Automatisierte Sicherheit mit

wazuh. + Event-Driven 

ATIX

The Linux & Open Source Company

Herzlich Willkommen

Agenda

1. Begrüßung und Vorstellung
2. Überblick Wazuh
3. Event Driven Ansible
4. Die Idee: Warum? Wieso? Weshalb?
5. Umsetzung / Wo fange ich an?
6. Live-Demos
7. EDA-Controller mit AWX
8. Ausblick
9. Q & A

Über uns

DIE Linux- & Open Source Company

- Mit über 30 Jahre Erfahrung das führende Linux-Systemhaus im deutschsprachigen Raum
- Experten für Open Source und Automatisierung in Rechenzentren sowie maßgeschneiderte Lösungen
- Drei Kernbereiche bieten wir individuell an:
  - IT-Consulting
  - orcharhino
  - Training

ATIX PROFESSIONAL SERVICES

Linux Platform Operations

Infrastructure Automation

Container Platforms & Cloud Solution

DevOps

Cloud Native Solution

Über uns

- **Name**: Alexander Pozdnyshev
- **Beruf/Position**: IT Consultant
- **Expertise**: Systemadministration, Automatisierung
- **Erfolge**: 4 Mio. Aufrufe bei IgorsLab (Tom’s Hardware)
- **Zertifiziert:** Red Hat, CompTIA Security+
- **Persönliches:** Suche Lagerhalle für 3D Druck Filament…

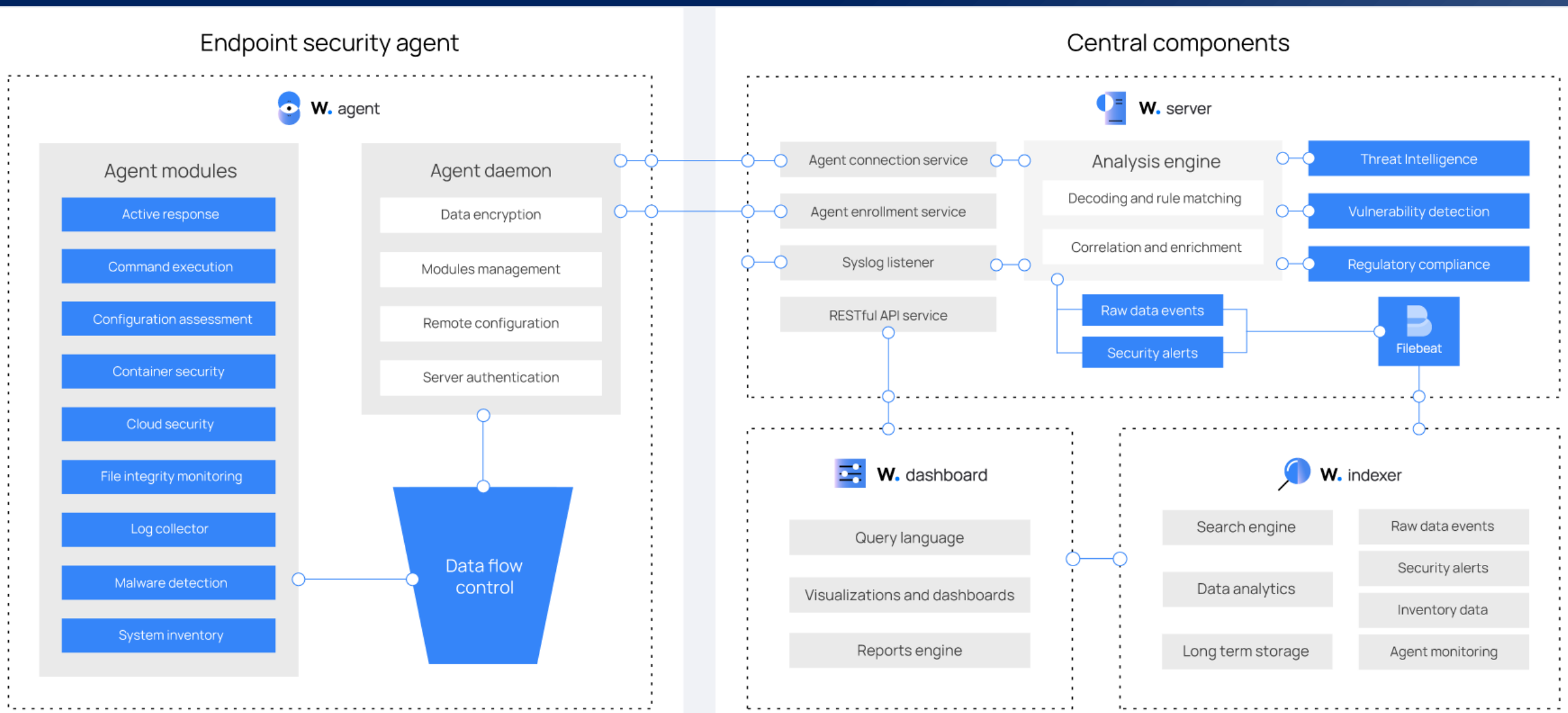
Über uns

- **Name**: Gergely Szalay
- **Beruf/Position**: Senior IT Consultant, Teamlead
- **Expertise**: DevOps, Container, Kubernetes
- **Zertifiziert:** CKA, CKAD, Scrum Master
- **Persönliches:** lesen, meine Kinder, Katzen

Wazuh: SUM()

- Security Information and Event Management (SIEM) = Monitoring, Erkennung, Alerting
- Extended Detection and Response (XDR) = Heuristik, externe APIs und Tools, automatische Reaktion auf Events
- Agent-sowie agentless, Open Source, kostenlose Demo
- Komponenten: Indexer, Server, Dashboard, Agent(s)
- Viele Installationsmöglichkeiten, auch offline möglich
- HA und Load-Balancing Support
- Offizielle Ansible und Puppet-Rollen

Wazuh: Aufbau



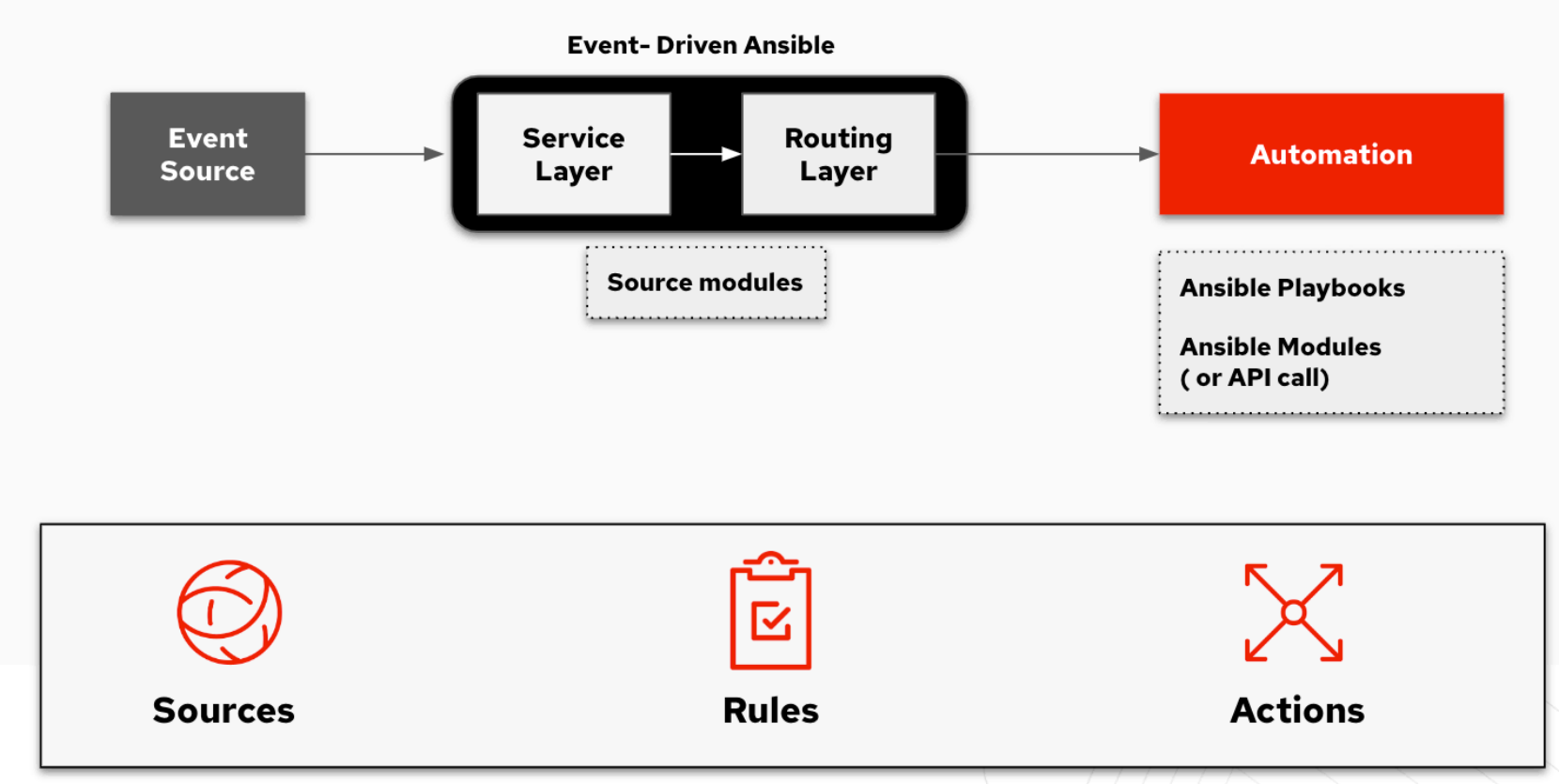
Demo: Wazuh Dashboard

Demo: Wazuh Events und Alerts

Event Driven Ansible: SUM()

- Eine neue Art der Arbeit mit Ansible: ereignisbasiert
- Ereignis X -> Aktion Y
- Dies ermöglicht eine sofortige und automatisierte Reaktion auf Probleme oder unerwartete Ereignisse.
- Derzeit eine Developer Preview
- Die Informationen darüber, welche Ereignisse überwacht und welche Maßnahmen ergriffen werden sollen, sind in einem so genannten "Ansible Rulebook" enthalten.

Event Driven Ansible: <image>



Event Driven Ansible: SUM()

- Rules, Rulebooks, Conditions, Events, Event source Plugins
- Am Beispiel:

```yaml
# check_url_rulebook.yml
---
- name: Check webserver
  hosts: all
  sources:
    - ansible.eda.url_check:
        urls:
          - https://<webserver_fqdn>
        delay: 10
  rules:
    - name: Restart Nginx
      condition: event.url_check.status == "down"
      action:
        run_playbook:
          name: atix.eda.restart_nginx
```

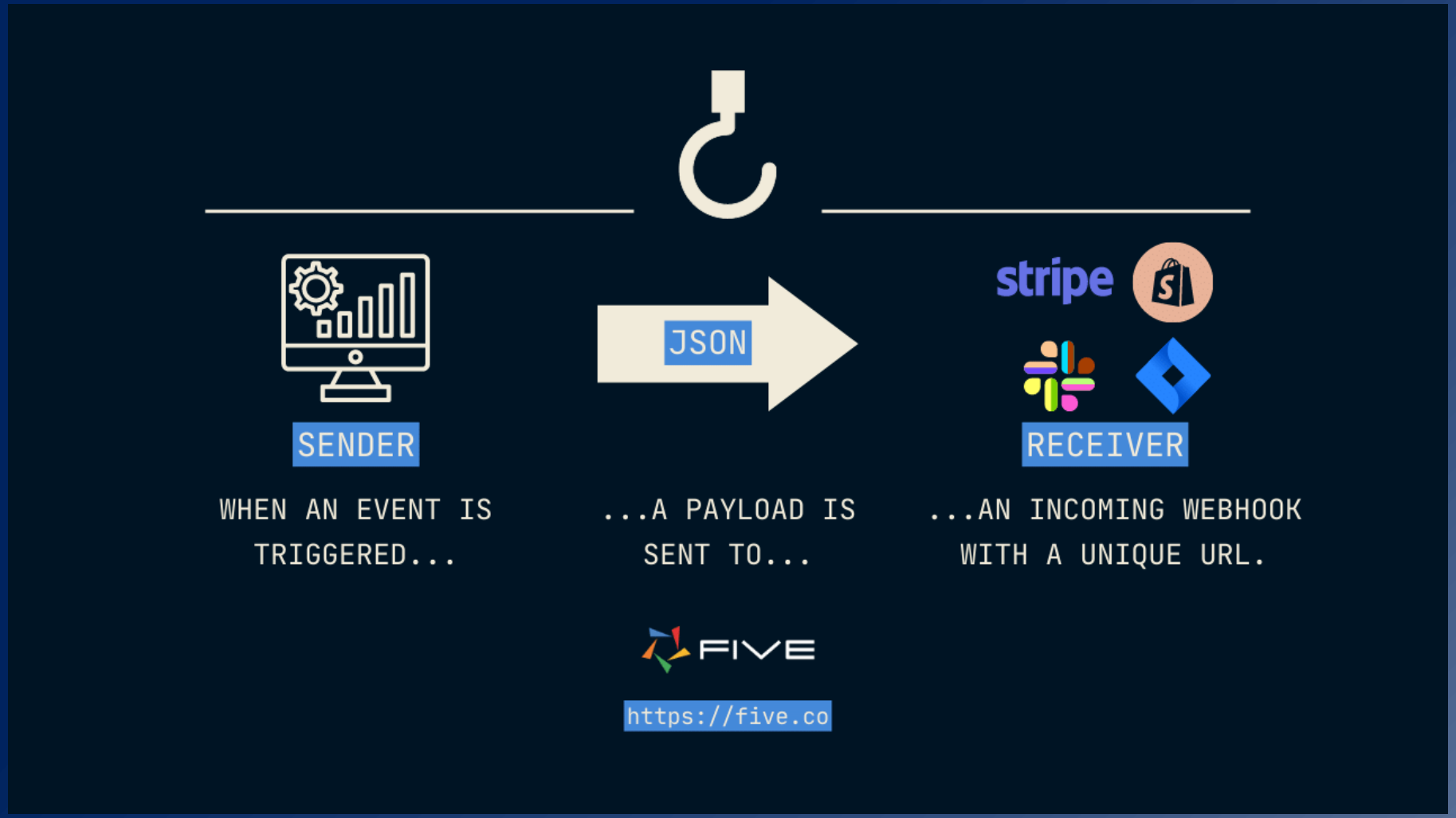
... beides zusammen??

Die Idee

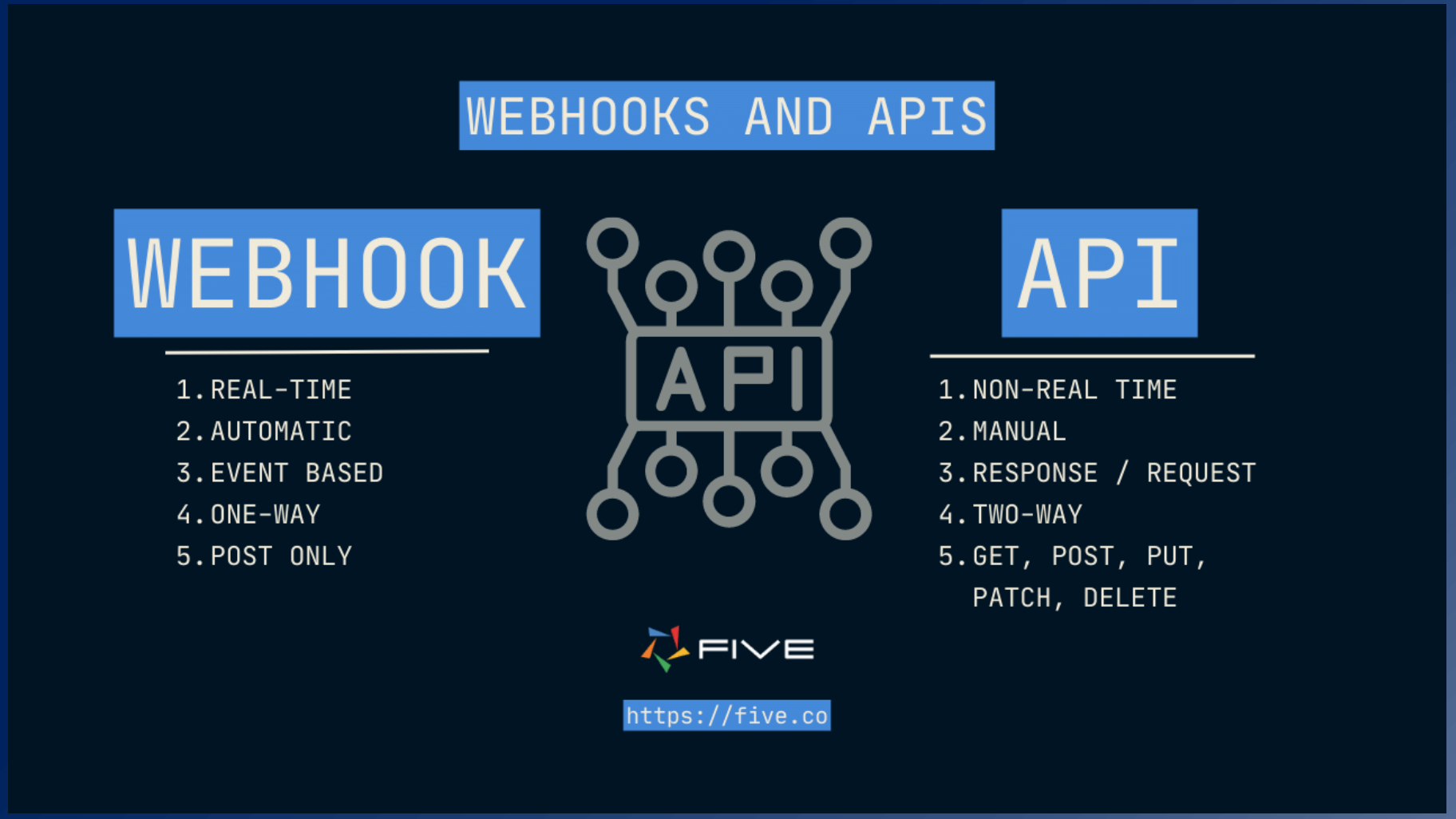
- **webhook**

  Provide a webhook and receive events from it

Webhooks: Basics



Webhooks sind praktisch



Event Driven Ansible x Wazuh

1) Endpoint loggt ein Event (matching rule aus der config)
2) Endpoint sendet Event an Wazuh Server als JSON
3) Wazuh Server loggt den Alert in einer alert-xyz.json
4) Custom Rule sagt: sende Notification an EDA. Notification Channel ist ein Custom Webhook mit JSON-Payload. Ein „Custom Integration Script“ wird empfohlen.
5) JSON Payload ist Input für das Ansible Rulebook. Listener ist ansible.eda.webhook (Event Source Plugin)
6) Ansible führt je nach Payload die passende Gegenmaßnahme als Playbook aus.

Demo: Wazuh Alerts und EDA in Aktion

Vorteile unserer Lösung

- Bereits vorhandene Ansible Playbooks wiederverwenden
- Die Exekutive bleibt bei Ansible
- Mehr Flexibilität, unbegrenzte Antwortmöglichkeiten auf Alerts (Triggern anderer Systeme, Port-Isolation auf Switch-Ebene, Trennung vom Netz, Ausrollen temporärer Firewall-Regeln, Neuinstallation ganzer VMs...)

Event Driven Ansible: on scale

- Der EDA Controller als Ergänzung zum AWX / AAP Controller
- Standalone oder als Bestandteil der AAP ist.
- EDA-Controller kann einzeln installiert werden und hat eine eigene Web-GUI. Damit lässt sich Event-Driven-Ansible einfacher managen, im Team benutzen und skalieren
- Repo: https://github.com/ansible/eda-server
- Einfachste Installationsmethode ist docker compose bzw. Podman.

Demo: EDA Controller und AAP GUI

Q & A

Der Schlüssel zum Lernen ist Feedback. Ohne ist es fast unmöglich, zu lernen.

Steven David Levitt
US-amerikanischer Ökonom und Professor an der University of Chicago

Danke für eure Aufmerksamkeit!

Bevorstehende Webinare

atix.de/events/webinare/

Danke für eure Aufmerksamkeit!

Bevorstehende Trainings

atix.de/schulungen/

Danke

Besucht unseren CLT Stand!


+49 (0)89 452 3538-0


info@atix.de


atix.de

Follow us!