Automatisierte Gefahrenabwehr am Netzwerkperimeter in dezentral administrierten Umgebungen

32. DFN-Konferenz: Sicherheit in Vernetzten Systemen

Nikolas Wintering, Eric Lanfer, Nils Aschenbruck

{**nwintering**, lanfer, aschenbruck}@uos.de

Institute of Computer Science - Distributed Systems Group

February 11, 2025

UNIVERSITÄT OSNABRÜCK

Table of Contents

1 Motivation
- Decentralized Network Administration
- SOAR
- Contributions

2 Architecture

3 Evaluation
- Test Deployment
- Attack Surface
- Time-to-Remediate
- User Survey

4 Conclusion

Outline

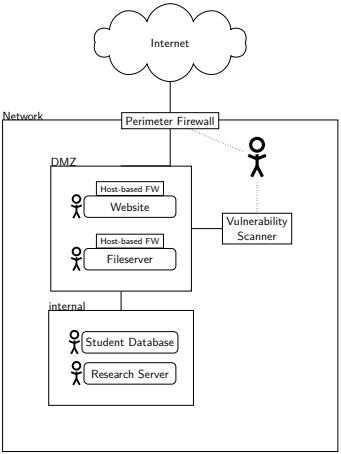
1 Motivation
- Decentralized Network Administration
- SOAR
- Contributions

2 Architecture

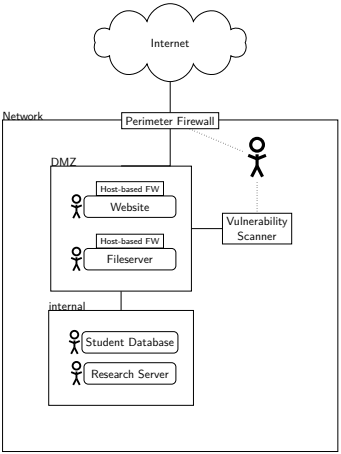
3 Evaluation
- Test Deployment
- Attack Surface
- Time-to-Remediate
- User Survey

4 Conclusion

Decentralized Network Administration

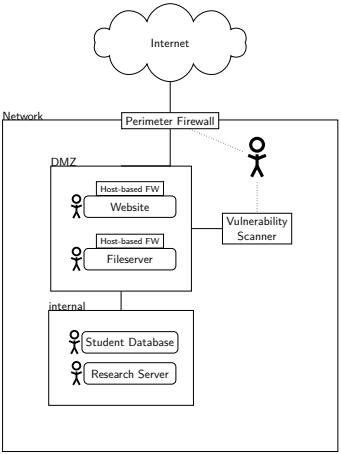


Decentralized Network Administration



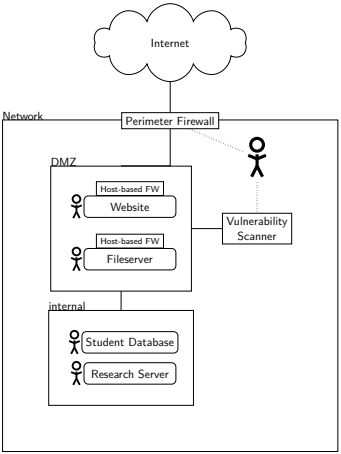
- Decentrally administered networks consist of many hosts which are administrated by different individuals

Decentralized Network Administration



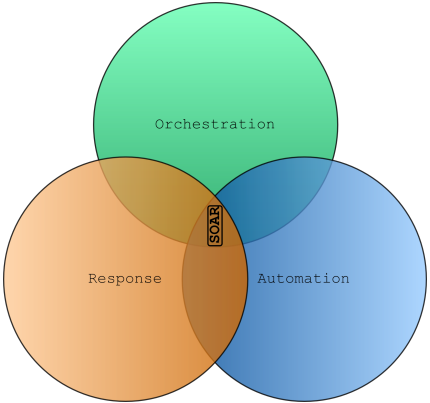
- Decentrally administered networks consist of many hosts which are administrated by different individuals
- important security tools:
  - Host-based Firewall (FW)
  - Perimeter FW
  - Vulnerability Scanner (V-Scanner)

Decentralized Network Administration



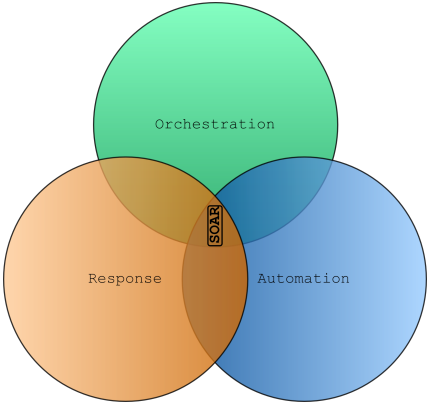
- Decentrally administered networks consist of many hosts which are administrated by different individuals
- important security tools:
  - Host-based Firewall (FW)
  - Perimeter FW
  - Vulnerability Scanner (V-Scanner)
- interaction between those tools has to be performed manually
  - time-consuming
  - inefficient

Security Orchestration, Automation and Response (SOAR)



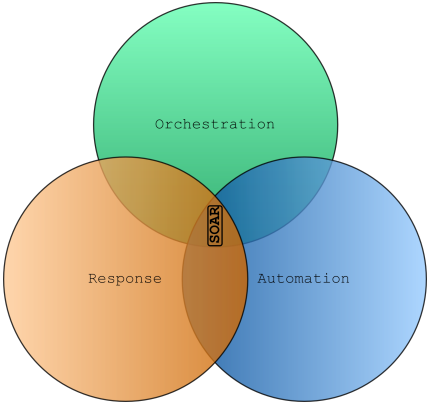
- integration/combination of different security tools

Security Orchestration, Automation and Response (SOAR)



- integration/combination of different security tools
- reduced workload at Security Operations Centers

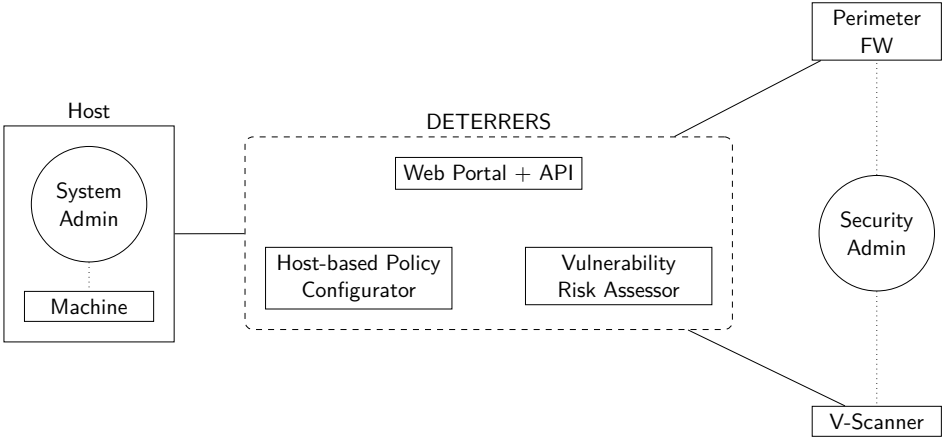
Security Orchestration, Automation and Response (SOAR)



- integration/combination of different security tools
- reduced workload at Security Operations Centers
- complete knowledge and control of network and systems expected

Solution

automateD nETwork pERimeter thREat pRevention System (DETERRERS)



Contributions

We:

1. automate (i) interactions between system administrators, security administrators, a V-Scanner, and a perimeter FW, (ii) a rule-based approach to vulnerability risk assessment, and (iii) the configuration of host-based FWs.

Contributions

We:

1. automate (i) interactions between system administrators, security administrators, a V-Scanner, and a perimeter FW, (ii) a rule-based approach to vulnerability risk assessment, and (iii) the configuration of host-based FWs.
2. decrease the attack surface of a decentrally administered university network.

Contributions

We:

1. automate (i) interactions between system administrators, security administrators, a V-Scanner, and a perimeter FW, (ii) a rule-based approach to vulnerability risk assessment, and (iii) the configuration of host-based FWs.
2. decrease the attack surface of a decentrally administered university network.
3. quantify the Time-to-Remediate (TTR) from vulnerabilities at the network perimeter and gain insights into the vulnerability lifetime during deployment.

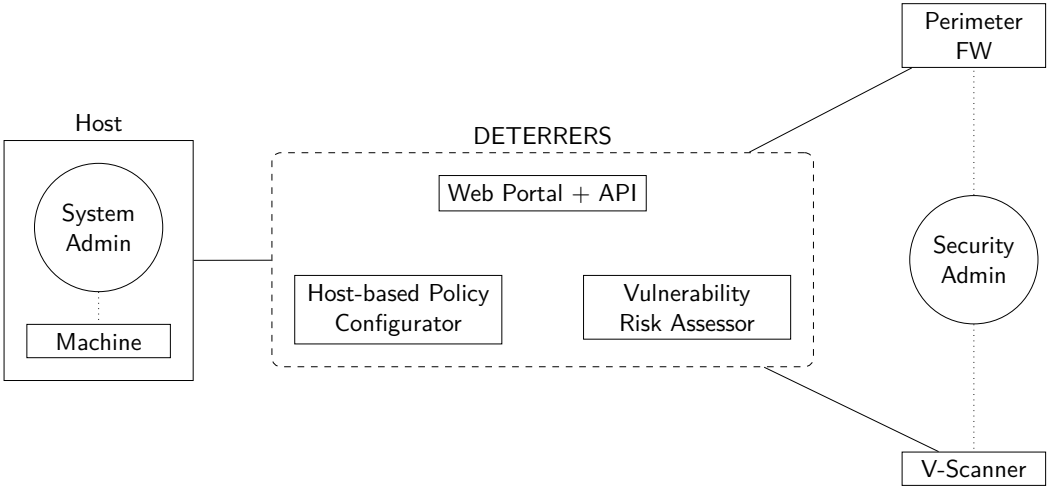
Outline

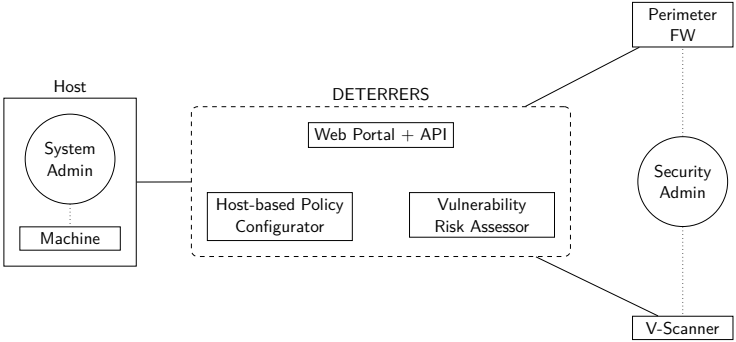
1 Motivation
- Decentralized Network Administration
- SOAR
- Contributions

2 Architecture

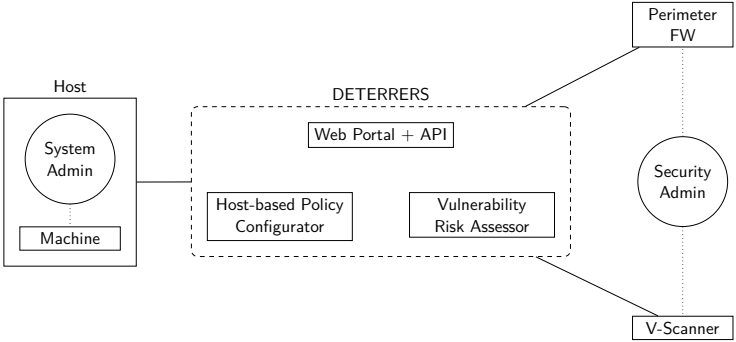
3 Evaluation
- Test Deployment
- Attack Surface
- Time-to-Remediate
- User Survey

4 Conclusion

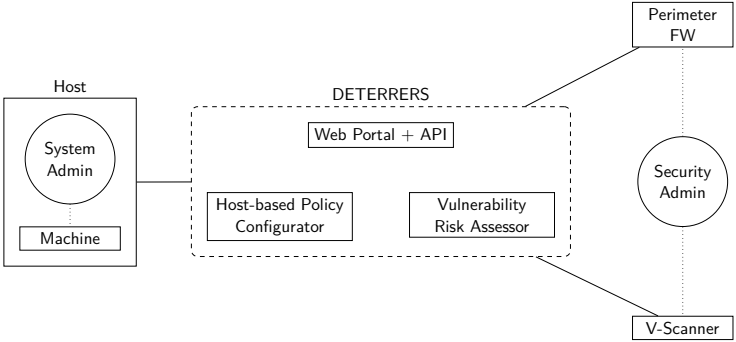

Perimeter FW
Host
DETERRERS
Web Portal + API
System Admin
Security Admin
Host-based Policy Configurator
Vulnerability Risk Assessor
Machine
V-Scanner



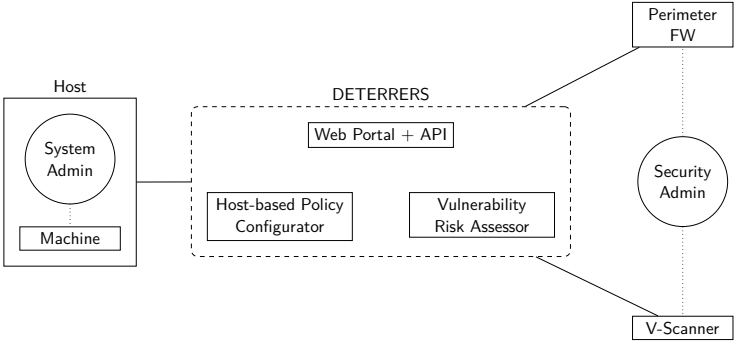
- build inventory of hosts and services at network perimeter



- build inventory of hosts and services at network perimeter
- orchestrated scans and perimeter FW policies

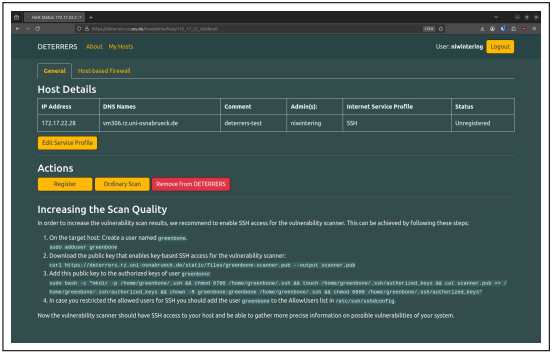


- build inventory of hosts and services at network perimeter
- orchestrated scans and perimeter FW policies
- automated risk assessment



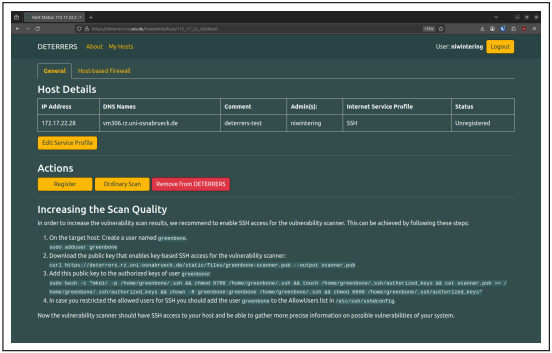
- build inventory of hosts and services at network perimeter
- orchestrated scans and perimeter FW policies
- automated risk assessment
- host-based firewall policy configuration

Host and Service Inventory



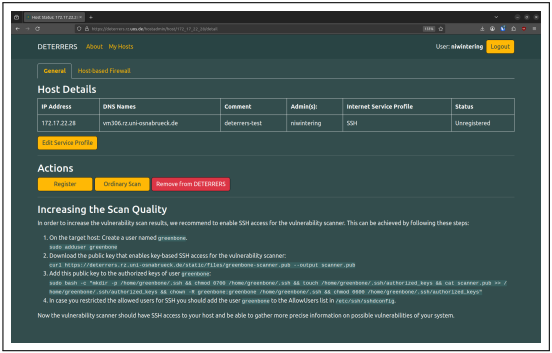
- system admins add all hosts they are responsible for

Host and Service Inventory



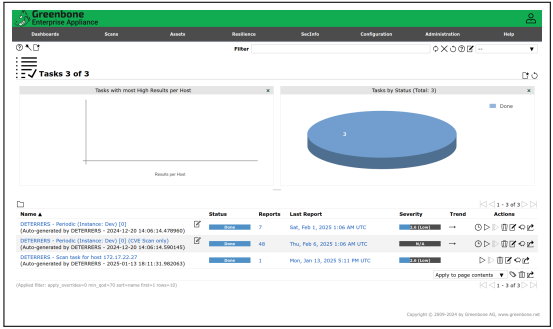
- system admins add all hosts they are responsible for
- each host gets an *Internet Service Profile*

Host and Service Inventory



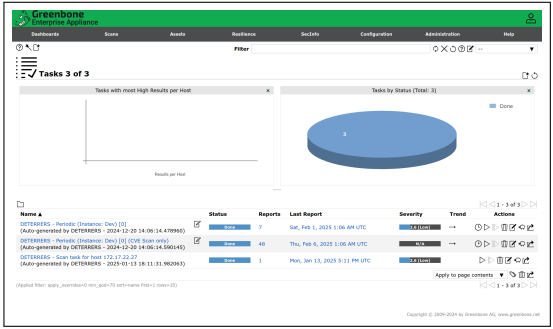
- system admins add all hosts they are responsible for
- each host gets an *Internet Service Profile*
- before exposure, hosts need to get registered

Scan Orchestration



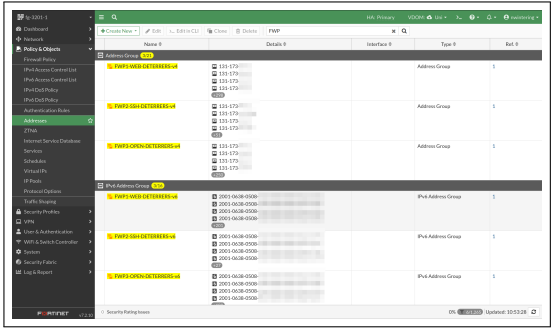
- implemented one V-Scanner interface
  - an API-wrapper for *Greenbone Management Protocol* and *Open Scanner Protocol* using the *Greenbone Vulnerability Management* Python library

Scan Orchestration



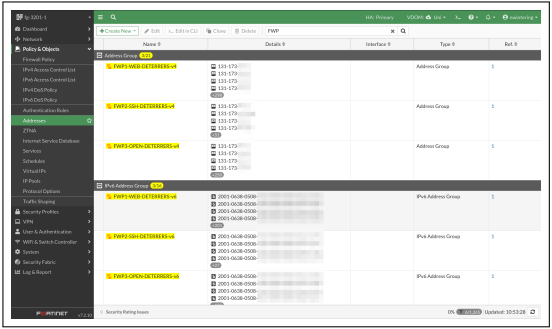
- implemented one V-Scanner interface
  - an API-wrapper for *Greenbone Management Protocol* and *Open Scanner Protocol* using the *Greenbone Vulnerability Management* Python library
- easily extensible for other V-Scanners

Perimeter FW Orchestration



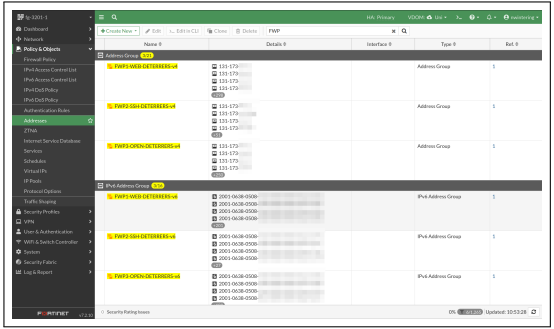
- implemented two interfaces to perimeter FWs

Perimeter FW Orchestration



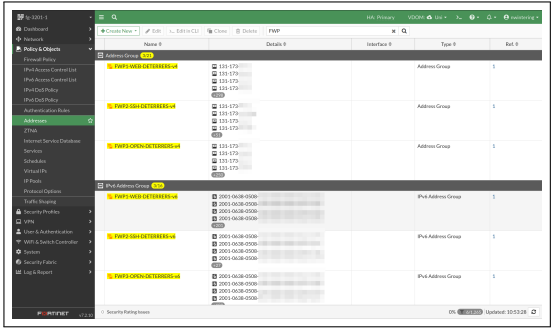
- implemented two interfaces to perimeter FWs
  - PaloAlto tested with PAN-OSv10.1 *(currently unmaintained)*

Perimeter FW Orchestration



- implemented two interfaces to perimeter FWs
  - PaloAlto tested with PAN-OSv10.1 *(currently unmaintained)*
  - Fortigate tested with ForitOSv7.2

Perimeter FW Orchestration



- implemented two interfaces to perimeter FWs
  - PaloAlto tested with PAN-OSv10.1 *(currently unmaintained)*
  - Fortigate tested with ForitOSv7.2
- easily extensible for other perimeter FWs

Automated Risk Assessment

- rule-based decision process

Automated Risk Assessment

- rule-based decision process
- three possible actions to take:

Automated Risk Assessment

- rule-based decision process
- three possible actions to take:
  - `None`: No serious risk

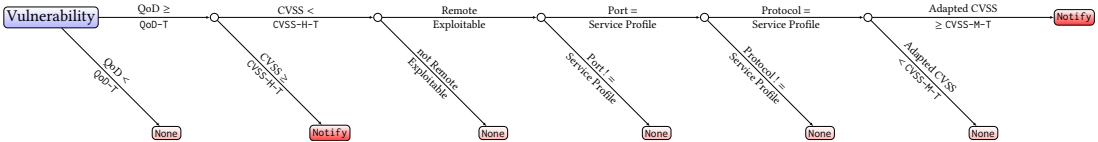
Automated Risk Assessment

- rule-based decision process
- three possible actions to take:
  - `None`: No serious risk
  - `Notify`: Low/medium risk (Internet-exposure) or high risk (internal exposure)

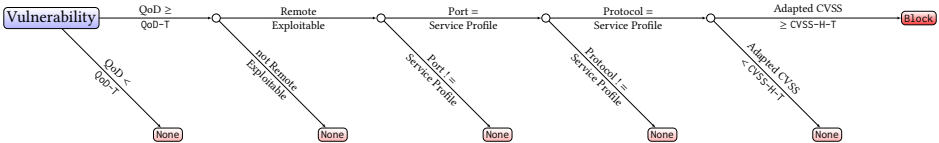
Automated Risk Assessment

- rule-based decision process
- three possible actions to take:
  - `None`: No serious risk
  - `Notify`: Low/medium risk (Internet-exposure) or high risk (internal exposure)
  - `Block`: High risk (Internet-exposure)

Automated Risk Assessment

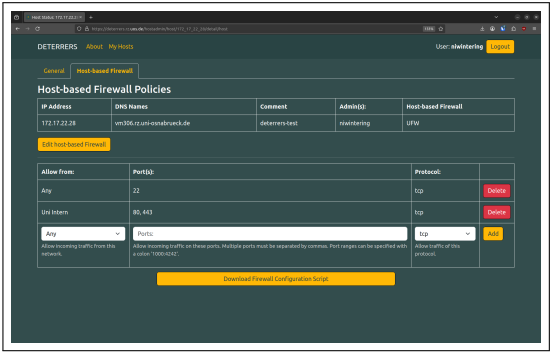


Notify Action



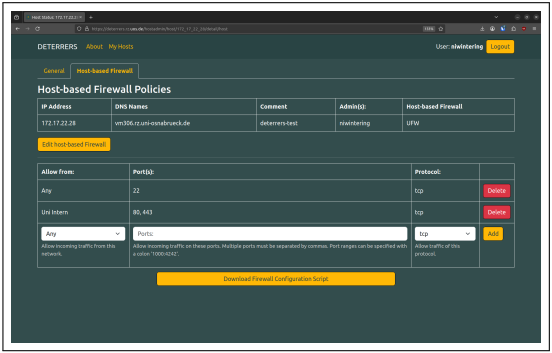
Block Action

Host-based FW Policy Configuration



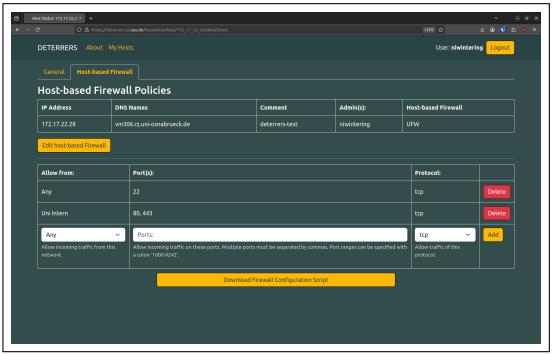
- generates configuration scripts for common firewall tools

Host-based FW Policy Configuration



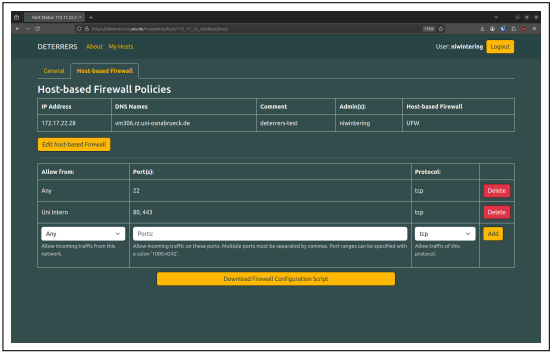
- generates configuration scripts for common firewall tools
- Outgoing: Default-Allow-Policy

Host-based FW Policy Configuration



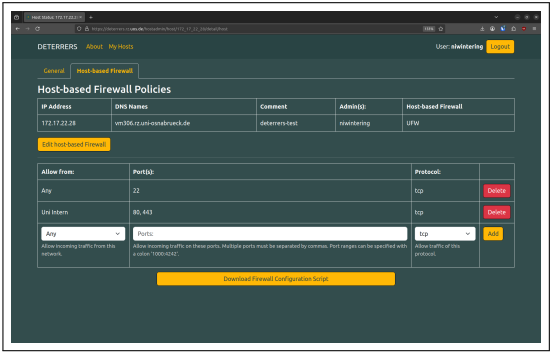
- generates configuration scripts for common firewall tools
- Outgoing: Default-Allow-Policy
- Incoming: Default-Deny-Policy

Host-based FW Policy Configuration



- generates configuration scripts for common firewall tools
- Outgoing: Default-Allow-Policy
- Incoming: Default-Deny-Policy
- custom exceptions:

Host-based FW Policy Configuration



- generates configuration scripts for common firewall tools
- Outgoing: Default-Allow-Policy
- Incoming: Default-Deny-Policy
- custom exceptions:
  - `Allow from:`
  - `Port(s):`
  - `Protocol:`

Outline

1 Motivation
- Decentralized Network Administration
- SOAR
- Contributions

2 Architecture

3 Evaluation
- Test Deployment
- Attack Surface
- Time-to-Remediate
- User Survey

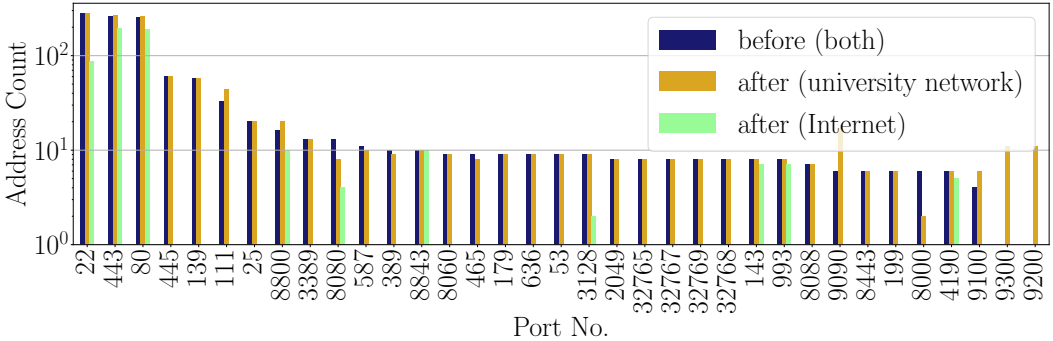
4 Conclusion

- selected subnets (max. 2048 IPs) in a university campus network

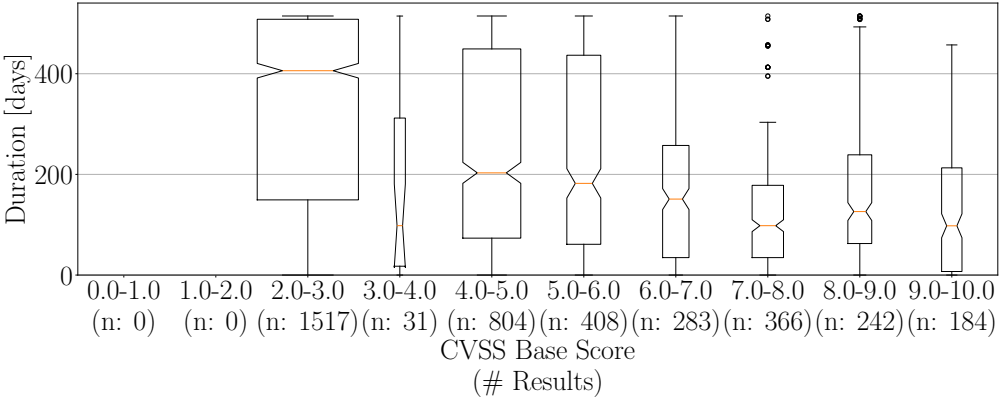
- selected subnets (max. 2048 IPs) in a university campus network
- port scans before and after deployment reached 595 and 738 hosts respectively

- selected subnets (max. 2048 IPs) in a university campus network
- port scans before and after deployment reached 595 and 738 hosts respectively
- $\sim$ 30 system administrators

- selected subnets (max. 2048 IPs) in a university campus network
- port scans before and after deployment reached 595 and 738 hosts respectively
- $\sim$ 30 system administrators
- $\sim$ 550 registered hosts

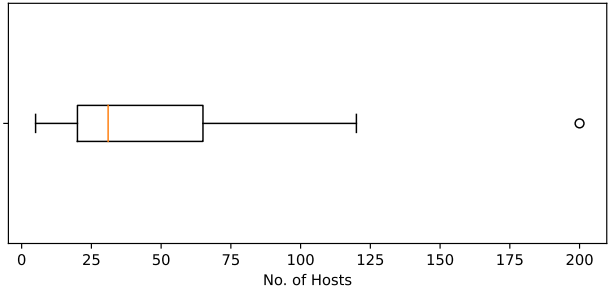


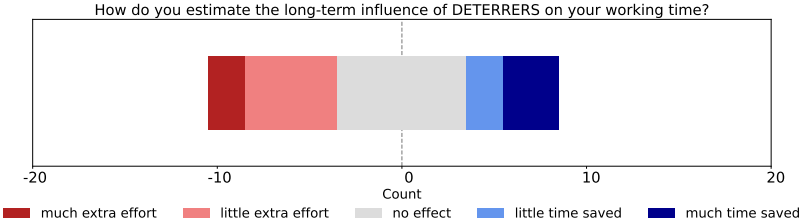
Number of IP addresses per open TCP port before and after 9 month deployment. Point of view in parentheses. n = 505 hosts. Excluded 98 ports which are open on $< 1\%$ of IPs.

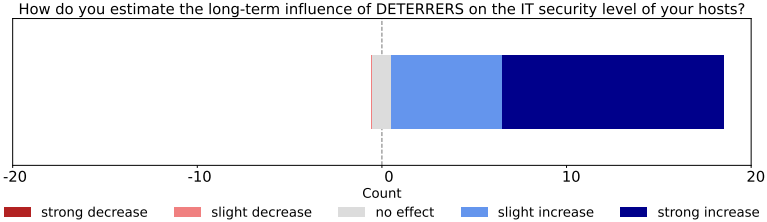


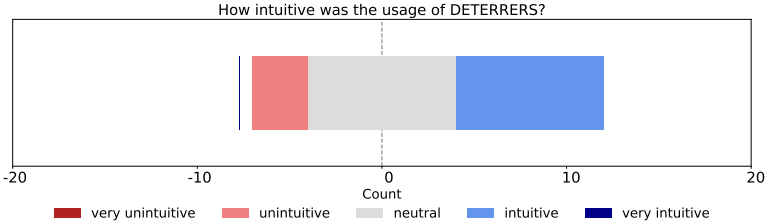
TTR of vulnerabilities per CVSS base score.

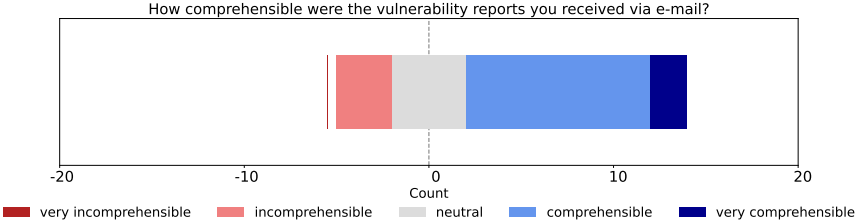
Number of hosts per system administrator




How do you estimate the long-term influence of DETERRERS on your working time?
-20
-10
0
10
20
Count
much extra effort
little extra effort
no effect
little time saved
much time saved


How do you estimate the long-term influence of DETERRERS on the IT security level of your hosts?
-20
-10
0
10
20
Count
strong decrease
slight decrease
no effect
slight increase
strong increase


How intuitive was the usage of DETERRERS?
-20
-10
0
10
20
Count
very unintuitive
unintuitive
neutral
intuitive
very intuitive


How comprehensible were the vulnerability reports you received via e-mail?
-20
-10
0
10
20
Count
very incomprehensible
incomprehensible
neutral
comprehensible
very comprehensible

Outline

1 Motivation
- Decentralized Network Administration
- SOAR
- Contributions

2 Architecture

3 Evaluation
- Test Deployment
- Attack Surface
- Time-to-Remediate
- User Survey

4 Conclusion

Conclusion

- proof-of-concept for SOAR in decentrally administered networks

Conclusion

- proof-of-concept for SOAR in decentrally administered networks
- automated workflows between system administrators, security administrators, V-Scanner, and perimeter FW

Conclusion

- proof-of-concept for SOAR in decentrally administered networks
- automated workflows between system administrators, security administrators, V-Scanner, and perimeter FW
- reduced attack surface towards the Internet

Conclusion

- proof-of-concept for SOAR in decentrally administered networks
- automated workflows between system administrators, security administrators, V-Scanner, and perimeter FW
- reduced attack surface towards the Internet
- estimation of vulnerability lifetimes

Future Work

- qualitative analysis of the risk assessment process

Future Work

- qualitative analysis of the risk assessment process
- comparison of other risk assessment approaches

Future Work

- qualitative analysis of the risk assessment process
- comparison of other risk assessment approaches
- incorporation of other security tools

Future Work

- qualitative analysis of the risk assessment process
- comparison of other risk assessment approaches
- incorporation of other security tools
- further deployments

Thank you for your attention!

https://github.com/UOS-RZ/deterrers

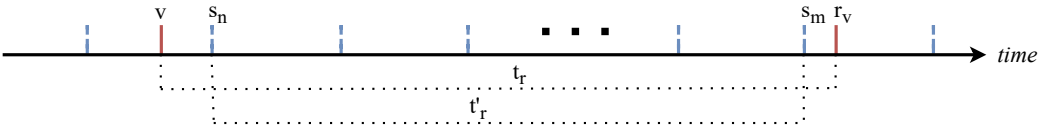
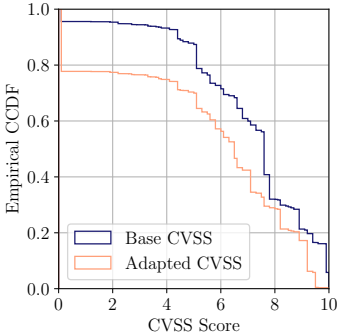
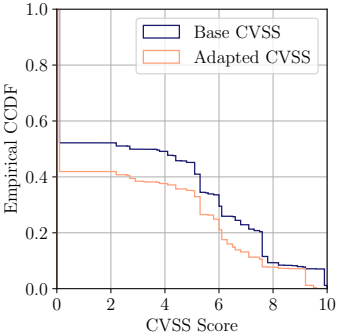


Figure: Schematic approach for approximating the TTR.



(a) All NVTs in the test corpus.



(b) Scan results before the test deployment.

Figure: Empirical Cumulative CDF of CVSS scores. Number of bins is 100 and they are equally sized.

Risk Assessment: Blocking

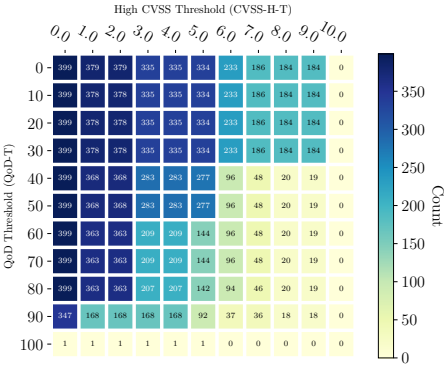


Figure: No. of blocked hosts

Risk Assessment: Notification

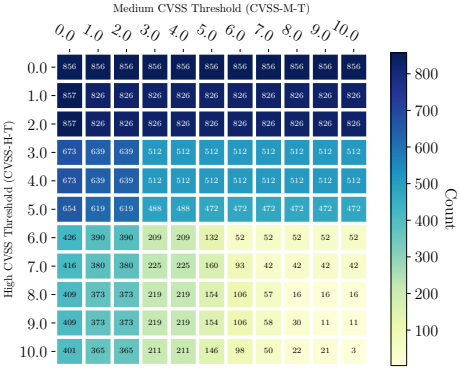


Figure: No. of notified hosts