OPEN SECURITY SUMMIT

Open Security Control Testing at Scale

BBVA Innovation Labs

BBVA

Creando Oportunidades

MM0003CA:~ whoami luissaiz

Luis Saiz Gimeno

@lsaiz

Telecomm. Eng. - Cryptography - Sys.Sec - Info.Sec - Tech. Fraud Prevention - Fraud Prevention Tech. - Global Security Center - Innovation in Security @BBVA

Madrid

bbva.com/en/featured/bb…

Se unió en julio de 2010

BBVA in numbers

€662.9 billion in total assets

81.7 million customers

>25 countries

6,083 branches

29,148 ATMs

110,432 employees

Data at the end of December 2021. Those countries in which BBVA has no legal entity or the volume of activity is not significant, are not included

BBVA
Creating Opportunities

Innovation Labs

- Innovation is about **new questions**, not new answers
- **AI, Cybersecurity**
- Multidisciplinar cross pollination
- Learning by doing
- Doing to learn

Project Team

Roberto (Ruso) Abdelkader
Security & Functional Programming
TW: @nilp0inter
GH: nilp0inter

César Gallego
Security & Data
TW: @CesarGallegoR
GH: CesarGallego

BBVA

BBVA

Madrid http://bbva.com opensource@bbva.com

Repositories 97 Packages People 36 Teams 6 Projects 1

Pinned repositories

kapow
Kapow! If you can script it, you can HTTP it.
Go 505 20

apicheck
The DevSecOps toolset for REST APIs
Python 118 30

qed
The scalable, auditable and high-performance tamper-evident log project
Go 73 13

patton
The clever vulnerability dependency finder
Gherkin 79 11

timecop
Time series based anomaly detector
Python 56 13

susto
Systematic Universal Security Testing Orchestration
10

Open Security Control Testing at Scale

BBVA
Creating Opportunities

WHAT?
WHY?
WHO?
HOW?

OPEN SECURITY SUMMIT

Open Security Control Testing at Scale

BBVA
Creating Opportunities

WHAT?

WHY?

WHO?

HOW?

OPEN SECURITY SUMMIT

Controls as First Class Citizens

"Controls" by Phil Venables (CISO Google Cloud)

We talk about attacks but a similar pattern exists for control failures that lead to other realized risk for other types of incidents across the full spectrum of enterprise risk domains. So, what to do.

Treat controls as first class objects like other parts of system function.

Controls as First Class Citizens

Treat controls (especially security controls) as automation/code
Build tests/coverage for control correctness as you would with other code

Test for the presence and integration of controls at build time in integration/deploy suites. *Different styles of test will be needed depending on the nature of the controls (component, software, hardware etc.)*

*When a control (or instance of a control) is detected as having failed then declare a "**control incident**" and handle as if a security incident has occurred*

Controls as First Class Citizens

OWASP A04:2021 – Insecure Design:

"Write **unit and integration tests** to validate that all critical flows are resistant to the threat model"

From Checklist to Tests - What we have now (some examples)

OWASP-ASVS

V1.9 Communications Architecture

#	Description	L1	L2	L3	CWE
1.9.1	Verify the application encrypts communications between components, particularly when these components are in different containers, systems, sites, or cloud providers. (C3)		✓	✓	319
1.9.2	Verify that application components verify the authenticity of each side in a communication link to prevent person-in-the-middle attacks. For example, application components should validate TLS certificates and chains.		✓	✓	295

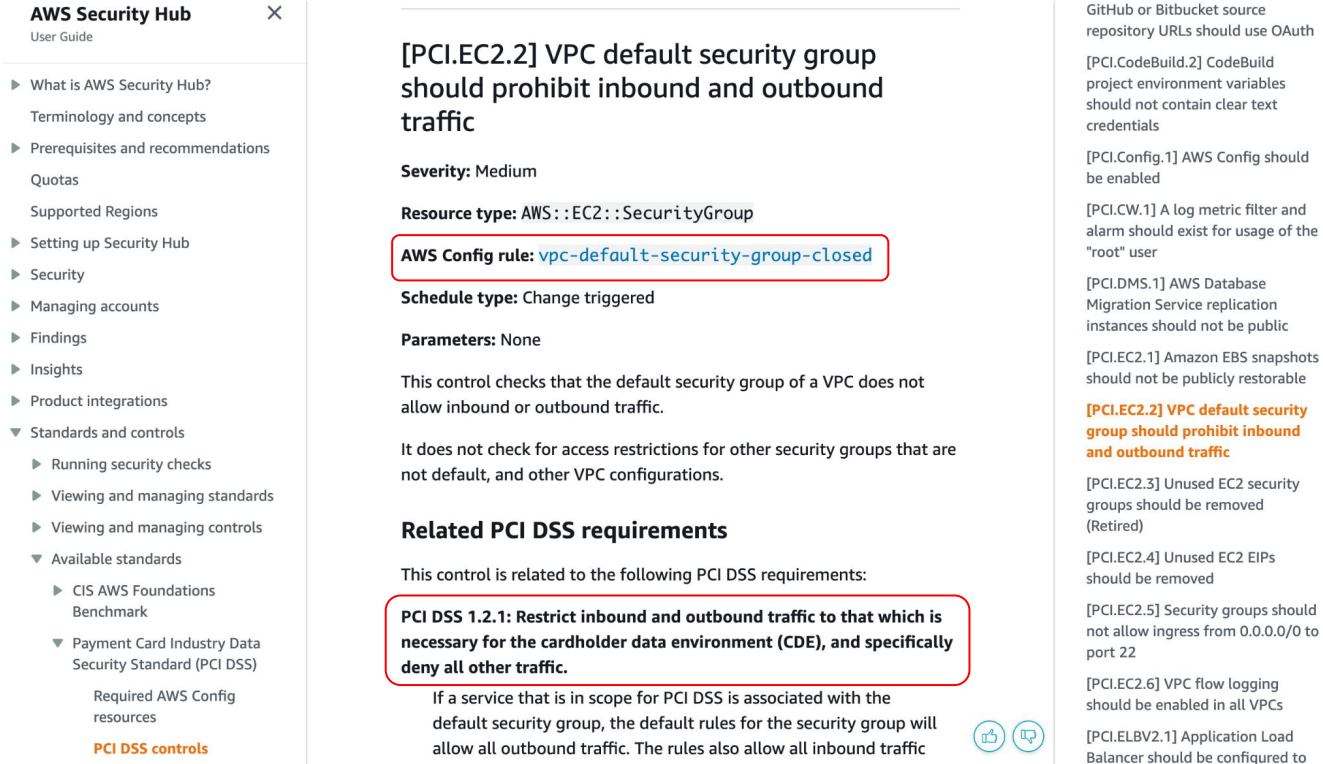
From Checklist to Tests - What we have now (some examples)

PCI-DSS

PCI DSS Requirements	Testing Procedures	Guidance
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	**1.2.1.a** Examine firewall and router configuration standards to verify that they identify inbound and outbound traffic necessary for the cardholder data environment.	Examination of all inbound and outbound connections allows for inspection and restriction of traffic based on the source and/or destination address, thus preventing unfiltered access between untrusted and trusted environments. This prevents malicious individuals from accessing the entity's network via unauthorized IP addresses or from using services, protocols, or ports in an unauthorized manner (for example, to send data they've obtained from within the entity's network out to an untrusted server). Implementing a rule that denies all inbound and outbound traffic that is not specifically needed helps to prevent inadvertent holes that would allow unintended and potentially harmful traffic in or out.
	1.2.1.b Examine firewall and router configurations to verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment.	
	1.2.1.c Examine firewall and router configurations to verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit "deny all" or an implicit deny after allow statement.	

From Checklist to Tests - What we have now (some examples)

PCI-DSS @ AWS



AWS Security Hub
User Guide

- What is AWS Security Hub?
- Terminology and concepts
- Prerequisites and recommendations
- Quotas
- Supported Regions
- Setting up Security Hub
- Security
- Managing accounts
- Findings
- Insights
- Product integrations
- Standards and controls
  - Running security checks
  - Viewing and managing standards
  - Viewing and managing controls
  - Available standards
    - CIS AWS Foundations Benchmark
    - Payment Card Industry Data Security Standard (PCI DSS)
      - Required AWS Config resources
      - PCI DSS controls

[PCI.EC2.2] VPC default security group should prohibit inbound and outbound traffic

Severity: Medium

Resource type: `AWS::EC2::SecurityGroup`

AWS Config rule: `vpc-default-security-group-closed`

Schedule type: Change triggered

Parameters: None

This control checks that the default security group of a VPC does not allow inbound or outbound traffic.

It does not check for access restrictions for other security groups that are not default, and other VPC configurations.

Related PCI DSS requirements

This control is related to the following PCI DSS requirements:

PCI DSS 1.2.1: Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment (CDE), and specifically deny all other traffic.

If a service that is in scope for PCI DSS is associated with the default security group, the default rules for the security group will allow all outbound traffic. The rules also allow all inbound traffic

- GitHub or Bitbucket source repository URLs should use OAuth
- [PCI.CodeBuild.2] CodeBuild project environment variables should not contain clear text credentials
- [PCI.Config.1] AWS Config should be enabled
- [PCI.CW.1] A log metric filter and alarm should exist for usage of the "root" user
- [PCI.DMS.1] AWS Database Migration Service replication instances should not be public
- [PCI.EC2.1] Amazon EBS snapshots should not be publicly restorable
- **[PCI.EC2.2] VPC default security group should prohibit inbound and outbound traffic**
- [PCI.EC2.3] Unused EC2 security groups should be removed (Retired)
- [PCI.EC2.4] Unused EC2 EIPs should be removed
- [PCI.EC2.5] Security groups should not allow ingress from 0.0.0.0/0 to port 22
- [PCI.EC2.6] VPC flow logging should be enabled in all VPCs
- [PCI.ELBV2.1] Application Load Balancer should be configured to

From Checklist to Tests - What we have now (some examples)

PCI-DSS @ AWS Config Rule

vpc-default-security-group-closed

Checks that the default security group of any Amazon Virtual Private Cloud (VPC) does not allow inbound or outbound traffic. The rule returns NOT_APPLICABLE if the security group is not default. The rule is NON_COMPLIANT if the default security group has one or more inbound or outbound traffic rules.

Identifier: VPC_DEFAULT_SECURITY_GROUP_CLOSED

Trigger type: Configuration changes

AWS Region: All supported AWS regions

Parameters:

None

AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates (p. 216).

From Checklist to Tests - What we have now (some examples)

NIST SP 800-53A Rev. 5

AC-02(03)	ACCOUNT MANAGEMENT | DISABLE ACCOUNTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-02(03)_ODP[01]	***time period within which to disable accounts is defined;***
	AC-02(03)_ODP[02]	***time period for account inactivity before disabling is defined;***
	AC-02(03)(a)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have expired;
	AC-02(03)(b)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts are no longer associated with a user or individual;
	AC-02(03)(c)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts are in violation of organizational policy;
	AC-02(03)(d)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have been inactive for ***<AC-02(03)_ODP[02] time period>***.

From Checklist to Tests - What we have now (some examples)

NIST SP 800-53A Rev. 5

Instantiation

AC-02(03)	ACCOUNT MANAGEMENT | DISABLE ACCOUNTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-02(03)_ODP[01]	***time period within which to disable accounts is defined;***
	AC-02(03)_ODP[02]	***time period for account inactivity before disabling is defined;***
	AC-02(03)(a)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have expired;
	AC-02(03)(b)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts are no longer associated with a user or individual;
	AC-02(03)(c)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts are in violation of organizational policy;
	AC-02(03)(d)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have been inactive for ***<AC-02(03)_ODP[02] time period>***.

From Checklist to Tests - What we have now (some examples)

AC-02(03)	ACCOUNT MANAGEMENT | DISABLE ACCOUNTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-02(03)_ODP[01]	***time period within which to disable accounts is defined;***
	AC-02(03)_ODP[02]	***time period for account inactivity before disabling is defined;***
	AC-02(03)(a)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have expired;
	AC-02(03)(b)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts are no longer associated with a user or individual;
	AC-02(03)(c)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts are in violation of organizational policy;
	AC-02(03)(d)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have been inactive for ***<AC-02(03)_ODP[02] time period>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-02(03)-Examine	[SELECT FROM: Access control policy; procedures for addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; system-generated list of accounts removed; system-generated list of emergency accounts disabled; system audit records; system security plan; other relevant documents or records].
	AC-02(03)-Interview	[SELECT FROM: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-02(03)-Test	[SELECT FROM: Mechanisms for implementing account management functions].

??

Open Security Control Testing at Scale

WHAT?

WHY?

WHO?

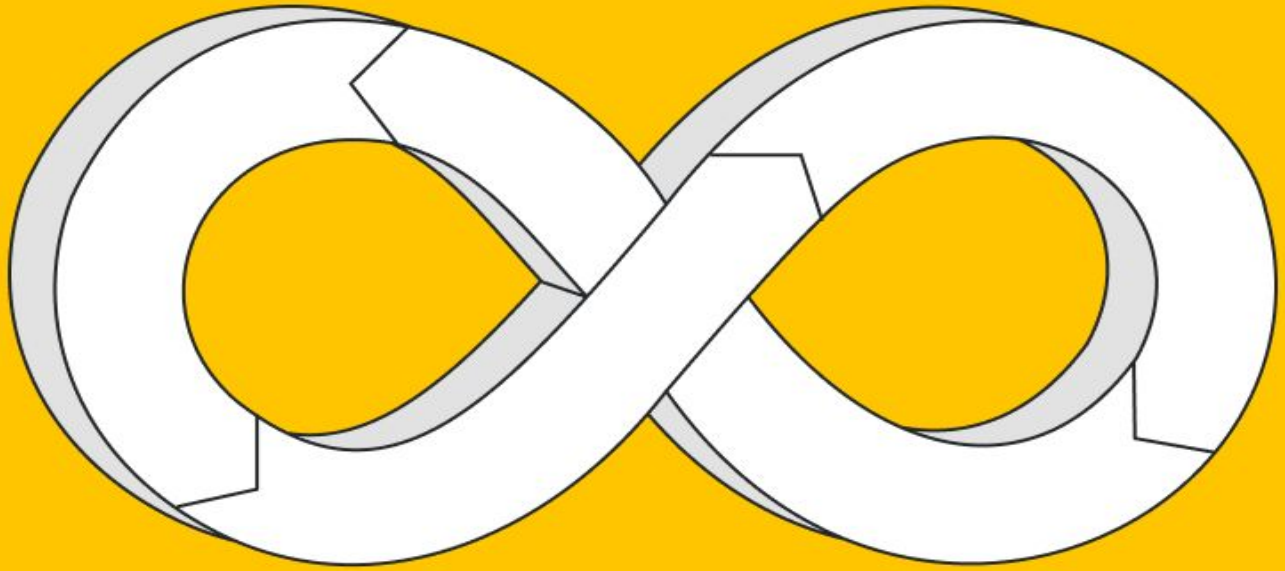
HOW?

BBVA

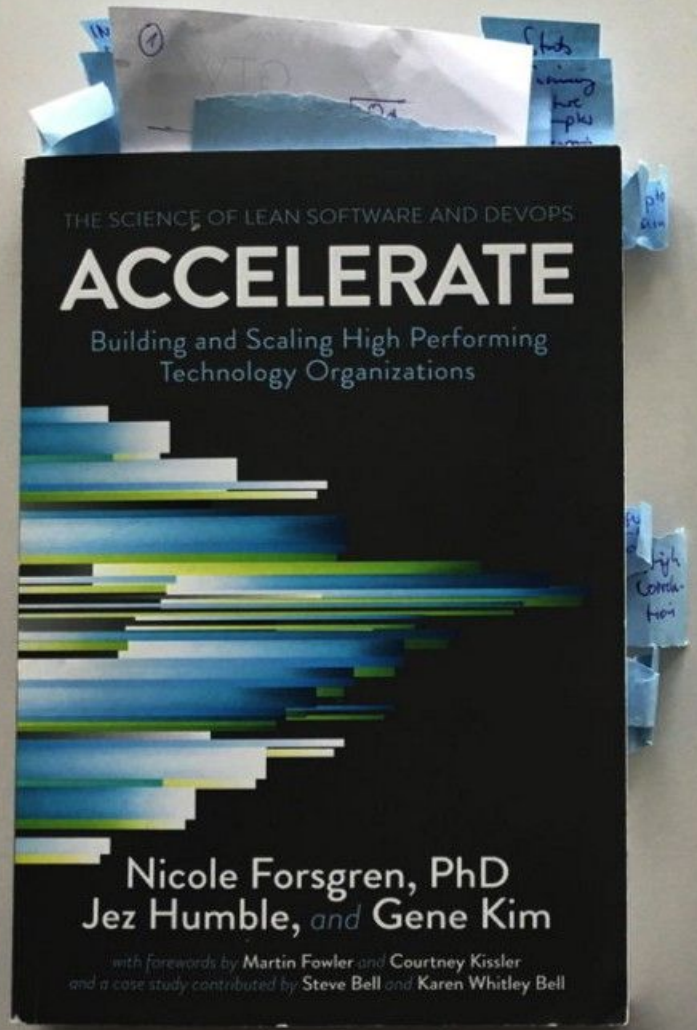
Creating Opportunities

OPEN SECURITY SUMMIT


NEED FOR SPEED
PAYBACK
POLICE



Accelerate!

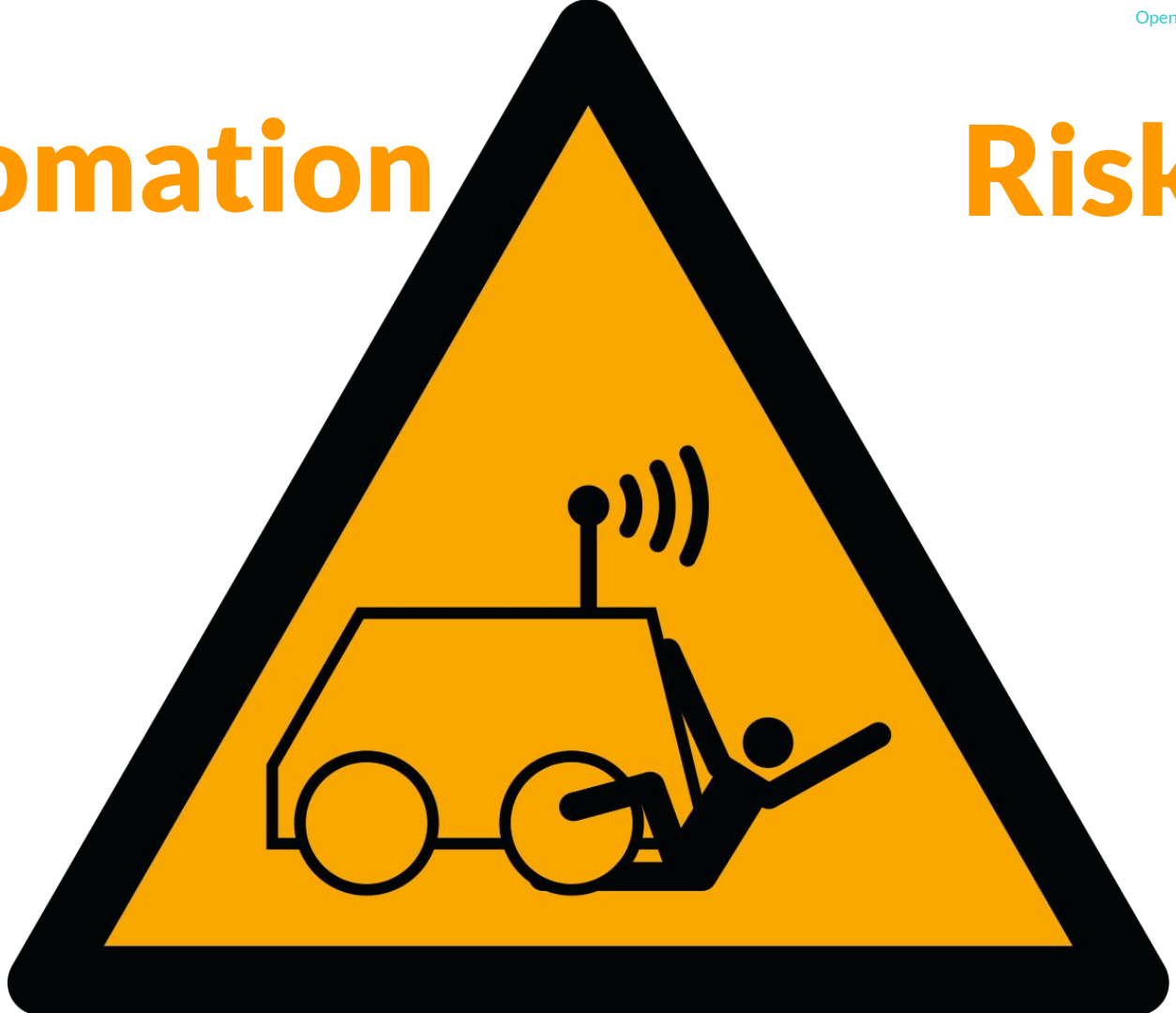


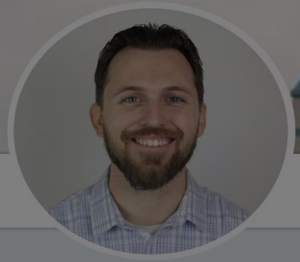
Accelerate

Building and Scaling
High Performing
Technology
Organizations

Keep Pace!

Automation Risks





Justin Garrison
@rothgar

Here to spread love and learn from others. Co-author of cnibook.info Tweets about tech and K8s. ❤ community & OSS. @DisneyAnimation - DMs open

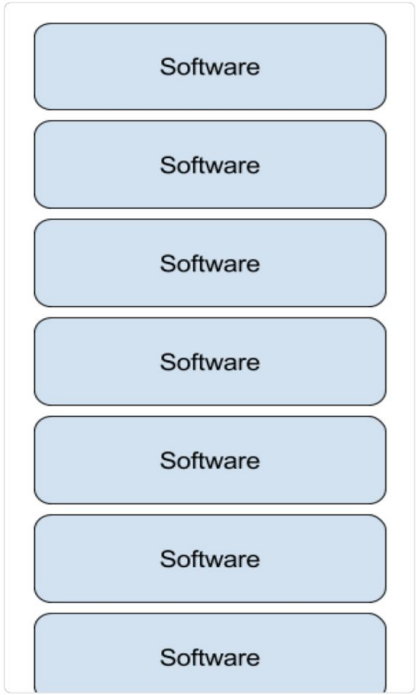
Clever phrase
medium.com/@rothgar
Se unió en abril de 2008

Justin Garrison
@rothgar

Siguiendo

The new OSI model is much easier to understand

Traducir Tweet



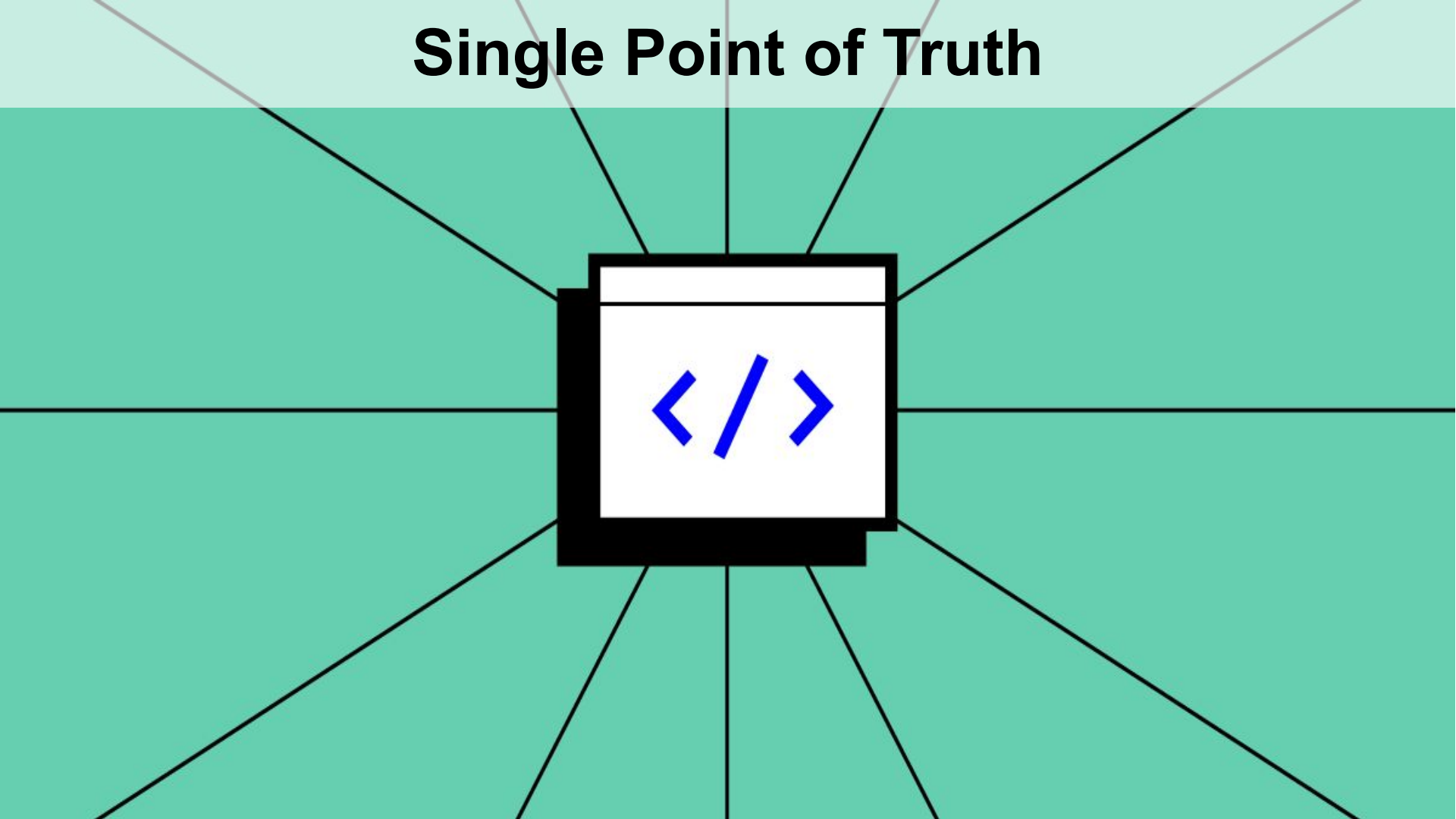
18:22 - 18 jul. 2017

2.820 Retweets **3.930** Me gusta

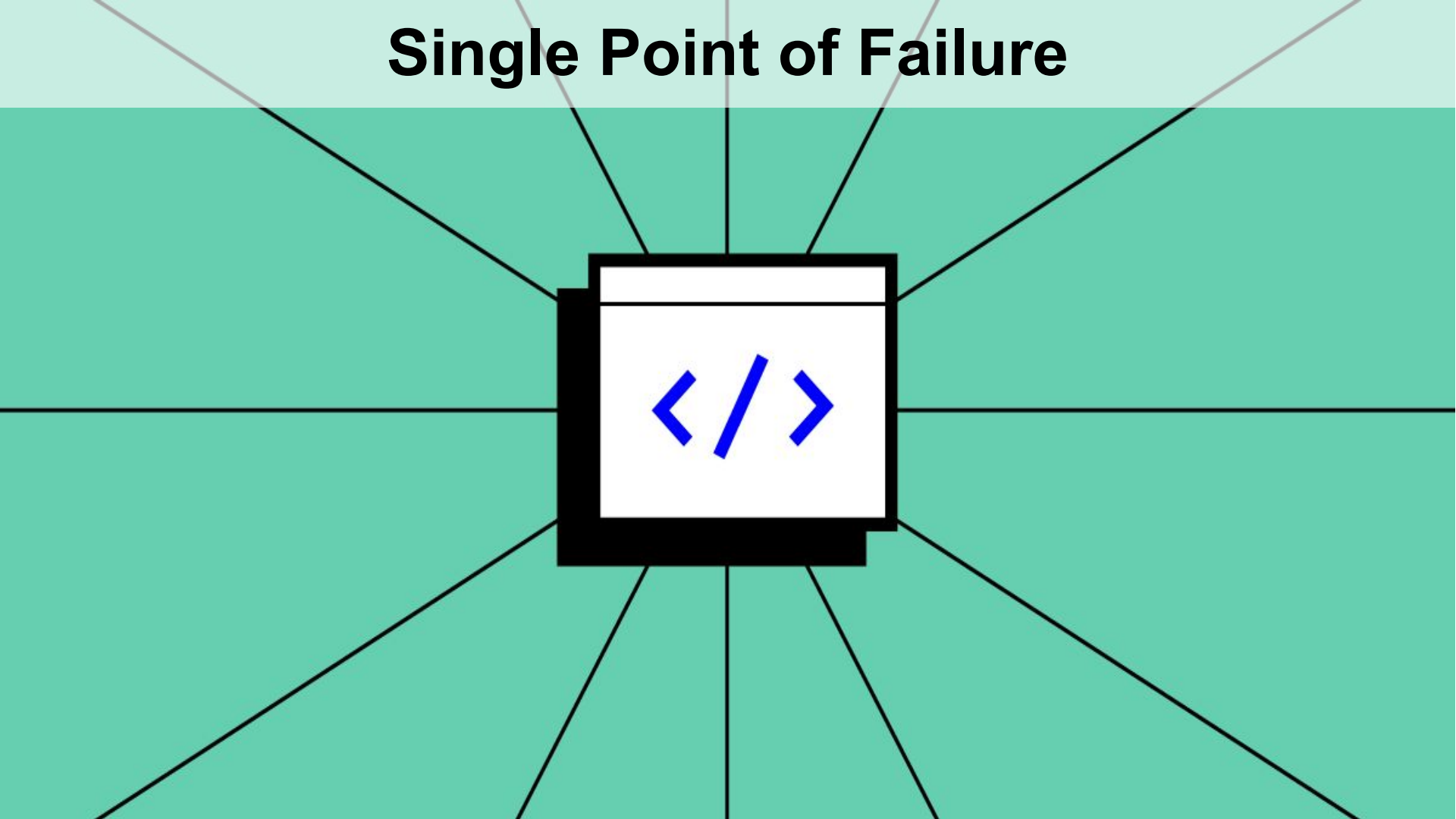
93 2,8K 3,9K

SdE

Single Point of Truth



Single Point of Failure



Complexity equals risk

The greater the cloud complexity in an enterprise, the greater the cybersecurity risks. The cloud's enterprise dominance brings more sophisticated, complex cybersecurity risks and breach attempts that require correspondingly higher-level security techniques. **The more complex an enterprise's cloud infrastructure is, the more challenging it becomes to secure. Gartner predicts that through 2025, more than 99% of cloud breaches will be traced back to preventable misconfigurations or mistakes by end users.** Gartner's latest Hype Cycle for


COMPLIANCE

Compliance [1]

OWASP A04:2021 – Insecure Design:

"Write **unit and integration tests** to validate that all critical flows are resistant to the threat model"

[1] OWASP is a reference for Standards like PCI-DSS

Open Security Control Testing at Scale

BBVA
Creating Opportunities

WHAT?
WHY?
WHO?
HOW?

OPEN SECURITY SUMMIT

CASTING

CASTING

Mat Rule

as
Rule Creator

Ana Lista

as
Security Risk Manager

Presley Leads

as
Project Tech Lead

Victor Stu Dior

as
Developer

Norman Auditore

as
Auditor

Mat Rule

- **Rule creator**
- Familiar with NIST/OWASP/PCI/CIS… controls and best practices
- Abstract thinker, not worried by implementation details
- Affiliated to a end-user organization / startup / big tech company / …
- Willing to collaborate with the community

Requirements

- Easy yet powerful syntax
- Easy to add value without solving the full problem with low coordination
- Environment and project agnostic
- Easy to reuse existing library of rule-checks

Ana Lista

- **Security Risk Manager**
- Threat Modeler
- Layer 2 of Protection
- Assess controls to be deployed, several from a (formal or informal) catalog of common controls / best practices
- Maintain same risk posture across projects/environments
- Has no vision or control over whether her instructions are followed or the effectiveness of the controls she establishes

Requirements

- Knowledge and certainty of control deployment and effectiveness across projects
- Integration with other ASR&TM / GRC tools
- Frequent/common controls tests libraries for different projects/environments
- Golden reference of control effectiveness
- Rule and checks authoring reputation and audit

Presley Leads

- **Project Tech Lead**
- Project/service/environment domain expert, knows the information needed but not always how to gather it.
- Layer 1 of Protection
- Parametrize rules
- Risk assessment agnostic

Requirements

- Easy to understand and expand rule syntax
- Expressive Types to detail information to be gathered specific to her project
- Comprehensive results data for troubleshooting and to react to failed checks

Victor
Stu Dior

- **Developer**
- Project/service/environment domain expert, knows where it is the information needed and how to gather it
- Programs the gathering logic
- Can write code to gather the information he needs
- Risk assessment agnostic

Requirements

- Clear and easy syntax
- Easy way to define new Types
- Easy to write interfaces to existing tools/services
- Easy troubleshooting

Norman Auditore

- **Auditor**
- Follows the standards but interprets good practices
- Without a clear “definition of done” he always will have “findings” on control selection and/or implementation
- Checks controls manually by himself, doesn’t trust Project/SecOps/GRC checks (3rd LoP > 1st/2nd LoP)

Requirements

- Control effectiveness auditing based on standards and best practices
- Audit trail on each step and instantiation parameters
- Automatic standards compliance mapping
- Able to define and execute their own tests

ALSO STARRING

Ernesto Aplicado
as
App Security

Ceri Watson
as
Attack Surface Reducer
@CERT

Kalinda
as
Pentester

Iga Turowska
as
Identity Governance

Maria de la Norma
as
Compliance

Mat Rule

Ana Lista

Presley Leads

Victor Stu Dior

Norman Auditore

Ernesto Aplicado

Ceri Watson

Kalinda

Iga Turowska

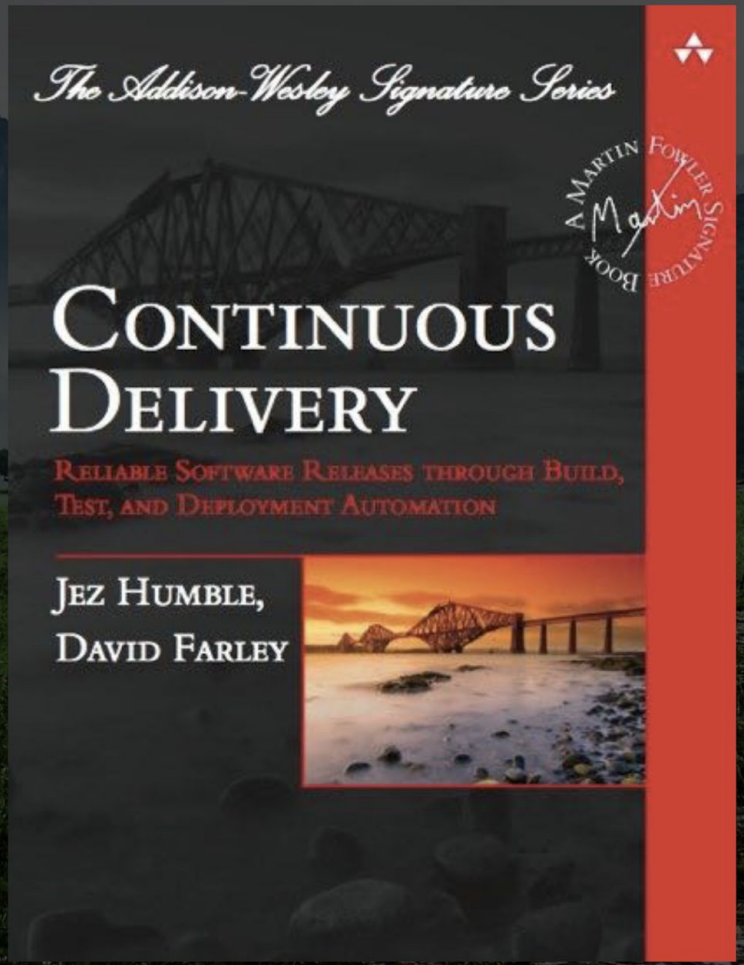
Maria de la Norma

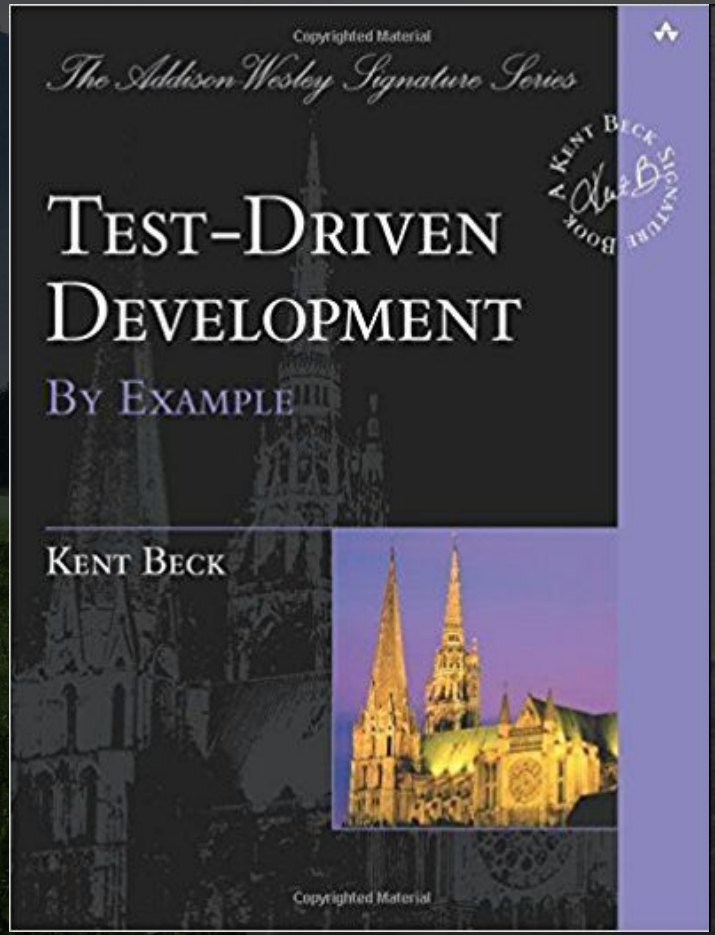
Open Security Control Testing at Scale

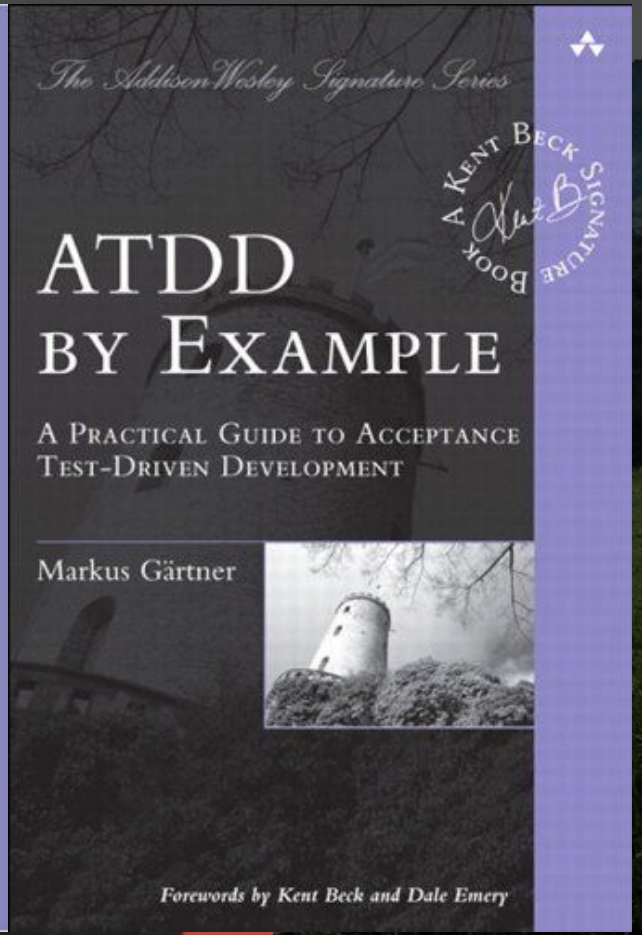
BBVA
Creating Opportunities

WHAT?
WHY?
WHO?
HOW? (others did)

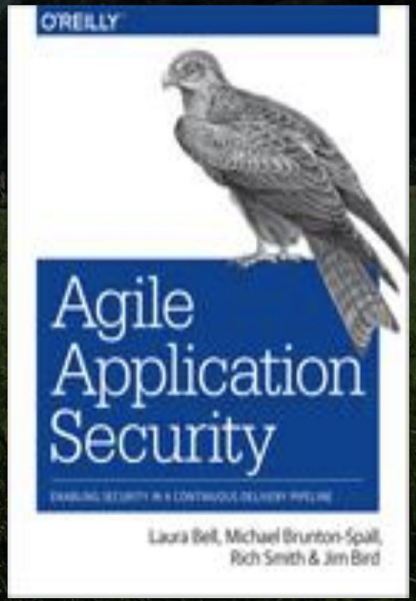
OPEN SECURITY SUMMIT


The Addison-Wesley Signature Series
A Martin Fowler Signature Book
Continuous Delivery
Reliable Software Releases through Build, Test, and Deployment Automation
Jez Humble,
David Farley


Copyrighted Material
The Addison Wesley Signature Series
A Kent Beck Signature Book
Test-Driven Development
By Example
Kent Beck
Copyrighted Material


The Addison Wesley Signature Series
A Kent Beck Signature Book
ATDD by Example
A Practical Guide to Acceptance Test-Driven Development
Markus Gärtner
Forewords by Kent Beck and Dale Emery

[Deploys] can be treated as standard or routine changes that have been pre-approved by management, and that don’t require a heavyweight change review meeting.



The scale problem

The scale problem

New NIST SP 800-53A Rev. 5: **1189 controls** (best practices)

Control Identifier	Control (or Control Enhancement) Name
AC-1	Policy and Procedures
AC-2	Account Management
AC-2(1)	Account Management | Automated System Account Management
AC-2(2)	Account Management | Automated Temporary and Emergency Account Management
AC-2(3)	Account Management | Disable Accounts
AC-2(4)	Account Management | Automated Audit Actions
AC-2(5)	Account Management | Inactivity Logout
AC-2(6)	Account Management | Dynamic Privilege Management
AC-2(7)	Account Management | Privileged User Accounts
AC-2(8)	Account Management | Dynamic Account Management
AC-2(9)	Account Management | Restrictions on Use of Shared and Group Accounts
AC-2(10)	Account Management | Shared and Group Account Credential Change
AC-2(11)	Account Management | Usage Conditions
AC-2(12)	Account Management | Account Monitoring for Atypical Usage
AC-2(13)	Account Management | Disable Accounts for High-risk Individuals

The scale problem

New NIST SP 800-53A Rev. 5: **1189 controls** (best practices)

X checks per control

AC-02(03)	ACCOUNT MANAGEMENT | DISABLE ACCOUNTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-02(03)_ODP[01]	***time period within which to disable accounts is defined;***
	AC-02(03)_ODP[02]	***time period for account inactivity before disabling is defined;***
	AC-02(03)(a)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have expired;
	AC-02(03)(b)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts are no longer associated with a user or individual;
	AC-02(03)(c)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts are in violation of organizational policy;
	AC-02(03)(d)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have been inactive for ***<AC-02(03)_ODP[02] time period>***.

The scale problem

New NIST SP 800-53A Rev. 5: **1189 controls** (best practices)

X checks per control

Y environments/check. “Account”: local, AD, LDAP, AWS, IoT…

AC-02(03)	ACCOUNT MANAGEMENT | DISABLE ACCOUNTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-02(03)_ODP[01]	***time period within which to disable accounts is defined;***
	AC-02(03)_ODP[02]	***time period for account inactivity before disabling is defined;***
	AC-02(03)(a)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have expired;
	AC-02(03)(b)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts are no longer associated with a user or individual;
	AC-02(03)(c)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts are in violation of organizational policy;
	AC-02(03)(d)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have been inactive for ***<AC-02(03)_ODP[02] time period>***.

The scale problem

New NIST SP 800-53A Rev. 5: **1189 controls** (best practices)

X checks per control

Y environments/check. “Account”: local, AD, LDAP, AWS, IoT…

AC-02(13)	ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-02(13)_ODP[01]	***time period within which to disable accounts of individuals who are discovered to pose significant risk is defined;***
	AC-02(13)_ODP[02]	***significant risks leading to disabling accounts are defined;***
	AC-02(13)	accounts of individuals are disabled within ***<AC-02(13)_ODP[01] time period>*** of discovery of ***<AC-02(13)_ODP[02] significant risks>***.

AC-02(03)	ACCOUNT MANAGEMENT | DISABLE ACCOUNTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-02(03)_ODP[01]	***time period within which to disable account***
	AC-02(03)_ODP[02]	***time period for account inactivity before dis***
	AC-02(03)(a)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have expired;
	AC-02(03)(b)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts are no longer associated with a user or individual;
	AC-02(03)(c)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts are in violation of organizational policy;
	AC-02(03)(d)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have been inactive for ***<AC-02(03)_ODP[02] time period>***.

The scale problem

New NIST SP 800-53A Rev. 5: **1189 controls** (best practices)

X checks per control

Y environments/check. “Account”: local, AD, LDAP, AWS, IoT…

Plus organization/project specific controls

The scale problem

New NIST SP 800-53A Rev. 5: **1189 controls** (best practices)

X checks per control

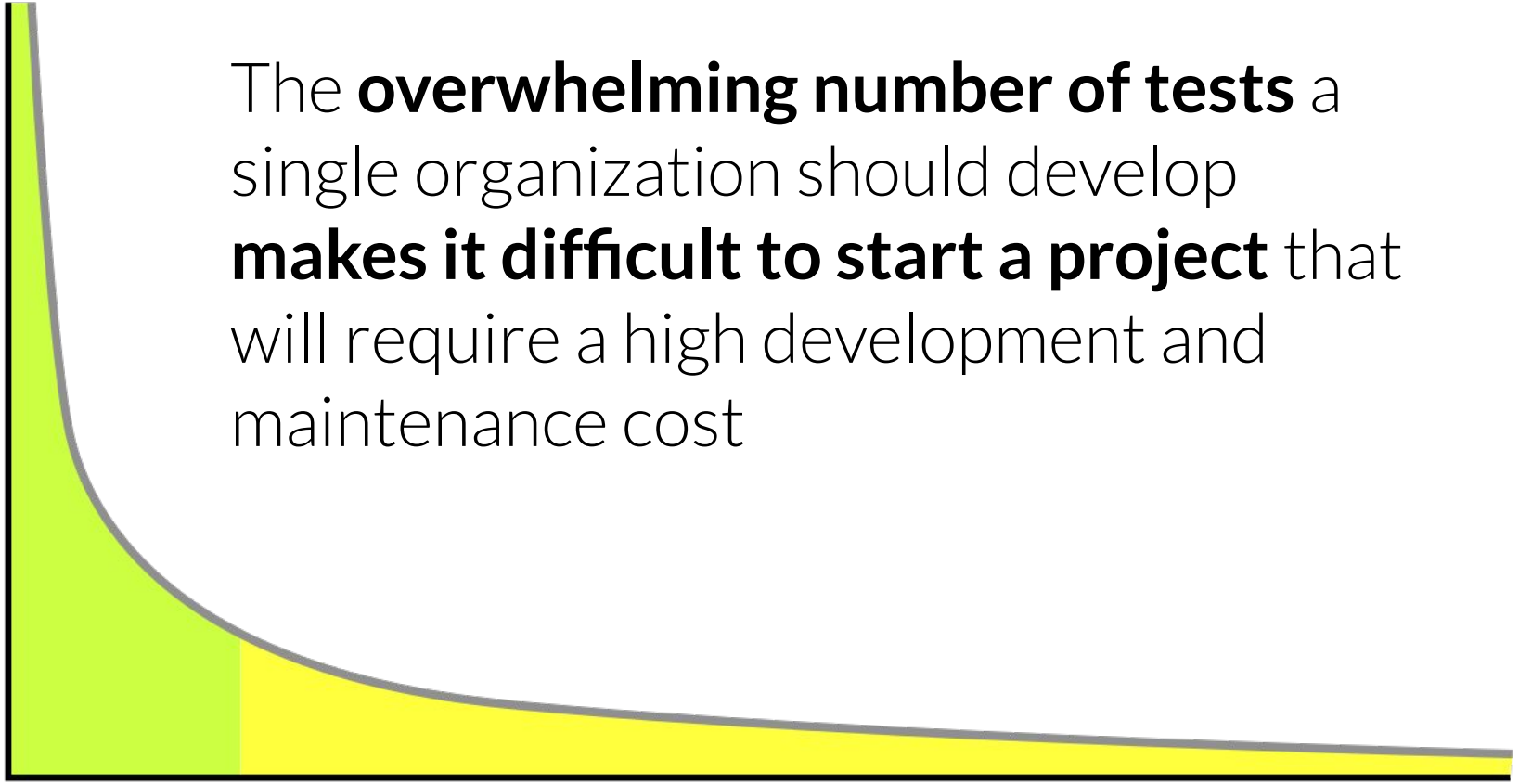
Y environments/check. “Account”: local, AD, LDAP, AWS, IoT…

Plus organization/project specific controls

YET…

"*Write **unit and integration tests** to validate that all critical flows are resistant to the threat model*"

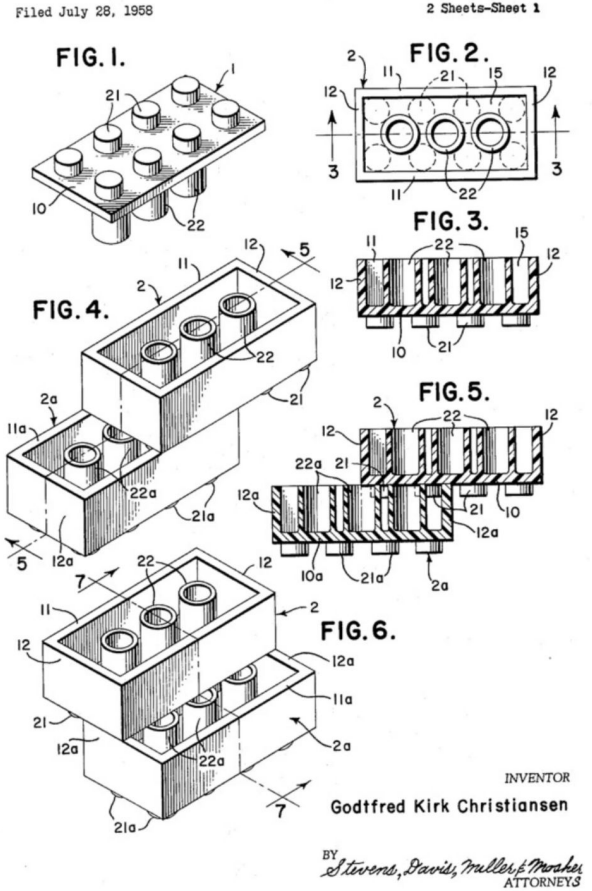
The long tail of security control checks

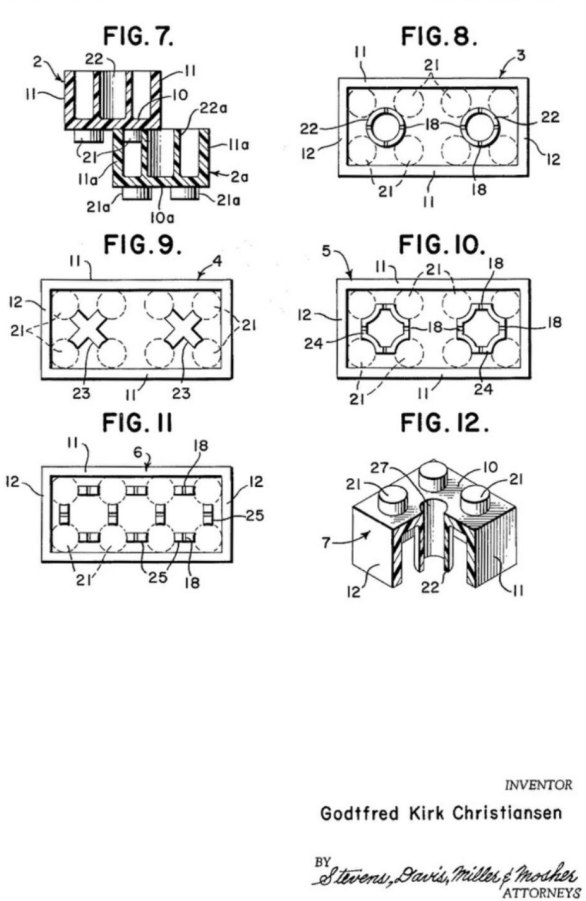


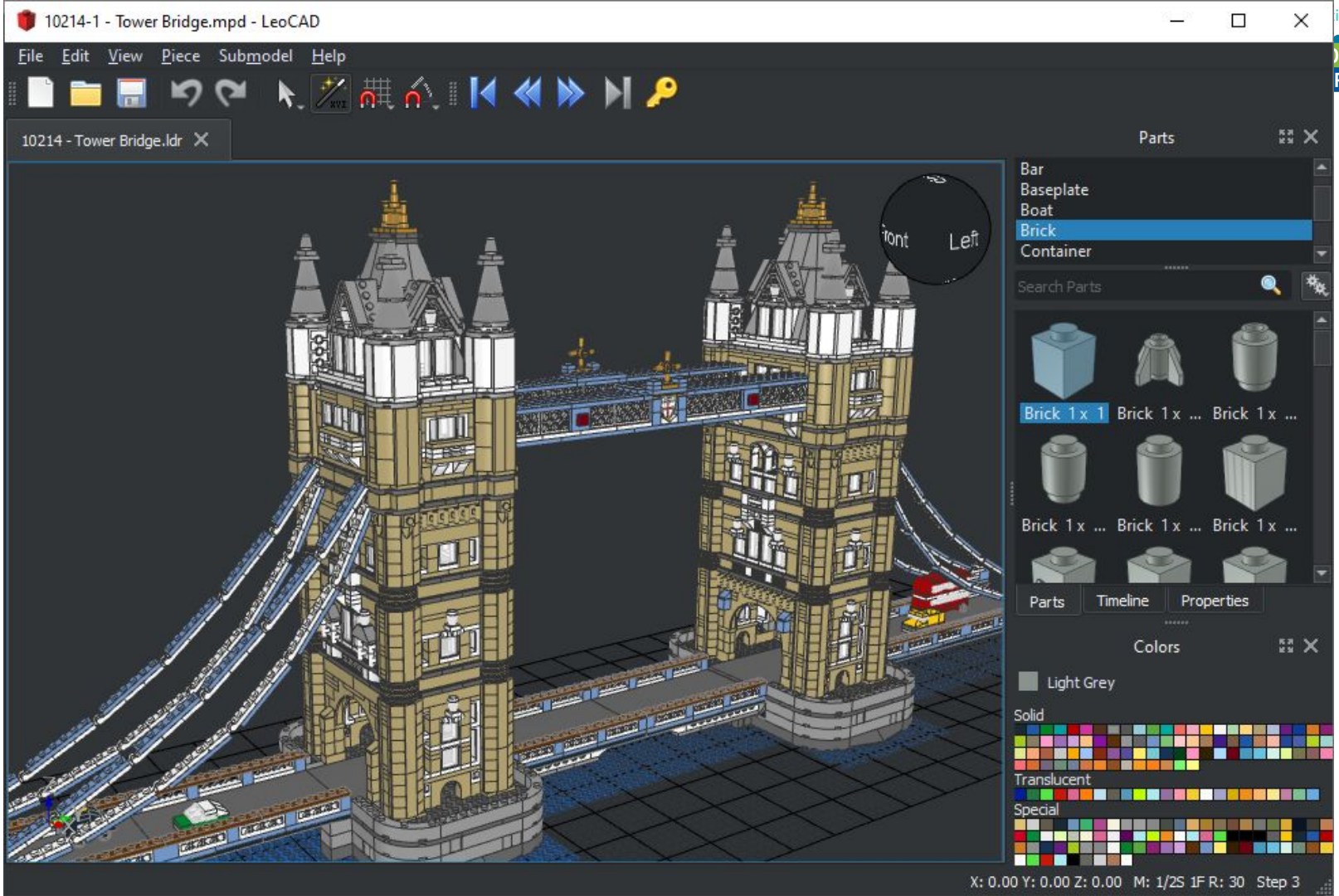
The **overwhelming number of tests** a single organization should develop **makes it difficult to start a project** that will require a high development and maintenance cost

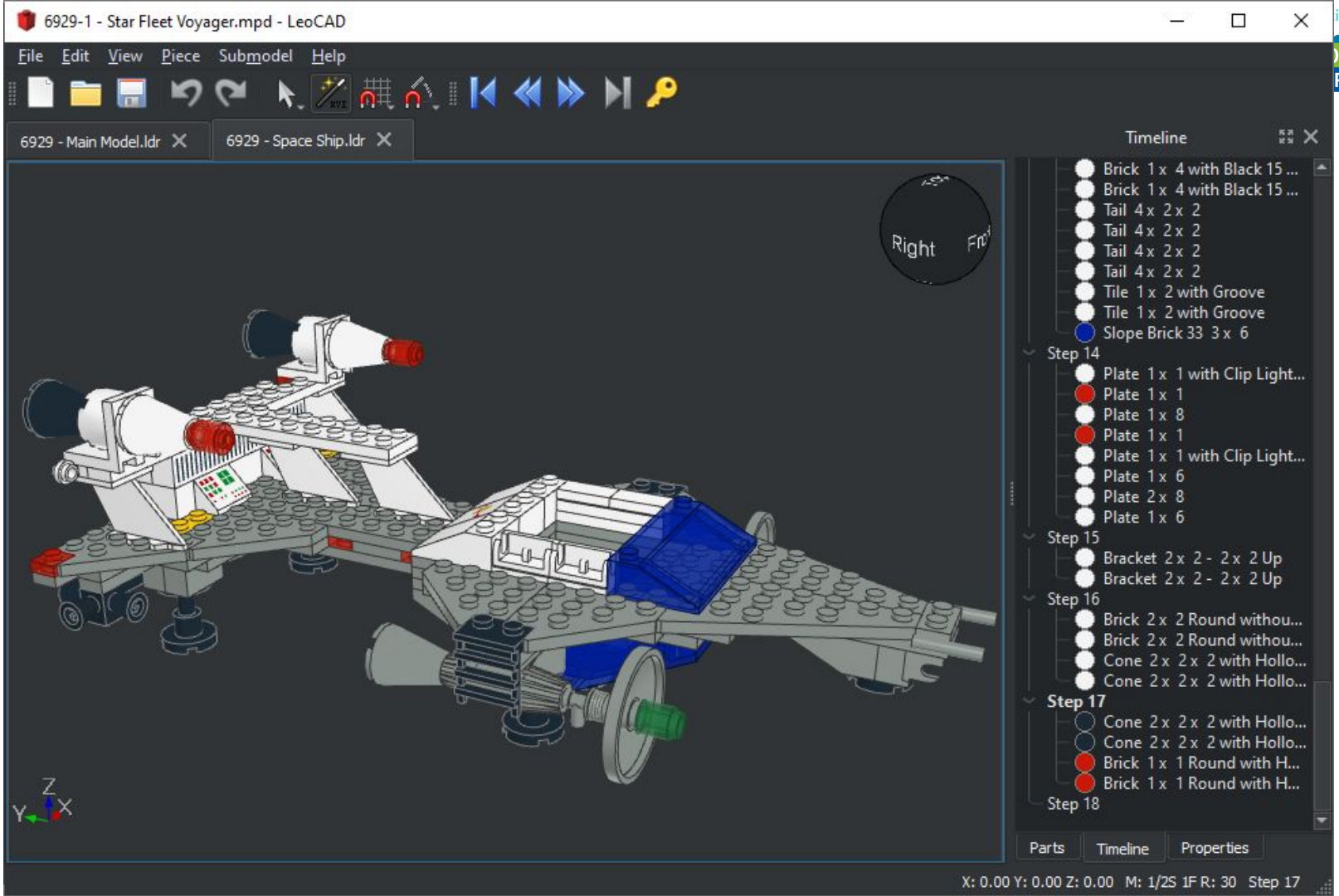
Reuse & Compose

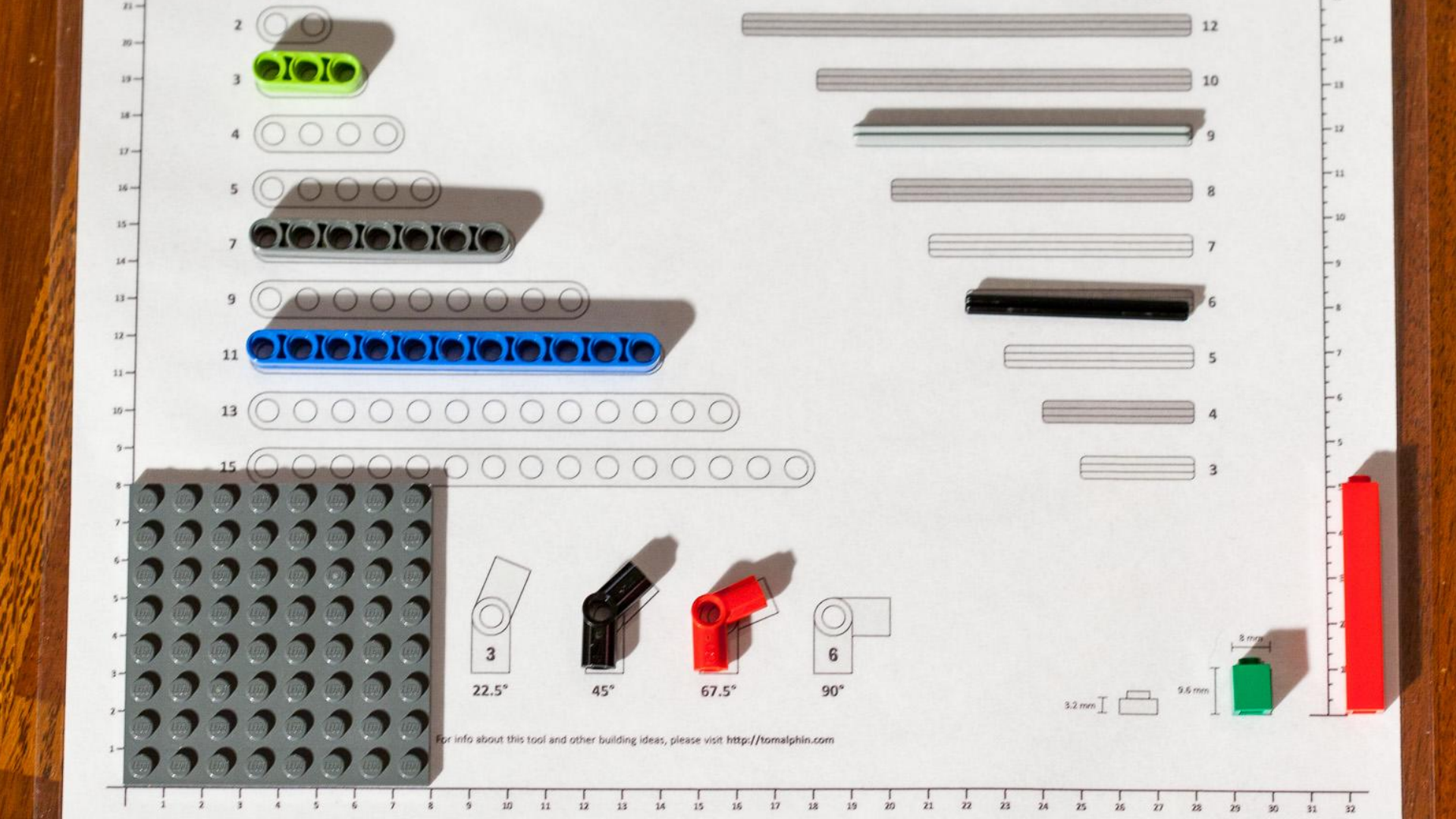
Reuse & Compose

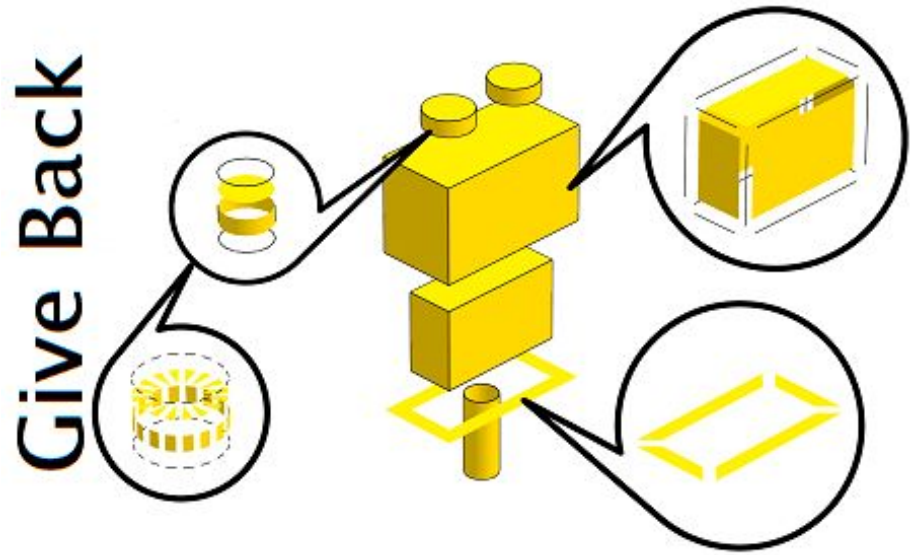





10214-1 - Tower Bridge.mpd - LeoCAD
File Edit View Piece Submodel Help
10214 - Tower Bridge.ldr
Parts
Bar
Baseplate
Boat
Brick
Container
Search Parts
Brick 1 x 1
Brick 1 x ...
Brick 1 x ...
Brick 1 x ...
Brick 1 x ...
Brick 1 x ...
Parts
Timeline
Properties
Colors
Light Grey
Solid
Translucent
Special
Front
Left
X: 0.00 Y: 0.00 Z: 0.00 M: 1/2S 1F R: 30 Step 3


6929-1 - Star Fleet Voyager.mpd - LeoCAD
File Edit View Piece Submodel Help
6929 - Main Model.ldr
6929 - Space Ship.ldr
Timeline
Right
Brick 1 x 4 with Black 15 ...
Brick 1 x 4 with Black 15 ...
Tail 4 x 2 x 2
Tail 4 x 2 x 2
Tail 4 x 2 x 2
Tail 4 x 2 x 2
Tile 1 x 2 with Groove
Tile 1 x 2 with Groove
Slope Brick 33 3 x 6
Step 14
Plate 1 x 1 with Clip Light...
Plate 1 x 1
Plate 1 x 8
Plate 1 x 1
Plate 1 x 1 with Clip Light...
Plate 1 x 6
Plate 2 x 8
Plate 1 x 6
Step 15
Bracket 2 x 2 - 2 x 2 Up
Bracket 2 x 2 - 2 x 2 Up
Step 16
Brick 2 x 2 Round withou...
Brick 2 x 2 Round withou...
Cone 2 x 2 x 2 with Hollo...
Cone 2 x 2 x 2 with Hollo...
Step 17
Cone 2 x 2 x 2 with Hollo...
Cone 2 x 2 x 2 with Hollo...
Brick 1 x 1 Round with H...
Brick 1 x 1 Round with H...
Step 18
Parts
Timeline
Properties
X: 0.00 Y: 0.00 Z: 0.00 M: 1/2S 1F R: 30 Step 17


2
3
4
5
7
9
11
13
15
12
10
9
8
7
6
5
4
3
3
22.5°
45°
67.5°
6
90°
3.2 mm
9.6 mm
8 mm
For info about this tool and other building ideas, please visit http://tomalphin.com



Printable Bricks

3D Print your own Lego compatible bricks

Popular bricks

Brick 1 x 6 x 5

More

Brick 2 x 2

More

Brick 2 x 6

More

Brick 2 x 4

More

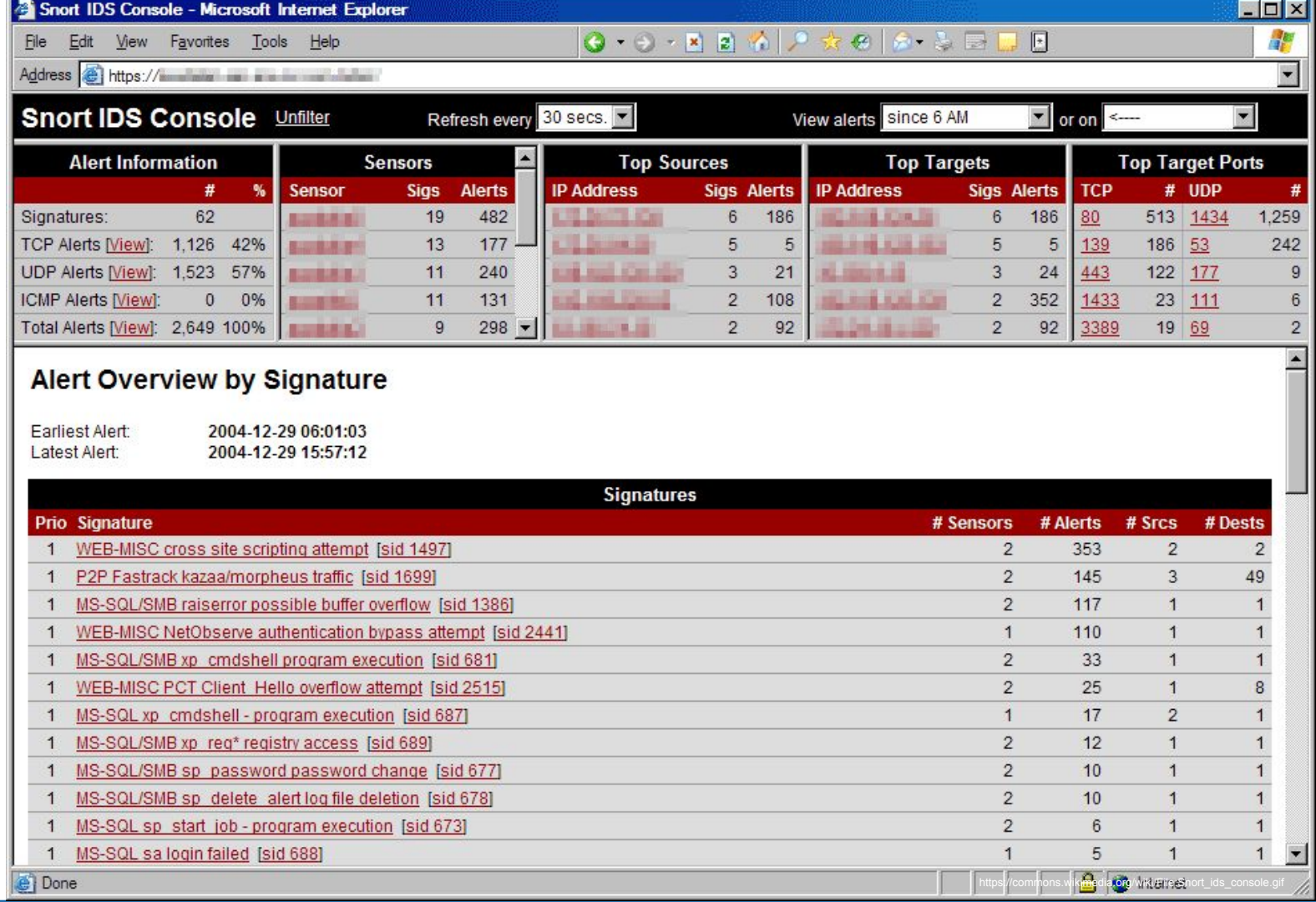
Arch 1 x 3 x 2 Inverted

More

Technic Brick 1 x 4 with Holes

More


COMMUNITY


Snort IDS Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://
Snort IDS Console Unfilter Refresh every 30 secs. View alerts since 6 AM or on <----
Alert Information
%
Signatures: 62
TCP Alerts [View]: 1,126 42%
UDP Alerts [View]: 1,523 57%
ICMP Alerts [View]: 0 0%
Total Alerts [View]: 2,649 100%
Sensors
Sensor Sigs Alerts
19 482
13 177
11 240
11 131
9 298
Top Sources
IP Address Sigs Alerts
6 186
5 5
3 21
2 108
2 92
Top Targets
IP Address Sigs Alerts
6 186
5 5
3 24
2 352
2 92
Top Target Ports
TCP # UDP #
80 513 1434 1,259
139 186 53 242
443 122 177 9
1433 23 111 6
3389 19 69 2
Alert Overview by Signature
Earliest Alert: 2004-12-29 06:01:03
Latest Alert: 2004-12-29 15:57:12
Signatures
Prio Signature # Sensors # Alerts # Srcs # Dests
1 WEB-MISC cross site scripting attempt [sid 1497] 2 353 2 2
1 P2P Fastrack kazaa/morpheus traffic [sid 1699] 2 145 3 49
1 MS-SQL/SMB raiserror possible buffer overflow [sid 1386] 2 117 1 1
1 WEB-MISC NetObserve authentication bypass attempt [sid 2441] 1 110 1 1
1 MS-SQL/SMB xp_cmdshell program execution [sid 681] 2 33 1 1
1 WEB-MISC PCT Client_Hello overflow attempt [sid 2515] 2 25 1 8
1 MS-SQL xp_cmdshell - program execution [sid 687] 1 17 2 1
1 MS-SQL/SMB xp_reg* registry access [sid 689] 2 12 1 1
1 MS-SQL/SMB sp_password password change [sid 677] 2 10 1 1
1 MS-SQL/SMB sp_delete_alert log file deletion [sid 678] 2 10 1 1
1 MS-SQL sp_start_job - program execution [sid 673] 2 6 1 1
1 MS-SQL sa login failed [sid 688] 1 5 1 1
Done
https://commons.wikimedia.org/wiki/File:Snort_ids_console.gif

Awesome YARA

A curated list of awesome YARA rules, tools, and resources. Inspired by awesome-python and awesome-php.

> YARA is an ancronym for: YARA: Another Recursive Ancronym, or Yet Another Ridiculous Acronym. Pick your choice.
>
> -- *Victor M. Alvarez (@plusvic)*

YARA, the "pattern matching swiss knife for malware researchers (and everyone else)" is developed by @plusvic and @VirusTotal. View it on GitHub.

build passing

Sigma

Generic Signature Format for SIEM Systems

What is Sigma

Sigma is a generic and open signature format that allows you to describe relevant log events in a straight forward manner. The rule format is very flexible, easy to write and applicable to any type of log file. The main purpose of this project is to provide a structured form in which researchers or analysts can describe their once developed detection methods and make them shareable with others.

Sigma is for log files what Snort is for network traffic and YARA is for files.

build passing

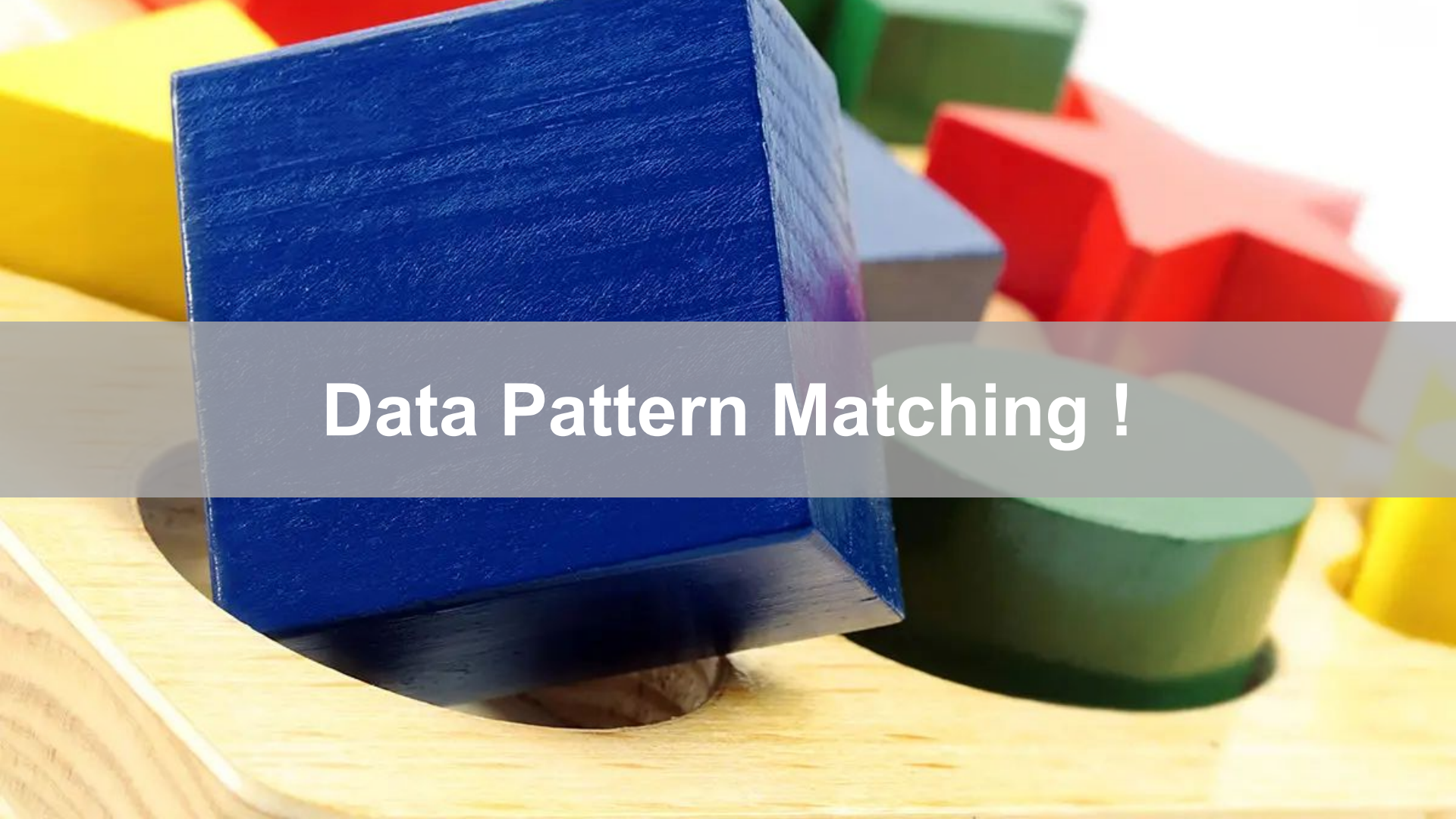
Sigma

Generic Signature Format for SIEM Systems

What is Sigma

Sigma is a generic and open signature format that allows you to describe relevant log events in a straight forward manner. The rule format is very flexible, easy to write and applicable to any type of log file. The main purpose of this project is to provide a structured form in which researchers or analysts can describe their once developed detection methods and make them shareable with others.

Sigma is for log files what Snort is for network traffic and YARA is for files.


Data Pattern Matching !

Open Security Control Testing at Scale

WHAT?

WHY?

WHO?

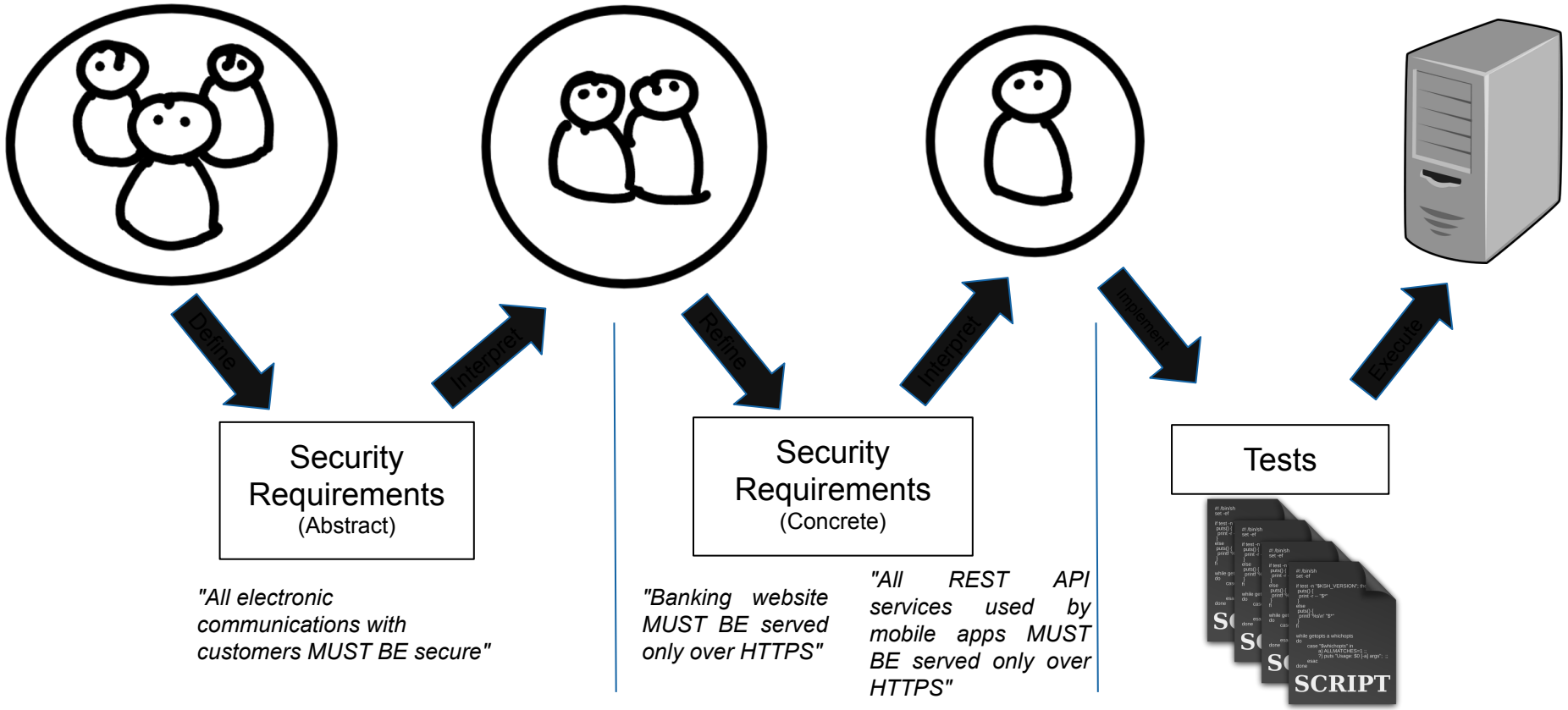
HOW?

BBVA

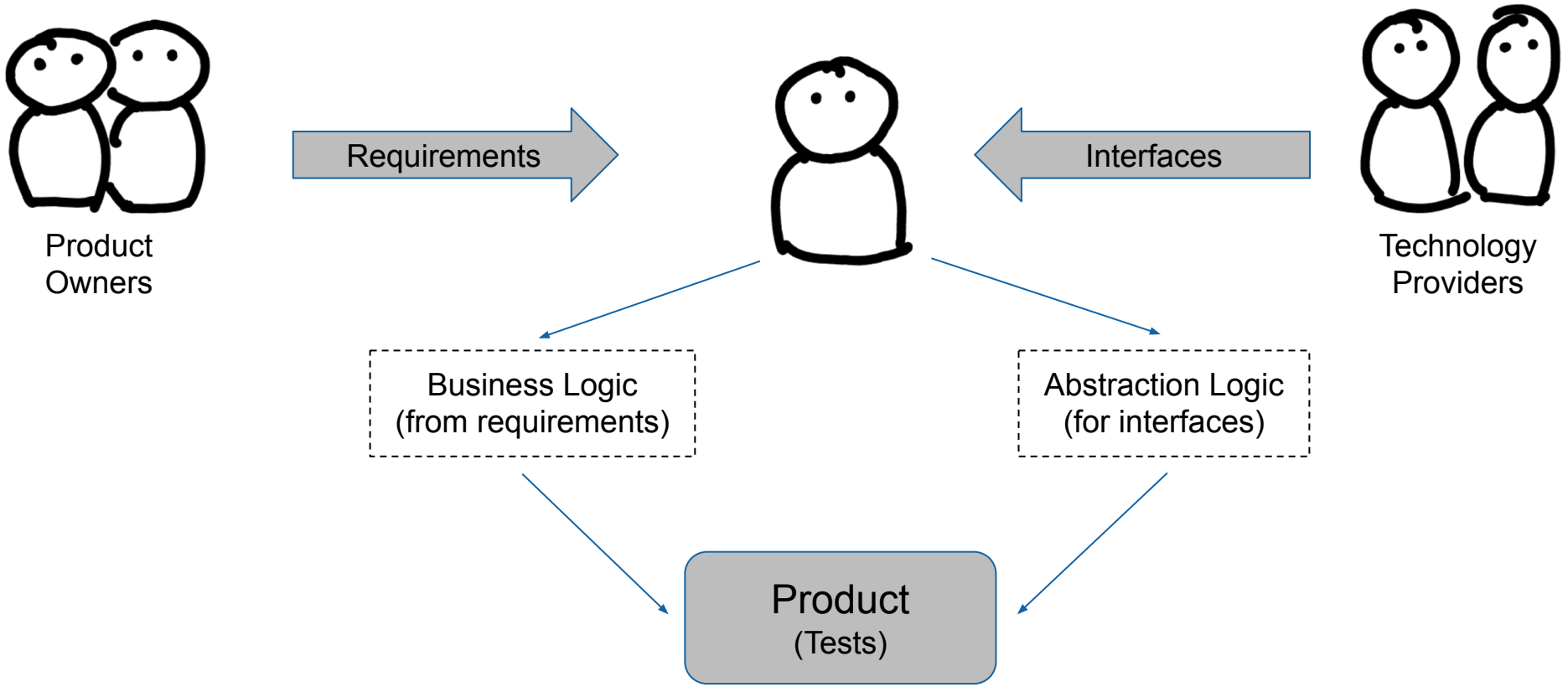
Creating Opportunities

OPEN SECURITY SUMMIT

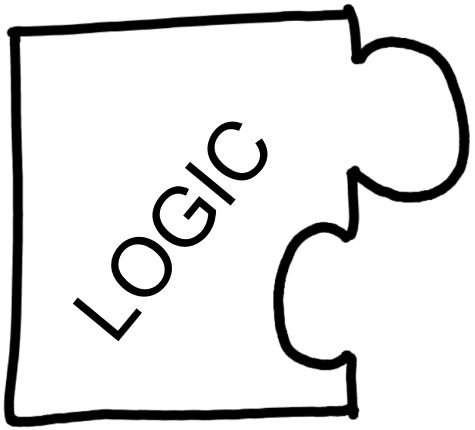
What is the "ideal" status quo?

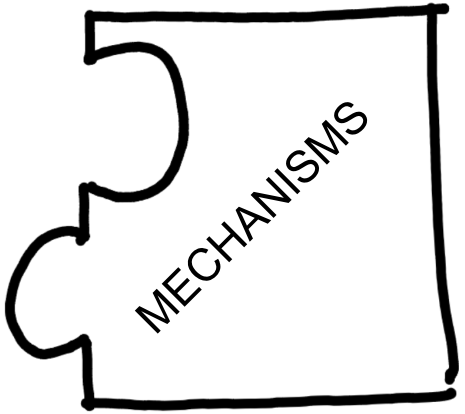


Two pieces of the puzzle



Logic + Mechanisms = Programs





I am the **what for**:

"I want to check that all incoming connections are forbidden"

But ... **how**?

I am the **how**:

"I can check if a given connection is allowed by an AWS security group"

But ... **what for**?

We **lack** a way to
share the logic

A concrete example

"Among all *system users*, only *root* may *modify* the *files* */etc/passwd, /etc/shadow and /etc/groups*"

A concrete example

"Among all *system users*, only *root* may *modify* the *files /etc/passwd, /etc/shadow and /etc/groups*"

"Among all *webapp users*, only *admin users* may *modify* the *Users table*"

A concrete example

"Among all *system users*, only *root* may *modify* the *files /etc/passwd, /etc/shadow and /etc/groups*"

"Among all *webapp users*, only *admin users* may *modify* the *Users table*"

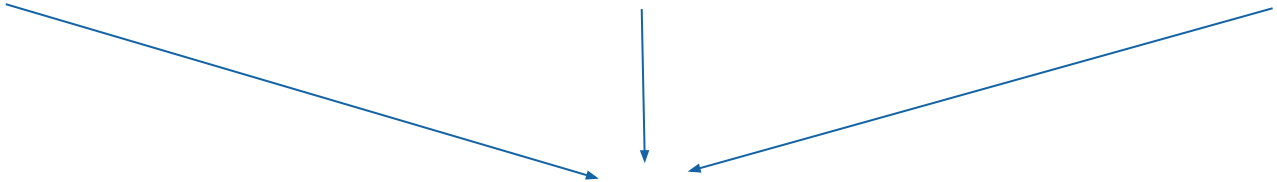
"Among all *IAM users*, only *those with admin role* may *have permission* to *add new users*"

A concrete example

"Among all *system users*, only *root* may *modify* the *files /etc/passwd, /etc/shadow and /etc/groups*"

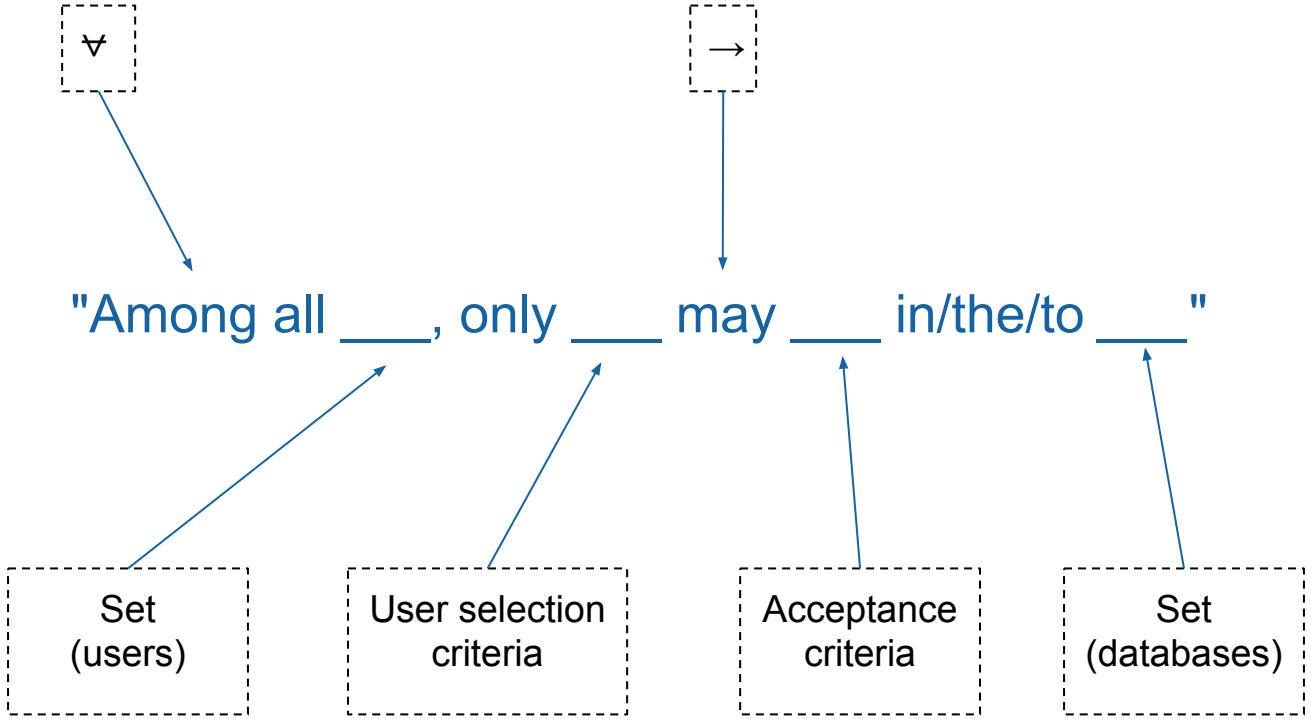
"Among all *webapp users*, only *admin users* may *modify* the *Users table*"

"Among all *IAM users*, only *those with admin role* may *have permission* to *add new users*"



"Among all ___, only ___ may ___ in/the/to ___"

A concrete example II



A concrete example III

"Among all ___, only ___ may ___ in/the/to ___"

$$\forall u \in USERS\ \forall d \in DBS \mid can\_modify(d, u) \rightarrow is\_admin(u)$$

"Among all *system users*, only *root* may *modify* the *files /etc/passwd, /etc/shadow and /etc/groups*"

USERS: *System users*
DBS: */etc/{passwd,shadow,groups}*
is_admin(): *Is user UID 0?*
can_modify(): *Does the user have write permission over the file?*

"Among all *webapp users*, only *admin users* may *modify* the *Users table*"

USERS: *Webapp users*
DBS: *Users table*
is_admin(): *Is the user marked as admin?*
can_modify(): *Has the user permission to INSERT/UPDATE?*

"Among all *IAM users*, only *those with admin role* may *have permission* to *add new users*"

USERS: *IAM Users*
DBS: *IAM*
is_admin(): *Has the user admin role?*
can_modify(): *Has the user permission to add new users?*

Lifecycle

Mat Rule

Ana Lista

Presley Leads

Victor Stu Dior

Lifecycle

Establishes parameter's ownership: **Who** will ***fill the blanks***

Mat Rule

Rule Definition

From Text to Rules

Standards & Best Practices

AC-02(03)	ACCOUNT MANAGEMENT | DISABLE ACCOUNTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-02(03)_ODP[01]	***time period within which to disable accounts is defined;***
	AC-02(03)_ODP[02]	***time period for account inactivity before disabling is defined;***
	AC-02(03)(a)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have expired;
	AC-02(03)(b)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts are no longer associated with a user or individual;
	AC-02(03)(c)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts are in violation of organizational policy;
	AC-02(03)(d)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have been inactive for ***<AC-02(03)_ODP[02] time period>***.

Lifecycle

Establishes parameter's ownership: **Who** will ***fill the blanks***

Mat Rule

AC-02(03)(d)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have been inactive for ***<AC-02(03)_ODP[02] time period>***.

```
=> Abstract
This two time periods are defined in many forms on several systems, in order to
have a more adaptable rule feel free to define the appropriate calculation for
your parameter:

  ch$max_disable_period = ch$max_inactivity_period + ch$max_time_to_disable

The g$account_inactivity_period should be calculated as the current date less
last login date

  g$account_inactivity_period = g$date_now - g$last_login_date

For further params operations, please refer to Overlord Documentation.

=> Rule
All $account must have g$status = $account_status_disabled when
g$account_inactivity_period > ch$max_disable_period

== Rule Id
ecf1cd961944b8af5c6e5ee61250aa710a1a34420460f53737d838aa83112944
```

Rule Definition

From Text to Rules

Standards & Best Practices

Lifecycle

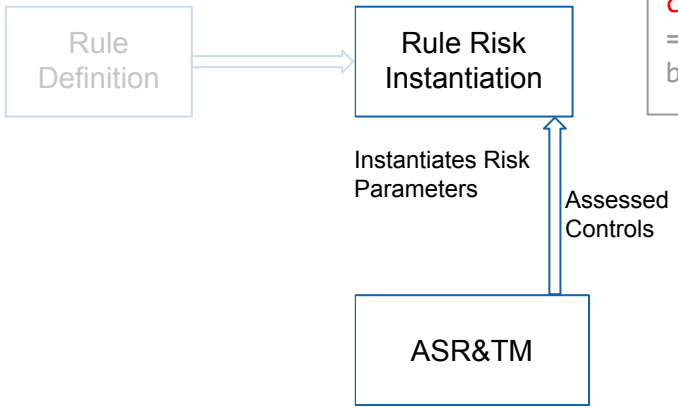
Mat Rule

Ana Lista

```
=> Rule
All $account must have g$status = $account_status_disabled when
g$account_inactivity_period > ch$max_disable_period

== Rule Id
ecf1cd961944b8af5c6e5ee61250aa710a1a34420460f53737d838aa83112944

=> Check Params
ch$max_inactivity_period:TimeDurationDays = 21
ch$max_time_to_disable:TimeDurationDays = 3
ch$max_disable_period = ch$max_inactivity_period+ch$max_time_to_disable
== Check Id
bd23cf7587a7899928ae930c286742601d1fb044624090ab5cee01416e38005e
```



Establish risk threshold parameters (risk appetite): Check Params

AC-02(03)_ODP[01]	*time period within which to disable accounts is defined;*
AC-02(03)_ODP[02]	*time period for account inactivity before disabling is defined;*

Lifecycle

AC-02(03)(d)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have been inactive for ***<AC-02(03)_ODP[02] time period>***.

Mat Rule

Ana Lista

Presley Leads

Instantiates Project Specific Parameters

Rule Definition

Rule Risk Instantiation

Rule Technical Instantiation

Gather Code Catalog
AWS*

```
=> Rule
All $account must have g$status = $account_status_disabled when
g$account_inactivity_period > ch$max_disable_period

== Rule Id
ecf1cd961944b8af5c6e5ee61250aa710a1a34420460f53737d838aa83112944

=> Check Params
ch$max_inactivity_period:TimeDurationDays = 21
ch$max_time_to_disable:TimeDurationDays = 3
ch$max_disable_period = ch$max_inactivity_period+ch$max_time_to_disable
== Check Id
bd23cf7587a7899928ae930c286742601d1fb044624090ab5cee01416e38005e

=> Params
$account_status_is_disabled = True
g$account_inactivity_period:TimeDurationDays =
    g$date_now:Date - g$last_login_date:Date
$account:AWSUser
g$status:AWSUserStatus
%aws_key:AWSKey
%aws_secret:AWSSecret
```

Lifecycle

AC-02(03)(d)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have been inactive for ***<AC-02(03)_ODP[02] time period>***.

Mat Rule

Ana Lista

Presley Leads

Instantiates Project Specific Parameters

Rule Definition

Rule Risk Instantiation

Rule Technical Instantiation

Gather Code Catalog
AWS*

```
=> Rule
All $account must have g$status = $account_status_disabled when
g$account_inactivity_period > ch$max_disable_period

By the usage of:
AWSUserStatus = Bool
Cannot derive a function (AWSUserStatus -> Bool)
=> Check Params
ch$max_inactivity_period:TimeDurationDays = 21
ch$max_time_to_disable:TimeDurationDays = 3
ch$max_disable_period = ch$max_inactivity_period+ch$max_time_to_disable
== Check Id
bd23cf7587a7899928e930c286742601d1b044624090ab5cee01416e38005e
=> Params
$account_status_is_disabled = True
g$account_inactivity_period:TimeDurationDays =
    g$date_now:Date - g$last_login_date:Date
$account:AWSUser
g$status:AWSUserStatus
%aws_key:AWSKey
%aws_secret:AWSSecret
```

Lifecycle

AC-02(03)(d)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have been inactive for ***<AC-02(03)_ODP[02] time period>***.

Mat Rule

Ana Lista

Presley Leads

Instantiates Project Specific Parameters

Rule Definition

Rule Risk Instantiation

Rule Technical Instantiation

Gather Code Catalog
AWS*

```
=> Rule
All $account must have g$status = $account_status_disabled when
g$account_inactivity_period > ch$max_disable_period

By the usage of:
AWSUserStatus = Bool
Cannot derive a function (AWSUserStatus -> Bool)
=> Check Params
ch$max_inactivity_period:TimeDurationDays = 21
ch$max_time_to_disable:TimeDurationDays = 3
ch$max_disable_period = ch$max_inactivity_period+ch$max_time_to_disable
== Check Id
bd23cf7587a7899928e930c286742601d1b044624090ab5cee01416e38005e
=> Params
$account_status_is_disabled = True
g$account_inactivity_period:TimeDurationDays =
    g$date_now:Date - g$last_login_date:Date
$account:AWSUser
g$status:AWSUserStatus
%aws_key:AWSKey
%aws_secret:AWSSecret
```

Lifecycle

AC-02(03)(d)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have been inactive for ***<AC-02(03)_ODP[02] time period>***.

Mat Rule

Ana Lista

Presley Leads

Rule Definition

Rule Risk Instantiation

Instantiates Project Specific Parameters

Rule Technical Instantiation

Gather Code Catalog
AWS*

```
=> Rule
All $account must have g$status = $account_status_disabled when
g$account_inactivity_period > ch$max_disable_period
```

By the usage of:
AWSUserStatus = Bool
Cannot derive a function (AWSUserStatus -> Bool)

```
def isAWSUserDisabled(user:AWSUserStatus) -> Bool:
    return not user.is_account_active
```

```
ctivity_period:TimeDurationDays = 21
e_to_disable:TimeDurationDays = 3
able_period = ch$max_inactivity_period+ch$max_time_to_disable
=> Params
$account_st
g$account_i
    g$date_now.Date - g$last_login_date.Date
$account:AWSUser
g$status:AWSUserStatus
%aws_key:AWSKey
%aws_secret:AWSSecret
```

Lifecycle

AC-02(03)(d)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have been inactive for ***<AC-02(03)_ODP[02] time period>***.

Mat Rule

Ana Lista

Presley Leads

```
=> Params
$account_status_is_disabled = True
g$account_inactivity_period:TimeDurationDays =
    g$date_now:Date - g$last_login_date:Date
```

AC-02(03)(a)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have expired;
AC-02(03)(b)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts are no longer associated with a user or individual;
AC-02(03)(c)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts are in violation of organizational policy;
AC-02(03)(d)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have been inactive for ***<AC-02(03)_ODP[02] time period>***.

Rule Definition

Rule Risk Instantiation

Rule Technical Instantiation

Gather Code Catalog
AWS*

```
def isAWSUserDisabled (user)
```

Lifecycle

AC-02(03)(d)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have been inactive for ***<AC-02(03)_ODP[02] time period>***.

Mat Rule

Ana Lista

Prometheus Leads

Instantiates Project Specific Parameters

Rule Definition

Rule Risk Instantiation

Rule Technical Instantiation

Gather Code Catalog
AWS*
AD*

```
=> Rule
All $account must have g$status = $account_status_disabled when
g$account_inactivity_period > ch$max_disable_period

== Rule Id
ecf1cd961944b8af5c6e5ee61250aa710a1a34420460f53737d838aa83112944

=> Check Params
ch$max_inactivity_period:TimeDurationDays = 21
ch$max_time_to_disable:TimeDurationDays = 3
ch$max_disable_period = ch$max_inactivity_period+ch$max_time_to_disable

== Check Id
bd23cf7587a7899928ae930c286742601d1fb044624090ab5cee01416e38005e
=> Params
$account_status_is_disabled = True
g$account_inactivity_period:TimeDurationDays =
    g$date_now:Date - g$last_login_date:Date
$account:ADUser
g$status:ADUserStatus
%AD_key:ADCredentials
```

Active Directory Accounts

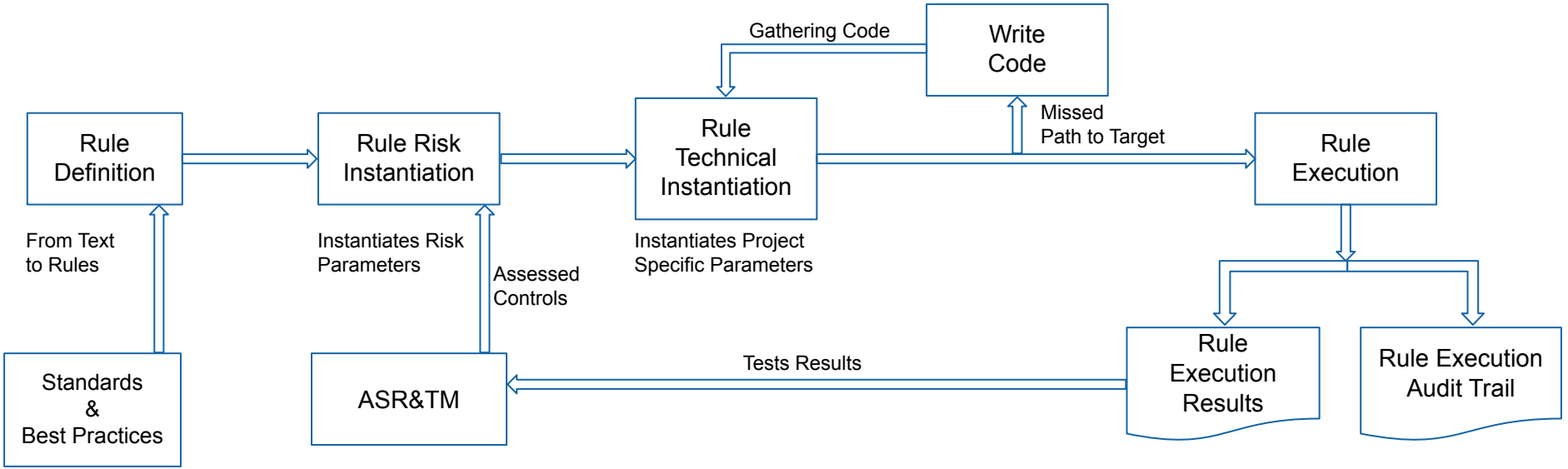
Lifecycle

Mat Rule

Ana Lista

Presley Leads

Victor Stu Dior



Lifecycle - Runtime

AC-02(03)(d)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have been inactive for ***<AC-02(03)_ODP[02] time period>***.

Mat Rule

Ana Lista

Presley Leads

Rule Definition → Rule Risk Instantiation → Rule Technical Instantiation


```
=> Rule
All $account must have g$status = $account_status_disabled when g$account_inactivity_period >
ch$max_disable_period
== Rule Id
ecf1cd961944b8af5c6e5ee61250aa710a1a34420460f53737d838aa83112944
=> Check Params
ch$max_inactivity_period:TimeDurationDays = 21
ch$max_time_to_disable:TimeDurationDays = 3
ch$max_disable_period = ch$max_inactivity_period+ch$max_time_to_disable
== Check Id
bd23cf7587a7899928ae930c286742601d1fb044624090ab5cee01416e38005e
=> Params
$account_status_is_disabled = True
g$account_inactivity_period:TimeDurationDays =
    g$date_now:Date - g$last_login_date:Date
$account:AWSUser
g$status:AWSUserStatus
%aws_key:AWSKey
%aws_secret:AWSSecret
== Params Id
5ea795a47dff8f2297846f40250c15d7ab6724e291eb4f962f9912640d3417f2
== Test Id
77bacb51b404efdd85e388412623c6627fc461d03d7d6c3aca00846c9aaeb091
```

Lifecycle - Runtime

AC-02(03)(d)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have been inactive for ***<AC-02(03)_ODP[02] time period>***.

Mat Rule

Ana Lista

Presley Leads

Rule Definition

Rule Risk Instantiation

Rule Technical Instantiation


```
=> Rule
All $account must have g$status = $account_status_disabled when g$account_inactivity_period >
ch$max_disable_period
== Rule Id
ecf1cd961944b8af5c6e5ee61250aa710a1a34420460f53737d838aa83112944
=> Check Params
ch$max_inactivity_period:TimeDurationDays = 21
ch$max_time_to_disable:TimeDurationDays = 3
ch$max_disable_period = ch$max_inactivity_period+ch$max_time_to_disable
== Check Id
bd23cf7587a7899928ae930c286742601d1fb044624090ab5cee01416e38005e
=> Params
$account_status_is_disabled = True
g$account_inactivity_period:TimeDurationDays =
    g$date_now:Date - g$last_login_date:Date
$account:AWSUser
g$status:AWSUserStatus
%aws_key:AWSKey
%aws_secret:AWSSecret
== Params Id
5ea795a47dff8f2297846f40250c15d7ab6724e291eb4f962f9912640d3417f2
== Test Id
77bacb51b404efdd85e388412623c6627fc461d03d7d6c3aca00846c9aaeb091
```

```
== Rule Id
ecf1cd961944b8af5c6e5ee61250aa710a1a34420460f53737d838aa83112944
```

Lifecycle - Runtime

AC-02(03)(d)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have been inactive for ***<AC-02(03)_ODP[02] time period>***.

Mat Rule

Ana Lista

Presley Leads

Rule Definition

Rule Risk Instantiation

Rule Technical Instantiation


```
=> Rule
All $account must have g$status = $account_status_disabled when g$account_inactivity_period >
ch$max_disable_period
== Rule Id
ecf1cd961944b8af5c6e5ee61250aa710a1a34420460f53737d838aa83112944
=> Check Params
ch$max_inactivity_period:TimeDurationDays = 21
ch$max_time_to_disable:TimeDurationDays = 3
ch$max_disable_period = ch$max_inactivity_period+ch$max_time_to_disable
== Check Id
bd23cf7587a7899928ae930c286742601d1fb044624090ab5cee01416e38005e
=> Params
$account_status_is_disabled = True
g$account_inactivity_period:TimeDurationDays =
    g$date_now:Date - g$last_login_date:Date
$account:AWSUser
g$status:AWSUserStatus
%aws_key:AWSKey
%aws_secret:AWSSecret
== Params Id
5ea795a47dff8f2297846f40250c15d7ab6724e291eb4f962f9912640d3417f2
== Test Id
77bacb51b404efdd85e388412623c6627fc461d03d7d6c3aca00846c9aaeb091
```

```
== Rule Id
ecf1cd961944b8af5c6e5ee61250aa710a1a34420460f53737d838aa83112944
== Check Id
bd23cf7587a7899928ae930c286742601d1fb044624090ab5cee01416e38005e
```

Lifecycle - Runtime

AC-02(03)(d)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have been inactive for ***<AC-02(03)_ODP[02] time period>***.

Mat Rule

Ana Lista

Presley Leads

Rule Definition → Rule Risk Instantiation → Rule Technical Instantiation


```
=> Rule
All $account must have g$status = $account_status_disabled when g$account_inactivity_period >
ch$max_disable_period
== Rule Id
ecf1cd961944b8af5c6e5ee61250aa710a1a34420460f53737d838aa83112944
=> Check Params
ch$max_inactivity_period:TimeDurationDays = 21
ch$max_time_to_disable:TimeDurationDays = 3
ch$max_disable_period = ch$max_inactivity_period+ch$max_time_to_disable
== Check Id
bd23cf7587a7899928ae930c286742601d1fb044624090ab5cee01416e38005e
=> Params
$account_status_is_disabled = True
g$account_inactivity_period:TimeDurationDays =
    g$date_now:Date - g$last_login_date:Date
$account:AWSUser
g$status:AWSUserStatus
%aws_key:AWSKey
%aws_secret:AWSSecret
== Params Id
5ea795a47dff8f2297846f40250c15d7ab6724e291eb4f962f9912640d3417f2
== Test Id
77bacb51b404efdd85e388412623c6627fc461d03d7d6c3aca00846c9aaeb091
```

```
== Rule Id
ecf1cd961944b8af5c6e5ee61250aa710a1a34420460f53737d838aa83112944
== Check Id
bd23cf7587a7899928ae930c286742601d1fb044624090ab5cee01416e38005e
== Params Id
5ea795a47dff8f2297846f40250c15d7ab6724e291eb4f962f9912640d3417f2
```

Lifecycle - Runtime

AC-02(03)(d)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have been inactive for ***<AC-02(03)_ODP[02] time period>***.

Mat Rule

Ana Lista

Presley Leads

Rule Definition → Rule Risk Instantiation → Rule Technical Instantiation


```
=> Rule
All $account must have g$status = $account_status_disabled when g$account_inactivity_period >
ch$max_disable_period
== Rule Id
ecf1cd961944b8af5c6e5ee61250aa710a1a34420460f53737d838aa83112944
=> Check Params
ch$max_inactivity_period:TimeDurationDays = 21
ch$max_time_to_disable:TimeDurationDays = 3
ch$max_disable_period = ch$max_inactivity_period+ch$max_time_to_disable
== Check Id
bd23cf7587a7899928ae930c286742601d1fb044624090ab5cee01416e38005e
=> Params
$account_status_is_disabled = True
g$account_inactivity_period:TimeDurationDays =
    g$date_now:Date - g$last_login_date:Date
$account:AWSUser
g$status:AWSUserStatus
%aws_key:AWSKey
%aws_secret:AWSSecret
== Params Id
5ea795a47dff8f2297846f40250c15d7ab6724e291eb4f962f9912640d3417f2
== Test Id
77bacb51b404efdd85e388412623c6627fc461d03d7d6c3aca00846c9aaeb091
```

```
== Rule Id
ecf1cd961944b8af5c6e5ee61250aa710a1a34420460f53737d838aa83112944
== Check Id
bd23cf7587a7899928ae930c286742601d1fb044624090ab5cee01416e38005e
== Params Id
5ea795a47dff8f2297846f40250c15d7ab6724e291eb4f962f9912640d3417f2
== Test Id
77bacb51b404efdd85e388412623c6627fc461d03d7d6c3aca00846c9aaeb091
```

Lifecycle - Runtime

AC-02(03)(d)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have been inactive for ***<AC-02(03)_ODP[02] time period>***.

Mat Rule

Ana Lista

Presley Leads

Rule Definition → Rule Risk Instantiation → Rule Technical Instantiation


```
=> Rule
All $account must have g$status = $account_status_disabled when g$account_inactivity_period >
ch$max_disable_period
== Rule Id
ecf1cd961944b8af5c6e5ee61250aa710a1a34420460f53737d838aa83112944
=> Check Params
ch$max_inactivity_period:TimeDurationDays = 21
ch$max_time_to_disable:TimeDurationDays = 3
ch$max_disable_period = ch$max_inactivity_period+ch$max_time_to_disable
== Check Id
bd23cf7587a7899928ae930c286742601d1fb044624090ab5cee01416e38005e
=> Params
$account_status_is_disabled = True
g$account_inactivity_period:TimeDurationDays =
    g$date_now:Date - g$last_login_date:Date
$account:AWSUser
g$status:AWSUserStatus
%aws_key:AWSKey
%aws_secret:AWSSecret
== Params Id
5ea795a47dff8f2297846f40250c15d7ab6724e291eb4f962f9912640d3417f2
== Test Id
77bacb51b404efdd85e388412623c6627fc461d03d7d6c3aca00846c9aaeb091
```

```
== Rule Id
ecf1cd961944b8af5c6e5ee61250aa710a1a34420460f53737d838aa83112944
== Check Id
bd23cf7587a7899928ae930c286742601d1fb044624090ab5cee01416e38005e
== Params Id
5ea795a47dff8f2297846f40250c15d7ab6724e291eb4f962f9912640d3417f2
== Test Id
77bacb51b404efdd85e388412623c6627fc461d03d7d6c3aca00846c9aaeb091
== Result
(True, 6e7d50e84f4731ef74187cf8cfa2672184eed8866b0b0074a772f4a64e0f4ba2)
```

Lifecycle - Community

Decentralized

Mat Rule

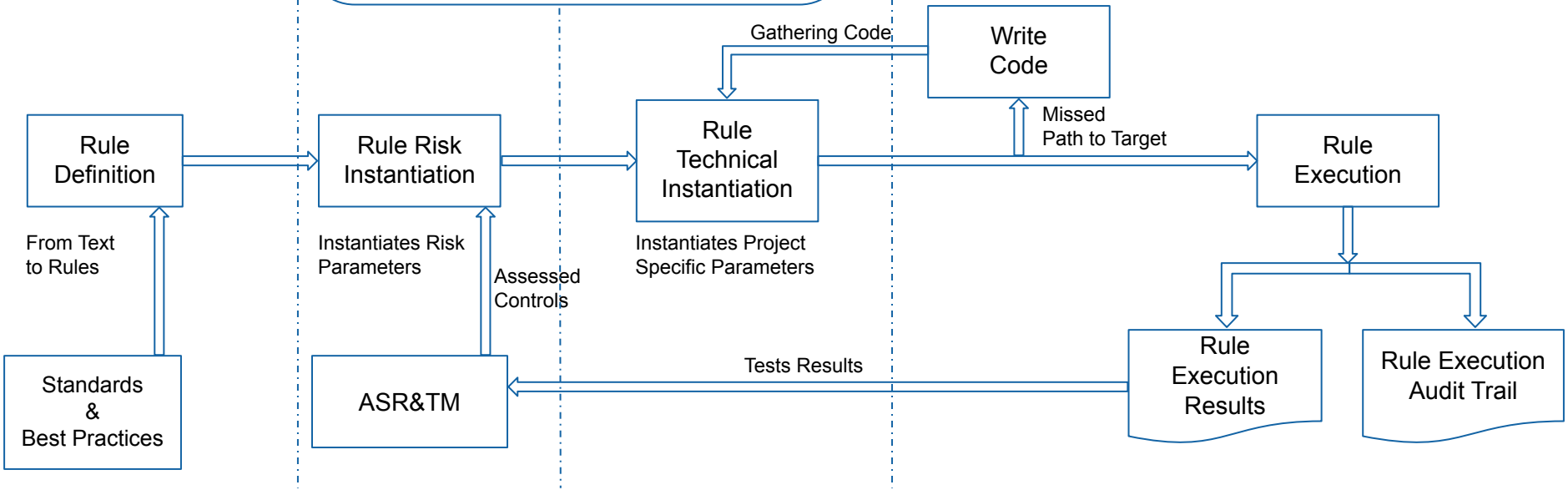
Org. X

Ana Lista

Presley Leads

Decentralized

Victor Stu Dior



Lifecycle - Community

Decentralized

Mat Rule

! Criteria

Ana Lista

Org. X

Presley Leads

Decentralized

Victor Stu Dior

Gathering Code

Write Code

Rule Definition

Rule Risk Instantiation

Rule Technical Instantiation

Missed Path to Target

Rule Execution

From Text to Rules

Instantiates Risk Parameters

Assessed Controls

Instantiates Project Specific Parameters

Standards & Best Practices

ASR&TM

Tests Results

Rule Execution Results

Rule Execution Audit Trail

Lifecycle - Community

Decentralized

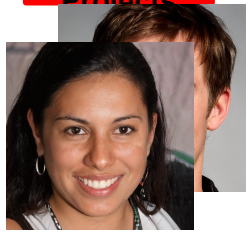
Mat Rule

! Criteria

Ana Lista

Org. X

∀ Projects



Presley Leads

Decentralized

Victor Stu Dior

Gathering Code

Write Code

Rule Definition

Rule Risk Instantiation

Rule Technical Instantiation

Missed Path to Target

Rule Execution

From Text to Rules

Instantiates Risk Parameters

Assessed Controls

Instantiates Project Specific Parameters

Standards & Best Practices

ASR&TM

Tests Results

Rule Execution Results

Rule Execution Audit Trail

Lifecycle - Community

Decentralized

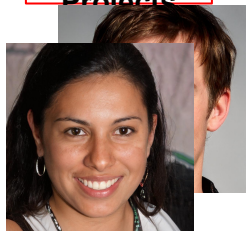
Mat Rule

! Criteria

Ana Lista

Org. X

∀ Projects



Presley Leads

Decentralized

Victor Stu Dior

Gathering Code

Write Code

Rule Definition

Rule Risk Instantiation

Rule Technical Instantiation

Missed Path to Target

Rule Execution

From Text to Rules

Instantiates Risk Parameters

Assessed Controls

Instantiates Project Specific Parameters

Standards & Best Practices

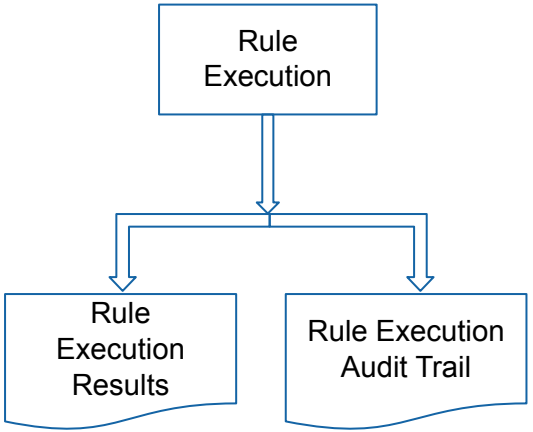
ASR&TM

Tests Results

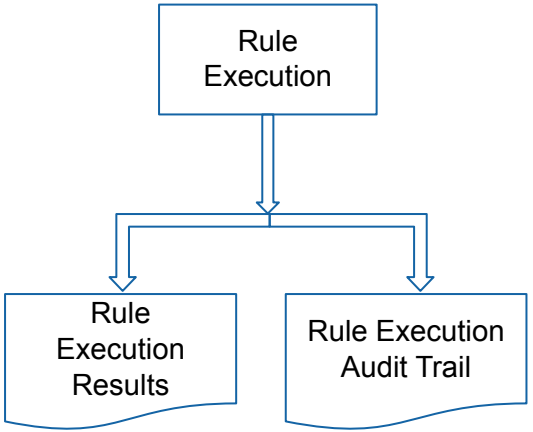
Rule Execution Results

Rule Execution Audit Trail

Lifecycle - Results

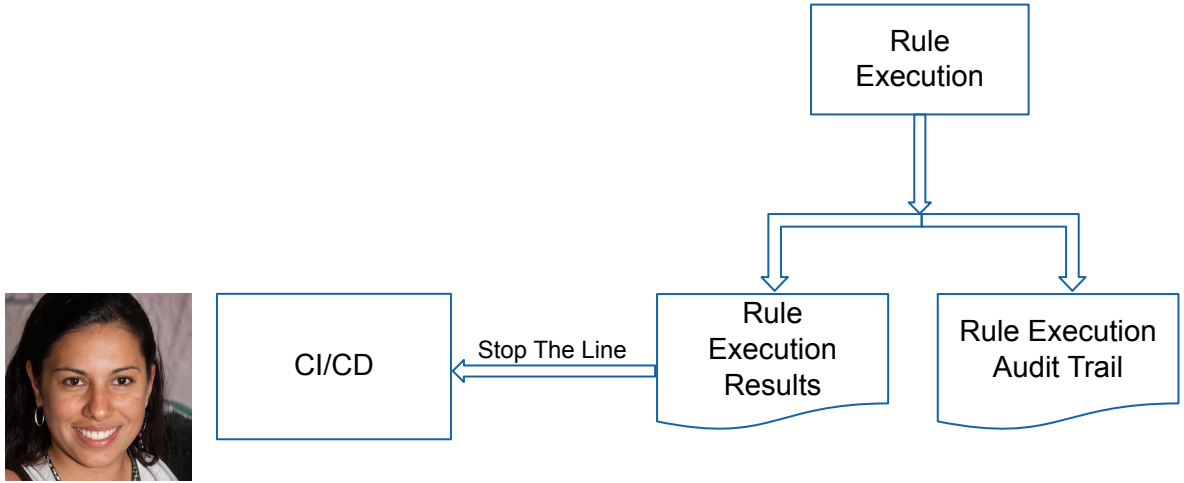


Lifecycle - Results



Norman Auditore

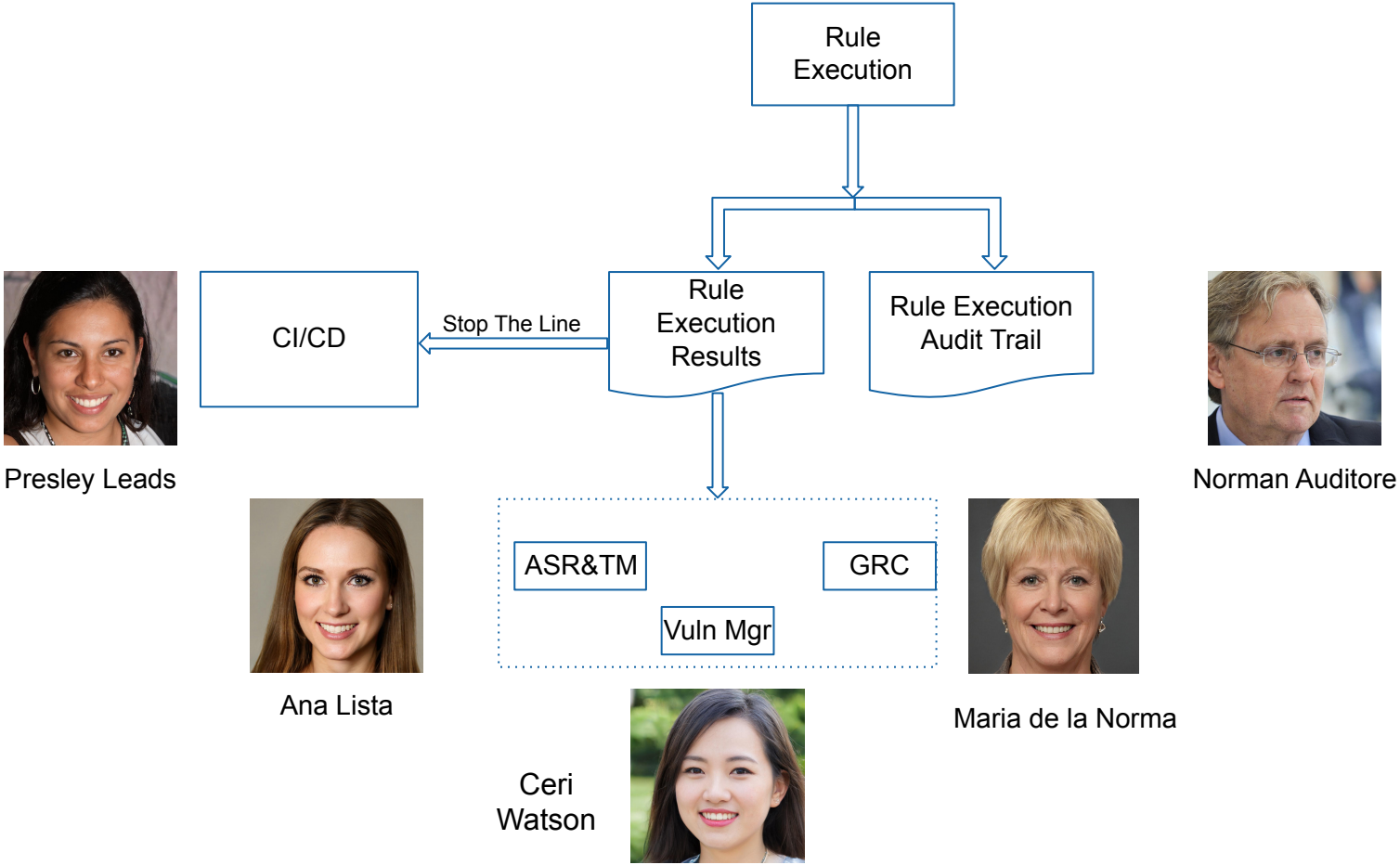
Lifecycle - Results



Presley Leads

Norman Auditore

Lifecycle - Results



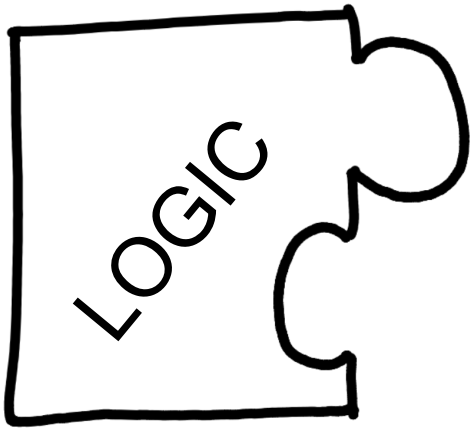
have

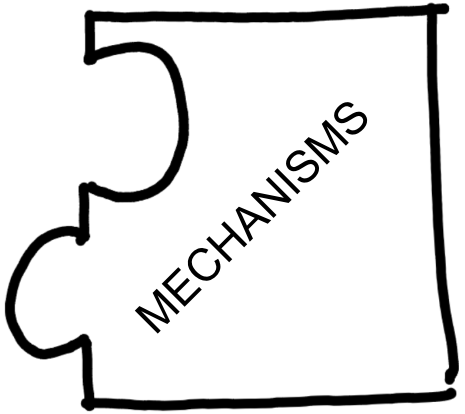
We ~~**lack**~~ a way to

share the logic

Sorcery?

Logic + Mechanisms = Programs





I am the **what for**:

"I want to check that all incoming connections are forbidden"

But ... **how**?

I am the **how**:

"I can check if a given connection is allowed by an AWS security group"

But ... **what for**?

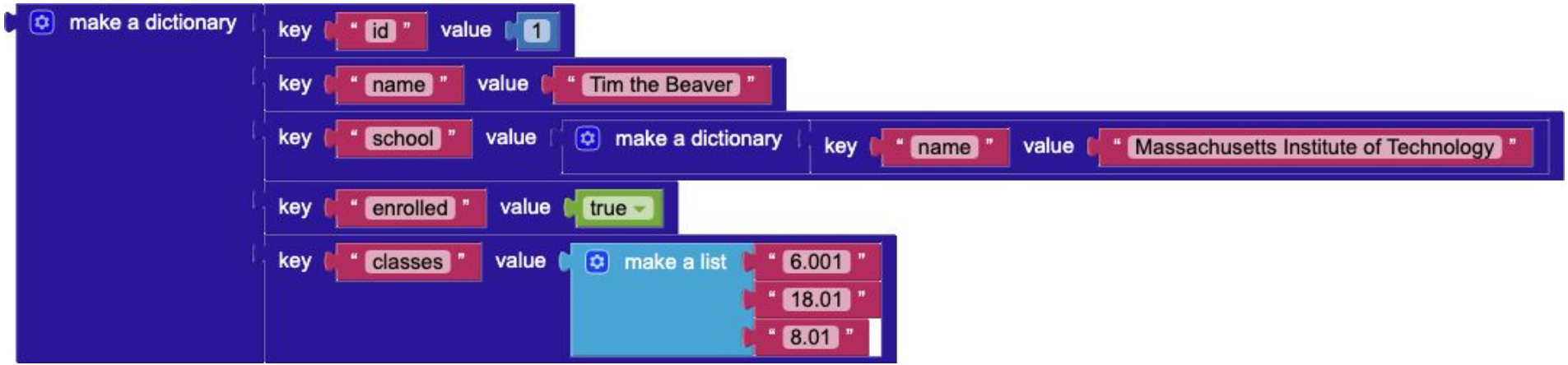
Parameters


initialize global name to
initialize local name to
in
get
initialize local name to
in
set to

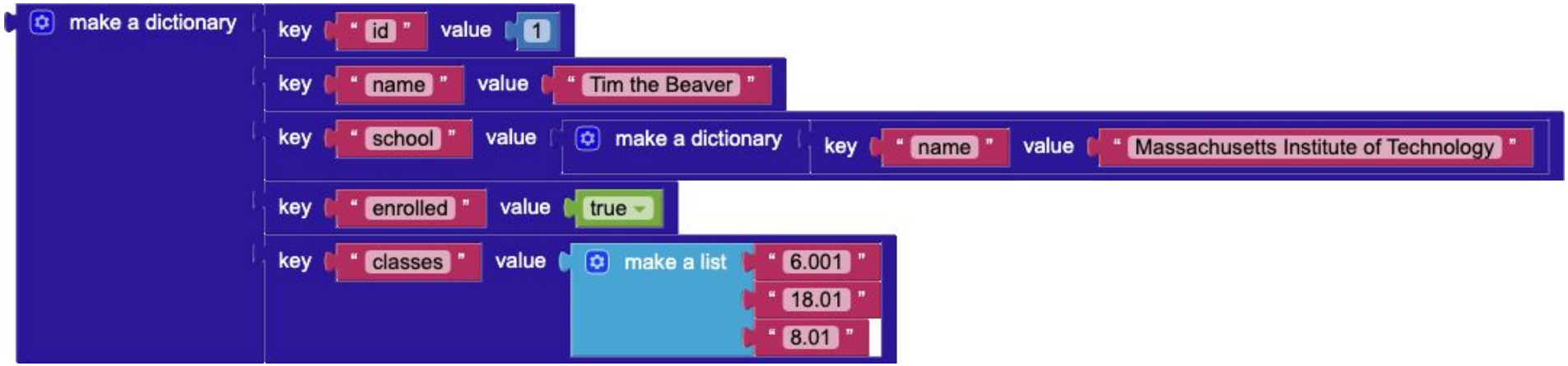
Parameters

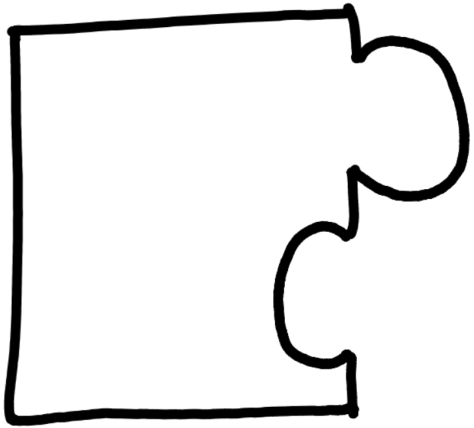
Parameters	Syntax	Usage
Definition	`($param)`	Generic unrestricted parameter established at rule definition time, resolved at compile time. Ex. Technical specification/environment, option selection, exception list,...
Check	`(ch$param)`	Risk established desired values/thresholds Immutable across rule expansion Ex. Minimum version, maximum CVSS, expired time, …
Gather	`(g$param)`	Cannot be setted manually. Gathered at run-time Ex. IPs in a VPC, files in a directory/bucket, registry value
Execution	`(%param)`	Execution instance argument needed to run the test. Ex. AuthZ data, Bastion IP address, …

Automatic Type Matching

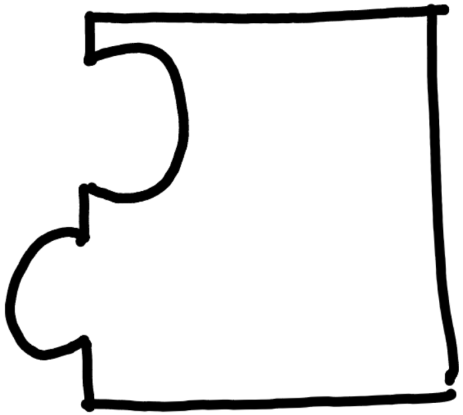


Automatic Type Matching



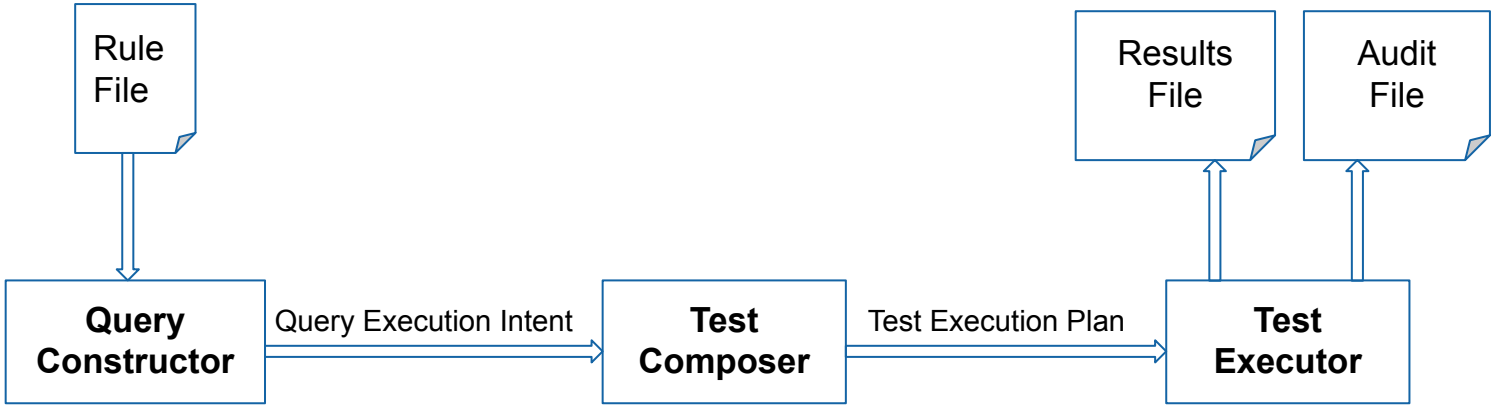


Bring Your Own Types




Types and Functions Pattern Matching !

Sorcery revealed



- Rule validation
- Check param constraints
- Keep track with IDs

- **Build execution path searching for expected types in a graph**
- Generates valid program

- Deal w/ real world execution
- Audit every step
- Distributed execution

Sorcery?

github.com/BBVA/susto

SUSTO

Systematic
Universal
Security
Testing
Orchestration

BBVA

Creando Oportunidades

Thanks

Questions?

BBVA

Creating Opportunities

Open Security Control Testing at Scale

BBVA Innovation Labs

March, 2022

OPEN SECURITY SUMMIT