

# 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



# 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

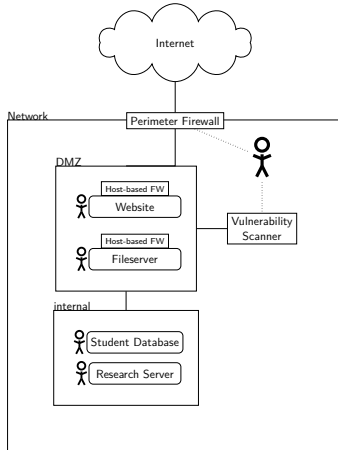
## 2 Architecture

## 3 Evaluation

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

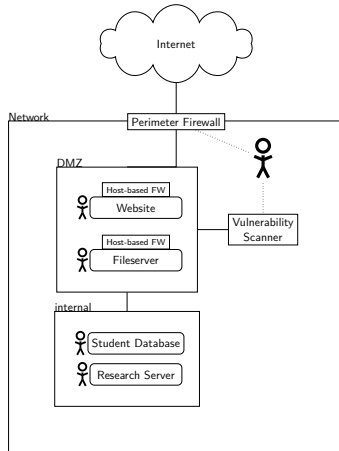
## 4 Conclusion

# Decentralized Network Administration

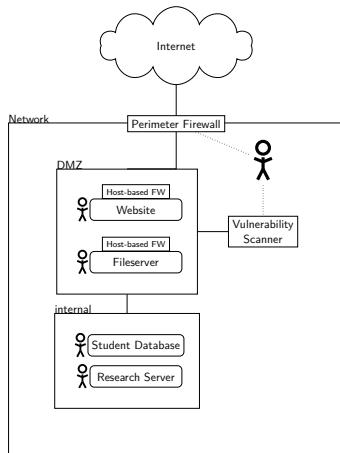


# Decentralized Network Administration

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

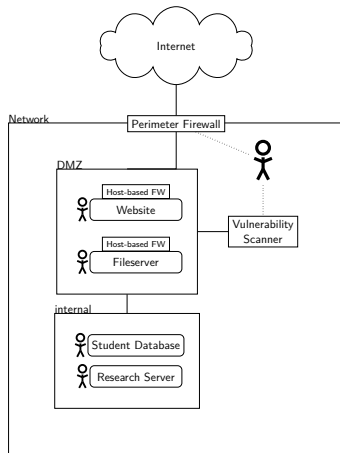


# Decentralized Network Administration



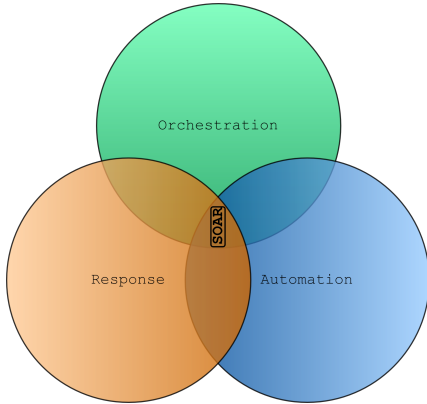
- Decentrally administered networks consist of many hosts which are administrated by different individuals
- important security tools:
  - Host-based Firewall (FW)
  - Perimeter FW
  - Vulnerability Scanner (V-Scanner)

# 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

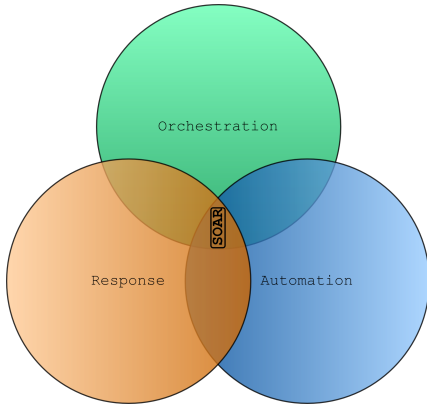
# Security Orchestration, Automation and Response (SOAR)



- integration/combination of different security tools

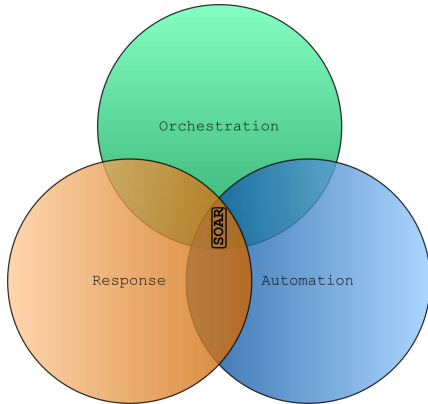


# Security Orchestration, Automation and Response (SOAR)



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

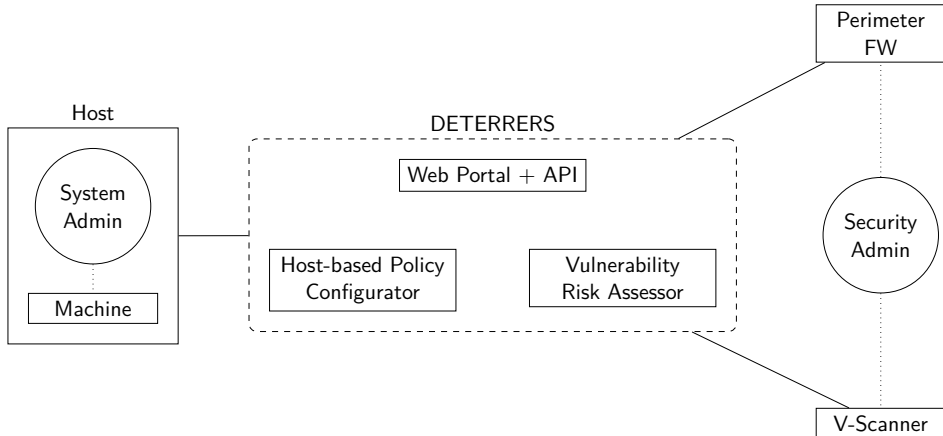
# Security Orchestration, Automation and Response (SOAR)



- 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

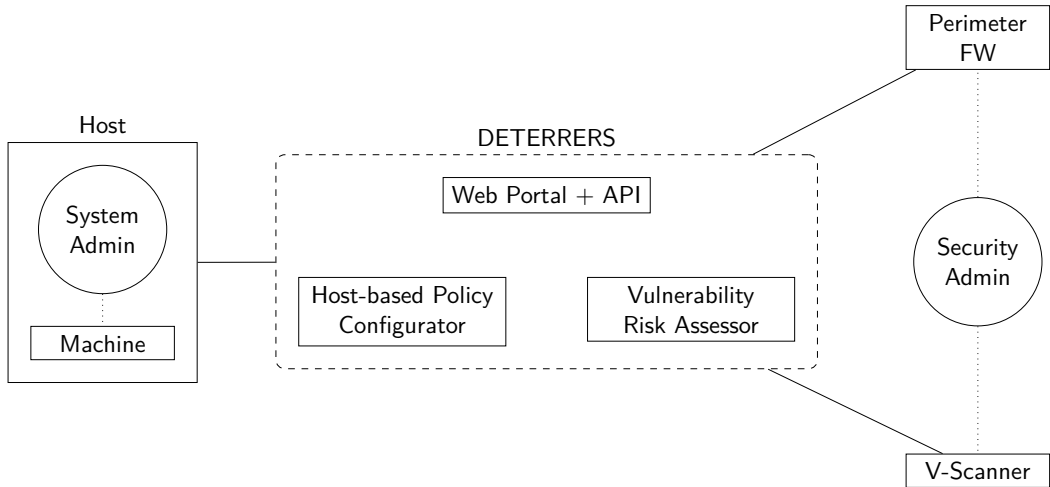
- Decentralized Network Administration
- SOAR
- Contributions

## 2 Architecture

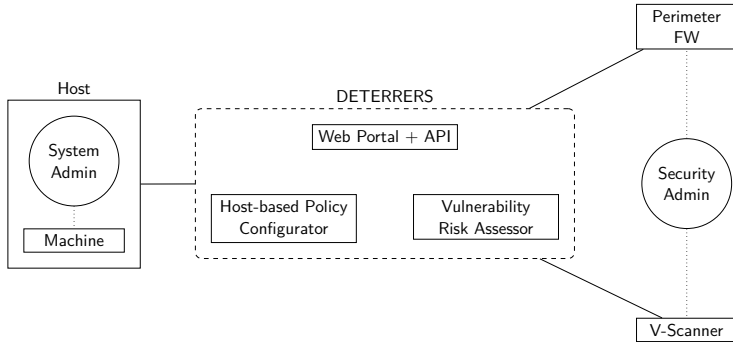
## 3 Evaluation

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

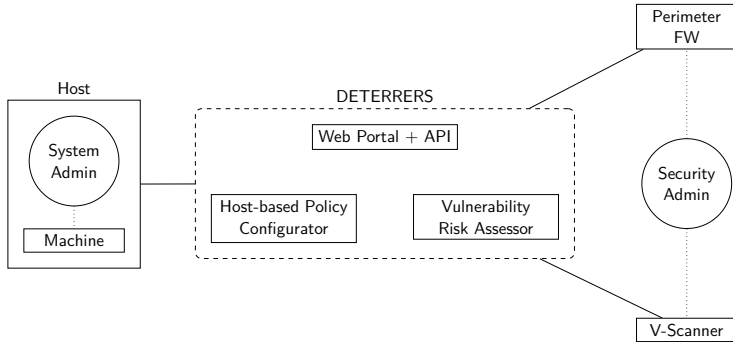
## 4 Conclusion



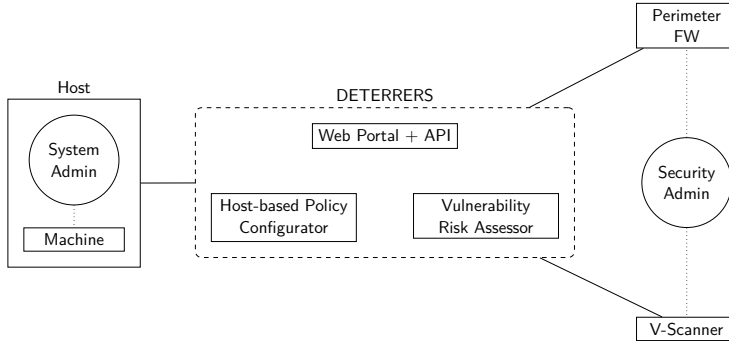




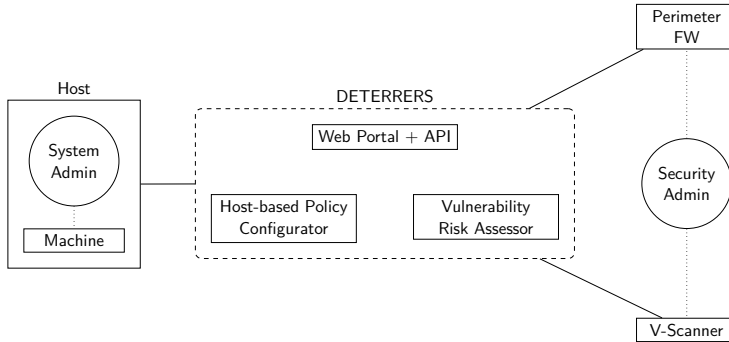
- build inventory of hosts and services at network perimeter



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

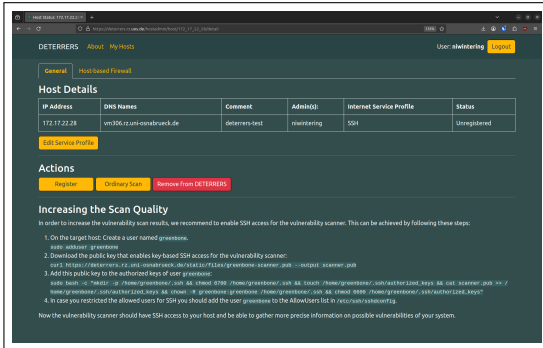


- build inventory of hosts and services at network perimeter
- orchestrated scans and perimeter FW policies
- automated risk assessment



- 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



The screenshot shows the DETERRERS web interface. At the top, there are tabs for 'General', 'Host-Based Firewall', and 'Host Details'. The 'Host Details' tab is active, displaying a table with host information. Below the table, there are buttons for 'Edit Service Profile', 'Register', 'Ordinary Scan', and 'Remove from DETERRERS'. A section titled 'Increasing the Scan Quality' provides instructions on how to enable SSH access for the vulnerability scanner.

IP Address	DNS Names	Comment	Admin(s)	Internet Service Profile	Status
172.17.22.28	vm356.rz.uni-osnabrueck.de	deterrens-test	nwintering	SSH	Unregistered

**Actions**

Register Ordinary Scan Remove from DETERRERS

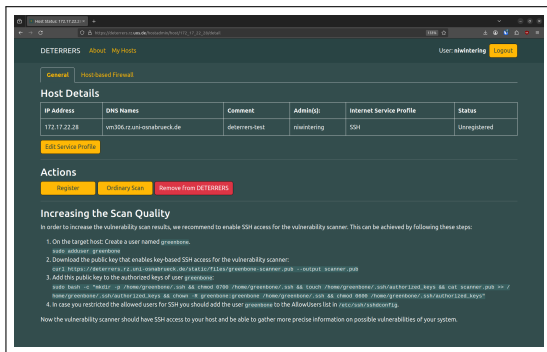
**Increasing the Scan Quality**

In order to increase the vulnerability scan results, we recommend to enable SSH access for the vulnerability scanner. This can be achieved by following these steps:

1. On the target host: Create a user named greenbone.
2. Download the public key that enables key-based SSH access for the vulnerability scanner:  
`curl https://deterrens.rz.uni-osnabrueck.de/atlatic/files/greenbone-scanner.pub --output scanner.pub`
3. Add this public key to the authorized keys of user greenbone:  
`ssh-keygen -i "ssh-rsa-1024 greenbone@greenbone.org" -f scanner.pub -C "greenbone@greenbone.org"`
4. In case you restricted the allowed users for SSH you should add the user greenbone to the AllowUsers list in /etc/ssh/sshd\_config.

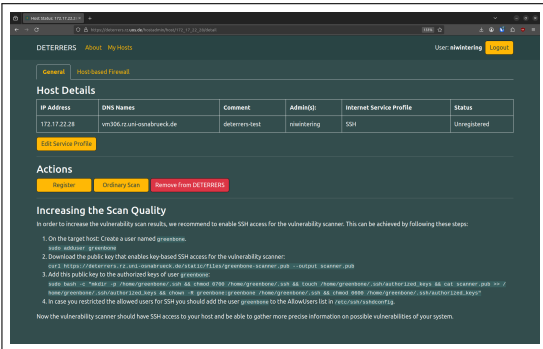
Now the vulnerability scanner should have SSH access to your host and be able to gather more precise information on possible vulnerabilities of your system.

- system admins add all hosts they are responsible for



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

# Host and Service Inventory



The screenshot shows the DETERRERS web interface. At the top, there are tabs for 'General', 'Host-Based Firewall', and 'Host Details'. The 'Host Details' tab is active, displaying a table with host information. Below the table, there are buttons for 'Edit Service Profile', 'Register', 'Ordinary Scan', and 'Remove from DETERRERS'. A section titled 'Increasing the Scan Quality' provides instructions on how to enable SSH access for the vulnerability scanner.

IP Address	DNS Names	Comment	Admin(s)	Internet Service Profile	Status
172.17.22.28	vm356.rz.uni-osnabrueck.de	deterrens-test	nwintering	SSH	Unregistered

**Actions**

Register Ordinary Scan Remove from DETERRERS

**Increasing the Scan Quality**

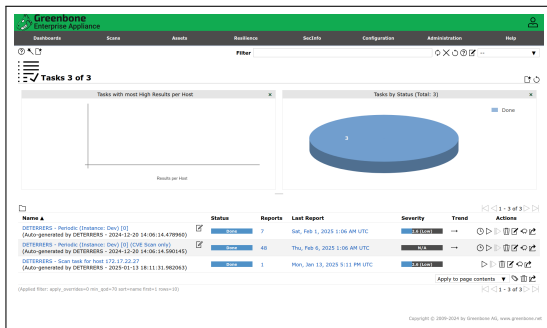
In order to increase the vulnerability scan results, we recommend to enable SSH access for the vulnerability scanner. This can be achieved by following these steps:

1. On the target host: Create a user named greenbone.
2. Download the public key that enables key-based SSH access for the vulnerability scanner:
3. Add this public key to the authorized keys of user greenbone:
4. In case you restricted the allowed users for SSH you should add the user greenbone to the AllowUsers list in /etc/ssh/sshd\_config.

Now the vulnerability scanner should have SSH access to your host and be able to gather more precise information on possible vulnerabilities of your system.

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

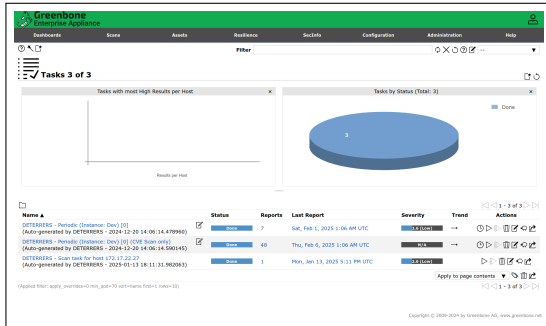
# Scan Orchestration



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

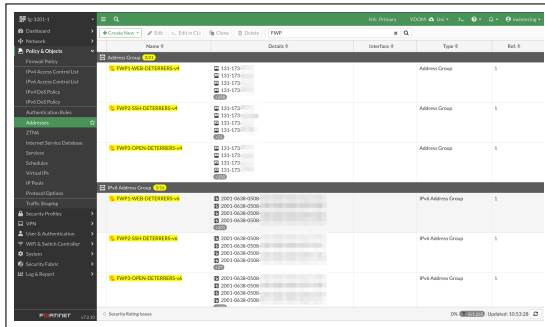


# Scan Orchestration



- 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



Name	Details	Interface	Type	Ref
FWP3-WEB-DETECTORS-v4	131-179 131-179 131-179 131-179		Address Group	1
FWP2-SM-DTECTORS-v4	131-179 131-179 131-179 131-179		Address Group	1
FWP3-OPEN-SCTHROUGHS-v4	131-179 131-179 131-179 131-179		Address Group	1
FWP3-WEB-DETECTORS-v6	2001:0a08:0500: 2001:0a08:0500: 2001:0a08:0500: 2001:0a08:0500:		IPv6 Address Group	1
FWP2-SM-DTECTORS-v6	2001:0a08:0500: 2001:0a08:0500: 2001:0a08:0500: 2001:0a08:0500:		IPv6 Address Group	1
FWP3-OPEN-SCTHROUGHS-v6	2001:0a08:0500: 2001:0a08:0500: 2001:0a08:0500: 2001:0a08:0500:		IPv6 Address Group	1

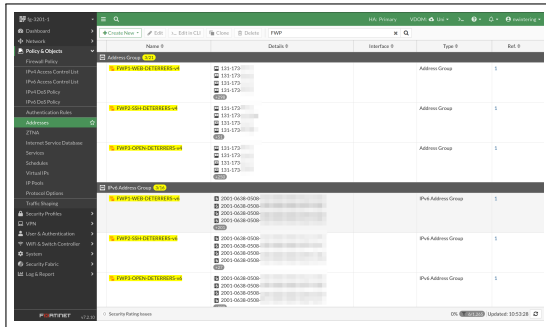
- implemented two interfaces to perimeter FWs

# Perimeter FW Orchestration

Name	Details	Interface	Type	Ref.
FWP3-WEB-DETECTORS-v4	131-179 131-179 131-179 131-179		Address Group	1
FWP3-SM-DETECTORS-v4	131-179 131-179 131-179 131-179		Address Group	1
FWP3-OPEN-DETECTORS-v4	131-179 131-179 131-179 131-179		Address Group	1
FWP3-WEB-DETECTORS-v6	2001:0a08-0508- 2001:0a08-0508- 2001:0a08-0508- 2001:0a08-0508-		IPv6 Address Group	1
FWP3-SM-DETECTORS-v6	2001:0a08-0508- 2001:0a08-0508- 2001:0a08-0508- 2001:0a08-0508-		IPv6 Address Group	1
FWP3-OPEN-DETECTORS-v6	2001:0a08-0508- 2001:0a08-0508- 2001:0a08-0508- 2001:0a08-0508-		IPv6 Address Group	1

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

# Perimeter FW Orchestration

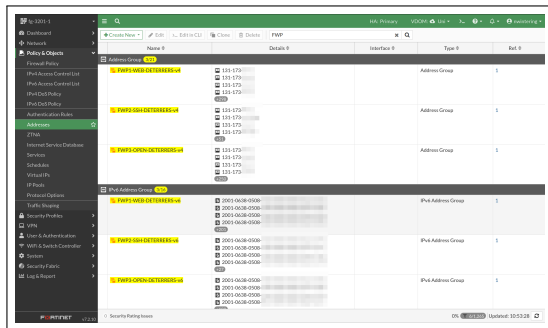


The screenshot displays the Palo Alto Networks PAN-OS configuration interface. The left sidebar shows the navigation menu with 'Policy & Objects' selected. The main pane shows the 'Address Groups' configuration page. A table lists several address groups, including 'FWP3-WEB-DETERRERS-v4', 'FWP3-SM-DETERRERS-v4', and 'FWP3-OPEN-SCT-DETERRERS-v4'. Each group is associated with a list of IP addresses (131.179.131.179) and is configured as an 'IPv4 Address Group'.

Name	Details	Interface	Type	Ref
FWP3-WEB-DETERRERS-v4	131.179.131.179		Address Group	1
FWP3-SM-DETERRERS-v4	131.179.131.179		Address Group	1
FWP3-OPEN-SCT-DETERRERS-v4	131.179.131.179		Address Group	1

- implemented two interfaces to perimeter FWs
  - PaloAlto tested with PAN-OSv10.1 (*currently unmaintained*)
  - Fortigate tested with FortiOSv7.2

# Perimeter FW Orchestration



The screenshot displays the Palo Alto Networks PAN-OS configuration interface for a Firewall Policy. The left sidebar shows the navigation menu with 'Policy & Objects' selected. The main pane shows a table of Firewall Policy rules. The table has columns for Name, Details, Interface, Type, and Ref. The rules are listed as follows:

Name	Details	Interface	Type	Ref.
FWP3 WEB DETERRERS-v4	131-179		Address Group	1
FWP2 SSH DETERRERS-v4	131-179		Address Group	1
FWP3 OPEN-SCT100002-v4	131-179		Address Group	1
FWP3 WEB DETERRERS-v4	2001-0608-0500	IPv4-Address Group	IPv4-Address Group	1
FWP2 SSH DETERRERS-v4	2001-0608-0500	IPv4-Address Group	IPv4-Address Group	1
FWP3 OPEN-SCT100002-v4	2001-0608-0500	IPv4-Address Group	IPv4-Address Group	1

- implemented two interfaces to perimeter FWs
  - PaloAlto tested with PAN-OSv10.1 (*currently unmaintained*)
  - Fortigate tested with FortiOSv7.2
- 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



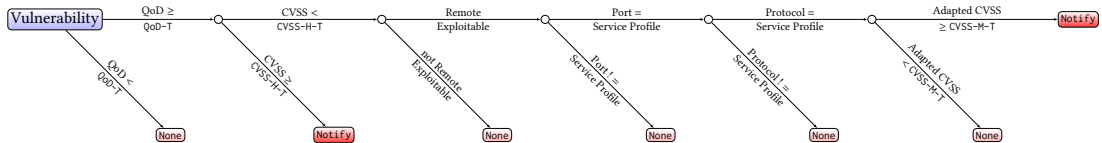
# Automated Risk Assessment

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

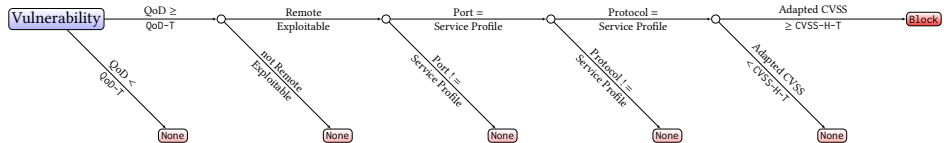
# Automated Risk Assessment

- 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

The screenshot shows the DETERRERS web interface. At the top, there are tabs for 'General' and 'Host-based Firewall'. The 'Host-based Firewall' tab is active. Below the tabs, there is a table titled 'Host-based Firewall Policies'. The table has columns: IP Address, DNS Names, Comment, Admin(s), and Host-based Firewall. The first row shows IP Address 172.17.22.28, DNS Names vm356.rz.uni-osnabrueck.de, Comment deterrers-test, Admin(s) rzwintering, and Host-based Firewall UFW. Below the table, there is a yellow button labeled 'Edit host-based Firewall'. Below the button, there is a form with fields for 'Allow from:', 'Port(s):', 'Protocol:', and 'Add'. The 'Allow from:' field has a dropdown menu with 'Any' selected. The 'Port(s):' field has a text input with '22'. The 'Protocol:' field has a dropdown menu with 'tcp' selected. There are 'Delete' buttons next to each row in the table. At the bottom, there is a yellow button labeled 'Download Firewall Configuration Script'.

IP Address	DNS Names	Comment	Admin(s)	Host-based Firewall
172.17.22.28	vm356.rz.uni-osnabrueck.de	deterrers-test	rzwintering	UFW

Edit host-based Firewall

Allow from:	Port(s):	Protocol:	
Any	22	tcp	Delete
Uni Intern	80, 443	tcp	Delete
Any	Port(s):	tcp	Add

Download Firewall Configuration Script

- generates configuration scripts for common firewall tools

# Host-based FW Policy Configuration

The screenshot shows the DETERRERS web interface. At the top, there are tabs for 'General' and 'Host-based Firewall'. The 'Host-based Firewall' tab is active. Below the tabs, there is a table titled 'Host-based Firewall Policies'. The table has columns: IP Address, DNS Names, Comment, Admin(s), and Host-based Firewall. The first row shows IP Address 172.17.22.28, DNS Names vm356.rz.uni-osnabrueck.de, Comment deterrers-test, Admin(s) rzwintering, and Host-based Firewall UFW. Below the table, there is a yellow button labeled 'Edit host-based Firewall'. Below the button, there is a form with two rows. The first row has 'Allow from:' set to 'Any', 'Port(s):' set to '22', 'Protocol:' set to 'tcp', and a red 'Delete' button. The second row has 'Allow from:' set to 'Uni Intern', 'Port(s):' set to '80, 443', 'Protocol:' set to 'tcp', and a red 'Delete' button. Below the form, there is a yellow button labeled 'Download Firewall Configuration Script'.

IP Address	DNS Names	Comment	Admin(s)	Host-based Firewall
172.17.22.28	vm356.rz.uni-osnabrueck.de	deterrers-test	rzwintering	UFW

[Edit host-based Firewall](#)

Allow from:	Port(s):	Protocol:	
Any	22	tcp	<a href="#">Delete</a>
Uni Intern	80, 443	tcp	<a href="#">Delete</a>

[Any](#) [Port\(s\):](#) [tcp](#) [Add](#)

Allow incoming traffic from this network.

Allow incoming traffic on these ports. Multiple ports must be separated by commas. Port ranges can be specified with a colon "1000-4242".

Allow traffic of this protocol.

[Download Firewall Configuration Script](#)

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

# Host-based FW Policy Configuration

The screenshot shows the DETERRERS web interface for configuring host-based firewall policies. The user is logged in as 'nwintering'. The 'Host-based Firewall' tab is active, displaying a table of existing policies and a form to add new ones.

**Host-based Firewall Policies**

IP Address	DNS Names	Comment	Admin(s)	Host-based Firewall
172.17.22.28	vm356.rz.uni-osnabrueck.de	deterres-test	nwintering	UFW

[Edit host-based Firewall](#)

**Add New Policy**

Allow from:	Port(s):	Protocol:	
Any	22	tcp	<a href="#">Delete</a>
Uni Intern	80, 443	tcp	<a href="#">Delete</a>
<input type="text" value="Any"/>	<input type="text" value="Port(s):"/>	<input type="text" value="tcp"/>	<a href="#">Add</a>

Allow incoming traffic from this network.

Allow incoming traffic on these ports. Multiple ports must be separated by commas. Port ranges can be specified with a colon '1000-4242'.

Allow traffic of this protocol.

[Download Firewall Configuration Script](#)

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

# Host-based FW Policy Configuration

The screenshot shows the DETERRERS web interface for configuring host-based firewall policies. The user is logged in as 'nwintering'. The 'Host-based Firewall' tab is active, displaying a table of existing policies and a form to add new ones.

**Host-based Firewall Policies**

IP Address	DNS Names	Comment	Admin(s)	Host-based Firewall
172.17.22.28	vm356.rz.uni-osnabrueck.de	deterres-test	nwintering	UFW

[Edit host-based Firewall](#)

**Add New Policy Form:**

Allow from:	Port(s):	Protocol:	
Any	22	tcp	<a href="#">Delete</a>
Uni Intern	80, 443	tcp	<a href="#">Delete</a>
<input type="text" value="Any"/>	<input type="text" value="Port(s):"/>	<input type="text" value="tcp"/>	<a href="#">Add</a>

Allow incoming traffic from this network.  
Allow incoming traffic on these ports. Multiple ports must be separated by commas. Port ranges can be specified with a colon '1000-4242'.  
Allow traffic of this protocol.

[Download Firewall Configuration Script](#)

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

# Host-based FW Policy Configuration

The screenshot shows the DETERRERS web interface for configuring host-based firewall policies. The user is logged in as 'nwintering'. The 'Host-based Firewall' tab is active, displaying a table of existing policies and a form to add new ones.

IP Address	DNS Names	Comment	Admin(s)	Host-based Firewall
172.17.22.28	vm356.rz.uni-osnabrueck.de	deterres-test	nwintering	UFW

[Edit host-based Firewall](#)

Allow from:	Port(s):	Protocol:	
Any	22	tcp	<a href="#">Delete</a>
Uni Intern	80, 443	tcp	<a href="#">Delete</a>
<input type="text" value="Any"/>	<input type="text" value="Port(s)"/>	<input type="text" value="tcp"/>	<a href="#">Add</a>

Allow incoming traffic from this network.

Allow incoming traffic on these ports. Multiple ports must be separated by commas. Port ranges can be specified with a colon "1000-4242".

Allow traffic of this protocol.

[Download Firewall Configuration Script](#)

- 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

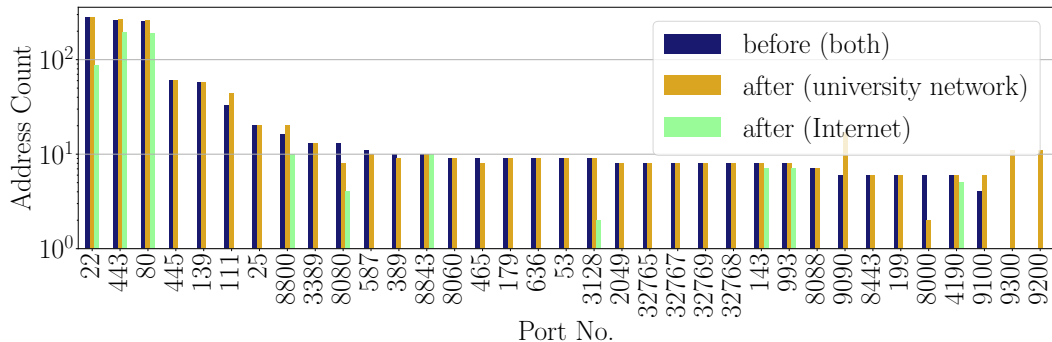
## 4 Conclusion

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

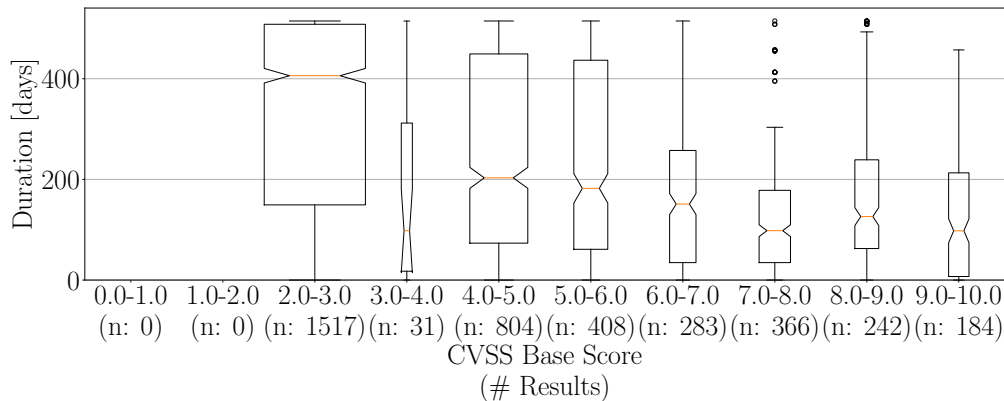
- selected subnets (max. 2048 IPs) in a university campus network
- port scans before and after deployment reached 595 and 738 hosts respectively

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

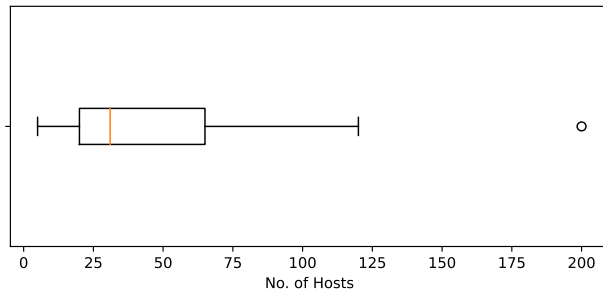


Number of IP addresses per open TCP port before and after 9 month deployment. Point of view in parentheses.  
 n = 505 hosts. Excluded 98 ports which are open on < 1% of IPs.



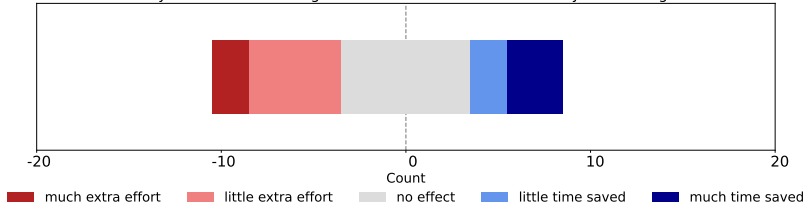
TTR of vulnerabilities per CVSS base score.

Number of hosts per system administrator

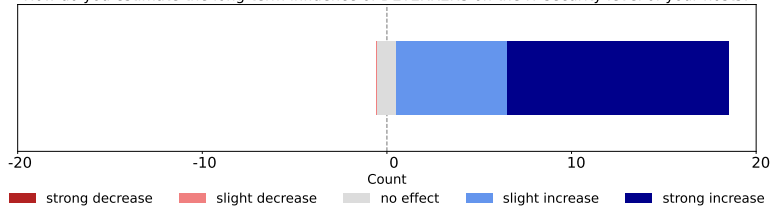


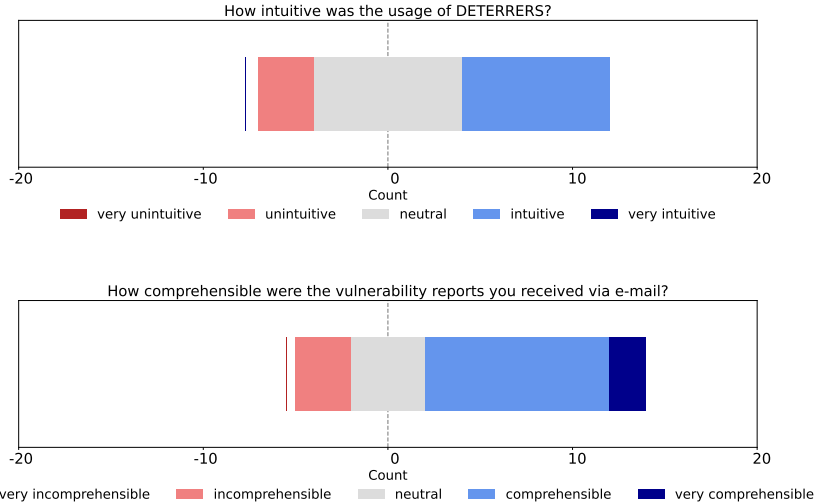


How do you estimate the long-term influence of DETERRERS on your working time?



How do you estimate the long-term influence of DETERRERS on the IT security level of your hosts?





# 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>

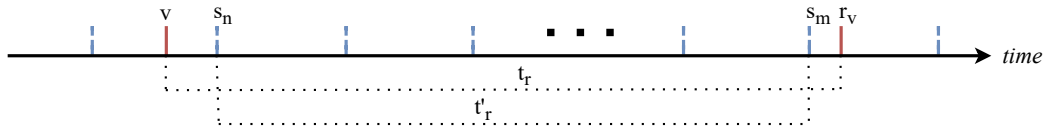
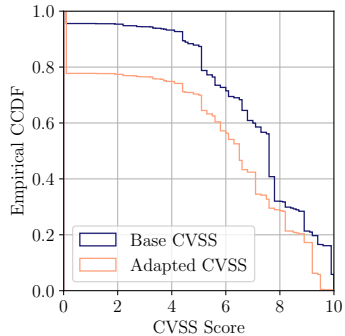
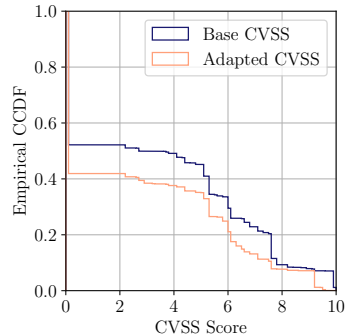


Figure: Schematic approach for approximating the TTR.



(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

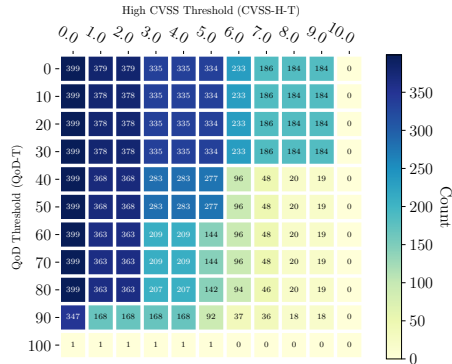


Figure: No. of blocked hosts

# Risk Assessment: Notification

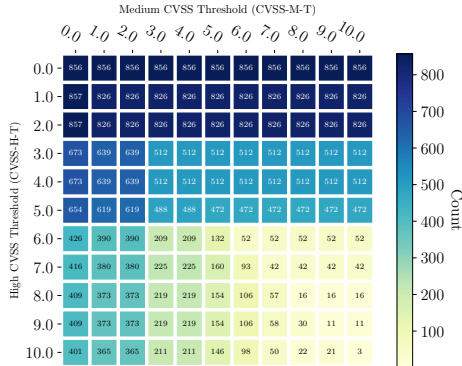


Figure: No. of notified hosts