

Isabelle Mauny Field Chief Technology Officer



REST API Security by Design with Azure Pipelines



Steven Murawski Cloud Developer Advocate





Security Matters in DevOps





The transformation begins

From the State of DevOps 2018 Report by DORA









The transformation begins

Automation helps low performers progress







From the State of DevOps 2018 Report by DORA





progress

The transformation begins

Increased automation demands more testing



From the State of DevOps 2018 Report by DORA

Automation helps low performers







progress

The transformation begins

Increased automation demands more testing



From the State of DevOps 2018 Report by DORA

Automation helps low performers



Technical debt is reduced, and test automation is introduced





progress

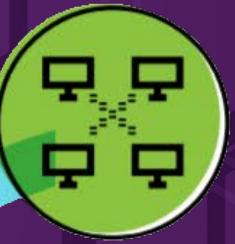
The transformation begins

Increased automation demands more testing



From the State of DevOps 2018 Report by DORA

Automation helps low performers



Continuous improvement reduces manual controls and process

Technical debt is reduced, and test automation is introduced



▶ Low

- Deploy once a month to once every six months
- ✓ Going from code commit to production can be one to six months
- ✓ Restoring service from an incident can be between one week to one month
- ✓ Approximate change failure rate of 46% to 60%



Medium

- ✓ Deploy once a week to once a month
- ✓ Going from code commit to production can be one week to one month
- ✓ Restoring service from an incident is usually less than a day
- ✓ Approximate change failure rate of 0% to 15%



Bern High

- ✓ Deploy once a day to once a week
- ✓ Going from code commit to production can be one day to one week
- ✓ Restoring service from an incident is usually less than a day
- ✓ Approximate change failure rate of 0% to 15%



■ Elite

- ✓ Deploy on-demand (multiple deploys a day)
- ✓ Going from code commit to production is less than one day
- ✓ Restoring service from an incident is usually less than a day
- ✓ Approximate change failure rate of 0% to 15%





AUTOMATION AND INTEGRATION - BUILD

Capability	Low	Medium	High	Elite
Automated build	64%	81%	91%	92%

a crunch From the State of DevOps 2019 Report by DORA – https://aka.ms/2019-state-of-devops

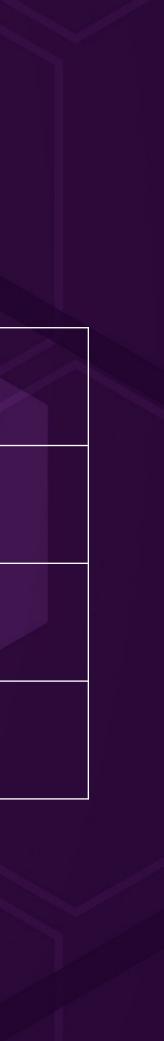




AUTOMATION AND INTEGRATION - TESTING

Capability	Low	Medium	High	Elite
Automated build	64%	81%	91%	92%
Automated unit tests	57%	66%	84%	87%
Automated acceptance tests	28%	38%	48%	58%

a crunch From the State of DevOps 2019 Report by DORA – https://aka.ms/2019-state-of-devops



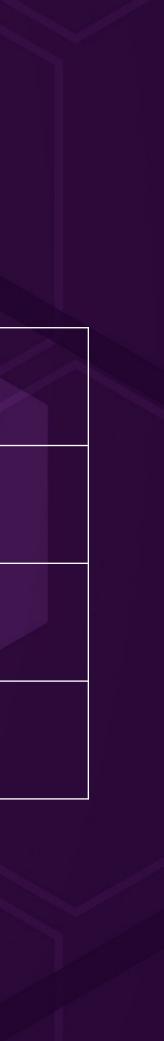


AUTOMATION AND INTEGRATION - TESTING

Capability	Low	Medium	High	Elite
Automated build	64%	81%	91%	92%
Automated unit tests	57%	66%	84%	87%
Automated acceptance tests	28%	38%	48%	58%

From the State of DevOps 2019 Report by DORA – https://aka.ms/2019-state-of-devops 4² crunch

More on how Microsoft shifts tests left at https://aka.ms/shift-tests-left

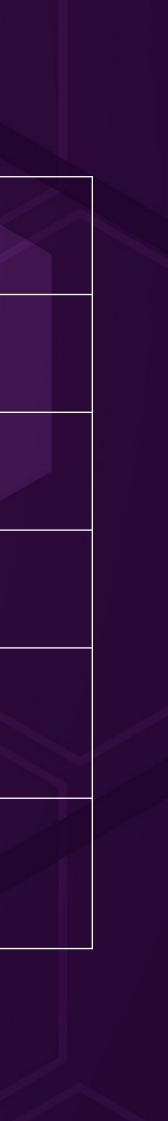




AUTOMATION AND INTEGRATION – DEPLOYMENT

Capability	Low	Medium	High	Elite
Automated build	64%	81%	91%	92%
Automated unit tests	57%	66%	84%	87%
Automated acceptance tests	28%	38%	48%	58%
Automated provisioning and deployment to test environments	39%	54%	68%	72%
Automated deployment to production	17%	38%	60%	69%

42 crunch From the State of DevOps 2019 Report by DORA – https://aka.ms/2019-state-of-devops





AUTOMATION AND INTEGRATION - SECURITY

Capability	Low	Medium	High	Elite
Automated security tests	15%	28%	25%	31%

a crunch From the State of DevOps 2019 Report by DORA – https://aka.ms/2019-state-of-devops

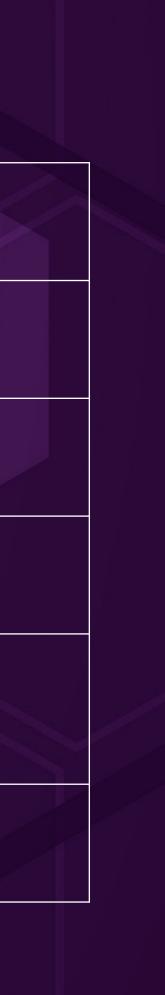




WHERE IS WORK TIME SPENT

Time Spent	Low	Medium	High	Elite
New work	30%	40%	50%	50%
Unplanned work and rework	20%	20%	20%	19.5%
Remediating security issues	10%	5%	5%	5%
Working on end user reported issues	20%	10%	10%	10%
Customer support work	15%	10%	10%	5%

42 crunch From the State of DevOps 2018 Report by DORA

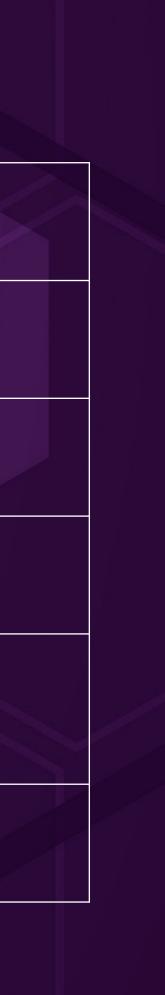




WHERE IS WORK TIME SPENT

Time Spent	Low	Medium	High	Elite
New work	30%	40%	50%	50%
Unplanned work and rework	20%	20%	20%	19.5%
Remediating security issues	10%	5%	5%	5%
Working on end user reported issues	20%	10%	10%	10%
Customer support work	15%	10%	10%	5%

42 crunch From the State of DevOps 2018 Report by DORA



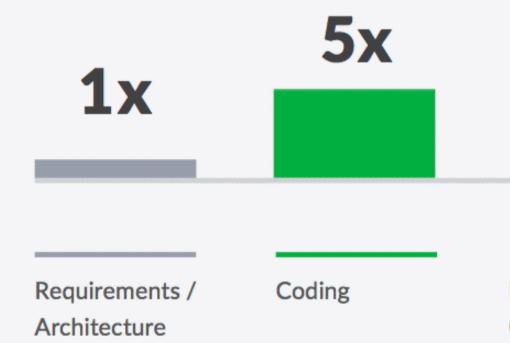
Cost of excess rework = Technical staff size × Average salary × Benefits multiplier × Percentage of technical staff time spent on excess rework



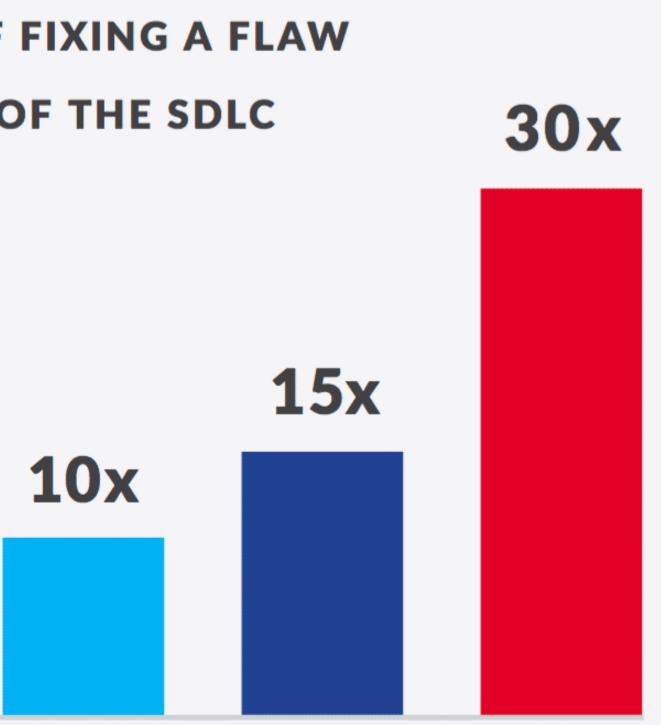


COST OF DEFECTS ALONG THE LIFECYCLE

THE RELATIVE COST OF FIXING A FLAW **AT DIFFERENT STAGES OF THE SDLC**







Integration / Component Testing

System / Acceptance Testing

Production / **Post-Release**

SOURCE: NIST



AUTOMATING API THREAT PROTECTION

CERTAIN OF TOTAL STREET





~ ~



APIS ARE THE NEW ATTACKS VECTOR...

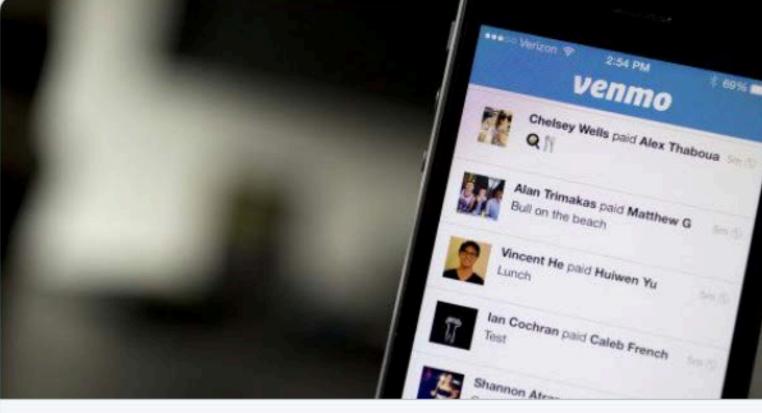
- Data breaches via APIs are on the rise
 - ✓ 200+ breaches reported on apisecurity.io since Oct. 2018
 - \checkmark And those are just the public ones!
- Most recurrent causes:
 - Lack of Input validation \checkmark
 - Data/Exception leakage \checkmark
 - Broken authentication \checkmark





APIsecurity.io @apisecurityio · 21h

Instead of adding proper authentication to transaction feed API, @venmo only sets rate limiting. @bltjetpack demonstrates the drawback by using the API to retrieve 7 mln transactions techcrunch.com/2019/06/16/mil... via @zackwhittaker / @TechCrunch



Millions of Venmo transactions scraped in warning over privacy setti... A computer science student has scraped seven million Venmo transactions to prove that users' public activity can still be easily obtained, a year afte ... techcrunch.com

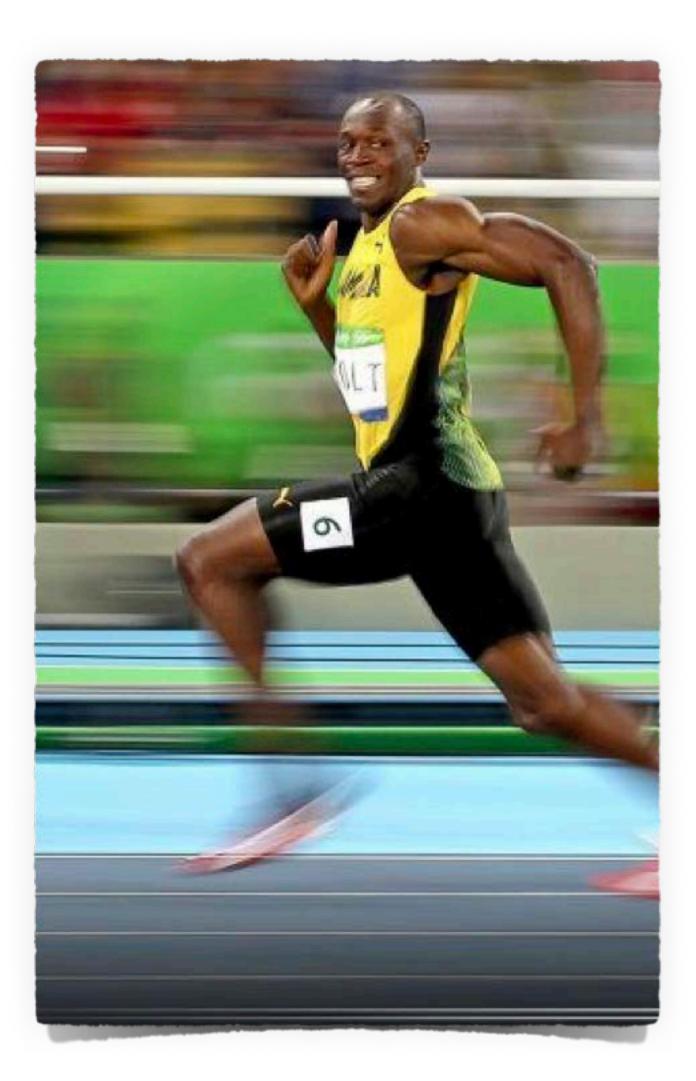




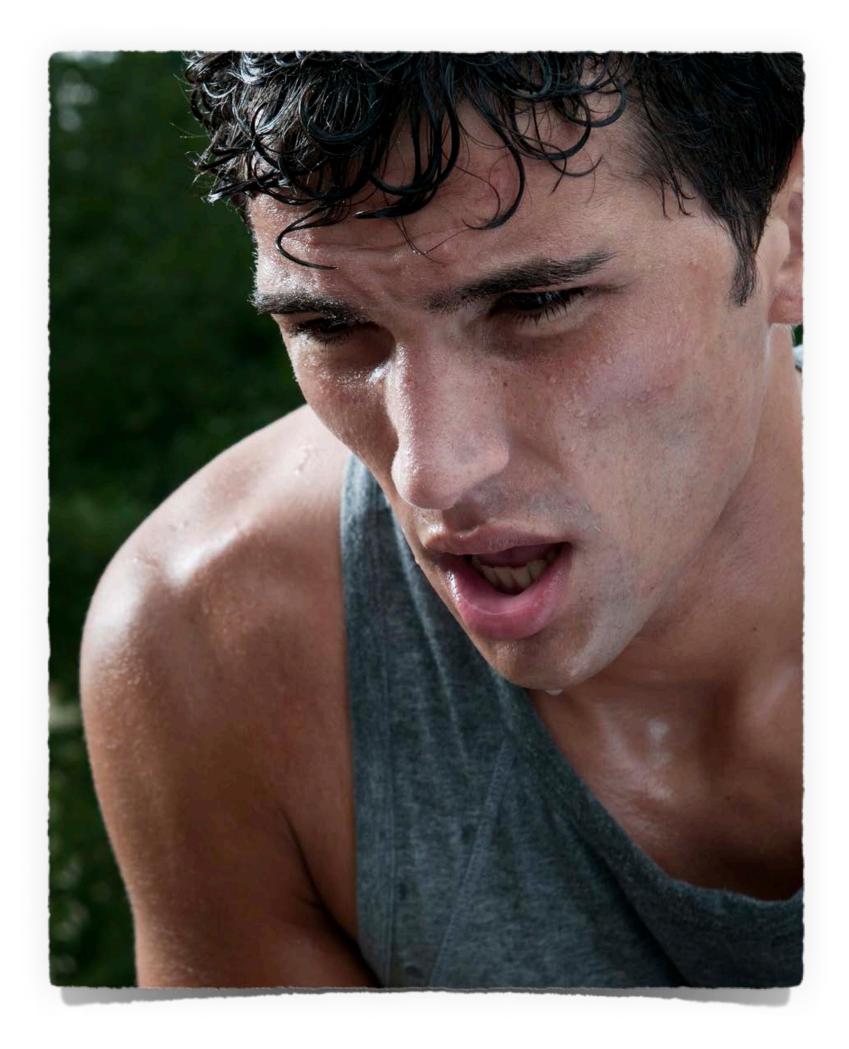
"By 2022, APIs will become the #1 attack vector." - Gartner, How to Build an Effective API Security Strategy -







APPLICATION DEVELOPMENT



APPLICATION SECURITY



SECURING APIS REQUIRES A NEW APPROACH

CERTAREDI (1014) OTO DECE



~ ~

Business

Operations

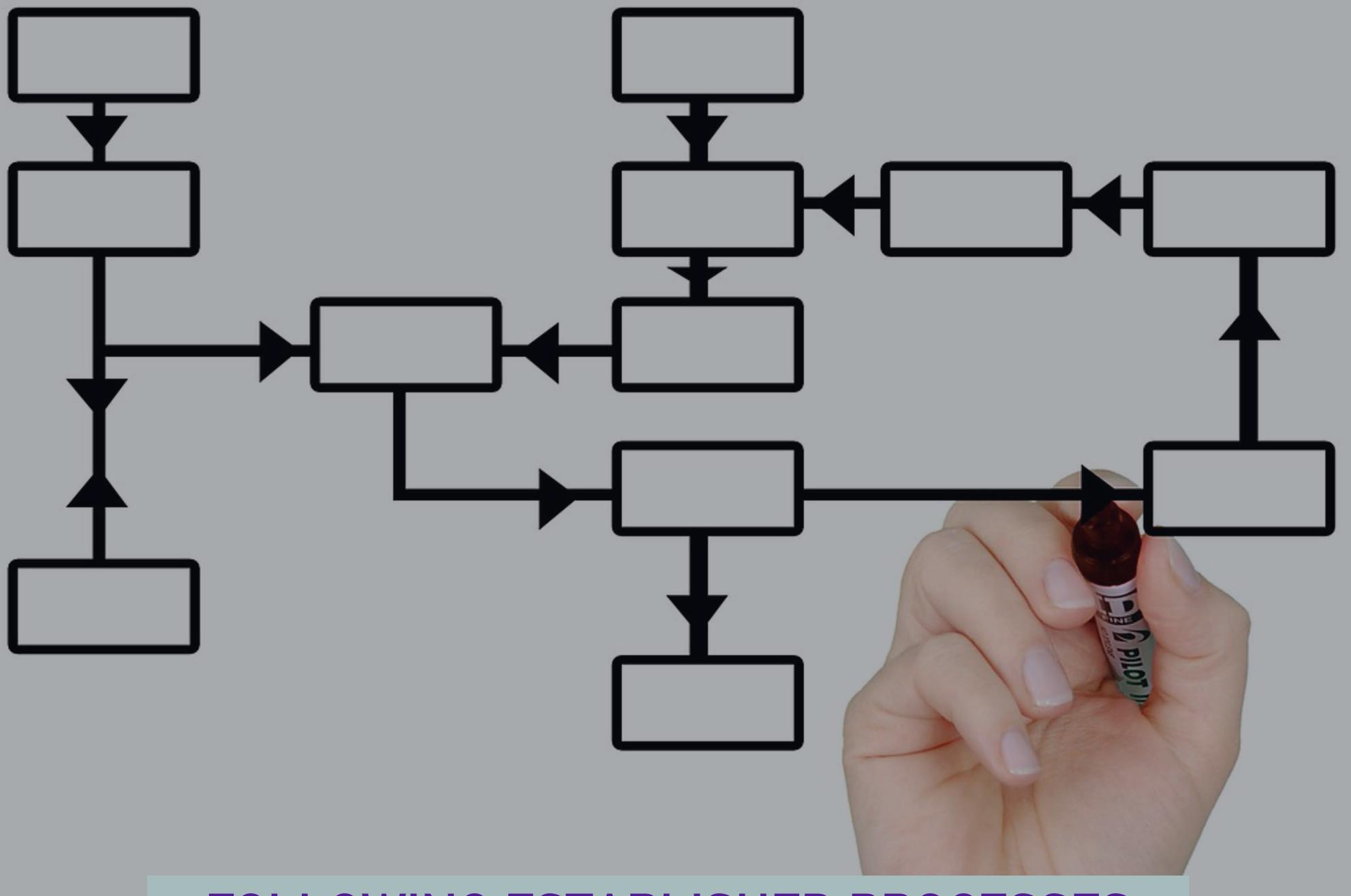


Security

Development

A CHANGE IN CULTURE: PEOPLE COLLABORATING...

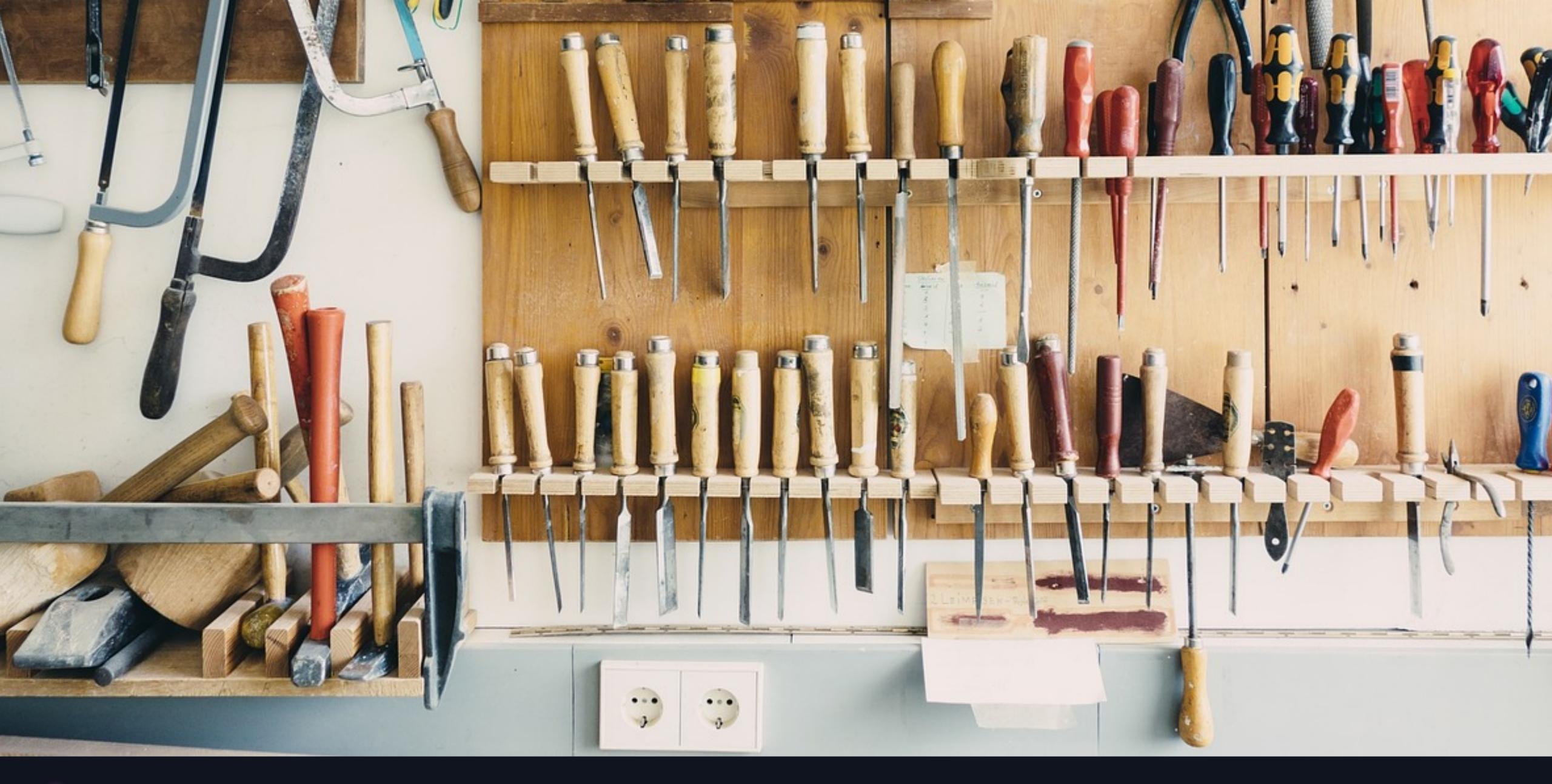




...FOLLOWING ESTABLISHED PROCESSES...





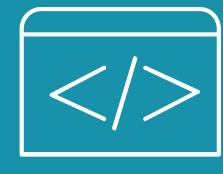




...AND USING THE RIGHT TOOLS.







Design

Developer initiates security work at design time.

Best practices and recommendations are documented.

Develop

Developer documents the API contract with OpenAPI/Swagger.

API Contract security is evaluated from VSCode using 42Crunch plugin.









Integrate & Test Deploy & Protect

API Contract quality is enforced via CI/CD pipeline. Builds are blocked when minimal security requirements defined by security teams are not met.

API implementation is tested via Conformance Scan

API Firewall is automatically configured from OAS file and deployed in line of traffic.

The firewall can be deployed as sidecar in Kubernetes or reverse proxy in front of API Management solutions.









Developers know how the application was built!

OpenAPI specification is leveraged to describe the API contract.

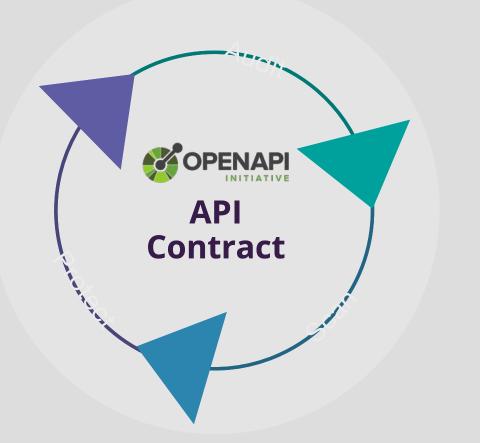
Once the API contract is defined by the developer, the security process becomes clear and straight forward !





"If you describe your API, we will secure it"





AUDIT





VALIDATE OPENAPI CONTRACT CONTENTS

Does it comply to best practices?

Does it comply to security requirements?

✓ Using API Keys ? OAuth ? Basic Auth?

EMPOWER DEVELOPERS TO BUILD THE ULTIMATE WHITELIST

How well is the data defined ?

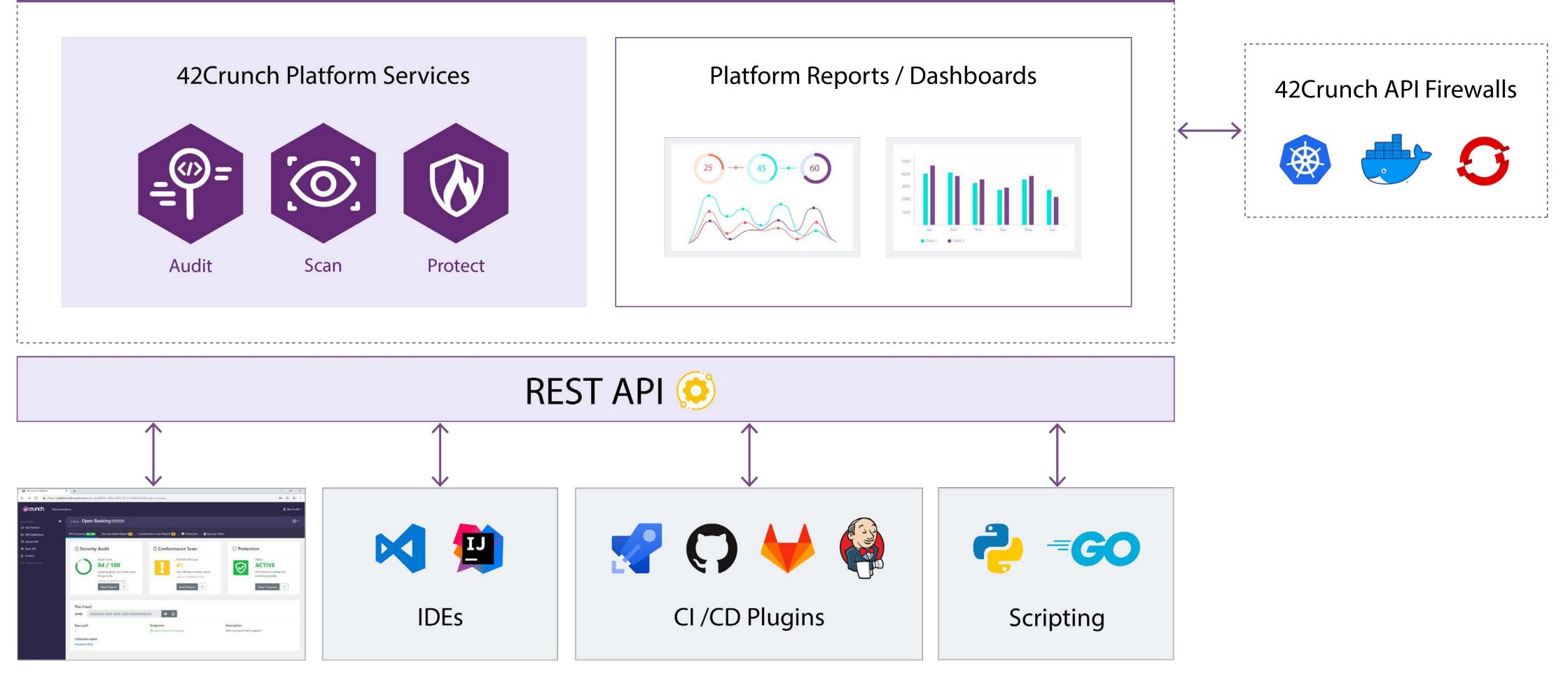
- ✓ Headers, query params, path params, form data
- Input/output payloads format (JSON) \checkmark
- \checkmark Is the data constrained?
 - Min/Max/Patterns/Max Items









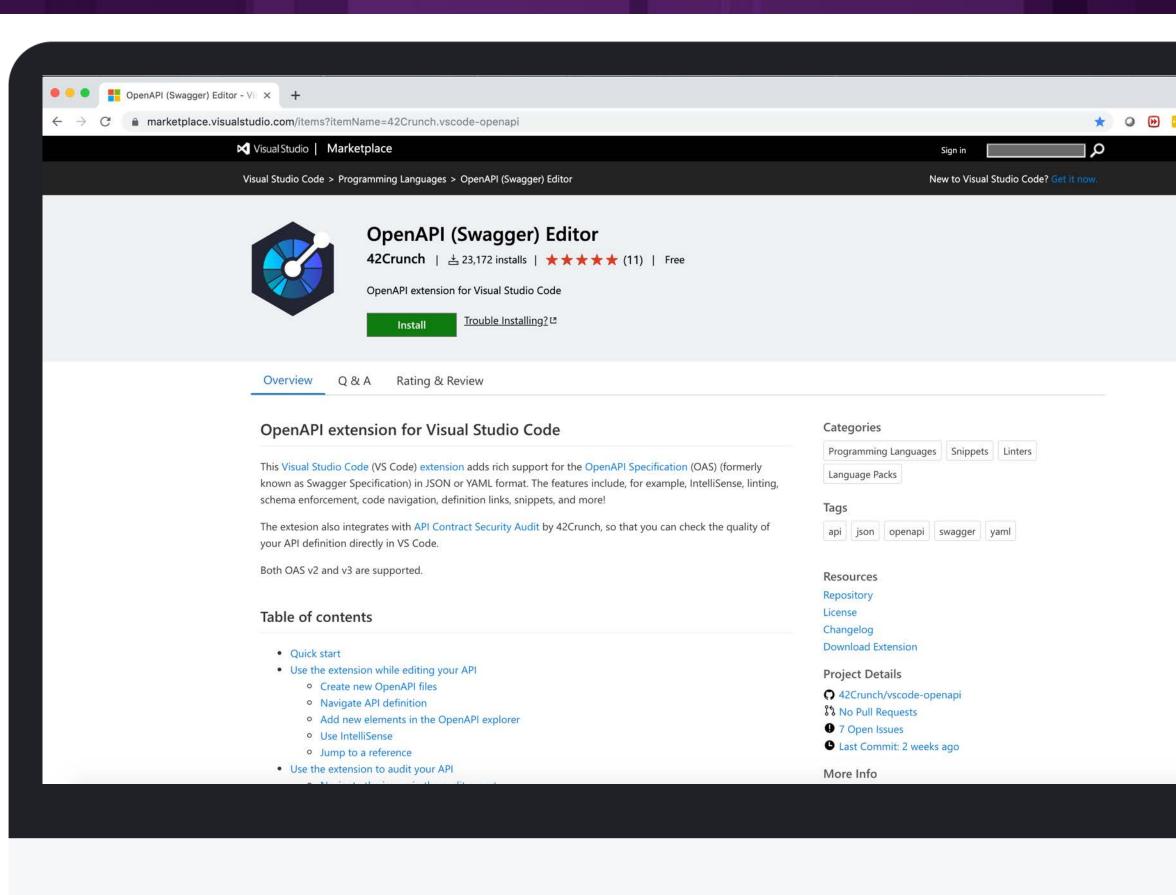






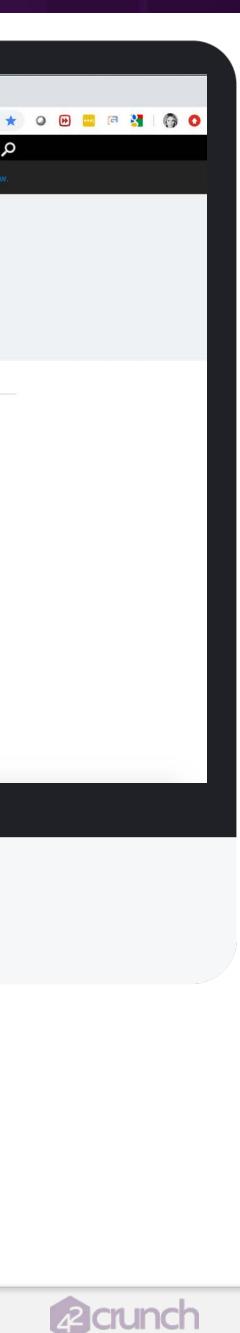
DEMO PART 1: OPENAPI EDITOR/AUDIT FOR VSCODE

© COPYRIGHT 42CRUNCH | CONFIDENTIAL





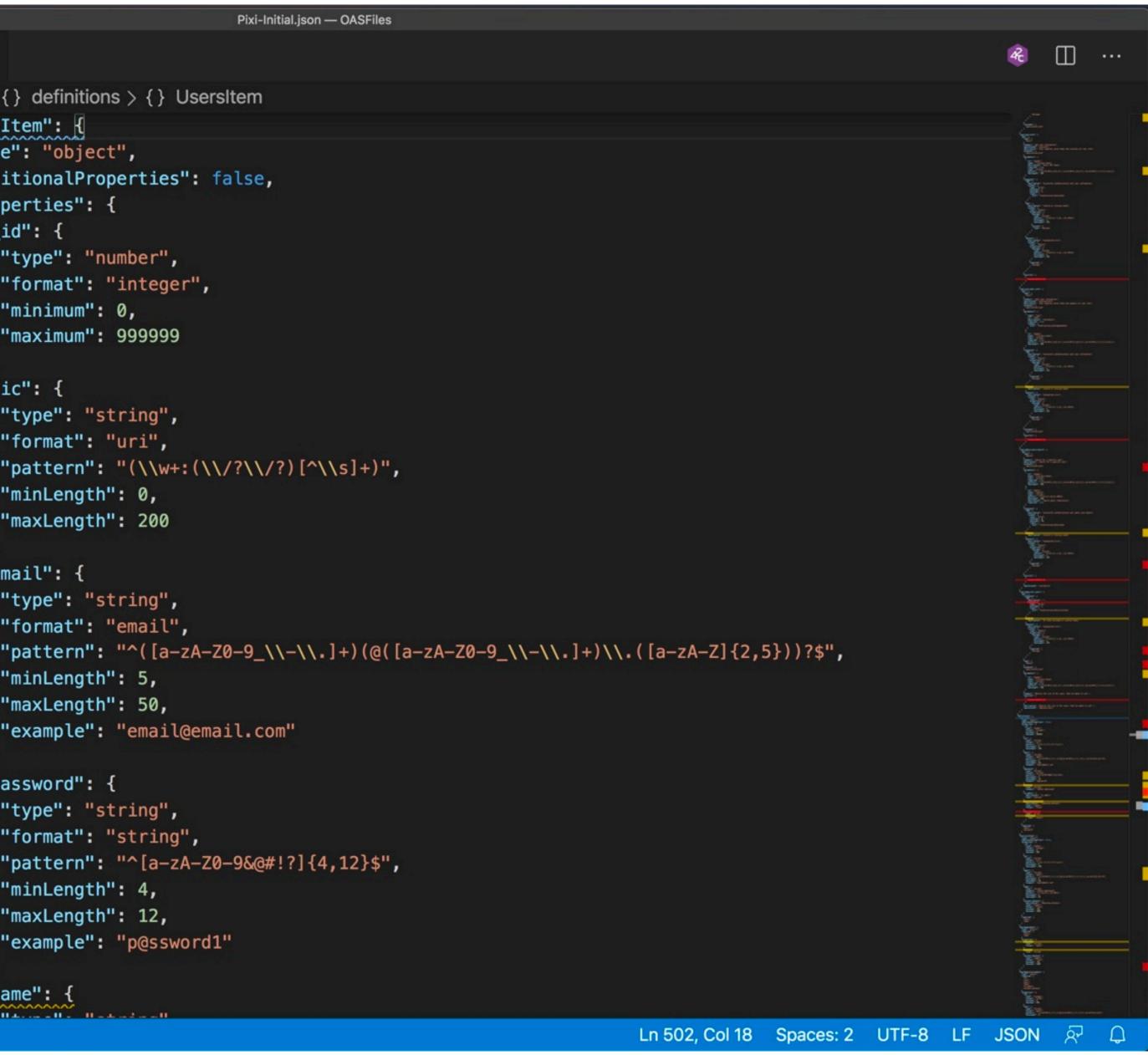
https://marketplace.visualstudio.com/items?itemName=42Crunch.vscode-openapi



✓ DEFINITIONS 518 } UserRegistrationData 519 "er UsersItem 520 521 UsersListItem 522 523 UserUpdateData 523 524 UserSListItem 525 524 UserUpdateData 523 524 ✓ SECURITY 526 } access-token 527 "pa 530 531 530 531 532 533 ✓ SECURITY DEFINITIONS 534 }	•••			
host 502 "Users: "type info 503 "type produces 506 "produces > /api/admin/all_users 509 / > /api/admin/all_users 509 / > /api/login 511 } > /api/login 513 ''''''''''''''''''''''''''''''''''''	رلال	OPENAPI	Pixi-Initial.json	•
info 503 "type info 504 "add: schemes 505 "prod produces 506 "prod > /api/admin/all_users 509 / > /api/login 511 } > /api/login 513 > /api/login 514 > Parameters 516 > Parameters 516 > Responses 517 ✓ Definitions 518 UserRegistrationData 519 UserUpdateData 523 524 525 ✓ SecURITY 528 529 530 531 532 533 533 534 access-token 535		swagger	Pixi-Initial.json	> {
Schemes 504 "add: produces 505 "proguces > /api/admin/all_users 509 > /api/admin/all_users 509 > /api/admin/users/se 510 > /api/login • 511 > /api/login • 512 > /api/login • 513 > /api/login • 513 > /api/login • 513 > /api/login • 513 > /api/login • 514 > Paraameters 515 > Responses 517 Userslistitem 522 Userslistitem 523 524 525 530 531 531 532 532 533 <	\cap	host	502 "Use	rs]
Schemes 504 "add: produces 506 "prog > /api/admin/all_users 509 > > /api/admin/users/se 510 "prog > /api/login 511 }, > /api/login 511 }, > /api/login 511 }, > /api/login 511 }, > /api/login 513 'prog > /api/login 515 16 > /api/login 516 16 > /api/login 517 518 > /api/login 518 17 UserRegistrationData 519 "enditionalized" UserUpdateData 523 524 > SecURITY 526 \$, 330 531 532 532 533 533 </th <th>\succ</th> <th>info</th> <th>503 "t</th> <th>ype</th>	\succ	info	503 "t	ype
Produces 505 506 ✓ PATHS 507 ✓ PATHS 508 > /api/admin/all_users 509 > /api/admin/users/se 510 ● > /api/login 511 ● > /api/login 511 > /api/login ● 512 > /api/login ● 511 > /api/login ● 512 > /api/login ● 512 > /api/login ● 512 > /api/login ● 513 > /api/login ● 514 > /api/loser/edit_info 514 > PARAMETERS 515 > PARAMETERS 516 > RESPONSES 517 ✓ DEFINITIONS 518 UserRegistrationData 519 UsersListitem 522 UserUpdateData 523 520 530 531 532 532 533 S24 523 532 533 533 534 533			504 "a	ddi
✓ PATHS 507 > /api/admin/all_users 509 > /api/admin/users/se 510 > /api/login 511 > /api/login 513 > /api/loser/edit_info 514 > PARAMETERS 516 > RESPONSES 517 > DEFINITIONS 518 UserRegistrationData 519 UsersListitem 522 UserUpdateData 523 524 525 ✓ SECURITY 528 529 530 531 532 533 533 534 534 535 535 534 536 535	90	scnemes	505 " p	rop
	S-	produces	506	"_i
 ✓ /api/admin/all_users ✓ /api/login ✓ /api/login ✓ /api/register ✓ /api/user/edit_info ✓ /api/user/user/info ✓ /api/user/user/user/info ✓ /api/user/user/user/user/user/user/user/user	~			
> /api/admin/users/se 510 > /api/login 511 > /api/register 512 > /api/register 513 > /api/user/edit_info 514 > /api/user/edit_info 514 > PARAMETERS 516 > RESPONSES 517 > DEFINITIONS 518 > UserRegistrationData 519 UsersItem 522 UsersUpdateData 523 S24 525 > S24 525 S30 531 S22 529 S30 531 S22 530 S31 532 S31 532 S31 532 S31 533 S32 533 S33 534 S35 535	~h	> /ani/admin/all users		
> /api/login > 110 > /api/login > 511 > /api/register > 513 > /api/login > 511 > /api/register > 513 > /api/login > 511 > /api/register > 513 > /api/login > 511 > /api/login > 511 > /api/login > 511 > /api/login > 511 > /api/login > 513 > PaRaMeters > 516 > Responses > 517 > Definitions > 518 > UserRegistrationData > 519 UsersLittem > 522 UserUpdateData > 523 > Security > 526 > 530 > 531 > 532 > 530 > Security Definitions > 34 > access-token > 352	~	이 이 사람이 있는 것 같은 것 같아요.		
> /api/register 512 "p: > /api/register 513 > > /api/user/edit_info 514 > > PARAMETERS 516 > > PARAMETERS 518 > UserRegistrationData 519 "er Usersltem 522 UserUpdateData 523 UserUpdateData 527 "paided" S28 530 > 532 533 > S22 533 > S24 532 > S28 531 > S33 >		> /api/admin/users/se		
> /api/register 513 > /api/user/edit_info 514 > /api/user/edit_info 514 > PARAMETERS 516 > RESPONSES 517 > DEFINITIONS 518 UserRegistrationData 519 UsersItem 520 UsersUpdateData 523 UserUpdateData 523 SecURITY 526 300 531 530 531 531 532 532 533 SecURITY DEFINITIONS 534 533 534 534 535	БŬ	> /api/login 🛛 🕂		},
> /api/user/edit_info 513 > PARAMETERS 516 > RESPONSES 517 > DEFINITIONS 518 UserRegistrationData 519 Usersltem 520 Usersltem 521 Usersltem 522 UserUpdateData 523 S24 525 S25 530 S31 531 S25 531 S26 523 S27 526 S30 531 S31 532 S33 531 S33 533 S33 534 S33 534 S33 534 S33 534 S34 535		> /api/register		b]
→ PARAMETERS 515 → RESPONSES 517 → DEFINITIONS 518 ● UserRegistrationData 519 ● UsersItem 520 ● UsersItem 521 ● UsersListItem 522 ● UserUpdateData 523 ● SECURITY 526 ● SECURITY 528 ● SECURITY DEFINITIONS 531 ● SECURITY DEFINITIONS 534		> /api/user/edit info		
> PARAMETERS 515 > RESPONSES 517 > RESPONSES 517 > DEFINITIONS 518 UserRegistrationData 519 UsersListItem 520 UserUpdateData 523 UserUpdateData 525 ✓ SECURITY S20 530 531 531 532 533 ✓ SECURITY DEFINITIONS 533 534 534 535	/API			
 ▶ RESPONSES ▶ SIT ▶ DEFINITIONS ▶ SIT ▶ UserRegistrationData ▶ Site ▶ Site ▶ DEFINITIONS ▶ Site ▶ Site ▶ DEFINITIONS ▶ Site ▶ Site ▶ Site ▶ Site ▶ Security ▶ Site ▶ Site				
✓ DEFINITIONS 517 ✓ DEFINITIONS 518 ✓ UserRegistrationData 519 ✓ UsersItem 520 ✓ UsersListItem 522 ✓ UserUpdateData 523 ✓ SECURITY 526 ✓ SECURITY 526 ✓ SECURITY 526 530 531 531 532 ✓ SECURITY DEFINITIONS 534 ✓ SECURITY DEFINITIONS 534 ★ SECURITY DEFINITIONS 535		> RESPONSES		
UserRegistrationData 519 UsersItem 520 UsersListItem 522 UserUpdateData 523 Securitry 526 Access-token 529 530 531 530 531 530 531 532 533 Securitry Definitions 534 access-token 535 Securitry Definitions 534 535 535	4			1
Weerslitem 520 UsersListlitem 522 UserUpdateData 523 SECURITY 526 Access-token 527 530 531 531 532 532 533 SECURITY DEFINITIONS 534 Access-token 537 530 531 531 532 533 533 SECURITY DEFINITIONS 534 Access-token 535				۲, "۵"
UsersListItem 521 UserUpdateData 523 UserUpdateData 524 525 524 SECURITY 526 access-token 529 530 531 532 533 SECURITY DEFINITIONS 534 access-token 533 533 534 534 534 535 534 535 534				
UsersListitem 522 UserUpdateData 523 524 525 525 526 access-token 527 528 529 530 531 532 533 SECURITY DEFINITIONS 534 access-token 533 533 533 533 534 535 "na	I	UsersItem		
Image: Wight with with with with with with with wi		UsersListItem		
 ✓ SECURITY Access-token 524 525 3, 328 529 530 531 532 532 533 533 SECURITY DEFINITIONS 534 3, 		UserUpdateData		
 ✓ SECURITY Access-token 527 528 529 530 531 532 532 533 ✓ SECURITY DEFINITIONS 534 535 				
 ✓ SECURITY access-token 527 528 529 530 531 532 532 533 ✓ SECURITY DEFINITIONS 534 354 354 354 354 354 				•
Image: Single state 528 529 530 531 531 532 533 533 534 access-token 535		\sim security		}.
Image: Single state 528 529 530 531 531 532 533 533 534 access-token 535		access-token		"pa
Image: Solution of the second state of the second stat	67		528	•
↓ 530 ↓ 531 ↓ 532 ↓ 533 ↓ 534 ↓ 535 ↓ 535 ↓ 535	Н		529	•
€ 531 532 533 533 533 SECURITY DEFINITIONS 534 access-token 535			530	•
۲ 532 ۲ 533 ۲ 534 ۵ 535 ۵ 535 ۵ 535			531	
SECURITY DEFINITIONS 535 access-token 535			532	
access-token 535 "na			533	•
	502	✓ SECURITY DEFINITIONS	534	},
⊗ 7 ⚠ 16 🛈 2	272	access-token	535	"na
	⊗7∠	∆ 16 () 2		

Item": { e": "object", litionalProperties": false, perties": { id": { "type": "number", "format": "integer", "minimum": 0, "maximum": 999999 ic": { "type": "string", "format": "uri", "pattern": "(\\w+:(\\/?\\/?)[^\\s]+)", "minLength": 0, "maxLength": 200 mail": { "type": "string", "format": "email", "minLength": 5, "maxLength": 50, "example": "email@email.com" assword": { "type": "string", "format": "string", "pattern": "^[a-zA-Z0-9&@#!?]{4,12}\$", "minLength": 4, maxLength": 12, "example": "p@ssword1" ame": {

© COPYRIGHT 42CRUNCH | CONFIDENTIAL

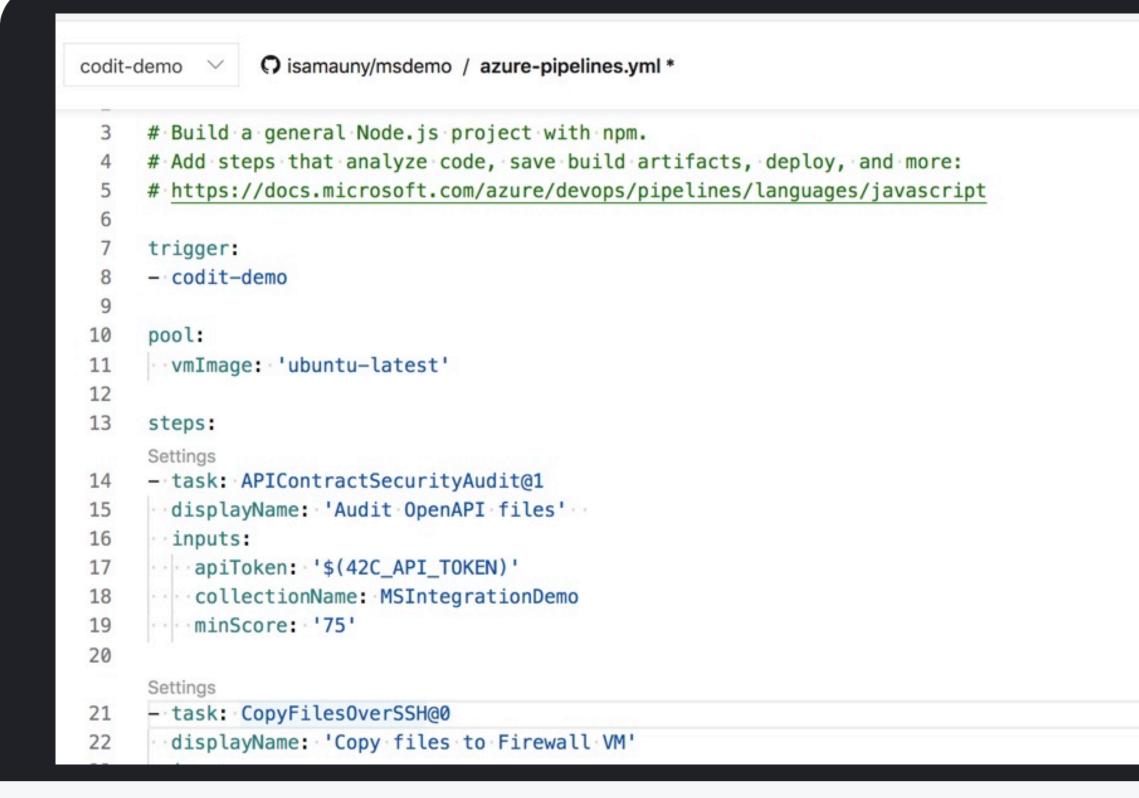


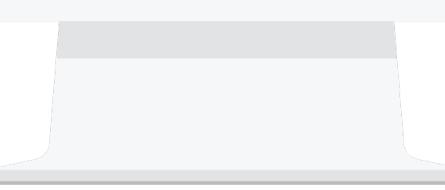
		Pixi-Initial.json — OASFiles	
	{} Pixi-Initial.json ×	æ 🔲 …	
	<pre>{} Pixi-Initial.json > { } paths > { } /api/admin/all_</pre>	users > { } get > { } responses	
GROUP 1	416 },	Second Second	Array schema has no maximum
× {} Pixi-Initial.j 9+	417 "required": [
GROUP 2	418 "message"	E	number of items defined
■ API Security Audit	419] 420 }		
	420 }		Line 436. Severity: High. Score impact 0.5
	422 },		Description
{} Pixi-Initial.json 9+	423 "security": [Description
{} PixiBasic-forScan.json	424 {		An array schema does not specify the maximum number of items it
PixiBasic-v1.0.json	425 "access-token": []		can contain.
	426 }		For more details, see the OpenAPI Specification.
	427], 428 "operationId": "userSear	ch!!	
/API	429 }		Example
	430 },		
	431 "/api/admin/all_users": {	Services.	The following is an example of how this type of risk could look in your API definition:
	432 "get": {		your APr definition.
	433 "responses": {		"post": {
	434 "200": {		"description": "Creates a new pet in the store", "operationId": "addPet",
	435 "description": "",		"parameters": [
	436 "schema": { 437 "type": "array",		{
	438 "minItems": 1,		"name": "pet", "in": "body",
	439 View detailed report for 1 OpenAPI issue(s	s)	escription": "Pet to add to the store",
	440		equired": true,
	441 Response that should contain a impact 0.2)	body nas no schema defined	<pre>(score chema": { "type": "object",</pre>
	442		"additionalProperties": "false",
	443 Peek Problem No quick fixes available 444 "403": {		"required": ["name"
	445 "description": "No to	oken provided or i],
	446 },		"properties": {
	447 "default": {		"name": { "type": "string"
ふろう > OUTLINE	448 "description": "unex	pected error",	},
> OUTLINE > BALLERINA PROJECT OV	449 "schema": {		"favfood": {
⊗ 7 ⚠ 16 🕕 2	450 "type" "object"		"type": "array". Ln 436, Col 16 Spaces: 2 UTF-8 LF JSON 🔗 (

Acrunch

DEMO STEP 2: AZURE DEVOPS INTEGRATION

© COPYRIGHT 42CRUNCH | CONFIDENTIAL



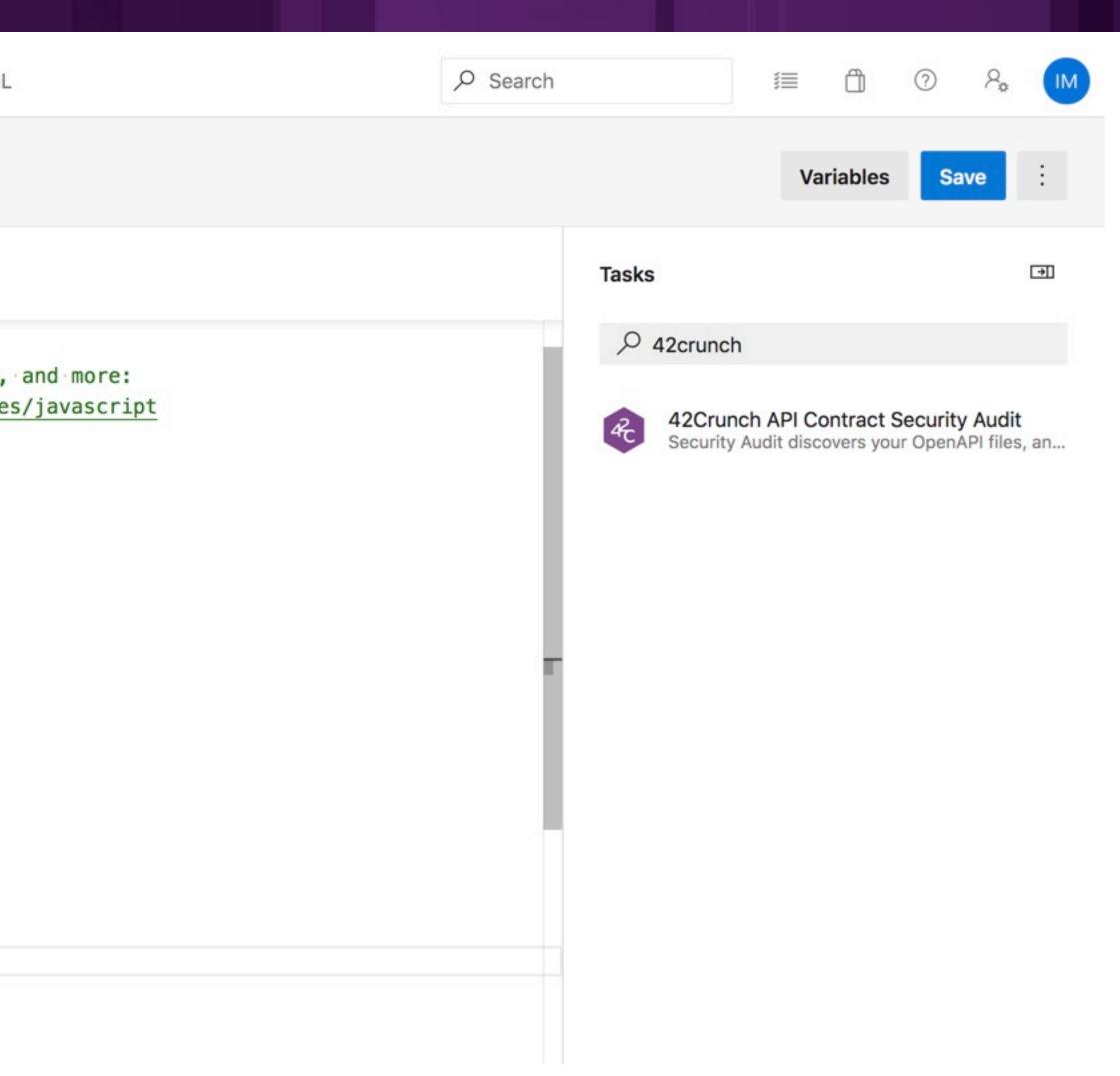




¢	42css /	APIMIntegration / Pipelines / Builds / msdemo deployment / YAML
▲ +	← n	nsdemo deployment
	codit-	demo V () isamauny/msdemo / azure-pipelines.yml *
	3	# Build a general Node.js project with npm.
8	4	# Add steps that analyze code, save build artifacts, deploy,
-0	5	<pre># https://docs.microsoft.com/azure/devops/pipelines/languages</pre>
2	6	
	7	trigger:
÷.	8	- codit-demo
e	9	
I	10	pool:
D	11	<pre>vmImage: 'ubuntu-latest'</pre>
<i>3</i> 2	12	
00	13	steps:
00 4		Settings
=	14	<pre>- task: APIContractSecurityAudit@1</pre>
	15	<pre>displayName: 'Audit OpenAPI files'</pre>
• •• •	16	· inputs:
	17	apiToken: '\$(42C_API_TOKEN)'
	18	<pre>collectionName: MSIntegrationDemo</pre>
	19	minScore: '75'
	20	
		Settings
	21	<pre>- task: CopyFilesOverSSH@0</pre>
	22	<pre>displayName: 'Copy files to Firewall VM'</pre>
	23	inputs:
	24	sshEndpoint: '42C-VM-France'

Automated audit and API discovery

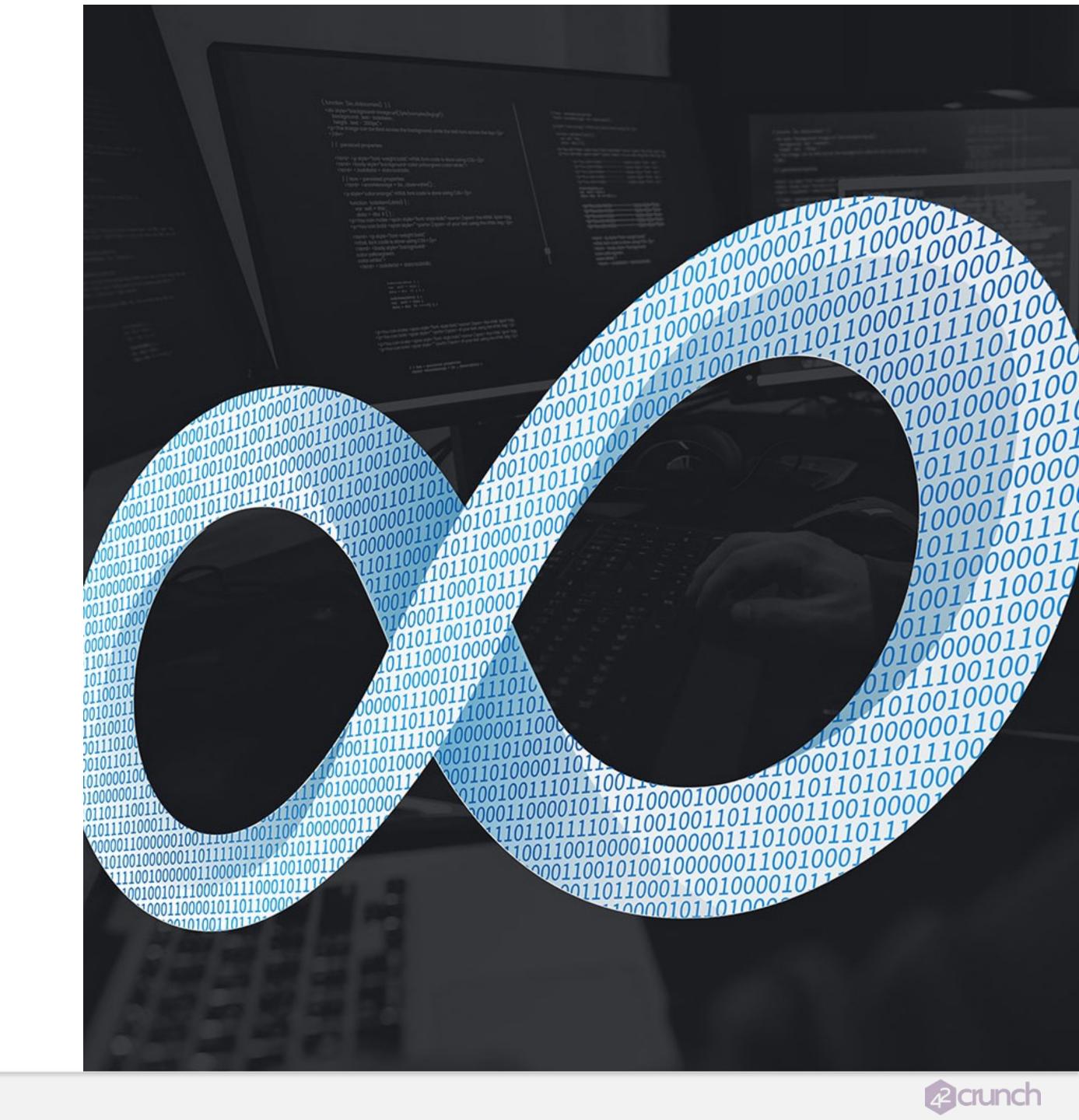
https://marketplace.visualstudio.com/items?itemName=42Crunch.cicd



DEV-SEC-OPS BENEFITS

When API security becomes **fully part** of the **API lifecycle**:

- Security is applied automatically and at scale
- Vulnerable APIs are detected early
- APIs are automatically protected as soon as the contract is defined



RESOURCES

- <u>42Crunch Website</u>
- <u>Azure DevOps SignUp</u>
- Free OAS Security Audit
- OpenAPI VS Code Extension
- OpenAPI Spec Encyclopedia
- OWASP API Security Top 10
- <u>APIsecurity.io</u>

election at the end -add _ob.select= 1 er_ob.select=1 ntext.scene.objects.acti "Selected" + str(modifie irror_ob.select = 0 bpy.context.selected_ob ita.objects[one.name].sel

int("please select exactle

ypes.Operator): X mirror to the select ject.mirror_mirror_x" ror X"

context):
context.active_object is not



42 crunch