

# Rumps Session: RUDDER

Continuous configuration compliance

Alexandre BRIANCEAU

✉ alexandre@rudder.io

🐦 @abriancaeu



Pass the SALT 2019



**RUDDER**

# What do we know about our security compliance?



Multiple teams, diluted expertise, harder reporting



MGMT



DEV



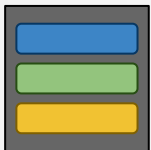
SEC



OPS



EXTERN



DEV



QA



PRODUCTION



RECOVERY

Heterogeneous systems, reduced visibility, ease of use and understanding

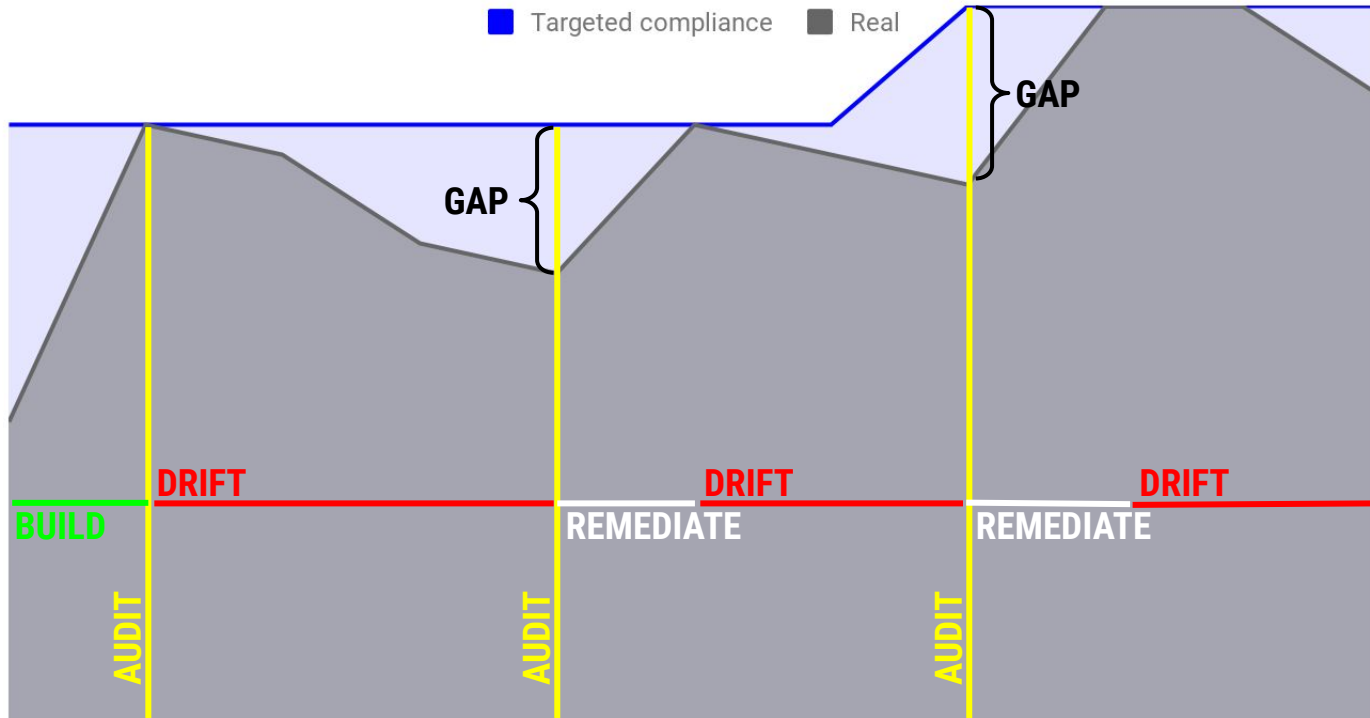
# How DevSecOps can help us?



RUDDER  
Pass The SALT 2019



# Compliance: target and reality gap could be painful



Imagine if you could **continuously** ensure your **compliance**...

French, mature and open-source of  
**continuous configuration compliance**



Manage OS, middleware and software level



Team oriented (WebUI, CLI, API)



Audit only or automatic drift remediation



Continuous reporting and dashboarding



# RUDDER

## CONTINUOUS AUDITING & CONFIGURATION



# Built-in configuration modules and a powerful editor



RUDDER  
Pass The SALT 2019

Status

Documentation

admin

LIBRARY

Techniques

Create

Import

CIS 5 OS Services

CIS 9.1 configuration cron

Company websites

Demo technique

Monitoring template

ntp configuration

Single database

SSSD

Telnet Deactivation

Wazuh windows install

Zabbix windows configuration

Name: CIS 5 OS Services

Description: CIS benchmark section for OS services.

Technique ID: CIS\_5\_OS\_Services

Version: 1.0

Parameters

Condition from command

condition\_prefix:inetd\_file\_exists

Condition: any.(inetd\_file\_exists\_true)

File lines absent

file:/etc/inetd.conf

Package absent

name:nis

Package absent

name:rsh-client

Package absent

name:rsh-reload-client

Package absent

name:talk

Service check disabled at boot

Add methods

Reset

Save

LIBRARY

Generic methods

Filters

Agent type: All Classic DSC

☐ Show deprecated generic methods

Command

Command execution

Execute a command

Command execution once

Execute a command only once on a node

Show

Command execution result

Execute a command and create result conditions depending on its exit code

Show

Condition

Condition from command

Execute a command and create result conditions depending on its exit code

Show

Condition from expression

Create a new condition

Show

Condition from expression persistent

Categories

Command

Condition

Directory

Environment

File

Group

Http

Monitoring

Package

Permissions

Registry

Schedule

Service

Sharedfile

User

Variable

Windows

# Get your compliance instantly



RUDDER  
Pass The SALT 2019

Search anything

Status

Documentation

admin

Audit

CIS 5 OS Services

100%

Enforce

CIS 9.1 configure cron - Critical

100%

Audit

Meltdown mitigation enabled (PTI)

100%

Enforce

Openssl version up to date

75%

25%

Component

Package

Value

openssl

Post-modification script

Status

Status

50%

50%

100%

Show 25 entries Showing 1 to 4 of 4 entries

First Previous 1 Next Last

Compliance by Node

Filter

Node

Status

Mixed

dev-www-01.lab.rudder.io

88%

12%

Mixed

prod-db-01.lab.rudder.io

93%

7%

Mixed

prod-infra-01.lab.rudder.io

100%

Mixed

prod-itop-01.lab.rudder.io

93%

7%

Delete

Disable

Clone

Save

# Thank you !

Any questions ?

**5mn Survey on SecOps:**  
**[bit.ly/pts19-secops](https://bit.ly/pts19-secops)**

**Alexandre BRIANCEAU**

✉ [alexandre@rudder.io](mailto:alexandre@rudder.io)

🐦 [@abrianceau](https://twitter.com/abrianceau)



Pass the SALT 2019



**RUDDER**