Proactive Discovery and Mitigation of Security Vulnerabilities Leveraged by Software-Defined Networks

Master in Telecommunications and Computer Science

João Francisco Rosa Polónio

Supervisors:

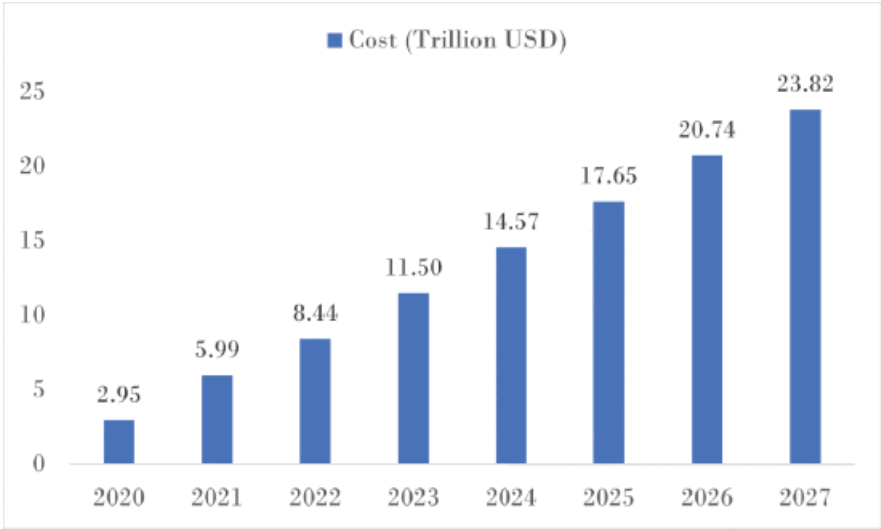
José André Moura, Assistant Professor, Iscte-IUL

Rui Neto Marinheiro, Associate Professor, Iscte-IUL

Contents

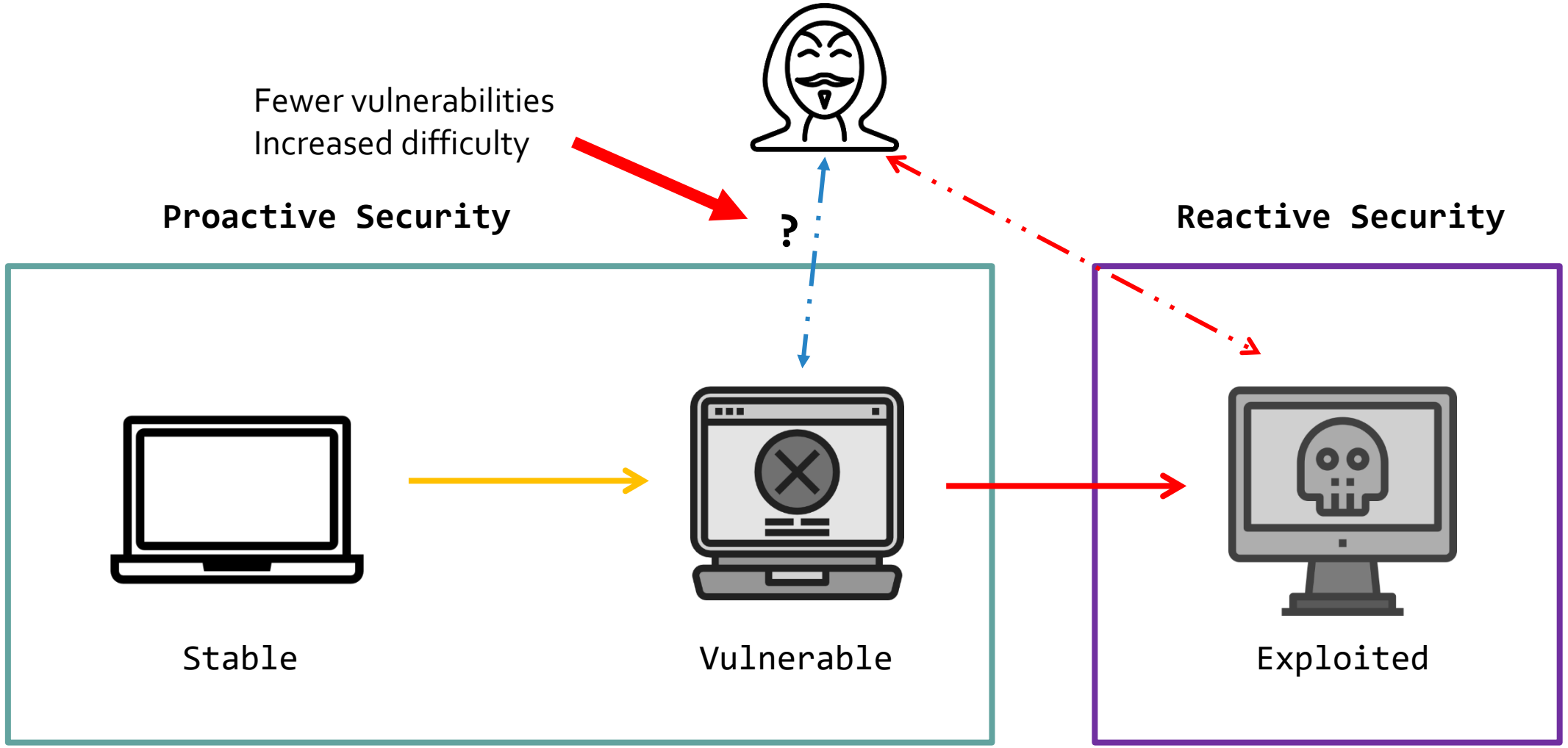
Context and Motivation

- Increase in the number of devices on the network (not security robust).
- Damage caused by cyber attacks costs a lot of money.
- Organizations must reduce the attack surface.
- Traditional Networks lack centralized control.
- Networks are increasingly programmable and solutions must follow the same path



SDN

Context and Motivation



Problem Statement

There is lack of solutions that address proactive and automated detection, and mitigation of vulnerabilities in the networked system.

Objectives

Proactive and automated detection, and mitigation of security vulnerabilities, addressed within a network environment controlled by SDN.

1) Development of a comprehensive architecture that integrates various open-source security technologies.
2) Evaluating the impact of these strategies on network and device performance, ensuring that they are executed efficiently and in a timely manner.

Research Questions

RQ1 - How to **automate** device security **vulnerabilities detection** on networks?

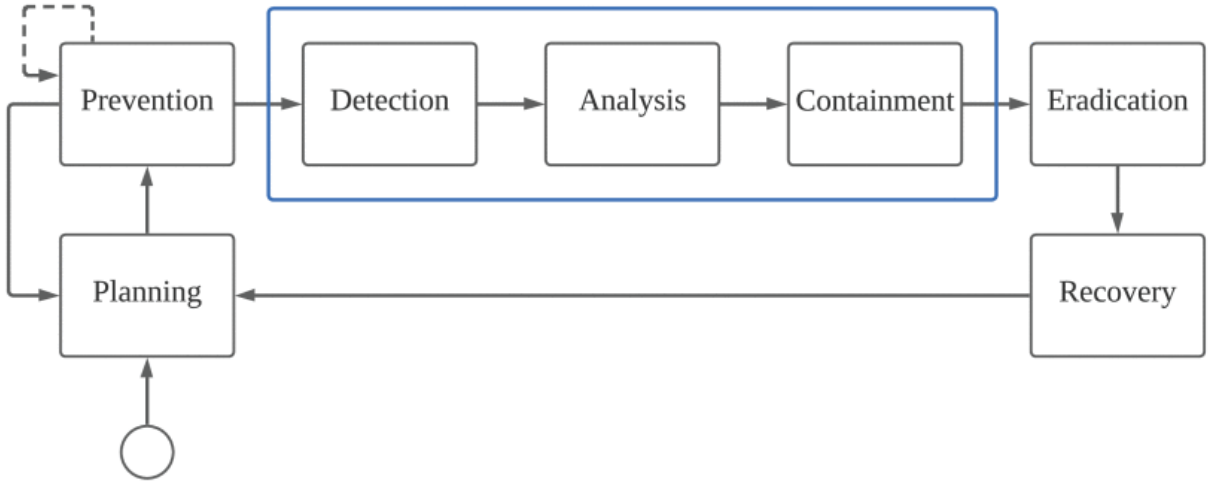
RQ2 - What **resources** the automated vulnerability **detection consumes** and their **impact** on the system **scalability**?

RQ3 - How the usage of the **SDN controller** capabilities can **enhance** the network **security**?

RQ4 - How **timely** can be the automated **deployment** of **mitigation** strategies?

Literature Review

- Articles collected using **Systematic Literature Review** using Parsifal.
- Search for works relevant to SDN and Vulnerability Detection and Mitigation.
- Analyzed **5%** of the works, about **52** papers.



IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 23 May 2024, accepted 10 July 2024, date of publication 16 July 2024, date of current version 24 July 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3429269

SURVEY

On the Road to Proactive Vulnerability Analysis and Mitigation Leveraged by Software Defined Networks: A Systematic Review

JOÃO POLÓNIO[1], JOSÉ MOURA[1,2], AND RUI NETO MARINHEIRO[1,2]
[1]Instituto Universitário de Lisboa (ISCTE–IUL), 1649-026 Lisbon, Portugal
[2]Instituto de Telecomunicações (IT), 1049-001 Lisbon, Portugal
Corresponding author: José Moura (jose.moura@iscte-iul.pt)

This work was supported by FCT - Fundação para a Ciência e Tecnologia, I.P. by project reference UIDB/50008/2020, and DOI identifier https://doi.org/10.54499/UIDB/50008/2020; and in part by the Instituto de Telecomunicações, Lisbon, Portugal.

Digital Library	Imported Studies	Accepted	Percentage
IEEEXplore	763	46	6.02%
ACM Digital Library	216	6	2.78%

Literature Review: Detection

- Few works focused on **Vulnerability Assessment**.
- Need to incorporate **active probing tools** into SDN.
- Need to use **standardized risk indicators** -> difficulty in assessing the **severity** of threats.
- Total of **8** papers.

Detection Papers Comparison

Paper	Vulnerability Assessment	SDN Controller	Automation	Risk Indicator	Passive Scanning	Active Probing	Proximity Score
[42]	●	POX	●	Custom	○	●	16.7
[43]	●	ODL, ONOS	◑	CVSS, Custom	○	●	15.0
[44]	●	ONOS	●	CVSS	○	●	16.7
[45]	●	ODL	●	Custom	●	○	16.7
[47]	○	N/A	●	○	●	○	6.7
[46]	○	ODL	●	○	●	○	10.0
[48]	○	N/A	●	○	●	●	10.0
[49]	○	N/A	●	Custom	●	○	10.0

Literature Review: Mitigation - Data Plane

- Methods designed to mitigate attacks but may be adapted.
- No use of **risk indicators**.
- Difficult to proactively detect security flaws.
- Total of **7** papers.

Mitigation Papers Comparison – Data Plane

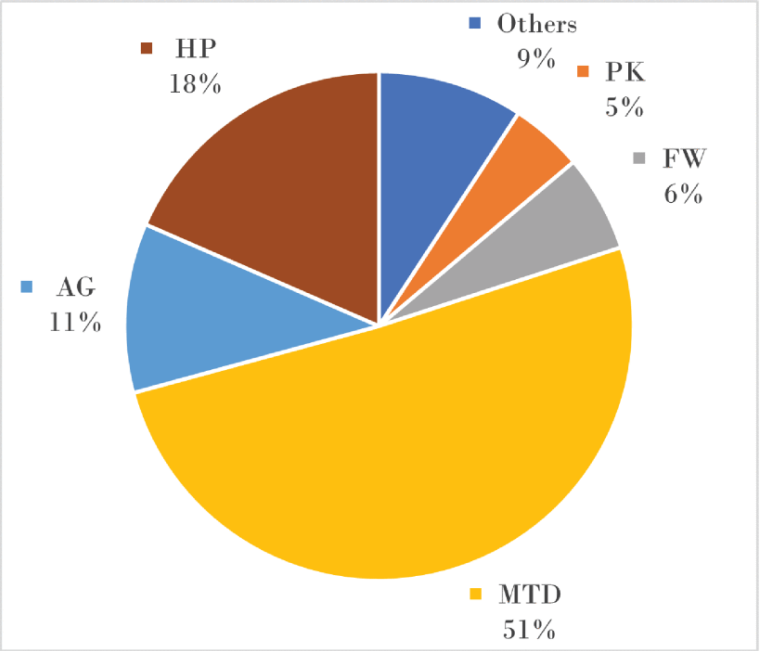
Paper	Technique	SDN Controller	Automation	Elasticity	Risk Indicator	Latency	Throughput	Proximity Score
[50]	CNN, FW	N/A	●	●	○	●	●	14.3
[51]	MTD	N/A	○	◑	○	●	○	7.1
[52]	MTD	N/A	○	●	○	●	○	8.6
[53]	PK	N/A	◑	◑	○	●	○	8.6
[54]	PK	N/A	●	○	○	○	○	5.71
[55]	FW, PK	N/A	○	○	○	○	○	2.9
[56]	FW	POX	●	●	○	◑	○	12.9

Literature Review: Mitigation – Control Plane

- Not enough use of **risk indicators**.
- Lacking complete solutions that demonstrate measurable effects on **network performance**.
- Total of **42** papers.

- Few works on **proactive** measures.
- Even those don't have fully **automated** measures

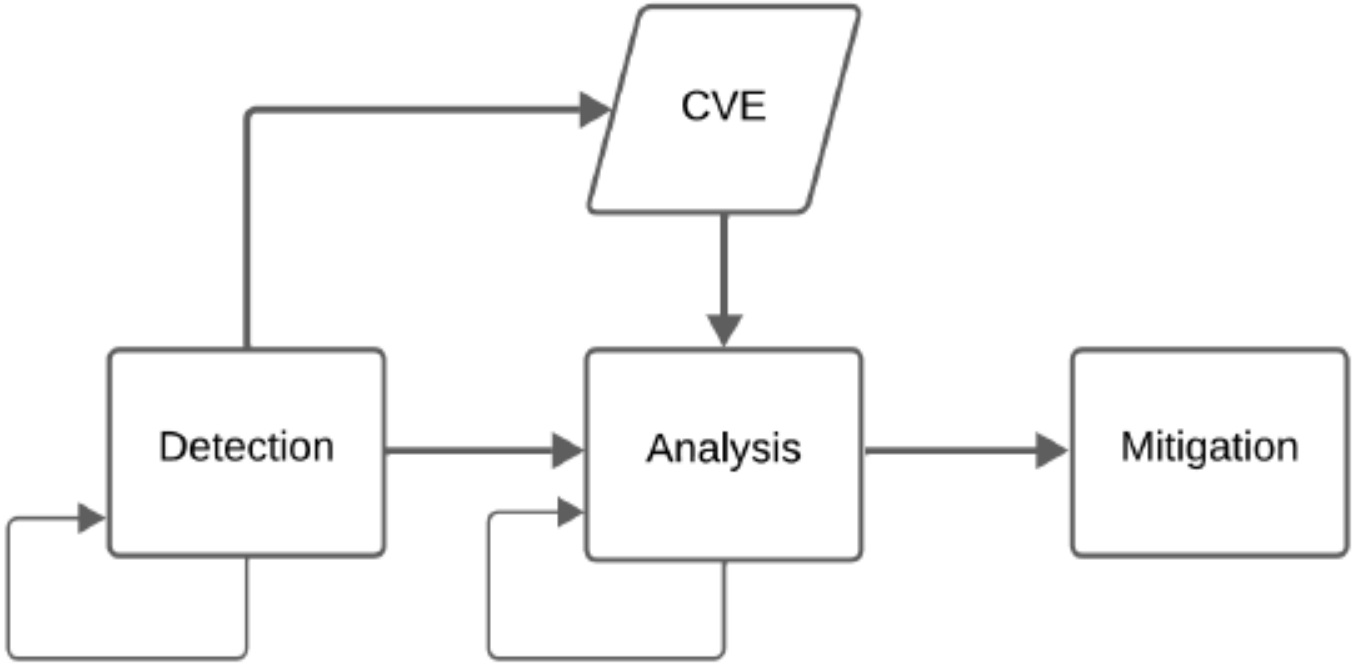
New approaches needed



Architecture Design

Building Blocks

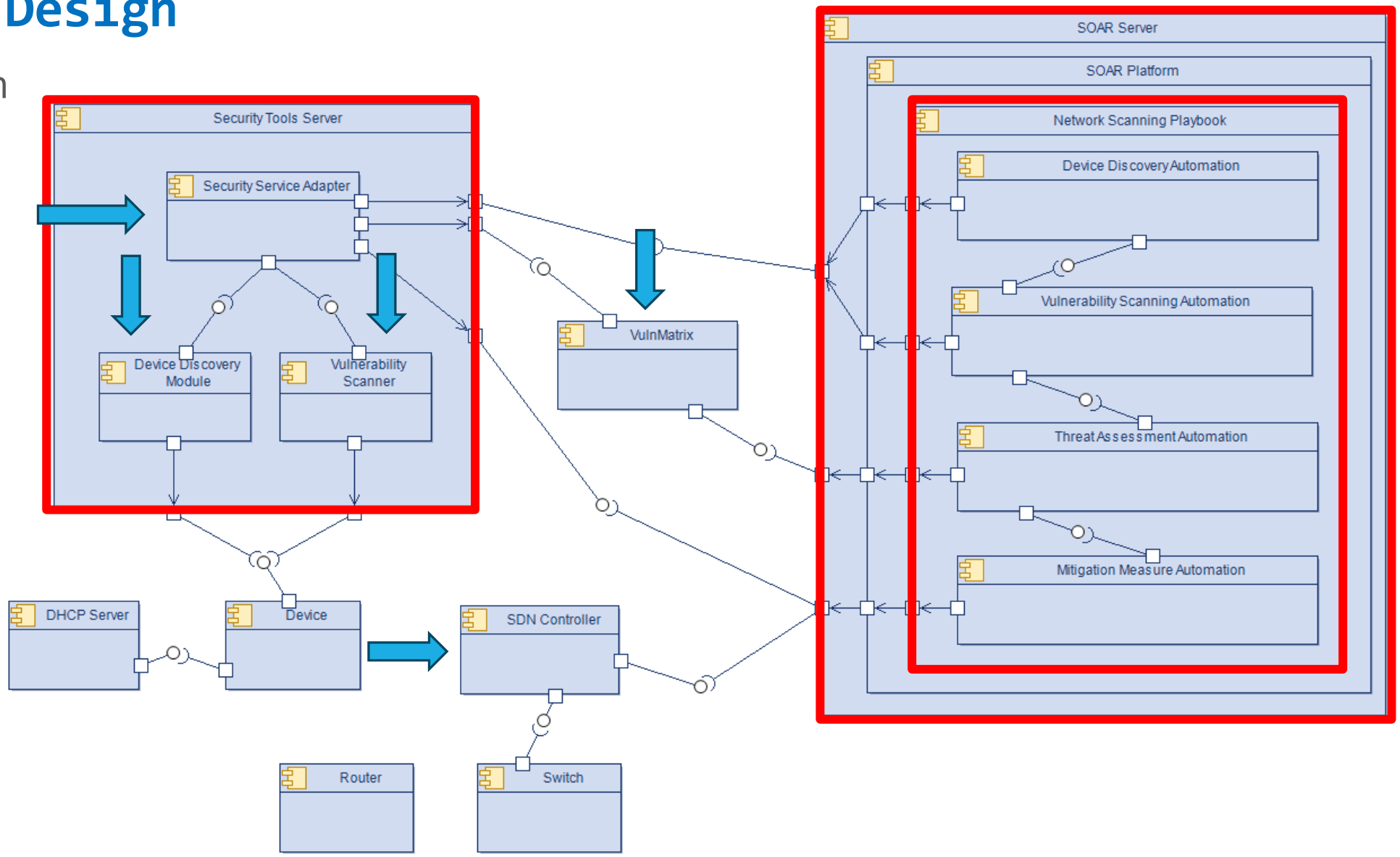
- Limited number of studies focusing on both vulnerability **detection** and **mitigation**.
- Absence of deploying a **SOAR** in SDN to coordinate the various tools.



✓ **Proactivity**
✓ **Interoperability**
✓ **Adaptability**

Architecture Design

Component Diagram

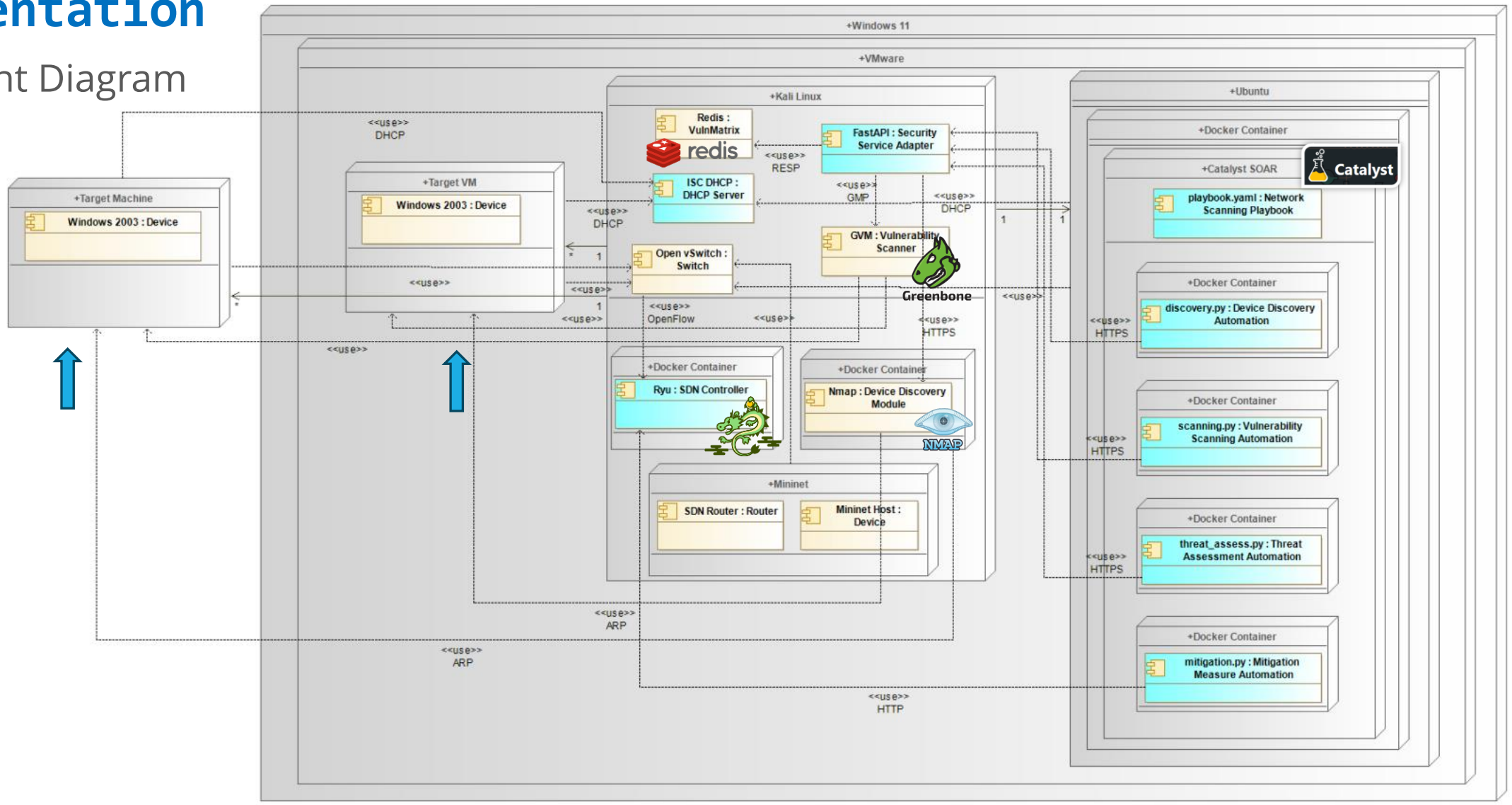


Implementation

Explored Technologies

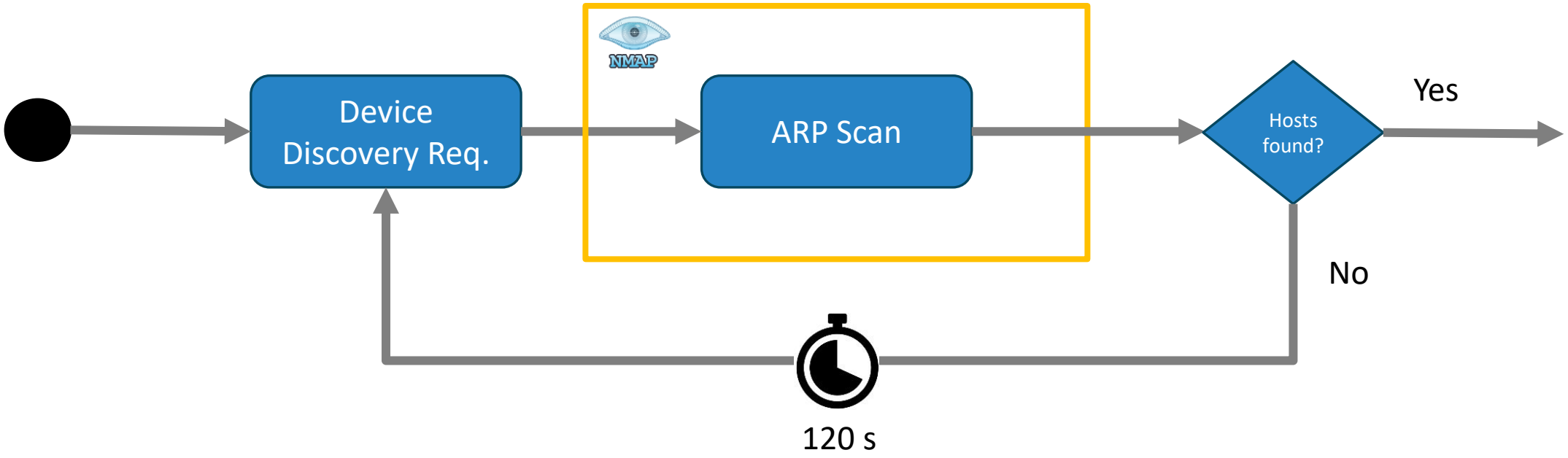
Implementation

Deployment Diagram



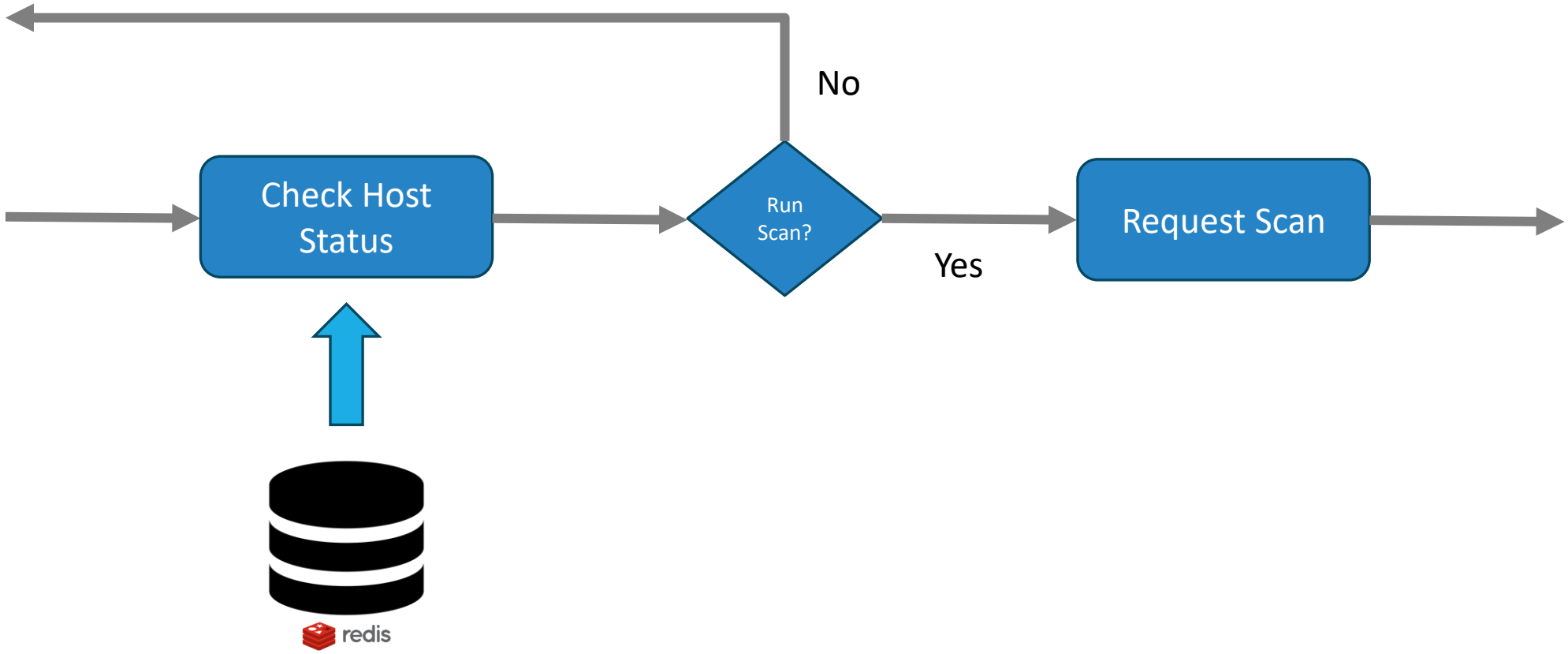
Implementation

Workflow



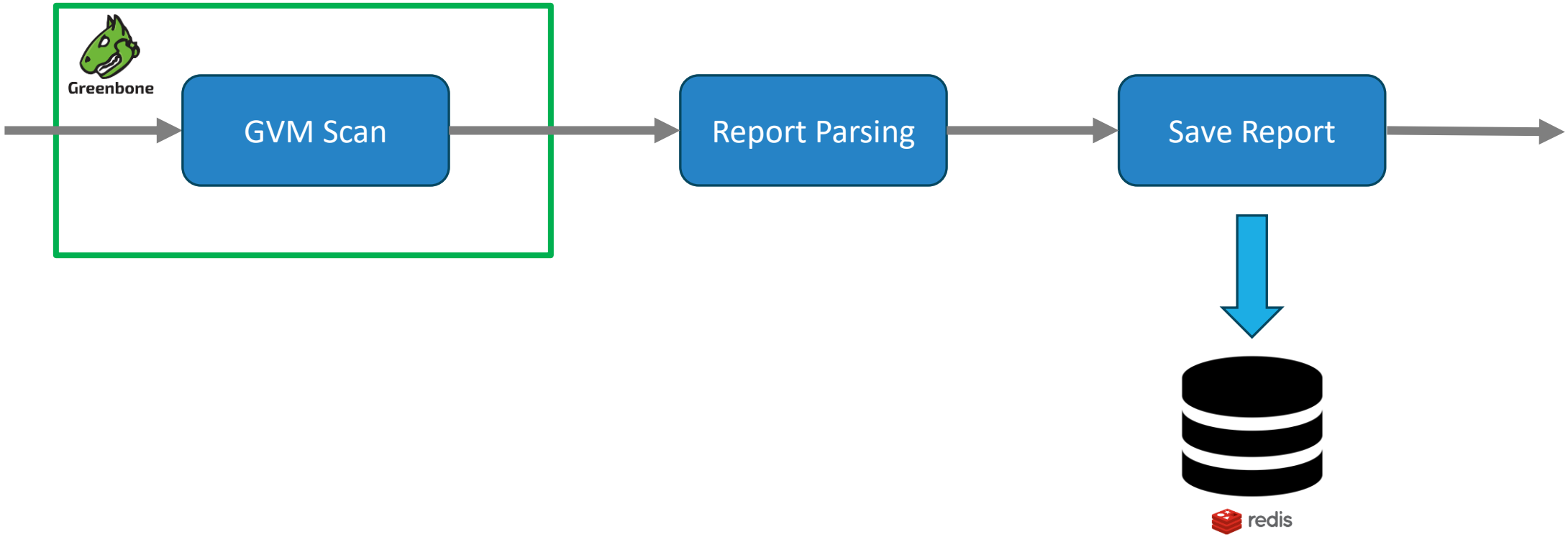
Implementation

Workflow



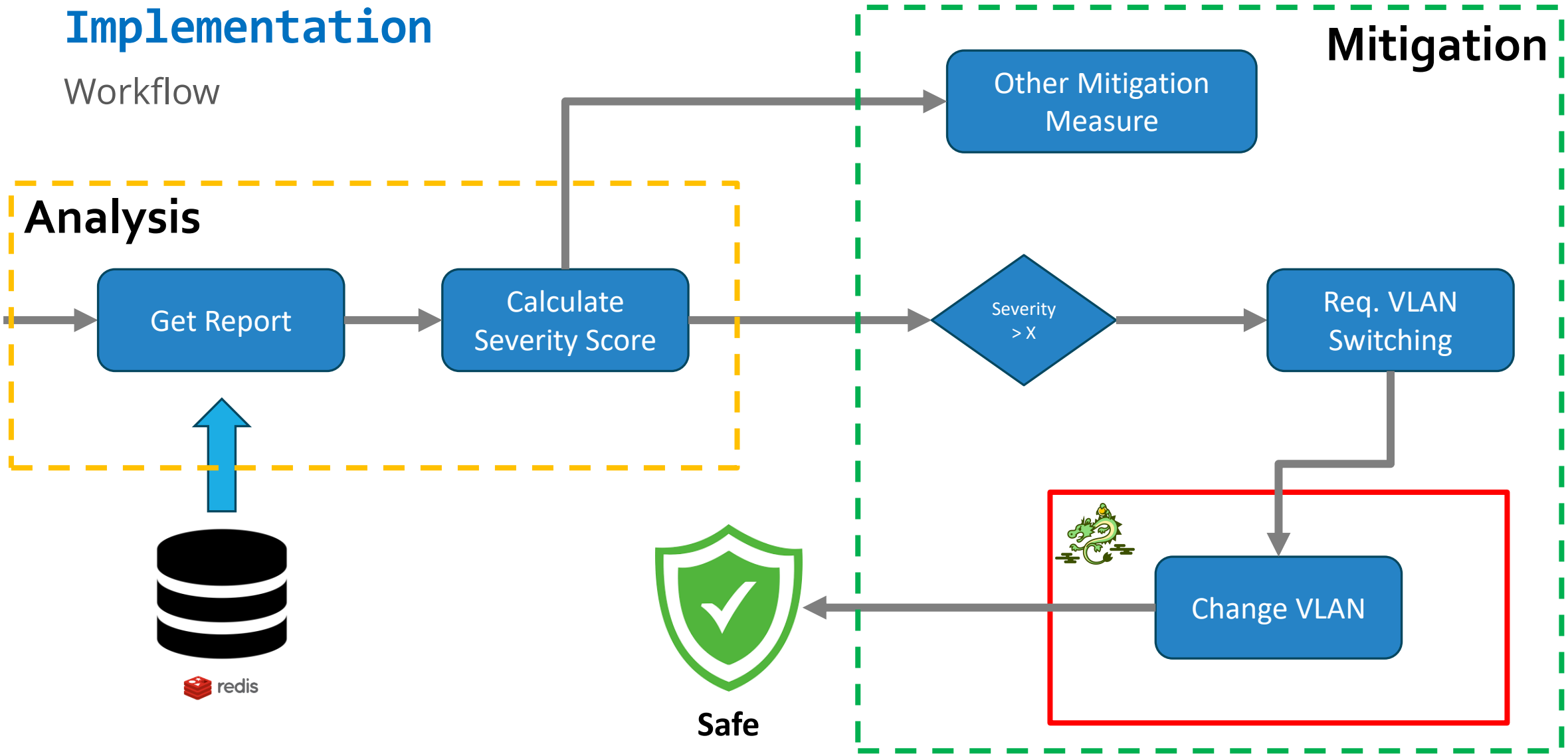
Implementation

Workflow



Implementation

Workflow



Experimental Setup

RQ1 - How to automate detection?
RQ2 - Detection scalable?

Scan Duration, CPU, RAM, Bandwidth

Laboratory Environment

RQ3 – SDN controller enhance security?
RQ4 – Timely deployment?

Duration of each stage
Time to complete

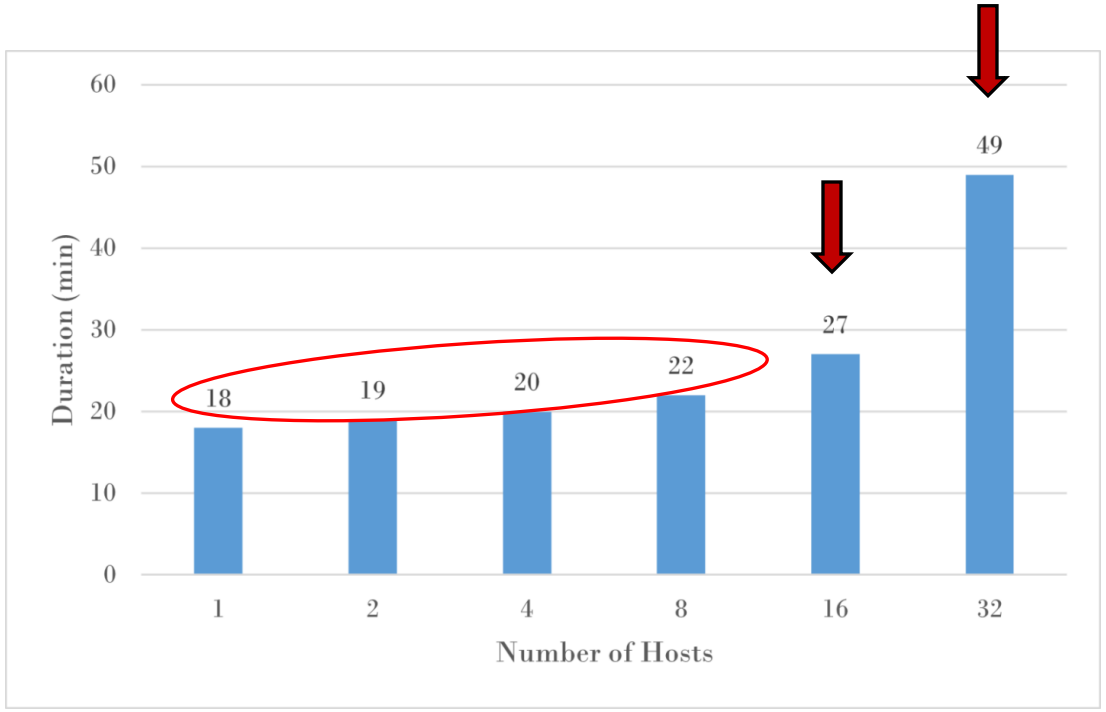
vmware

Virtual Environment

RQ1 - How to automate detection?
RQ2 - Detection scalable?
RQ3 – SDN controller enhance security?
RQ4 – Timely deployment?

Results

Scan Duration



Scan Duration

- From 1 to 8 hosts there is only a small increase of 4 minutes.
- For 16 hosts the increase is more noticible.
- For 32 hosts the scan duration reaches 49 minutes!

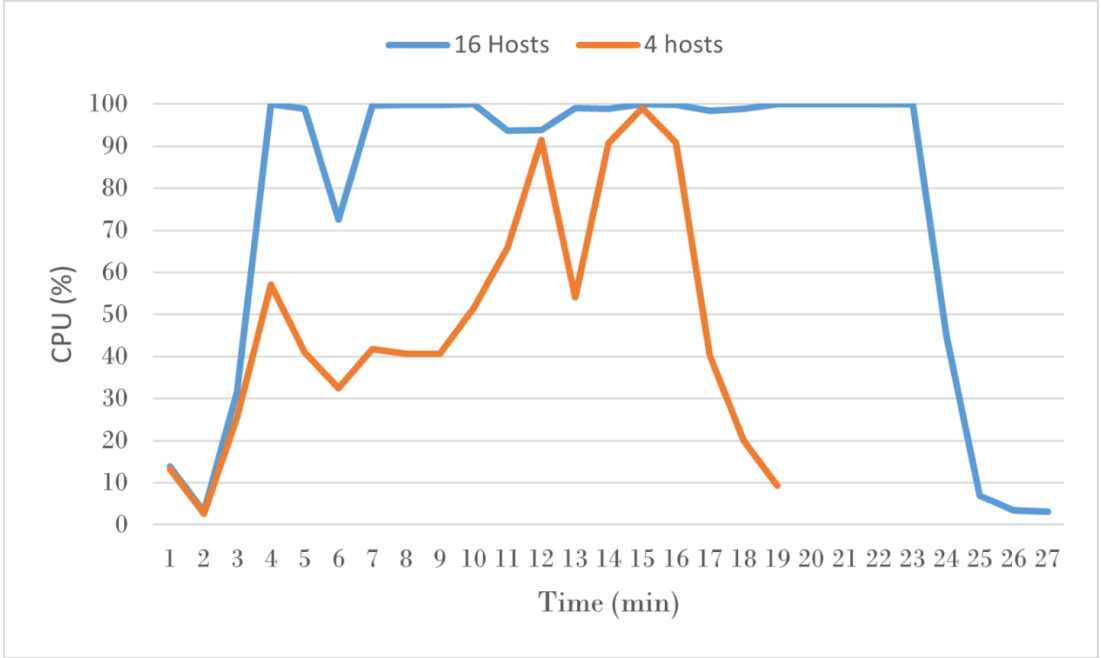
What can explain this?

RQ1 - How to automate detection?
RQ2 - Detection scalable?
RQ3 – SDN controller enhance security?
RQ4 – Timely deployment?

Results

CPU

- For 4 hosts the CPU only saturates one single time.
- For 16 hosts the system is saturated much more time.
- This explains the increase in the Scan Duration.



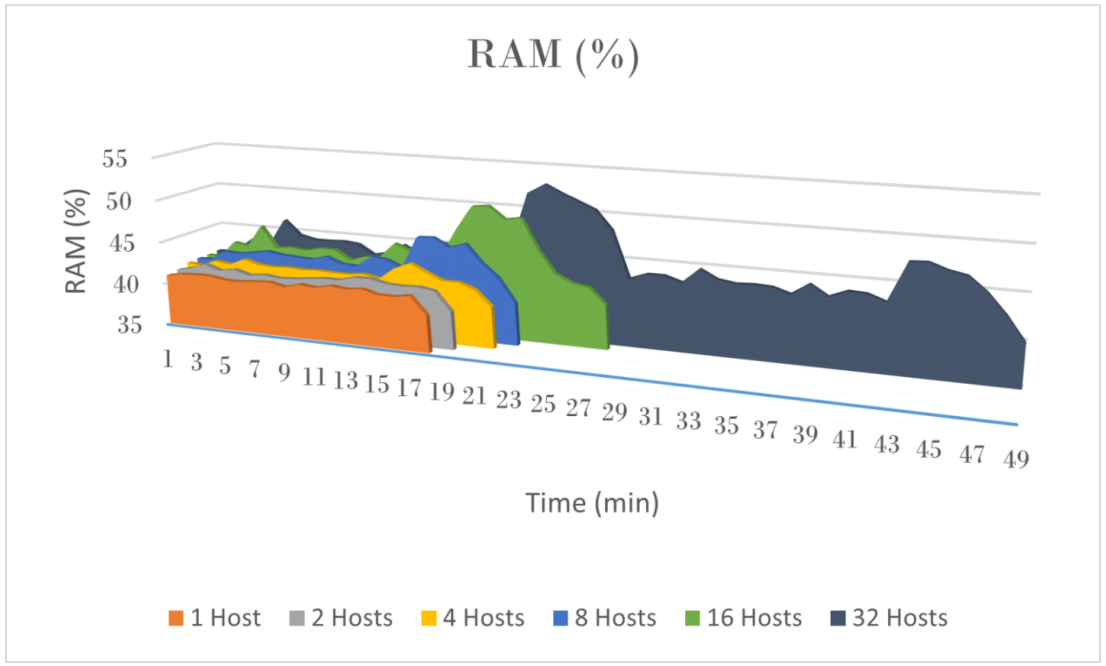
CPU

CPU Saturation → Difficult to promptly serve all hosts → Scan Duration Increases

RQ1 - How to automate detection?
RQ2 - Detection scalable?
RQ3 – SDN controller enhance security?
RQ4 – Timely deployment?

Results

RAM



RAM

- No noticible increase.
- No saturation.
- No outliers.

RQ1 - How to automate detection?
RQ2 - Detection scalable?
RQ3 – SDN controller enhance security?
RQ4 – Timely deployment?

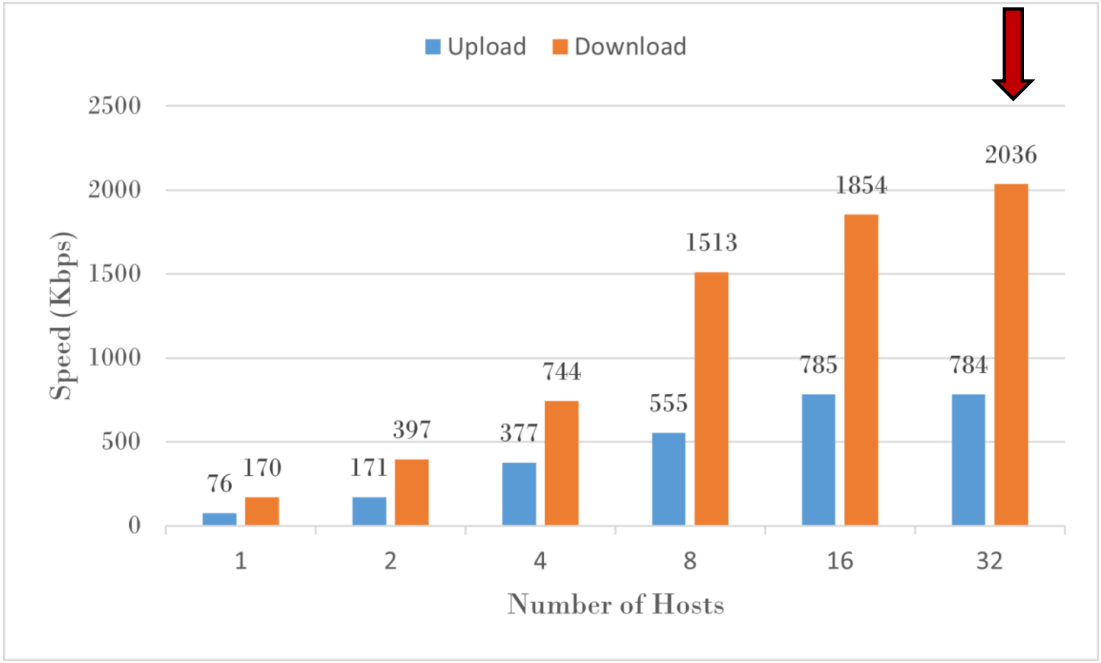
Results

Bandwidth

- LAN capacity is 100 Mbps.
- The scanning process does not reach near that value.

2 Mbps << 100 Mbps

Bandwidth doesn't disrupt the system



Bandwidth

Results

Time Analysis

RQ1 - How to automate detection?
RQ2 - Detection scalable?
RQ3 – SDN controller enhance security?
RQ4 – Timely deployment?

Device Discovery = 1,5 sec

Prepare Vulnerability Scan = 0,98 sec

Executing Vulnerability Scan = 18 min → **Expected doing the complexity**

Request and Parsing Report = 0,019 sec

Isolating the device = 0,000075 sec

} **Fast to secure the device**

Conclusions

RQ1 - The system **automates vulnerability detection** using Nmap for **device discovery** and GVM to **scan for vulnerabilities**. The SOAR Platform **orchestrates** these tools, automating workflows.

RQ2 - The vulnerability scanner shows **acceptable RAM** and **bandwidth** usage, but consumes **significant CPU** resources when scanning multiple devices simultaneously.

RQ3 - The SDN controller improves network security by enabling **isolation** of vulnerable devices by **changing VLANs**.

RQ4 - The entire process is **fast**, with the vulnerability scanning being the **longest delay**. The VLAN change occurs almost **instantly** in the SDN Controller.

Proactive and Automated System

Future Work

Applying more mitigation measures:

- **DPI** and/or **MTD** as a complementary measure to VLAN isolation for devices with low-risk vulnerabilities.
- **Analyze** the **CVSS vector** to **apply more appropriate mitigation measures.**

Node Classification and Scanning:

- SDN controller can be enhanced to classify nodes based on the context of the network topology, based on their proximity to critical assets.
  - Use the information gathered about the device's **location** on the network and the **number of connections** it has and **adjust** the **aggressiveness** and **periodicity** of the scans accordingly.
  - **Prioritize scanning** on devices that perform **critical functions** on the network.
- Perform **less aggressive** scans during periods of **high activity**, and reserve **more aggressive** scans for periods of **lower activity**.