CrowdSec

bwInfoSec

Intrusion Detection / Prevention

TechTalk Reihe

bwInfoSec - Stefan Machmeier - 20.11.24

TechTalks

Ablauf

- 10 Min. - Impulsvortrag zum Thema Intrusion Detection / Prevention
- 15 Min. - Vorstellung von CrowdSec
- 10 Min. - Vorstellung Umsetzung bei bwInfoSec
- Fragerunde

Agenda
TechTalk

- Betrachtung bestehender Lösungen
- CrowdSec’s Security Engine
- Integrationsmöglichkeiten
- Live-Demo

Intrusion Detection

Definition

- Definition des BSI's
  "aktive Überwachung von Computersystemen und/oder -netzen mit dem Ziel der Erkennung von Angriffen und Missbrauch"
- Unterscheidung von **Komponenten** und **Methoden** zur Angriffserkennung
- Arten
  - NIDS
  - HIDS
  - …

Unterschied HIDS - NIDS

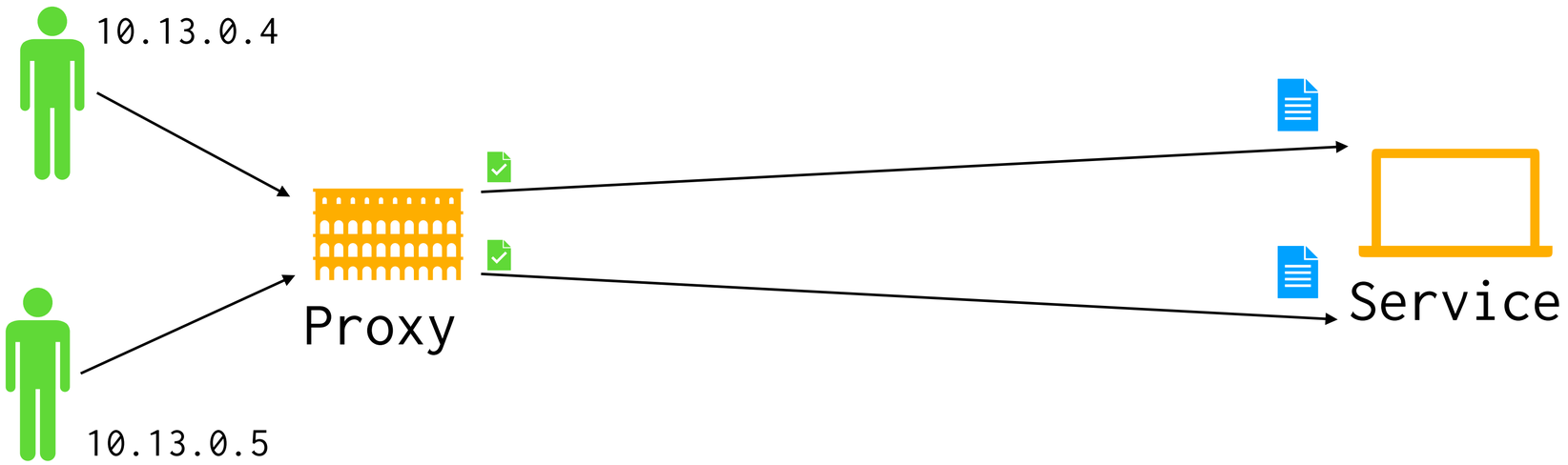
- Kurz:
  - **NIDS** überwacht **Netzwerkverkehr** und ist für die Erkennung von Angriffen geeignet, die über das Netzwerk stattfinden.
  - **HIDS** überwacht **Host-Aktivitäten** und erkennt Bedrohungen, die direkt auf einem Gerät (Host) auftreten.

Intrusion Prevention

Definition

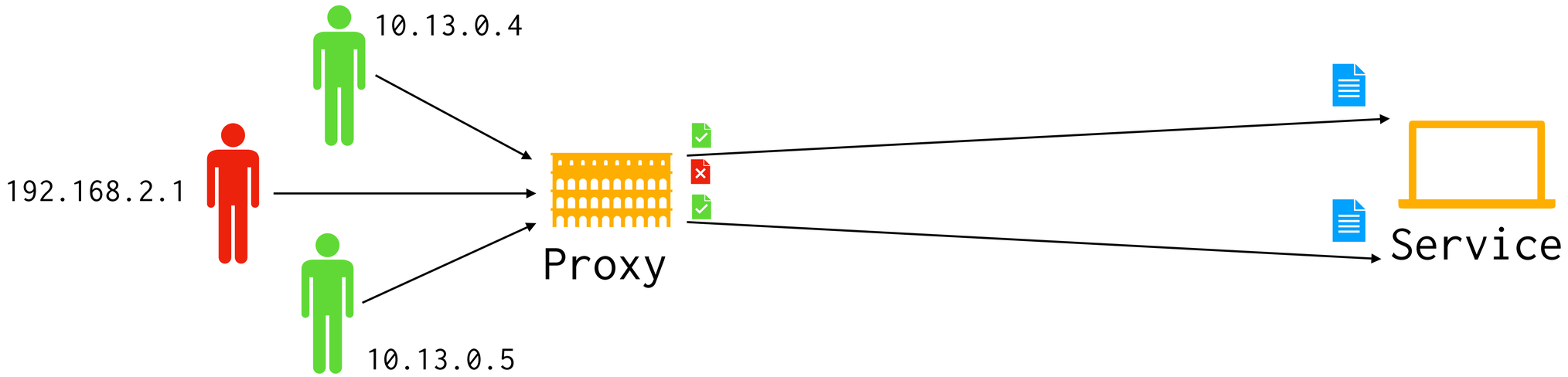
- Agiert **proaktiv**, um **Angriffe zu verhindern** oder **zu stoppen**
- **Ergreift** automatisch Maßnahmen, wie die Blockierung von Netzwerkverbindungen
- Arten
  - NIPS
  - HIPS
  - NBA IPS

Grundlage



Malicious?
http://testsite.com/index.php

Grundlage



Malicious?
http://testsite.com/index.php?arg=1; phpinfo()

Blocking durch iptables o.ä.

Betrachtung bestehender Lösungen

Blocklisten, warum?

- Bereits durch `fail2ban` eingeführt
- Umsetzung durch `iptables`, `nftables` oder in Applikationen direkt (`NGiNX`)
- Als Beispiel:
  - Suricata
  - SLIPS
  - Web Application Firewall (ModSecurity)

Suricata

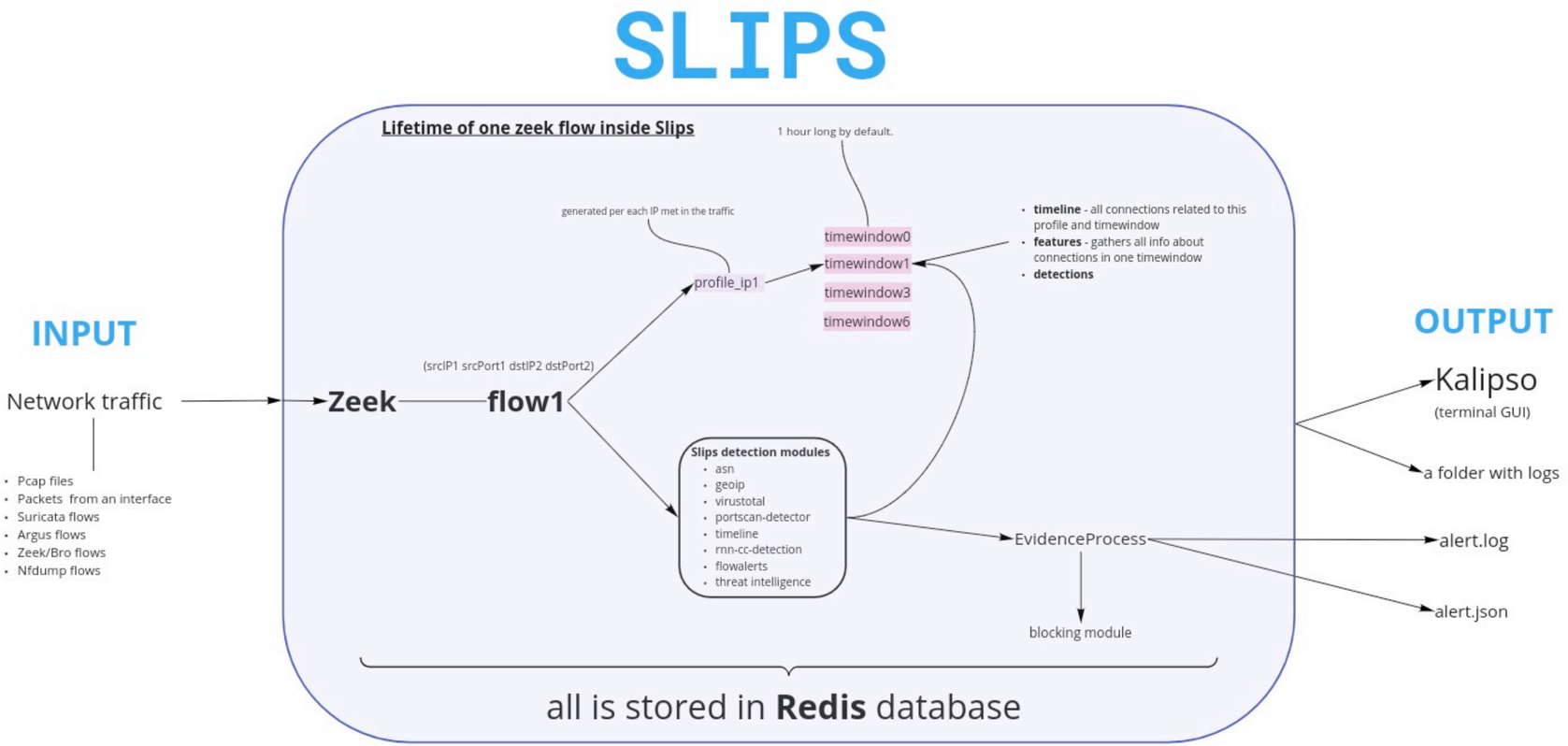
IDS / IPS Lösung

- **Signatur-basiertes** IDS / IPS
- **Netzwerk-basiert** (auch Host-basiert möglich)
- Einfach Einbindung von Regelsätzen
- Leichtgewichtig und schnelle Verarbeitung

SLIPS

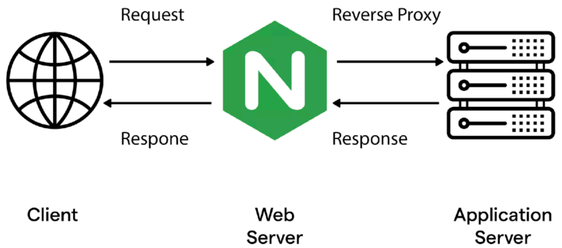
Stratosphere Labs

- Behavioural IPS
- Verwendung von
  - RNN
  - RandomForest
  - …



Web Application Firewall

- OWASP ModSecurity
- Unterstützt
  - NGiNX
  - Apache
  - OpenResty
- Einfach Integration
  https://hub.docker.com/r/owasp/modsecurity-crs/



CrowdSec

Nur ein Blockliste?

- Produkte
  - **CrowdSec Blocklist**
    Global verfügbare Blockliste
  - **CrowdSec Security Stack**
    CrowdSec’s Lösung vom Verarbeiten von Anfragen bis zum Sperren.
  - **CrowdSec Cyber Threat Intelligence**
    Threat Hunting Lösung für mehr Information zu auffälligen IPs.

CrowdSec

Nur eine Blockliste?

- Produkte
  - **CrowdSec Blocklist**
  - **CrowdSec Security Stack**
  - **CrowdSec Cyber Threat Intelligence**

Mehr Informationen
https://app.crowdsec.net/

CrowdSec

Eine einfache Blockliste?

- Nicht ganz!
  - Teilt anonym Ergebnisse (IP und verletzte Regel) mit seiner Community
  - Unterstützt *“behaviour-based detection”*
  - Unterstützt verschiedene Ebenen (OSI Schichten) zum Blockierung
- Weitere Blocklisten, Kollektionen, und mehr: https://app.crowdsec.net/

CrowdSec's Security Engine

Übersicht

- Log Source
- Engine
- CAPI
- LAPI

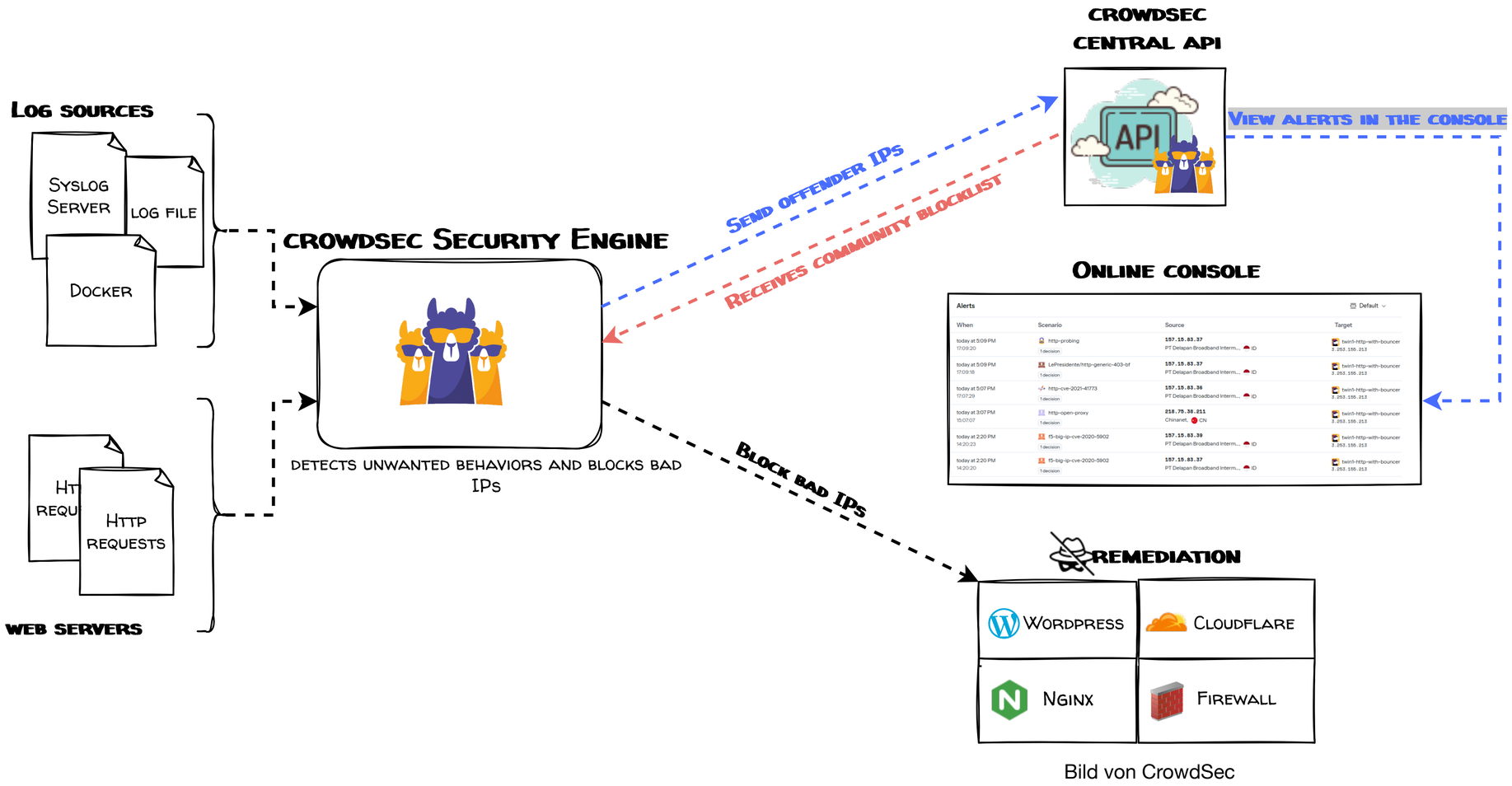


Bild von CrowdSec

CrowdSec's Security Engine

Übersicht

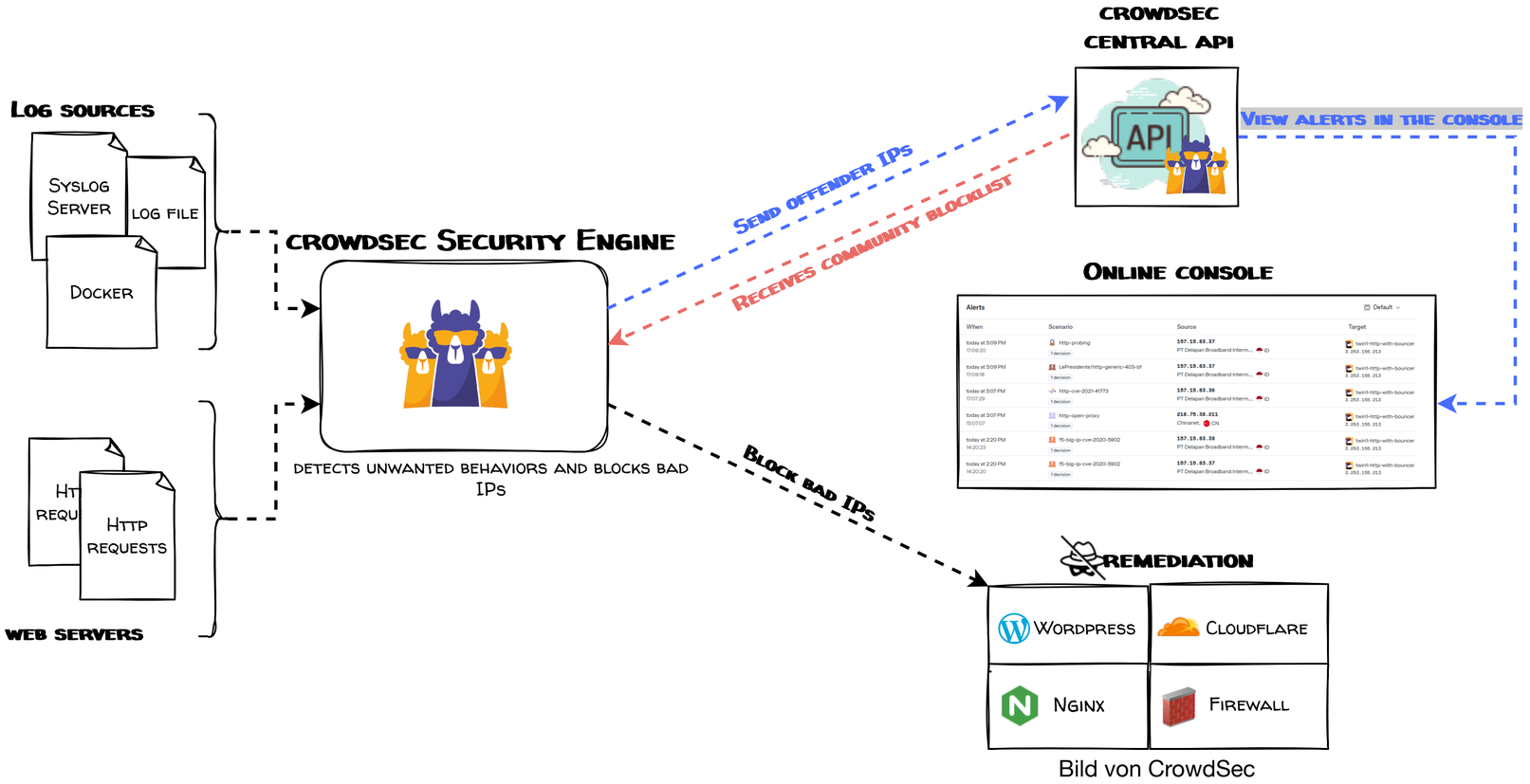


Bild von CrowdSec

Datasources → Parser → Scenario → Alert

an LAPI ← Bouncer

CrowdSec's Security Engine

Datasources

- Unterstützung verschiedener Log-Dateien
  - Docker
  - `syslogs`
  - Windows Events
  - …

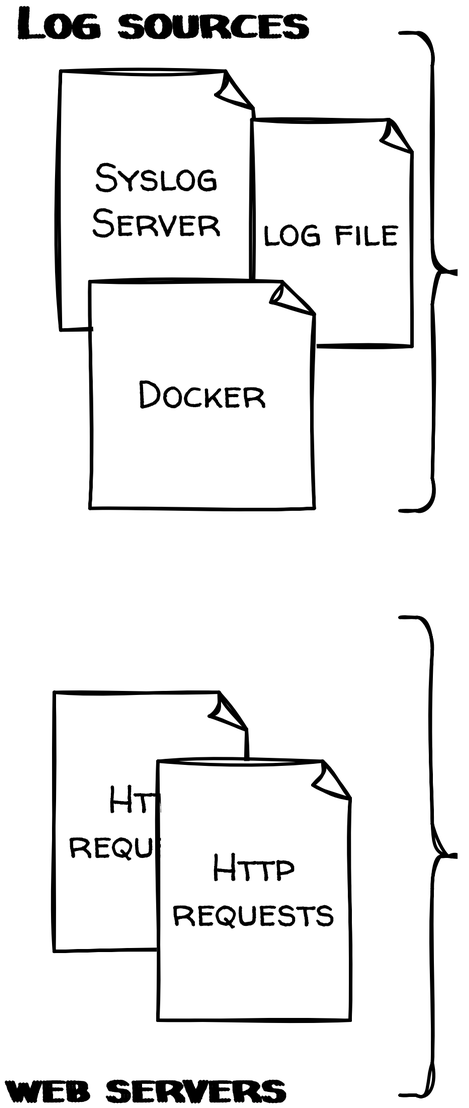


Bild von CrowdSec

CrowdSec's Security Engine

Übersicht

- Bouncer

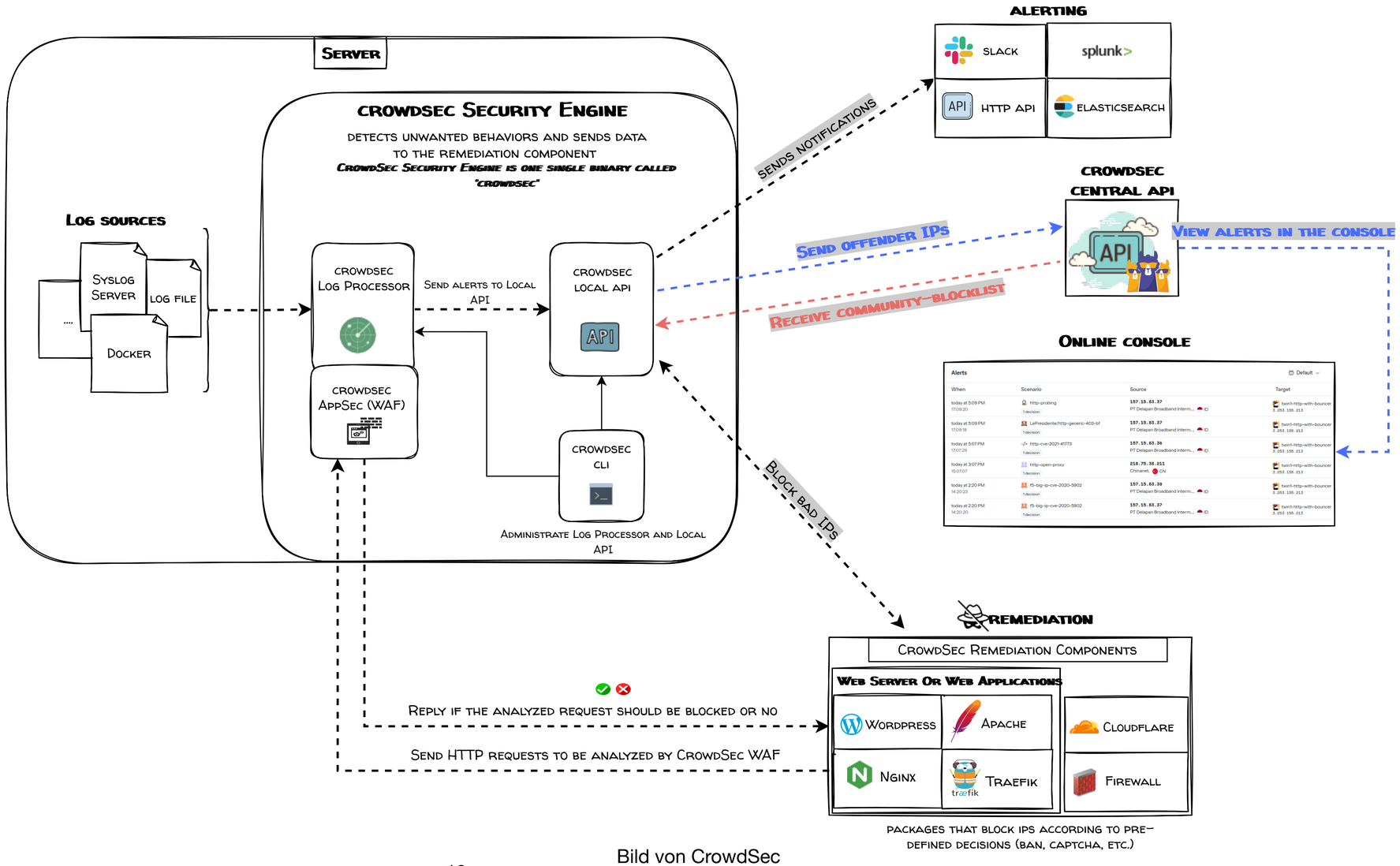
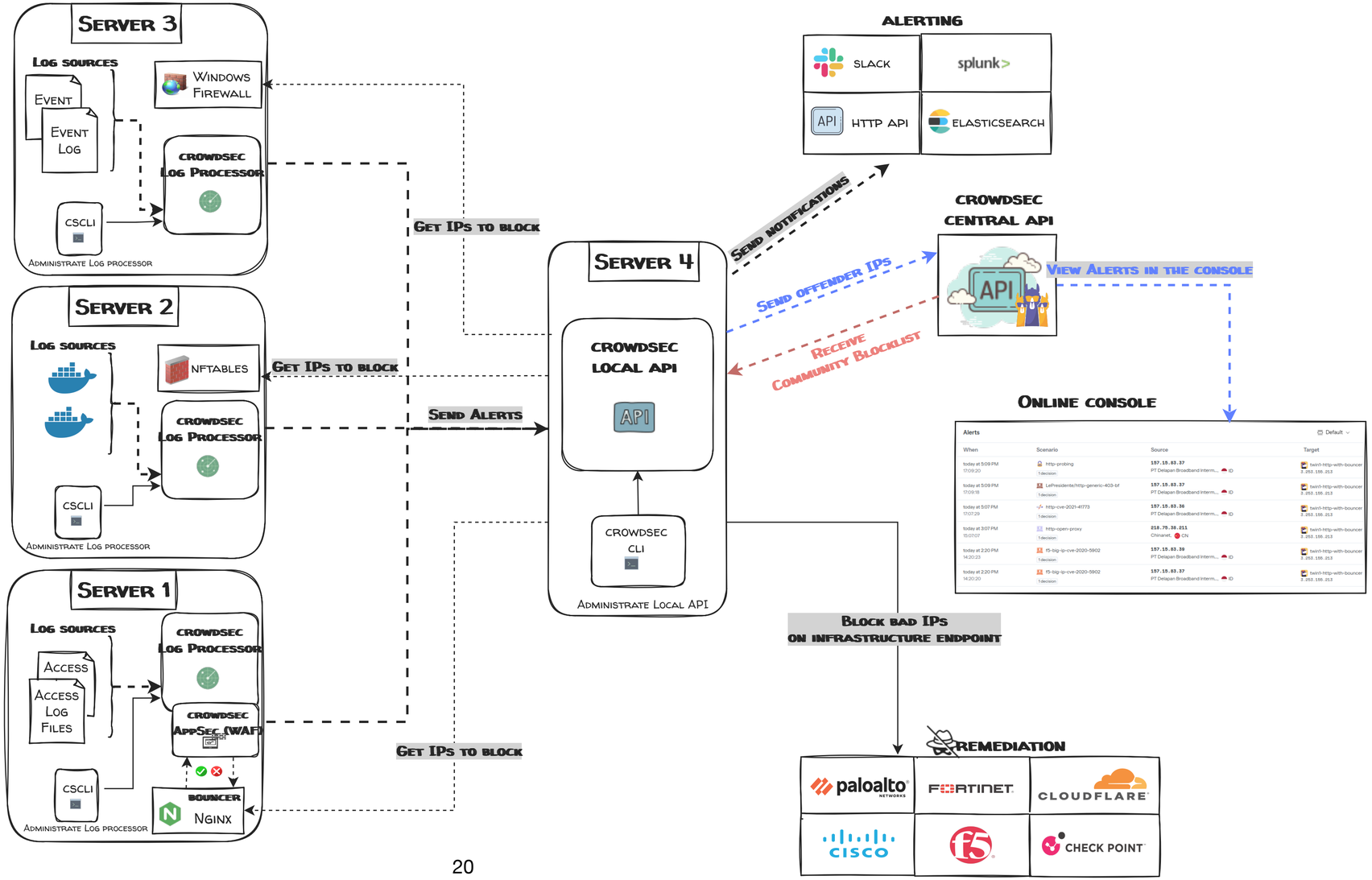


Bild von CrowdSec

CrowdSec's Security Engine

Übersicht



CrowdSec's Security Engine

Parser

- Parser können selbst eingebunden werden
- Einteilung in verschiedenen **Stages**
- Als **YAML Konfiguration** definiert

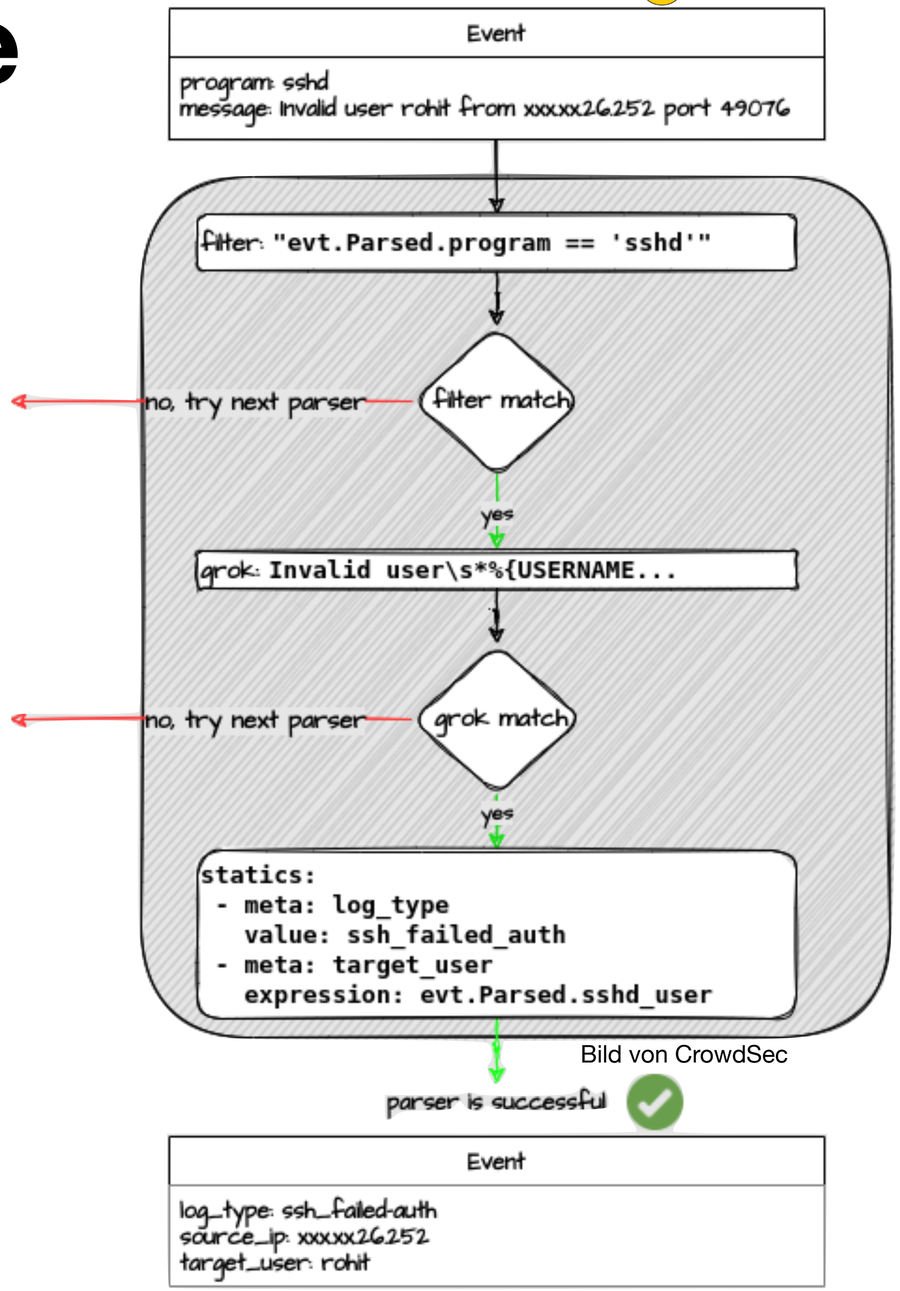


Bild von CrowdSec

CrowdSec's Security Engine

Parser

- Als Beispiel mit drei Stages
  - `s00-raw`
  - `s01-parse`
  - `s02-enrich`

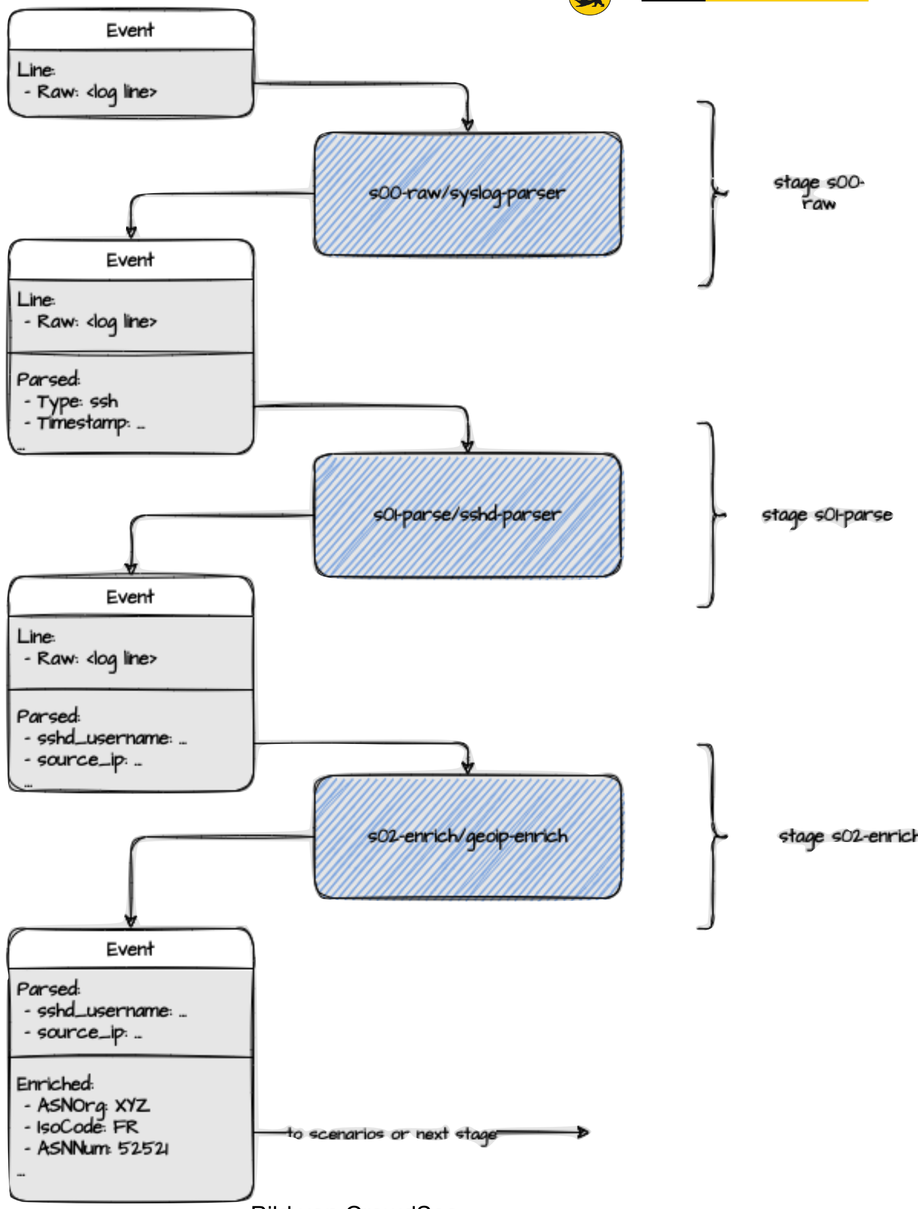


Bild von CrowdSec

CrowdSec's Security Engine

Scenarios

- Ermöglicht das Testen eines **bestimmten Verhaltens**, in der Regel einen Angriff, zu **erkennen**.
- Empfangen **Ereignisse** und können mithilfe des **Leaky-Bucket-Algorithmus** Warnungen erzeugen.

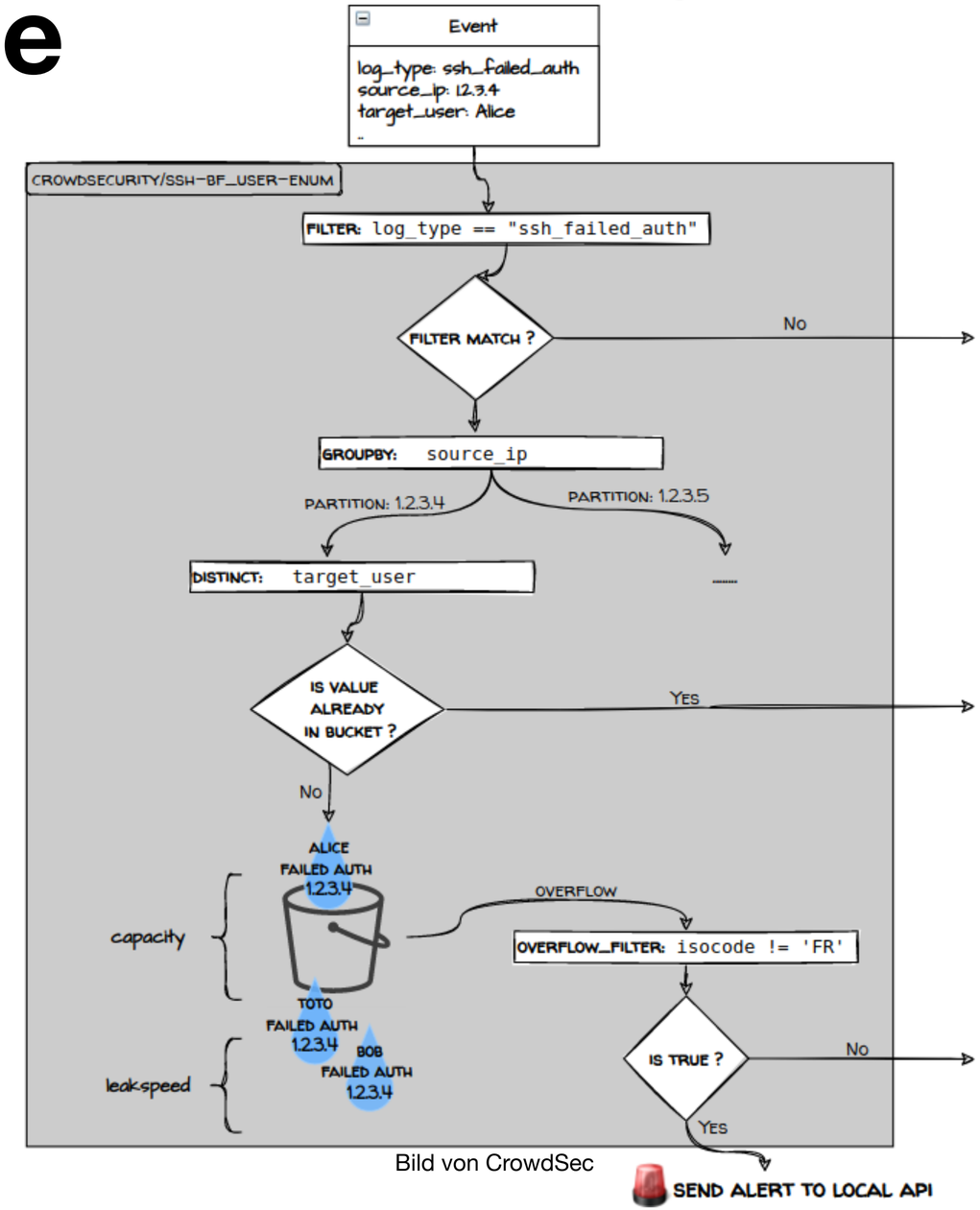


Bild von CrowdSec

CrowdSec's Security Engine

CLI

- `cscli`
- `cscli metrics show engine`
- `cscli scenarios list`
- `cscli parsers list`
- `cscli explain`

Integrationsmöglichkeiten

- Docker Container
- Windows
- Linux
- und mehr …

Lizenzmodell

Optionen

- Community
  eingeschränkter Zugriff, nur “**free**” und “**third-party**” zugänglich
- Premium
  unbeschränkter Zugriff, mehr verfügbar
- Platinum
  weiter Blocklisten exklusiv für Platinum

Lizenzmodell

Kosten

- Community
  frei
- SaaS Enterprise
  31$ monatlich; Zugriff auf Premium Blocklisten
- Platinum
  3900$ monatlich

Live-Demo

CrowdSec’s Blocklist in Produktion

- Aufbau von CrowdSec in bwInfoSec
- Validierung der Anfragen an Nextcloud
- Umsetzung CrowdSec Bouncer

Interesse geweckt?

https://doc.crowdsec.net/

Andere Lösungen

Kleiner Zusatz

- Security Onion 2: https://securityonionsolutions.com/software