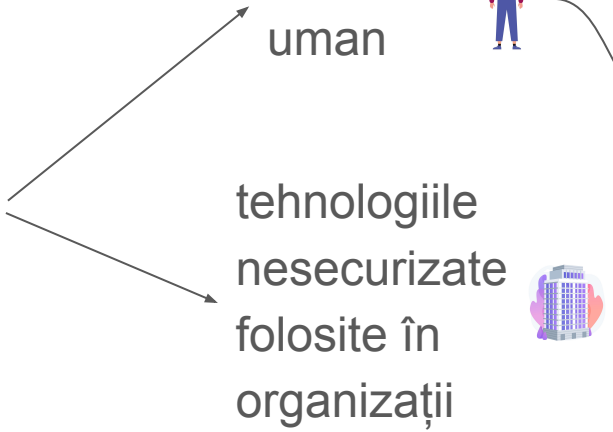
Tehnici de asigurare a continuității serviciilor EDR

Anamaria-Larisa PAȘA

Coordonator: Ș.l.dr.ing. Cătălin MIRONEANU
Departamentul de Calculatoare, Facultatea de Automatică și Calculatoare
Iași, România

Problematica observată

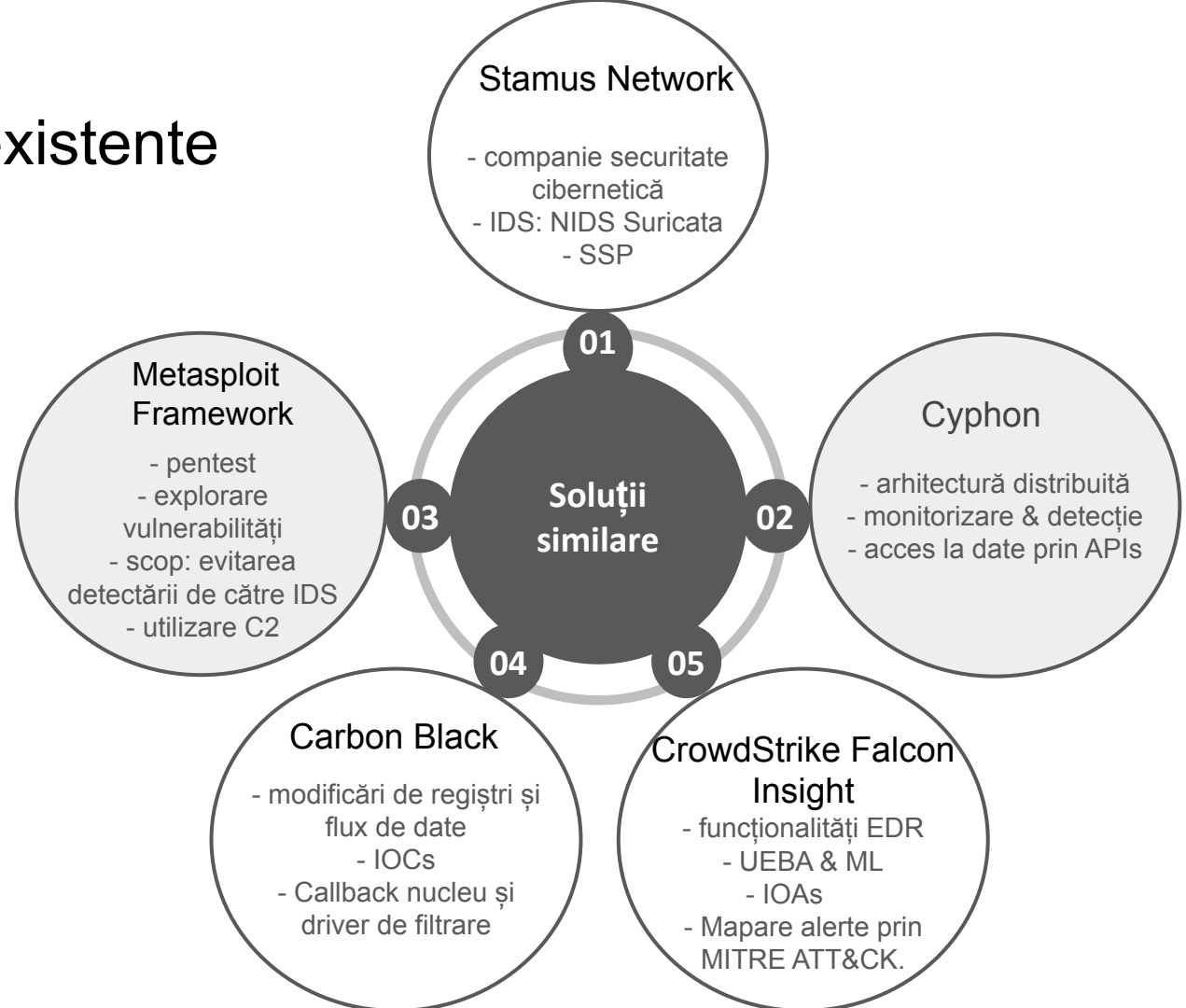
- atacurile vizează vulnerabilități cauzate de



lipsa focusului pe informațiile primite

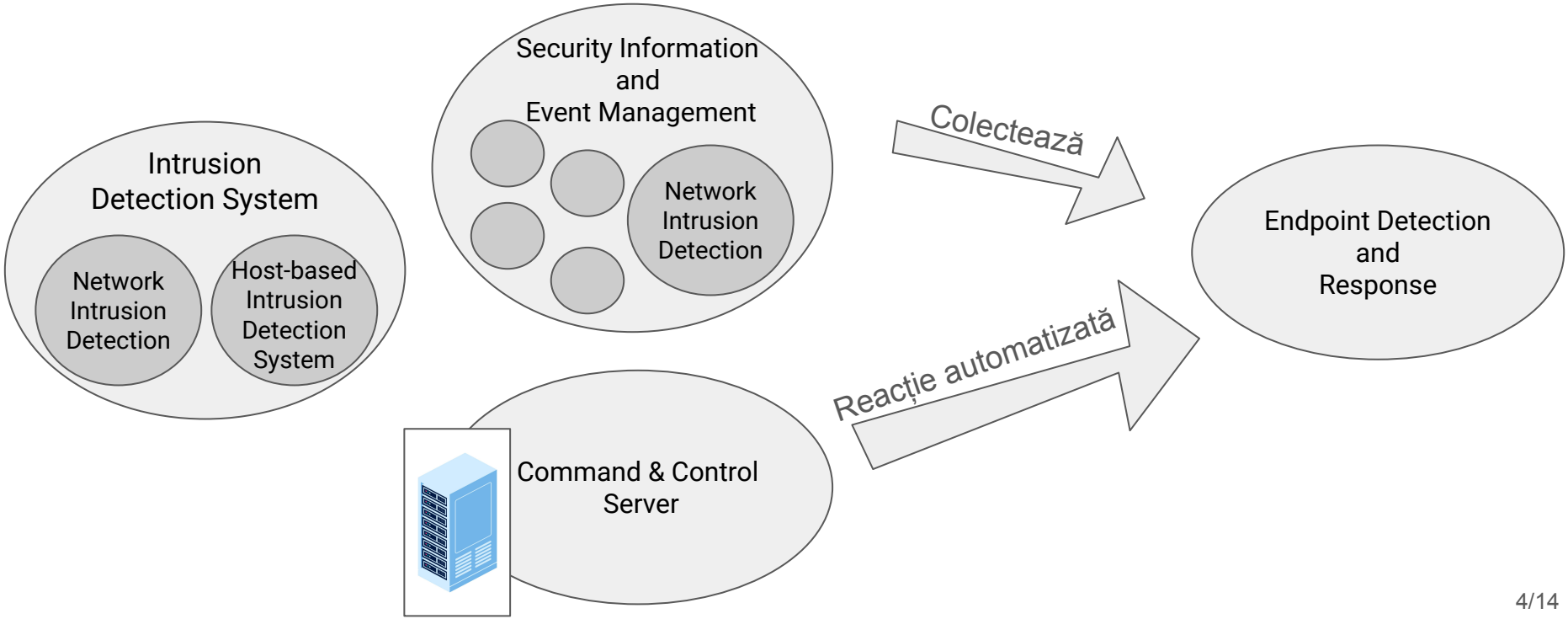
dificultatea de a diferenția un comportament normal față de un atac

Soluții existente



Tehnici actuale de securitate

- tehnici specifice ariei defensive a securității, folosite în soluția propusă



Instrumentele principale folosite

Suricata

- inspectează fluxurile de date dintr-un sistem informatic

- funcționează cu seturile de reguli Snort

- generează date NSM (Network Security Monitoring)

Wazuh

- platformă open-source pentru monitorizare și detectare amenințări

-agenți integrați cu IDS

EC2

- posibilitate de scalare

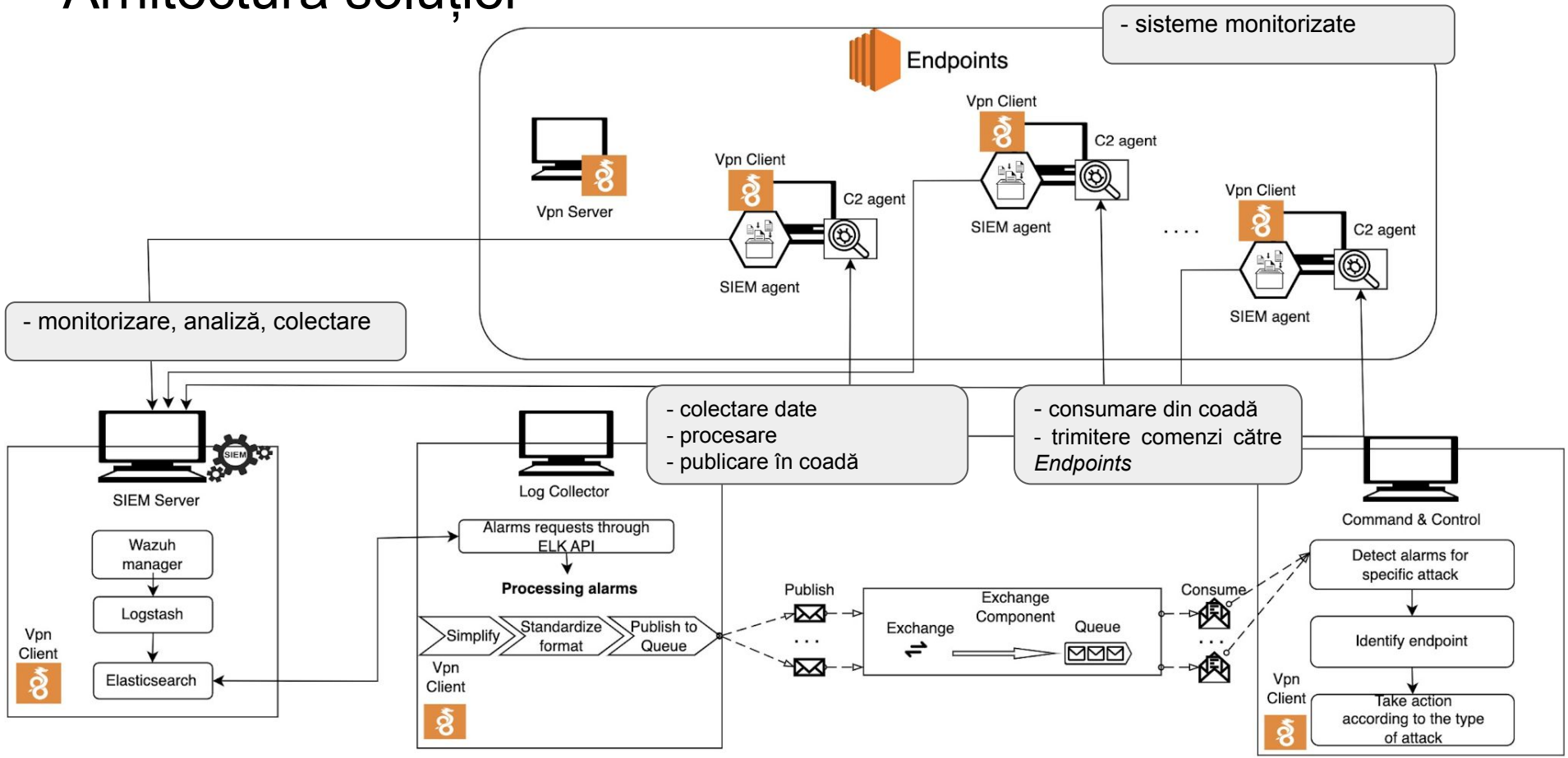
- reduce costul de configurare al unei infrastructuri software

RabbitMQ

- livrare mesaje prin metoda Point-to-Point

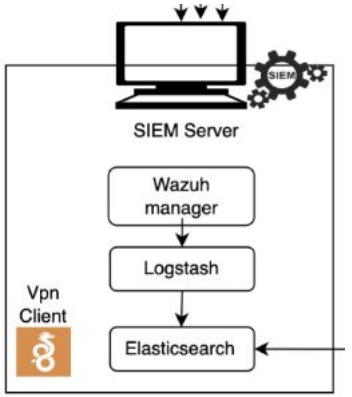
- utilizare algoritm FIFO

Arhitectura soluției

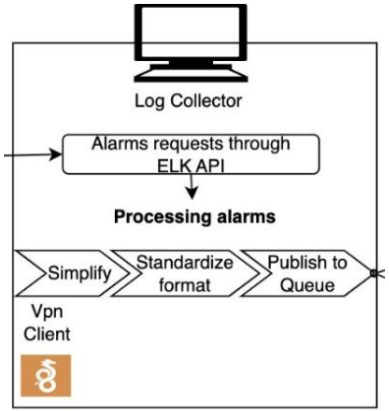


Componente (1/2)

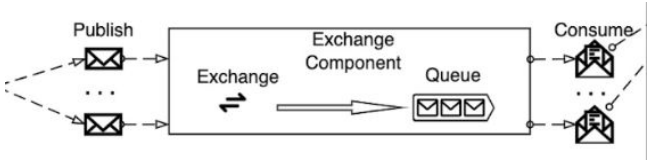
- Componenta *SIEM*
  - reguli predefinite de corelare
  - Logstash, Elasticsearch
  - asigură preluarea alertelor IDS
  - rol: container de transfer



- Componenta *Log Collector*
  - elimină colectarea manuală a datelor
  - preluare periodică alerte
  - rol: procesare personalizată a alertelor

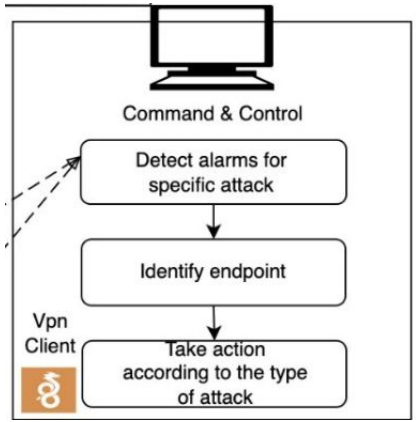


- Componenta *Exchange*
  - protocol AMQP
  - rol: lipsa interdependențelor între componente

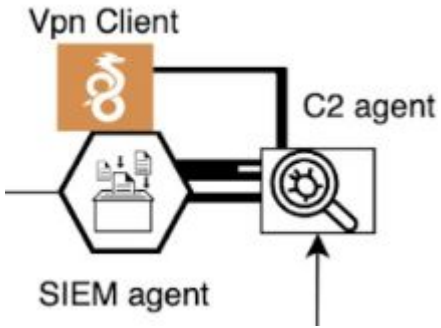


Componente (2/2)

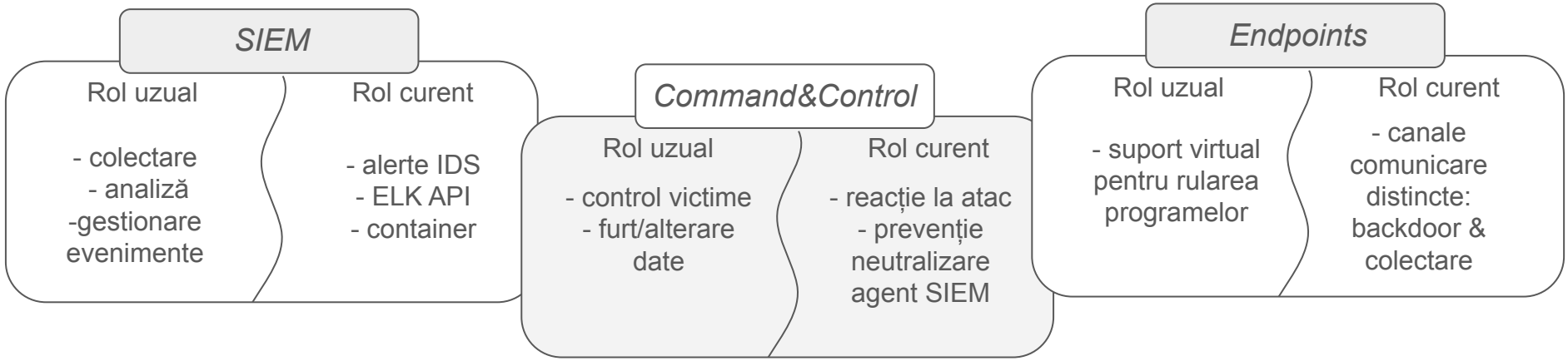
- Componenta *Command&Control*
  - agenții stabilesc conexiuni de tip callback
  - scop defensiv
  - identificare sisteme compromise
  - reacții automatizate la alerte



- Componenta *Endpoints*
  - agent reactiv: agent C2
  - agent proactiv: agent SIEM
  - agent SIEM integrare cu IDS
  - rol: canale de comunicare distincte
    - scop: strat suplimentar de securitate



Implementare - aspecte cheie



- Realizarea implementării:
  - configurări tehnologii
  - cod

▼ Inbound rules

Filter rules

Name	Security group rule ID	Port range	Protocol	Source	Security groups
–	sgr-0f62956c7207c60f9	All	All	sg-0ae644709a6e087a7	Endpoint2Rules
–	sgr-0341601c4db04e277	80	TCP	0.0.0.0/8	Endpoint2Rules
–	sgr-0682aa0c8d986880a	443	TCP	0.0.0.0/0	Endpoint2Rules
–	sgr-08c59b9354d810cb1	22	TCP	0.0.0.0/0	Endpoint2Rules

▼ Outbound rules

Filter rules

Name	Security group rule ID	Port range	Protocol	Destination	Security groups
–	sgr-08e1255a27b58c573	All	All	0.0.0.0/0	Endpoint2Rules

Rezultate obținute (1/2)

Procesare alerte

timestamp
-
necesar pentru testele de timpi

dest_ip, src_ip
-
analiza pentru comunicari suspecte


```
{
    "data": {
        "dest_ip": "10.177.186.5",
        "timestamp": "2024-06-30T18:05:03.0816
        "dest_port": "22",
        "src_port": "57504",
        "src_ip": "10.177.186.9",
        "proto": "TCP",
        "event_type": "alert",
        "alert": {
            "signature_id": "2001219",
            "action": "allowed",
            "severity": "2",
            "signature": "ET SCAN Potential SSH Scan",
            "category": "Attempted Information Leak"
        }
    },
    "agent": {
        "id": "002",
        "name": "Endpoint2",
        "ip": "10.177.186.5"
    }
}
```


agent
-
acces facil către date despre sistemul controlat

alert
-
identificare tipologii de atac pentru reacții adecvate

Prevenție neutralizare agent SIEM, persistență agent C2

Motiv: studierea mecanismului de persistență al agenților Wazuh de către atacatori

```
ubuntu@ip-172-31-93-122:~$ sudo systemctl stop wazuh-agent
ubuntu@ip-172-31-93-122:~$ sudo systemctl status wazuh-agent
○ wazuh-agent.service - Wazuh agent
     Loaded: loaded (/lib/systemd/system/wazuh-agent.service; e
     Active: inactive (dead) since Sun 2024-06-30 17:58:27 UTC;
```

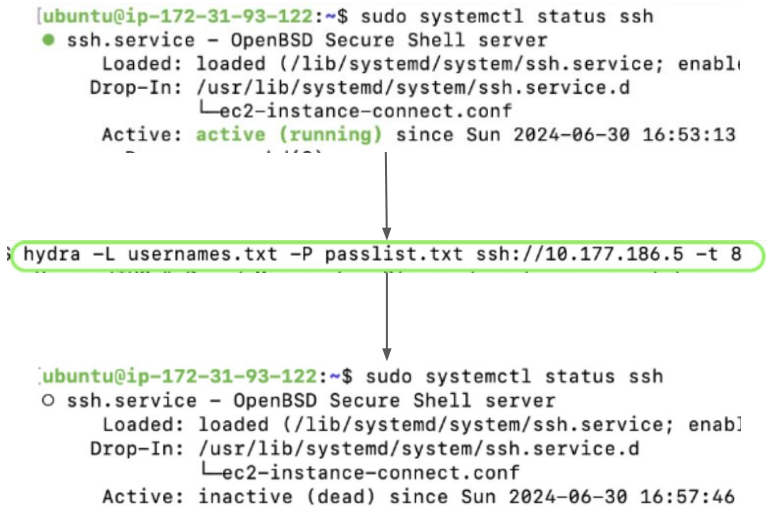
```
[++][check_wazuh_agents()] INFO: Agent <('10.177.186.5', 52492)> seems to be inactive
[++] INFO: Waiting for c2_agent response...
[++] INFO: Waiting for c2_agent response...
[++][check_wazuh_agents()] INFO: Agent <('10.177.186.5', 52492)> successfully activated.
```

```
ubuntu@ip-172-31-93-122:~$ sudo systemctl status wazuh-agent
● wazuh-agent.service - Wazuh agent
     Loaded: loaded (/lib/systemd/system/wazuh-agent.service;
     Active: activating (start) since Sun 2024-06-30 17:59:14
```

Rezultate obținute (2/2)

Reacție la alerte

- Scenariu - exemplu demonstrativ:
  - verificare stare inițială serviciu SSH
  - inițiere atac - Hydra
  - reacție transmisă de componenta *Command&Control*
  - verificare stare ulterioară serviciu SSH



Timpi de procesare alerte

- Context:
  - mediu controlat
  - testare pe mașini virtuale
- Timpi rezultați:
  - durata medie procesare alerte: 0.06 secunde
  - timp mediu procesare periodică alerte / agent: 0.05 ÷ 0.08 secunde

Concluzii

- folosirea tehnicilor atacatorilor (server C2) în scop defensiv într-o soluție de securitate
- este posibilă folosirea SIEM cu un alt scop și cu un alt rol în soluția propusă
- este posibilă întărirea rolului IDS prin adăugarea capabilităților de SIEM
- canale comunicare distincte

Direcții de dezvoltare

- Renunțare generalitate IDS
  - funcționalități SIEM extinse

- Securizare *Command&Control*
  - mecanisme evitare detecție de către sistemele de securitate
  - IDS poate identifica nereguli în comunicarea agent - server C2

- Integrare IA
  - creștere acuratețe alerte
  - reacții adecvate la atacuri noi / modificate

- Scalare proiect
  - monitorizare *endpoints*

Vă mulțumesc pentru atenție !