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



Decentralized Network Administration SOAR Contributions

Outline

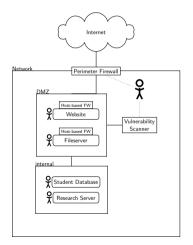
1 Motivation

- Decentralized Network Administration
- SOAR
- Contributions
- 2 Architecture
- 3 Evaluation
 - Test Deployment
 - Attack Surface
 - Time-to-Remediate
 - User Survey
- 4 Conclusion



Decentralized Network Administration SOAR Contributions

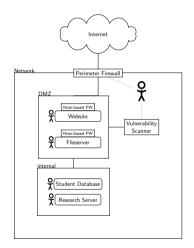
Decentralized Network Administration





Decentralized Network Administration SOAR Contributions

Decentralized Network Administration

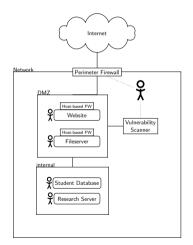


 Decentrally administered networks consist of many hosts which are administrated by different individuals



Decentralized Network Administration SOAR Contributions

Decentralized Network Administration

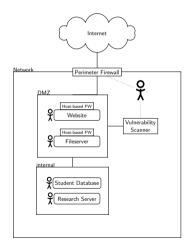


- Decentrally administered networks consist of many hosts which are administrated by different individuals
- important security tools:
 - Host-based Firewall (FW)
 - Perimeter FW
 - Vulnerability Scanner (V-Scanner)



Decentralized Network Administration SOAR Contributions

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

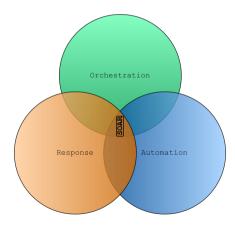


 Motivation
 Decentralized Network Administration

 Architecture
 SOAR

 Evaluation
 Conclusion

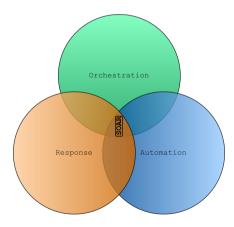
Security Orchestration, Automation and Response (SOAR)



integration/combination of different security tools



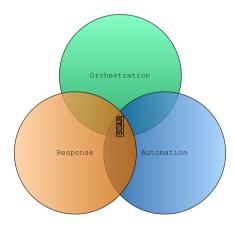
Security Orchestration, Automation and Response (SOAR)



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



Security Orchestration, Automation and Response (SOAR)



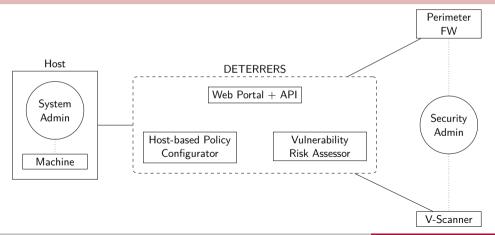
- integration/combination of different security tools
- reduced workload at Security Operations Centers
- complete knowledge and control of network and systems expected



Decentralized Network Administration SOAR Contributions

Solution

automateD nETwork pERimeter thREat pRevention System (DETERRERS)





Decentralized Network Administration SOAR Contributions

Contributions

We:

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.



Decentralized Network Administration SOAR Contributions

Contributions

We:

- 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.



Decentralized Network Administration SOAR Contributions

Contributions

We:

- 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.



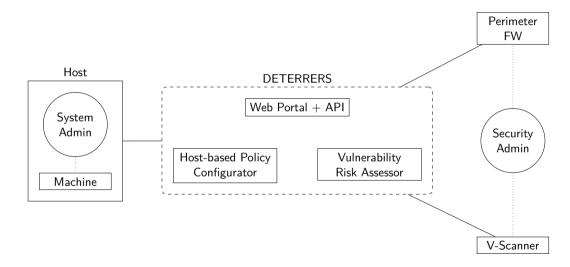
Outline

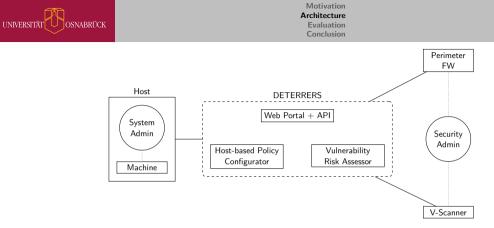
- 1 Motivation
 - Decentralized Network Administration
 - SOAR
 - Contributions

2 Architecture

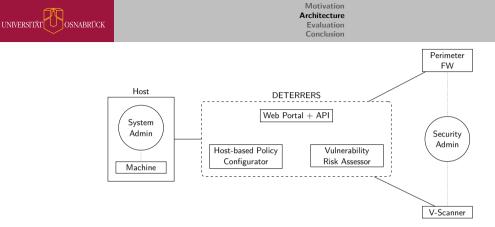
- 3 Evaluation
 - Test Deployment
 - Attack Surface
 - Time-to-Remediate
 - User Survey
- 4 Conclusion





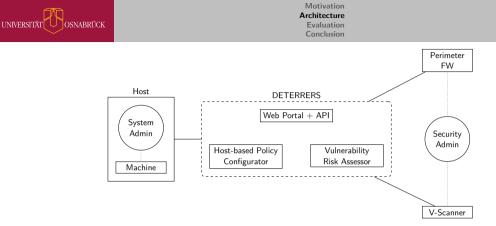


build inventory of hosts and services at network perimeter

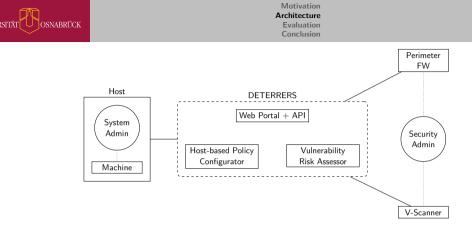


build inventory of hosts and services at network perimeter

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

0	HOR MODE TRATEZZEN +					÷	
e - 1						± @ 🖬 b	
	DETERRERS Abo					niwintering Logast	
	Host Details						
	IP Address	DNS Names	Comment	Admin(s):	Internet Service Profile	Status	
		vm306.rz.uni-osnabrueck.de	deterrers-test	niwintering	55H	Unregistered	
	Edit Service Profile						
	Actions						
	Register	Ordinary Scan Remove from DETERRE	RS				
		e Scan Quality					
		t: Create a user named grownbore. Informe Hic key that enables key-based SSH access for					
		errers, r2, and onserveck, de/static/file					
		y to the authorized keys of user greentione: til:r -p /heme/greentione/.sin 44 ctmod 07					
		ssh/author1zed_keys_88_chown = #_greenbo ted the allowed users for SSH you should add					

system admins add all hosts they are responsible for



Host and Service Inventory

DETERRERS A					nhvintering Logost
Host Detail:					
IP Address	DNS Names	Comment	Admin(s):	Internet Service Profile	Status
					Unregistered
Edit Service Profile					
Actions Register	Ordinary Scan Remove from DETER	ALAS			
Register	Dedinary Scan Sensor from DETER he Scan Quality he volverability scan results, we recorrered				

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



Host and Service Inventory

DETENDENT Out information Out information Out information Out information First Detention Information Information Information Information First Detention Information Information Information Information First Detention Information Information Information Information College Information Information Information Information Point Constrained Information Information Information Detention Information Informat						± • • • •
					100 0	
Host D tables material devices from the set of	ETERRERS Abou					niwintering Logost
Image: second						
TYT 1222.00 with/distributionalized.de metricing Spit metricing Fall Support Output part descendent metricing Spit descendent Part Support Part Part Part Part Part Part Part Part	lost Details					
Actions Market and the set of the s	IP Address	DNS Names	Comment	Admin(s):	Internet Service Profile	Status
Actions More from (CLUME) Device a cost of body part on the more from (CLUME) International part of the cost of the c						
The second	Edit Service Profile					
 On the Larger hout, Count's a serie named prevenses, series advect representation (2) Download the public key bits evablise key based SSM access for the vulnerability scannes: exist: Histopy: //decimients.cc.acm/scannes/access/	ncreasing th	e Scan Quality				
namergreennamer, sith/airther1zed.xeys. 48. chown -#. greenbare: greenbare: /homogreenteer, san 44. chood date //homogreenteer/, sah/airther1zed.xeys* 4. In case you restricted the allowed users for SSH you should add the user greenbare to the AllowUsers list in zecursanzanecomrag.	1. On the target host: sude woldser gree 2. Download the public our 1. https://deta 3. Add this public key sude bash ~ 1 minor / 1 home/greenbone/ .1	E: Crocké a usér nármed grouensem. nerkomi Nic key tákz enables key basied SSH access fo commerse na zurosomarneka. Auf statilorfal y to the outhorized keys of user greeenkomi nátz na zhome/grouenseen/. som da cheved i stafunatharized-langs da cheve i greeen	r the vuinerability scanner Lus/greentone-scarner.p 2700./home/greentone/.s 2000.greentone./home/gr	: ub cutput scarren sh 44 touch /home/j centoro/.ssh 44 (fr	: ;pull proof dobt :/ routs/artherized_keys &&.co	

- 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



	Create New * 2 Edit 3., Editis CLI	The Close B Delete	EWP	ж О		
	Name 0		Details 0	Interface 0	Tape 8	Ext.0
Policy & Objects	Address Group (NTI)		CHURTY		17,100 0	
	PWP5-WEP-DETERMENS-W	131-173			Address Group	
	WPS WIR CETERLIS	131-170 181-170			Address Group	
		131-173				
		I 131-172				
	TWP2-554 DETERMENTS-14	E 121-172			Address Group	
	- INFASSION CONTRACTOR	131-170			Address Group	
Addresses	\$	131-173				
		E 131-172				
	TWP3 OPDN DETERBERS of	E 131-172			Address Group	1
		131-173				
		131-173				
		000				
	E ENd Address Group 570					
	TO PWP5 W/D OFTERHEIS	2001 0438-0509			Pv6 Address Group	1
		B 2001-0638-0508-				
		2001-0528-0508- 2001-0538-0508-				
		030				
	IS FWP2-55H DETERRERS-VE	2001-0638-0508-			IPvé Address Group	5
		2001-0538-0508 2001-0538-0508				
		2001-0638-0508- 2001-0638-0508-				
		œ				
	FWP3-OPEN-DETERRERS-66	2001-0508-0508-			IPvé Address Group	1
		2001-0638-0508 2001-0638-0508				
		2001-0528-0509				
PRADDET	O Securits Rating boses	ditter.				Univer 1053.28 Ø

 implemented two interfaces to perimeter FWs



ke-3201-1							
	Create New * / Edit 1., Editin CL	G Close B Delete	TWP	н	Q.		
	Name 0		Details 0	Interface 0	Tape 9	Ext.0	
Policy & Objects	E Address Group (ATT)		Linki V		175= 1		-
	T PWPS WOR DETERMENS of	131-173			Address Group		
	- Intra wall contraction	181-170			Address Group		
		131-173					
		E 121-172					
	TWP2-55H DETERMENT	E 131-173			Address Group		
Authentication Rules		131-170			Parameter on only		
Addresses	\$	131-173					
		GD					
	TWP CON DETERDED A	II 131-173			Address Group	1	
		131-170					
		131-173 131-173					
		010					
	E ENd Address Group (576)						
	S PAPEWER OFFICERS	2001 0438-0509			Pv6 Address Grean	3	_
		2003-0538-0508-					
		2001-0638-0508- 2001-0638-0508-					
		633					
	TWP2-55H DETERMERS-VE	2003-0538-0508-			IPvé Address Group	5	
		2001-0638-0508- 8 2001-0638-0508- 8 2001-0638-0508-					
		2001-0528-0508-					
		00					
	FWP3 OPEN-DETERRERS #5	B 2003-0408-0508-			IPvé Address Group	4	
		2001 0638-0508					
		B 2001-0608-0508-					
	Securits Exting hours	APRIL 1				Undated: 10:53	

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



Mc-3201-1	· = 0,						
	Create New 1	🖋 DAL D. DALIN CU	G Close B Delete	PWP	ж	۵.	
	>	Name 0		Details 0	Interface 0	Taxe 0	Ext.0
Policy & Objects	Halderes Group					10-1	
		B-OETERHERS-M	# 131-172			Address Group	1
	- Intram	out out of w	183-170			Annessoroup	
			131-173				
			G 121-172				
	- PWP140	DETERMENT	E 121-172			Address Group	
Authentication Bules	- 11172 531		181-170			reserves of the	
Addresses 1	άr.		131-173				
			CD 131-173				
	E DWD CO	N-DETERMENT-14	E 121-172			Address Group	
			131-173			Parameter of only	
			131-173				
			G131-173				
	E Pyt. Address C	ress (314)					
		B-OFTGREES-VE	2001-0438-0508			Puti Address Grean	1
			B 2001-0538-0508-			1 111100-000 01000	
	>		2001-0408-0508- 2001-0408-0508-				
	>		1 2001 0638 0308-				
	TWP2.55	OFTERRES-V6	B 2001-0438-0508			Put Address Group	
	>		B 2001-0638-0508				
	>		2001-0638-0508- 2001-0608-0508-				
	>		CD ALL COMPANY				
	P FWP2-OP	IN-DETERBERS of	B 2001-0528-0508			Pvé Address Group	1
			B 2001 0658-0508				
			2001-0638-0508- 2001-0608-0508-				
		boses	ann.				D Underset 10:53:28 Ø

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



Mc-3201-1	· = 0,						
	Create New 1	🖉 DAL D. DALIN CU	G Close B Delete	PWP	ж	۵.	
	>	Name 0		Details 0	Interface 0	Tate 0	Ext.0
Policy & Objects	Address Group					10-1	
		B-OETERHERS-M	# 131-172			Address Group	1
	- Intram	out out of w	183-170			Annessoroup	
			131-173				
			G 121-172				
	- PWP140	DETERMENT	E 121-172			Address Group	
Authentication Bules	- 11172 531		181-170			reserves of the	
Addresses 1	άr.		131-173				
			GD 131-173				
	E DWD CO	N-DETERMENT-14	E 121-172			Address Group	
			121-172			Parameter of only	
			131-173				
			G131-173				
	E Pyt. Address C	ress (314)					
		B-OFTGREES-VE	2001-0438-0508			Puti Address Group	1
			B 2001-0538-0508-			1 111100-000 01000	
	>		2001-0408-0508- 2001-0408-0508-				
	>		1 2001 0638 0308-				
	TWP2.55	OFTERRES-V6	B 2001-0438-0508			Put Address Group	
	>		B 2001-0638-0508				
	>		2001-0638-0508- 2001-0608-0508-				
	>		CD ALL COMPANY				
	P FWP2-OP	IN-DETERBERS of	B 2001-0528-0508			Pvé Address Group	1
			B 2001 0658-0508				
			2001-0638-0508- 2001-0608-0508-				
		boses	ann.				D Underset 10:53:28 Ø

- 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



rule-based decision process



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



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

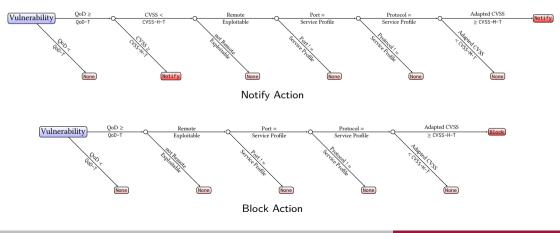


- rule-based decision process
- three possible actions to take:
 - None: No serious risk
 - Notify: Low/medium risk (Internet-exposure) or high risk (internal exposure)



- 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)







Host-based FW Policy Configuration

DETENDED. Out Synthem Control Mark Alexand Floward? Hotschassed Floward? Mark Alexand Floward? Hotschassed Floward? Mark Alexand Floward? 172172238 ward Alexand evaluation with alexand evaluation Mark Alexand Floward? 172172239 ward Alexand evaluation with alexand evaluation Mark Alexand Floward? 172172239 ward Alexand evaluation Mark Alexand Floward? 17217239 ward Alexand evaluation Mark Alexand Floward? 17217239 ward Alexand evaluation Mark Alexand Floward? 17217239 ward Alexand evaluation Mark Alexand Alexand? 17217239 ward Alexand evaluation Mark Alexand Alexand? 17217239 ward Alexand evaluation Mark Alexand Alexand? 17217239 ward Alexand? Mark Alexand Alexand? 17217239 ward Alexand? Mark Alexand? 17217239 ward Alexand? Mark Alexand? 17217239 ward Alexand? Mark Alexand?
Most-based Firewall Policies Pradem Des Nume Connext Admit() Muit-based Freuell 17/1 7227.02 vm350-connext-month uture uture Fatture Firewall multi-based Firewall uture uture Admit() multi-based Firewall uture uture <tr< th=""></tr<>
Pademin Data function Generation Admit(s) Interfaceout/Prevail 172.122.03 unblock-animeterbenk.de determinister interfaceout/Prevail utbr 172.122.03 unblock-animeterbenk.de determinister interfaceout/Prevail utbr 172.122.04 motion determinister interfaceout/Prevail utbr Interfaceout motion animation interfaceout/Prevail utbr Allow frame motion animation interfaceout/Prevail interfaceout/Prevail Allow frame motion animation animation interfaceout/Prevail interfaceout/Prevail Allow frame motion animation animation interfaceout/Prevail interfaceout/Prevail Animation animation animation animation interfaceout/Prevail interfaceout/Prevail Animation animation animation animation interfaceout/Prevail Animation animation animation animation interfaceout/Prevail Animatine animatine animation<
N2.77.22.01 whiles deams test mass masses masses Chites have finance Falled 7 and Ang Falled 7 and 22 Falled 7 and 23 Falled 7 and 24 Falled 7 and 24 </th
Instructions Portical
Interface Political Political Arg 22 lug formal pit triane 86.40 19 formal
Ary 22 00 000 initian initian ip 000
Intern 85,433 trp Desc
Any v Ports top v Add
Download Firewall Configuration Script

 generates configuration scripts for common firewall tools



• HER BERGE FERTILIZED * +	Morrania	um de/hostadenie/host/112_17_32_33/detail/host			398 0	v
DETERRERS About	DETERRERS About My Hosts Use: alivitation (Logost				g Logout	
Host-based Fir	ewal	l Policies				
IP Address	DNS	Nanes	Contrent	Admin():	Host-based Firewall	
	172.17.22.28 vm306.rz.uni-osnabrueck.de					
Edit host-based Firewall	Edit back based Firmuth					
Allow from:		Port(s):			Protocol	
					Delete	
						Delete
Any	v	Ports:			tcp ~	Add
Download Firewall Configuration Script						

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



• HER BERGE FERTILIZED * +	Morrania	um de/hostadenie/host/112_17_32_33/detail/host			398 0	v
DETERRERS About	DETERRERS About My Hosts Use: alivitation (Logost				g Logout	
Host-based Fir	ewal	l Policies				
IP Address	DNS	Nanes	Contrent	Admin():	Host-based Firewall	
	172.17.22.28 vm306.rz.uni-osnabrueck.de					
Edit host-based Firewall	Edit back based Firmuth					
Allow from:		Port(s):			Protocol	
					Delete	
						Delete
Any	v	Ports:			tcp ~	Add
Download Firewall Configuration Script						

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



en statute (TR TF201)+ + 0					с у 2 Ф Ф А	
DETERRERS Abou	DETERRERS About MyHists			User: niwinterin	User: niwintering Logout	
Host-based F	rewall	Policies				
IP Address	ONS P	lanes	Comment	Admin(s):	Host-based Firewall	
	vm30					
Lift hast based Firewalk						
Allow from:		Port(s):			Protocol	
						Delete
						Delete
kay v		Ports			tcp ~	Add
Download Firewall Configuration Script						

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



	s under traitingstein 5 O A hetpsychologienen scom de bestelen best				
DETERRERS About My Hosts User al-Adverting Logout			logout		
Host-based Fir	rewall Policies				
IP Address	DNS Names	Connent	Admin(s):	Host-based Firewall	
Lift hashbacel Firewall					
Allow from:	Port(s):	Port(s):			
					Delete
					Delete
Any	✓ Ports:	Parts			Add
	Allow incoming traffic from this active/k. Allow incoming traffic on these ports. Multiple por a color '1000/4242'.				
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



 Motivation
 Test Deployment

 Architecture
 Attack Surface

 Evaluation
 Time-to-Remediate

 Conclusion
 User Survey

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

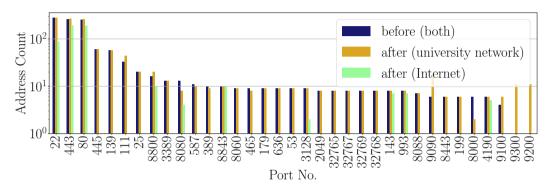


- selected subnets (max. 2048 IPs) in a university campus network
- port scans before and after deployment reached 595 and 738 hosts respectively
- $\blacksquare~\sim$ 30 system administrators



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

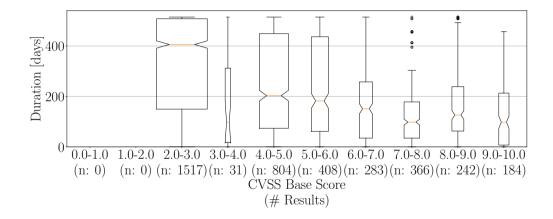
A	Motivation Test Deployment Architecture Attack Surface	
UNIVERSITÄT UOSNABRÜCK		



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.



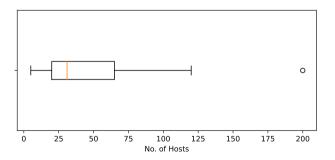
Motivation	Test Deployment
Architecture	Attack Surface
Evaluation	Time-to-Remediate
Conclusion	User Survey



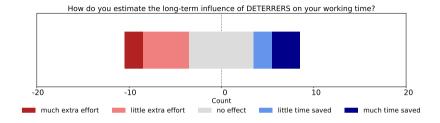
TTR of vulnerabilities per CVSS base score.



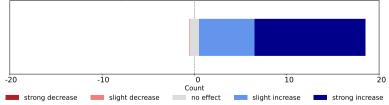
Number of hosts per system administrator





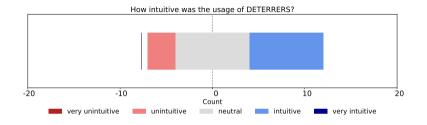


How do you estimate the long-term influence of DETERRERS on the IT security level of your hosts?

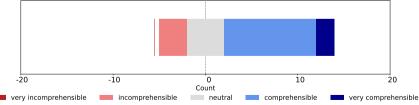


22





How comprehensible were the vulnerability reports you received via e-mail?



23



Outline

- 1 Motivation
 - Decentralized Network Administration
 - SOAR
 - Contributions
- 2 Architecture
- 3 Evaluation
 - Test Deployment
 - Attack Surface
 - Time-to-Remediate
 - User Survey



proof-of-concept for SOAR in decentrally administered networks



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



- 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



- 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





- 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

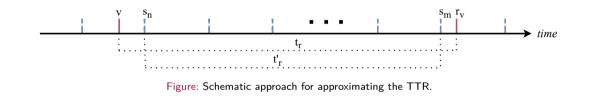


Thank you for your attention!



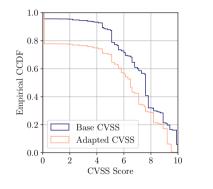
https://github.com/UOS-RZ/deterrers



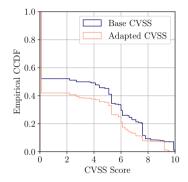




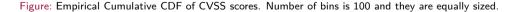
Motivation Architecture Evaluation Conclusion



(a) All NVTs in the test corpus.









Risk Assessment: Blocking

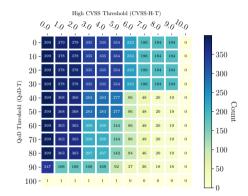


Figure: No. of blocked hosts



Risk Assessment: Notification

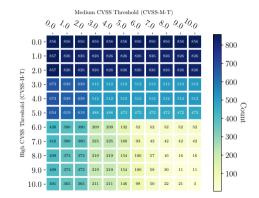


Figure: No. of notified hosts