Re-thinking penetration testing

Dr. Luka Malisa luka.malisa@sdx.com Dr. Stefan Frei stefan.frei@sdx.com

ISF Grey Chapter Meeting 17.09.2021



Who are we?



Dr. Luka Malisa Head Information Security

Be kind – be empathetic



Dr. Stefan Frei

Senior Information Security Officer

Tame complexity

https://www.sdx.com



SDX will set the standard for digital assets, embedded in the existing financial market infrastructure





SDX will set the standard for digital assets, embedded in the existing financial market infrastructure



- Traditional and new market participants try to disrupt existing market infrastructure and business models
- SDX is creating a regulated B2B market infrastructure solution allowing access only to institutional participants
- SDX offers its members access to new products and services and enables the creation of new business models
- SDX is connecting banks through existing connectivity to SIX



Security Stereotypes

1 Ivory Tower





Security Stereotypes





1

Ivory Tower

Requirements





7

Security Stereotypes





Security Stereotypes





Challenges Securing SDX





SITUATION	SECURITY CHALLENGES
1. SDX at frontier of new tech	Manual approaches not helpful
2. High uncertainty	Slow security is a liability
3. Permanent change	Spot fixes are insufficient



WHAT	HOW	WHY
STRATEGIC	Enabling & Scalable	 Point fixes don't work Duct-tape is our friend Scalability through automation



WHAT	HOW	WHY
STRATEGIC	Enabling & Scalable	 Point fixes don't work Duct-tape is our friend Scalability through automation
TRANSPARENT	Clear & Facts-based	 Validate reasoning through transparency Clear communication Facts, over biases and beliefs



WHAT	HOW	WHY
STRATEGIC	Enabling & Scalable	 Point fixes don't work Duct-tape is our friend Scalability through automation
TRANSPARENT	Clear & Facts-based	 Validate reasoning through transparency Clear communication Facts, over biases and beliefs
EMPATHIC	Supportive & Understanding	 We shut-up and listen, then solution We ask for, and act on, feedback We trust and support our organization



WHAT	HOW	WHY
STRATEGIC	Enabling & Scalable	 Point fixes don't work Duct-tape is our friend Scalability through automation
TRANSPARENT	Clear & Facts-based	 Validate reasoning through transparency Clear communication Facts, over biases and beliefs
EMPATHIC	Supportive & Understanding	 We shut-up and listen, then solution We ask for, and act on, feedback We trust and support our organization
PRAGMATIC	Resourceful & Risk-based	 Approximately right today tops late precision Get the basics right first Know our big fires / risks





Thinking pattern





Thinking pattern

Results in



Quo Vadis Penetration Testing?

TRADITIONAL MODEL

- Compliance driven security
- Testing monolithic artifacts
- Pentesting outside of development
- Service-oriented





Quo Vadis Penetration Testing?





Approximately right today >> Precisely right tomorrow





ACCURACY

PRECISION

Quo Vadis Penetration Testing?



Classification: P1 Public

台 SECURIT \

Security Smoke Test (SST)

Re-thinking penetration testing for agile environments



Security Testing - Traditional Model



- Test completeness or quality?
- Feedback & learnings for deveoplers?
- Trends over a series of tests?



LIMITATIONS

Security Testing - Traditional Model Penetration tests are rare, one-off events at end of development

- Compliance driven security
- Designed for big monolithic artifacts
- Pentesting disconnected from development





LATE TESTING

- No reduction of uncertainty
- **Overload** to address findings
- High risk of project delay

Penetration tests are typically rare one-off events at t



Security is blocking us!



Drawing Inspiration

- Development of disruptive products & services always comes with surprises
- No issues means no innovation (you are only optimizing)





Reduction of Uncertainty

- Actual cause of failure WAS NOT ON OUR RISK LIST
- We will **TAKE A LOT OUT** of that

PERSPECTIVE

- Many failures happened simply because a new system tries to do unusual things
- Controlling all the way to putting the crater in the right spot was epic







Security Testing - New Model Agile environments require a novel approach

- Agile and continuous testing
- Pentesting integrated in development
- Early validation of assumptions

EARLY & CONTINUOUS TESTING

- Test new function when ready
- Early reduction of uncertainty
- Buy time to learn and fix





OUR APPROACH

Get more by removing unnecessary things rather than adding more things



Phase 1 - Pre Test Early documentation by test provider

METHODOLOGY

Outline testing methodology

TOOLS

Define list of tools to be used

OBJECTIVES

- Align expectations
- Early identification of testing gaps
- Guard rails for test execution
- Ensure consistency & quality across tests

PREPARE





PREP/ Daily meeting with stakeholders generates trust and consistency

DAILY TOUCHPOINT

Briefing with **testers**, **developers**, and **application owners**

DAILY REPORT

Template based, consistent, and continued documentation

OBJECTIVES

- Q&A
- Communication & learning
- Key findings
- Ensure consistency and quality

EXECUTE



157 Daily Report Day 1	SET Daily Report Day 2	
Instant booksessi Tanana mentangga (p $1.113, 100 - emotionspace (g_{1}) Tanana mentangga (g_{2}) Tanana $		







Public

+ Issues owned and quickly addressed

Phase 3 - Post Test Standardized deliverables and classification across tests

REPORT

Red teaming section and test automation information

RESULTS

Raw results from tools, positive & negative findings

OBJECTIVES

- Facilitate automation of testing in CI/CD
- Track testing coverage and trends across tests

bugcrowd VRT

REPORT

		Specific Vulnerability Name	Tartant or Affected Function	BUGG
D4	Server Security Theoreficeursteen	Type Infed Cedentide		1
P1	Server-Skie Ingerteen	The bulkston	tend	-
	Territor Sale Internation	Remote Calls Execution INCE		
	Second State Tex	WY binches		
	Server/Advision	106. External Entity Islantion (111)		
	Roden Automission and Sevine Measurem	Authentication Bureau		
	Institution in the second	Delever of Jacob	The Bubble Investigation	
	And a second second	Constant and		
	THE OFFICE AND A DESCRIPTION OF THE OFFICE AND A DESCRIPTION OFFICIAL AND A DESCRIPTION OFFICAL AND A DESCRIPTION OFFICIAL AND A DESCRIPTION OFFICAL A		An Annual A	
	The of Continue	Reacting Patrony	Persegue sur	
	manan oʻyyaqı ant	Cryprapagna, run	marine, i chage	
	Automotive Security Micromotion	Motorial Contract	Prisonge Vice Sch Charles	
	Automotive Security Hisconfiguration	W Hat	ney red Cloning	
P2	server security integration	Micompand (HS	Second George	
	server security mecaniquation	(num meanganan	Account tensore	
	Service A Cura Exposure	Weak Password has at singlementation	Tokan Laakage vantoet teader rosoning	
	CrearSite Scripting (135)	Stored	San Prolegel Ever to Jayone	
	Brahan Access/Santral (BAC)	Sarverbile Request Pargery (NWP)	brand rightingal	
	Coordina Request Nargery (CMP)	Ардисацияла		
	Replication-Lovel Devid-of-Service (Doll)	Ortical impact and/or Easy Officulty		
	Inserver OS/Termane	Kardooded Passward	Nam Private gent Uniter	
	Automotive Security Hisconfiguration	Infoldment	Cade Execution (CAN Bus Post)	
	Automotive Security Viloconfiguration	M Hub - Citil Injection	Interaction	
D2	Server Security Wassenfiguration	Macarifipund DV3	Kask Subdonan Takeover	
	Server Security Wasserfiguration	Mal Sener WaserApuration	No Spoofing Pretoction on Timuel Domain	
	Server-Side Injection	x119 Reporce Manpulation	Response Splitting (CRUF)	
	Server-Side Injurition	Content Speaking	Burne Light Kon	El con
	CRIASP Top Ten + Bugcrowd Extres	Specific Vulnerability Name	Variant or Affected Function	BUGG
	Broken Authentication and Session Management	Week Look Durch Rep.	WTTPS not Available or HTTP by Default	
P3				
	Bolion Authentication and Session Management	Sector Poston	Remote Attack Welter	v
	Resten Authentication and Sester Management Sensitive Data Septeme	Textern Praillen Disclosure of Secrets	Renate Intalk Inches Na Internal Acad	
	Brainn Auflentikulist and Invite Management Senathe Data Separate Senathe Data Separate	Senden Rivalien Disboew of Secrets Diff Gebication Oats Nat Stripped Fron Tipleaded Images	Remate Atlashmeter Parthernal Auet Automatic Uar Enumeration	
	Bolan Aufterlisisten and Insien Management Sendhe Dira Septure Sendhe Dira Septure Deserfer Solgting (2019	Innian Frailin Dialoare of Saloris UIF Galacetion Ours hat Singped from Uplaated Images Shared	Neneta Itilak Itelar Na Itelana Auat Adonutic Uar Enumeration Privileged Uar Ita Phologya Elevation	v
	Bolen Aufleetikulies and knaae Management Senothe Data Soperare Senothe Data Soperare Crean-Sire Sorging (2020) Crean-Sire Sorging (2020)	Sector Fruiten Disboure of Scotts Ethil Gesteurism Cars hat Singled From Spitabell Images Shared Second	Remote Interk Incide Par Norval Assoc Par Norval Assoc Automatic User Enumeration Prodeped User to Photoge Elevation CORFURCEMEnt	ľ
	Roben Authentischen and Sexilien Management Sexilien de DSA Segueure Einsteine Ortsv Sessene Coundres Knylling (XSB) Coundres Knylling (XSB) Coundres Knylling (XSB)	Excitan Rustian Disboard of Second Disboard of Second Disboard of Second EVE description Onto Second Provided Images Source Source Rowel Rowel	Remarke Klack Status Par Norral Acast Automatic Care Source plane Prodeged User to Pholege Elevation COP/Refutured Namber	ľ
	Broken Aufwertschen and Ensien Management Sentite Data Separae Sentite Data Separae Consolie Sentiteg (2010 Consolie Sentiteg (2010 Consolie Sentiteg (2010 Consolie Sentiteg (2010	Index Rules Distance of Saver UP Generation for Service Service Service Index Index Index Index Internal Internal Internal Internal	Rende Rick Worker Rethonal Aust Rethonal Aust Autorutiv Une Source also Produged Exection Produged Exection CORFAR-Source CORFAR-Source Nachof Heard Source and/or Merken Insue1	ľ
	Index Aufweitsutes and Ensier Management Section Data Separate Section Data Separate Cranditis Separate Cranditis Separate (2010 Cranditis Separate (2010 Cranditis Separate (2010 Relation Associations (2010) Relation Control Section 2010	Exclusion Fix utility Declassion of Shore Declassion of Shore Or of conductoriate Cherns that Shore Sound Sound Marchael Marchae	Rende Rick Note: Re tokrad Aust Autoristic use Insulvation Professor Last Information COMPAREMENT COMPAREMENT Standal Heard Loss and/or Hedun Impact	ľ
<u></u>	Balan Andremsteine and Instein Management Dentrite (Das Bajature Stendtre (Das Bajature Casedra Engling (OB) Casedra Engling (OB) Casedra Engling (OB) Balan Association (BRO) Application-cased Case and BRO) Application-case (Das Case)	Marian Anaton Dockowa of Societ Of Groups description isplashed integer Societ Societ Mariani Mariani Mariani Mariani Angel Inger (2001) Maja Inger and Status Otholay Para Propria	Reurs Nach Neter Neterior Xanon Augendi User to Hologe Disartes Prologad User to Hologe Disartes Otto Aug Otto Aug Nachod Nachod Missing Xanon Sanon Xanon Sanon Sanon Xanon Sanon Sanon Xanon Sanon Sanon Xanon S	ľ
	Autor Automations on Family and Autor Management Mathia Gas Segment Harthe Gas Segment Canadras Hartings (1996 Canadras Hartings (1996 Canadras Hartings (1996) Canadras Hartings (1996)	Bolan Purger Bolan Purger Bolan Purger Bolan Purger Bolan Purger Inter Inter Marci Marci Marci Marcia Mar	Reurs Islachines Reurs Islachines Reurs Islachines Annetic Use Somer Rein Annetic Prologic David Somer Rein CREFAGARE CREFAGARE Somer Somer Rein Somer Somer Reinsen Reinsen Somer Reinsen Reinsen Rei	v
<u></u>	Kelan Aluktistukse od Faster Kongorum Sanche Ost Sepana Canolin Sepana Canolin Sepana Canolin Sepana Canolin Sepana Canolin Sepana Kalan Konstanter Aluktistukse	Interest Prutier Destant Anton's Of Generation (Interest Barel Barel Marcia) Inter-Sin Regist Papers (2011 Ing System) (Interest Papers (2011) Ing System) (Interest Papers (2011) Ing System) (Interest Papers (2011) Ing System) (Interest Papers (2011) Interest Papers (2011) I	Reury Stack Textus Reury Stack Textus Automoti Use Textus Textus Prological User Textus Textus Prological User Auto	v
<u></u>	Ken Aufensider of leant hospital Service Scholauser Service Scholauser Conder Songle (19) Conder Songle (19) Conder Songle (19) Conder Songle (19) Rear Nanciental Mich Aphanet Antonio Africa Page Charles Alexies (1) Anti-figuratio Antonio Sang) Thanifipation Antonio Sang) Thanifipation	Boakan human Boakan human Boakan human Boakan human Iof Gamcana diya ku Innya (Human Jakaha) human Board Marcia Marcia Marcial Marcial (Human Jakaha) (Boakan) Markina (Human Jakaha)	Kenzi kata hatar Narian (Alama) Narian	ľ
	Notes Automatics of facility Responses Secretics Data Responses Secretics Data Seguran Canadra Sergingar (DB) Canadra Sergingar (DB) Canadra Sergingar (DB) Canadra Sergingar (DB) Canadra Sergingar (DB) Canadra Seguran Antonia Canadra Seguran Sector Antonia Canadra Seguran Sector Antonia Sector Canadra Sec	Endown from Produces from Fore	Kenzi Asia Yatu Ya Yataraf Audi Akunuci (ua biountata Nuhugi (ua biountata) Dinkipa (ua high Kenku Kenzi (ua high Kenzi (ua hi	·
	Relate Abduetandes of faces Mongenes Bennie Abduetandes Sente Abduetandes Geneda Konstepano Candrá Sanger Candrá Sanger Candrá Sanger Candrá Sanger Candrá Sanger Candrá Sanger Candrá Sanger Kannan Kanger Kandhala Adamata Kanger Kandhala	Learn human Technical Tacht Technical Tacht Technical Cacht Technical Cacht Technical Learn Learn Learn Machine Tacht Machine Machine Tacht Machine Machi	Kenzi kasa tasta tast Yanasa Aue Kutoni (ula tasta Kutoni Kutoni (ula tasta Kutoni Kuo	•
P4	Natura Manakaraka antinam Kanganan Santa Ka Sayaan Santa Ka Sayaan Santa Ka Sayaan Santa Ka Sayaan Santa Sayaa Santa Sayaa Santa Sayaa Santa Santa Santa Santa Santa Santa Santa Santa Santan Santa Santa Santa Januaria Santa Santa Santa Santan Santa Santa Santa Santa	Extension Balance from Or Graduate from the theyer from spland from Form Comparison of the theyer from spland from Here with theyer from the theyer Responses Response Respo	Anna Markinski Varianci Anni Parkani Anni Hangari San Yahagi Bahasi Sandari Sandari Sandari Sandari Sandari Hangari Sandari Sandari Hangari Sandari Sandari Hangari Sandari Sandari Hangari Sandari Sandari Sandari Mangari Sandari Sa	ľ
P4	Note Methods of team Koopenet Sector & Schopenet Sector & Schopenet Constra Schopenet Constra Schopenet Schopenet Schopenet Schopenet Schopenet Automatical Schopenet Automatica	Index Anales Enclosed Yook (Constraints) Of Enclosed Yook (Constraints) Enclosed Yook (Constraints) Enclosed Yook (Constraints) Unclosed Yook (Constraints)	Insues Stankards Verstankard Auss Jonachi zei Senantista Vander istensisten Stankard Stanka	ľ
P4	Network Anticulation and Angeneration Developed Science Spectra Search Science Spectra Construction and Science Spectra Construction and Science Spectra Constructions and Science Spectra Report Science Spectra Report Science Spectra Anticipation and Anticipation Anticipation and Anticipation Anticipation and Anticipation Anticipation Anticipat	Markanis Datasar Zhao, Markanisha M	Incus Nacional Incus Antonio Van Antonio La Sectoria de Carlos Antonio de la Sectoria de Carlos Antonio de la Sectoria de Carlos Colonia Antonio Machine de Sectoria de La Sectoria de Carlos Sectoria de La Sectoria de Carlos En Sectoria de Carlos de La Sectoria de La Sec	ľ
P4	New Animatica in Anima Neurona Composed Sector Data Sector	Markense Status Arben Status Arben Status Arben Status Arben Status Arben Status	Nexa Markania Versinaria Aura Versinaria Aura O Stancia Aura O Olito Aura Sant	ľ
P4	New Animates and Section Magneties Section Conference on Conference Section Conference on Conference Section Conference on Conference Control Section Conference Conference on Conference Conference Conference on Conference Conf	Andrawika Skalars/angle	Nexes Marchan Ser Martinana Juan Martana Juan Martana Juan Selandaharan Selandaharan Selandahar Juan Martana Juan Martana Martana Juan Martana Martana Juan Martana	•
P4	New Advances of the New York of New York o	Hereards and the second	Amon Amon San Amon San Amon San Amon San Amon San Amon San Amon San Amon San Amon San Amon San Amon San Amon Amon San Amon Amon San Amon Amon San Amon Amon San Amon	ľ
P4	New Annuals of the Integrand Compared Sector Conference on	Handbar Handradu Handradu Handbar H	None Markense None Markense Nonpolitieren Markense Oktober Oktober State S	Ĭ
P4	East Andreak an activate trappet East Andreak and Andreak Andreak East Andreak Andreak East Andreak Andreak East Andreak Andreak East East Andreak East Ea	Hardware Rolar Jawa Rolar Jawa Bartan	Jour Indus Annual Journal Annual Indus Annual Indus Annual Indus Statut	
P4	Ease Andreak and Andreak Transport Ease Andreak Andreak Ease Andreak	Handbard Standbard Standba	Near Hanks Hannessen	v
P4	Extende Seguer Extende	Hardwain Roar Andrewain	even instruction eveen instruction even instruction even instruction eve	v
P4	Extende la seguera Extende la seguer	Second Second	even instruction even	
P4	Line Andreas Artika Service Negret Service Negret Carden Service Service Negret Service Negret S	actor actor <td>even server even serv</td> <td></td>	even server even serv	
P4	Extende Services Exte	Instantia	even instruction	v
P4	Extende la seguera Extende la seguera E	Second Second	even information even e	v



+ Deeper security understanding



Reduce, Simplify, & Optimize

Prepare organization for testing at scale rather than testing as a one-off

SETUP FOR TESTER

- Company notebooks and accounts
- Shared folders and AD groups
- Templates

Objectives

- Reduced preparation and turnover time
- Better rapport between engineering & testers
- Streamlined communication & documentation

TEMPLATES & WORKFLOW

- Naming convention SST-YYYY-NN
- Chat-Ops from **prep to close** with all stakeholders



Consistent naming supports scalable automation and linking between Confluence, Reports, JIRA tickets, ...



Our Result – Agile Penetration Testing

TRADITIONAL MODEL

- Compliance driven security
- Testing monolithic artifacts
- Pentesting outside of development
- Service-oriented



NEW MODEL

- Agile driven development & security
- Continuous and step-wise testing
- Pentesting integrated in development
- Pentest provider is a partner





Security Smoke Testing - Lessons Learned

EXPERIENCE & BENEFITS

- Know how transfer between developers & security
- Early reduction of uncertainty
- Reduced load on developers
- Increasing familiarity with security testing

LEARNINGS

- Testing often exerts healthy pressure on organization
- More security issues are fixed by testing often
- Increased security awareness in dev community
- Increased efficiency of testing









Trends, Patterns, Learnings



Conclusion & Key Takeaways

- Common security controls (e.g., pentesting) need not be painful
- Embrace change and unpredictability
- Cybersecurity is about people technology just makes it go faster
- Be kind, be empathetic, build genuine relationships

Conclusion & Key Takeaways

- Common security controls (e.g., pentesting) need not be painful
- Embrace change and unpredictability
- Cybersecurity is about people technology just makes it go faster
- Be kind, be empathetic, build genuine relationships

$$\frac{\partial \text{Security}}{\partial \text{Security}} = \frac{SDA}{\partial \text{Security}}$$

Q & A



"Plan for the difficult whilst it is easy – act on the large while it is minute." – Lao Tzu