HTL | MÖSSINGERSTRASSE

Elektronik und technische Informartik

In Kooperation mit der: kelag

THREATDETECTOR WITH ELASTIC

Phillipos Mazaris (5BHEL) , Michael Schneider (5BHEL)

2023/24

Idee

Das Projekt verwendet den Elastic-Stack, um das Stoppen der Datenübermittlung an die Server zu erkennen. Dies soll mithilfe KI und Algorithmen erkannt werden.

Warum

Sicherheitsüberprüfungen bei Firmen zeigen immer wieder, dass Angreifer die Logübermittlung ihrer Endgeräte deaktivieren können. Das Projekt dient dazu, dies frühzeitig zu erkennen

Wie

Die Erkennung dieses Verhaltens wird mit der KI von Elastic realisiert. Im Gegensatz dazu gibt es auch regelbasierte Methoden. Das Ganze wird im UI von Kibana implementiert.

Elastic

Kibana

```
client_ep = base_url + "winlogbeat-fake/_doc/"
server_ep = base_url + "logs-fake/_doc/"

print("Starting with ip {0} as {1}".format(cl_ip,"threat" if attack else "normal"))

cl_doc = {
    "winlog.provider_guid": "{1c95126e-7eea-49a9-a3fe-a378b03ddb4d}",
    "winlog.provider_name": "Microsoft-Windows-DNS-Client",
    "host.hostname": "threatdt2",
```