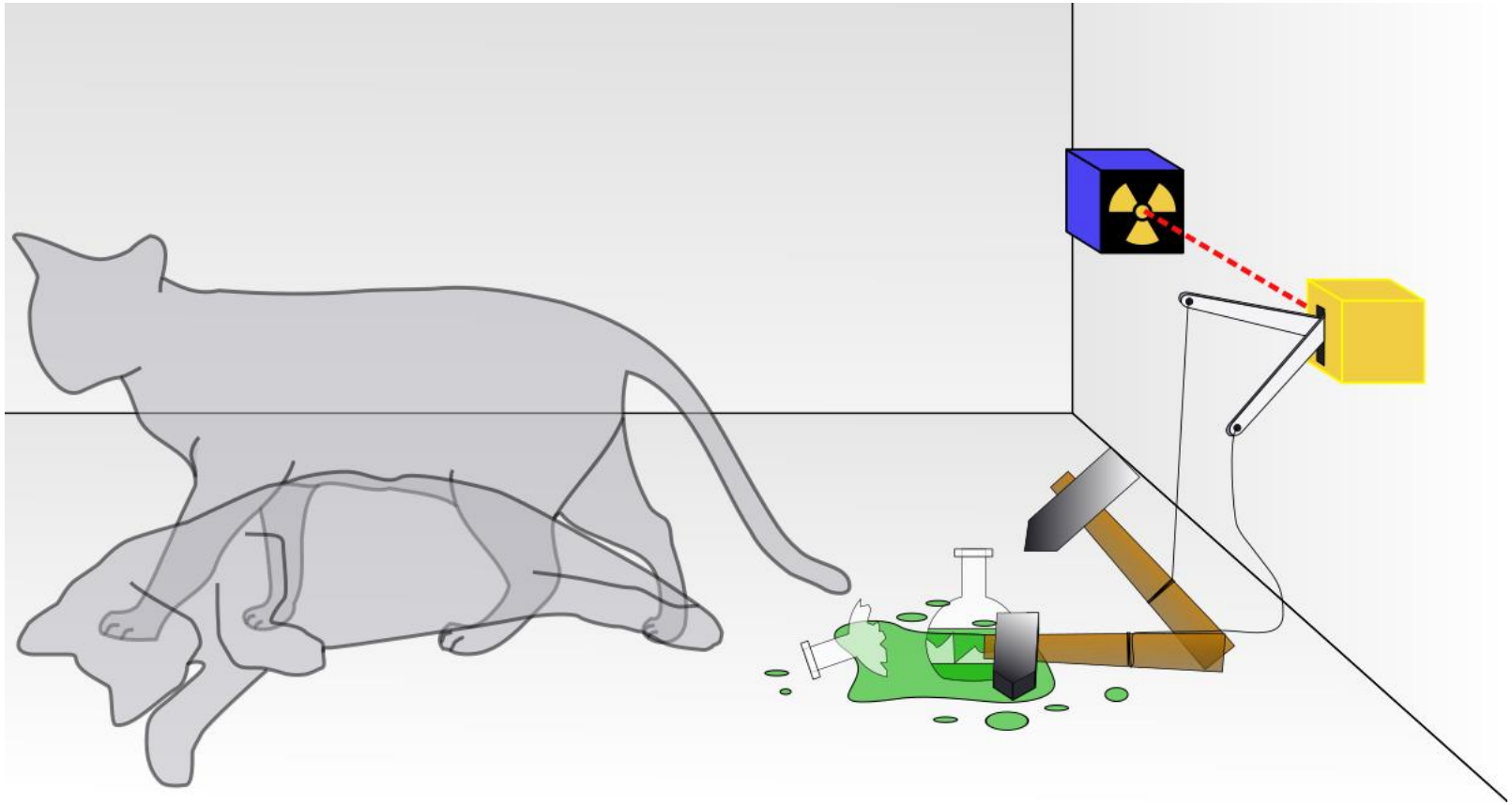
PvIB Platform voor InformatieBeveiliging

CASB – SIEM integratie



PvIB Platform voor InformatieBeveiliging

SIEM en onbekende dreigingen



Schrödinger’s kat

PvIB Platform voor InformatieBeveiliging

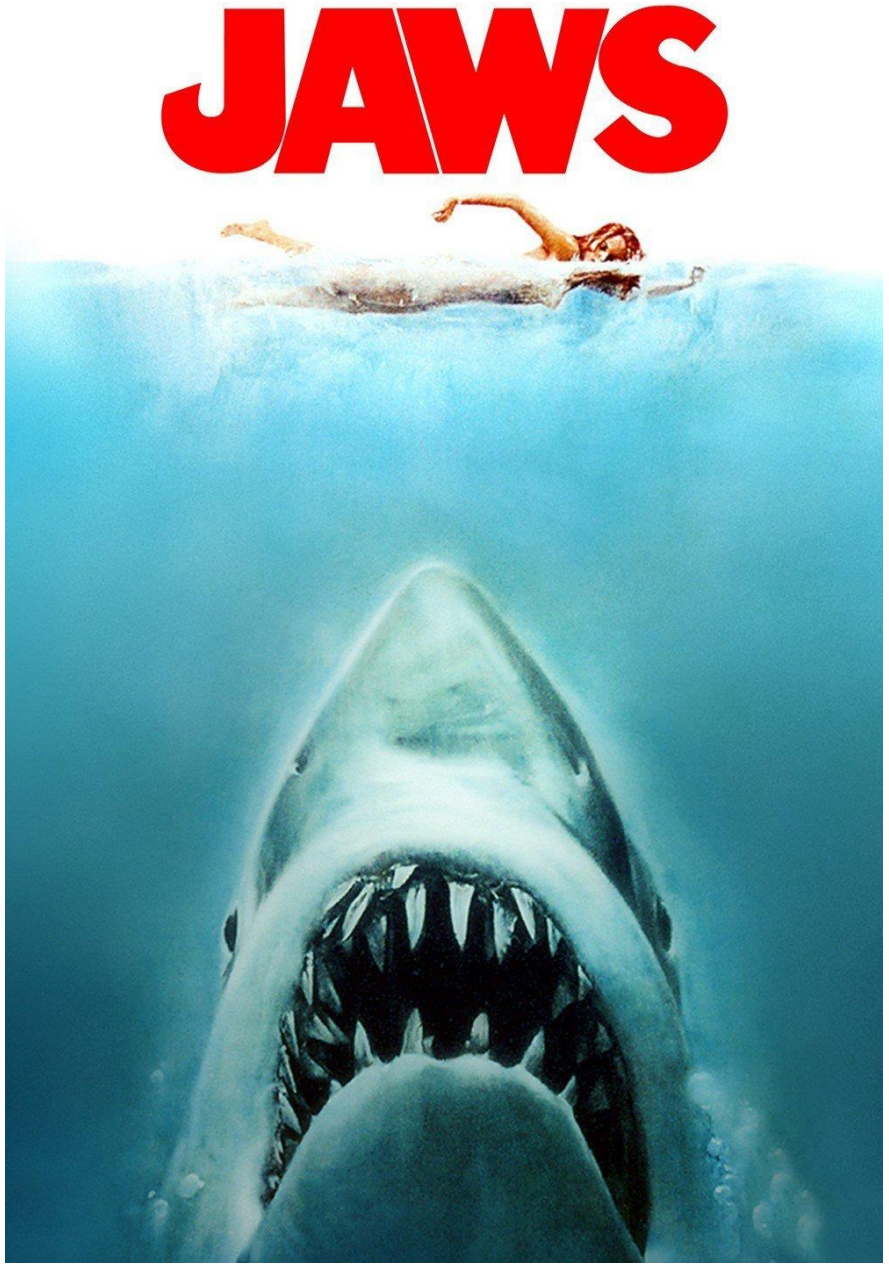
SIEM en onbekende dreigingen

PvIB Platform voor InformatieBeveiliging

SIEM en onbekende dreigingen

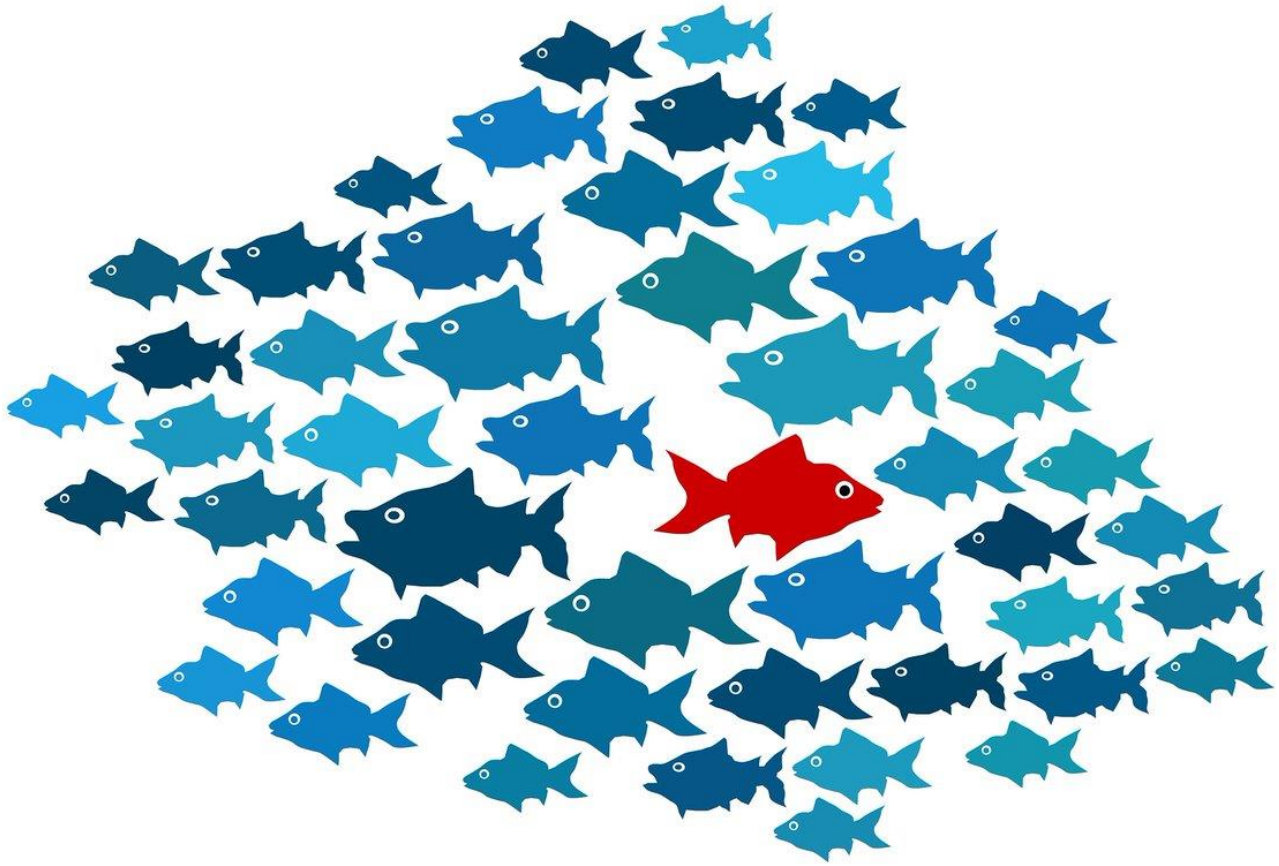
PvIB Platform voor InformatieBeveiliging

SIEM en onbekende bedreigingen



PvIB Platform voor InformatieBeveiliging

Anomaly detection

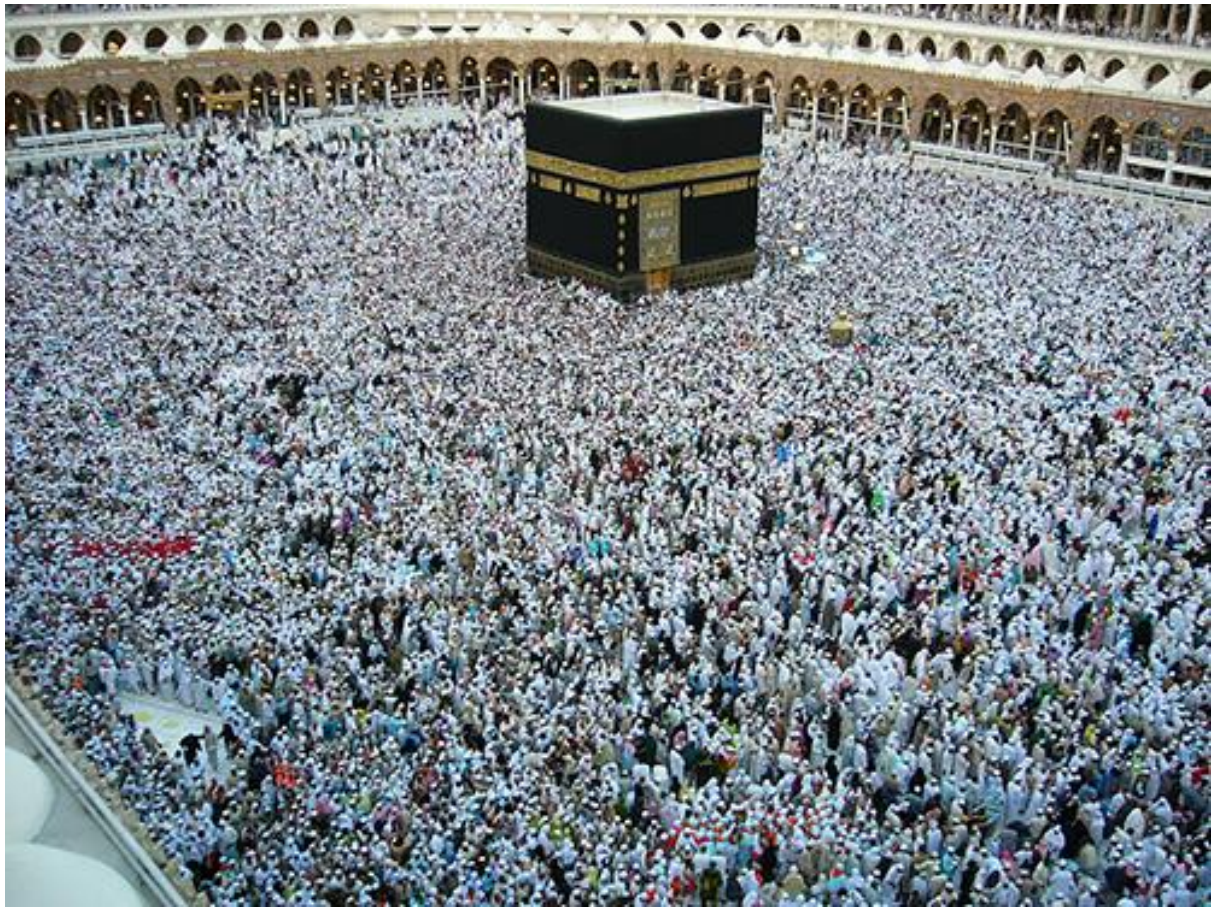


PvIB Platform voor InformatieBeveiliging

Anomaly detection

PvIB Platform voor InformatieBeveiliging

Anomaly detection



PvIB Platform voor InformatieBeveiliging

Anomaly detection