

Amazon Inspector

Julien Simon

Principal Technical Evangelist, AWS

julsimon@amazon.fr

@julsimon



Agenda

Qu'est-ce qu'Inspector peut faire pour vous ?

Disponibilité et tarification

Installation

Démonstration

Conseils et ressources

Questions et réponses



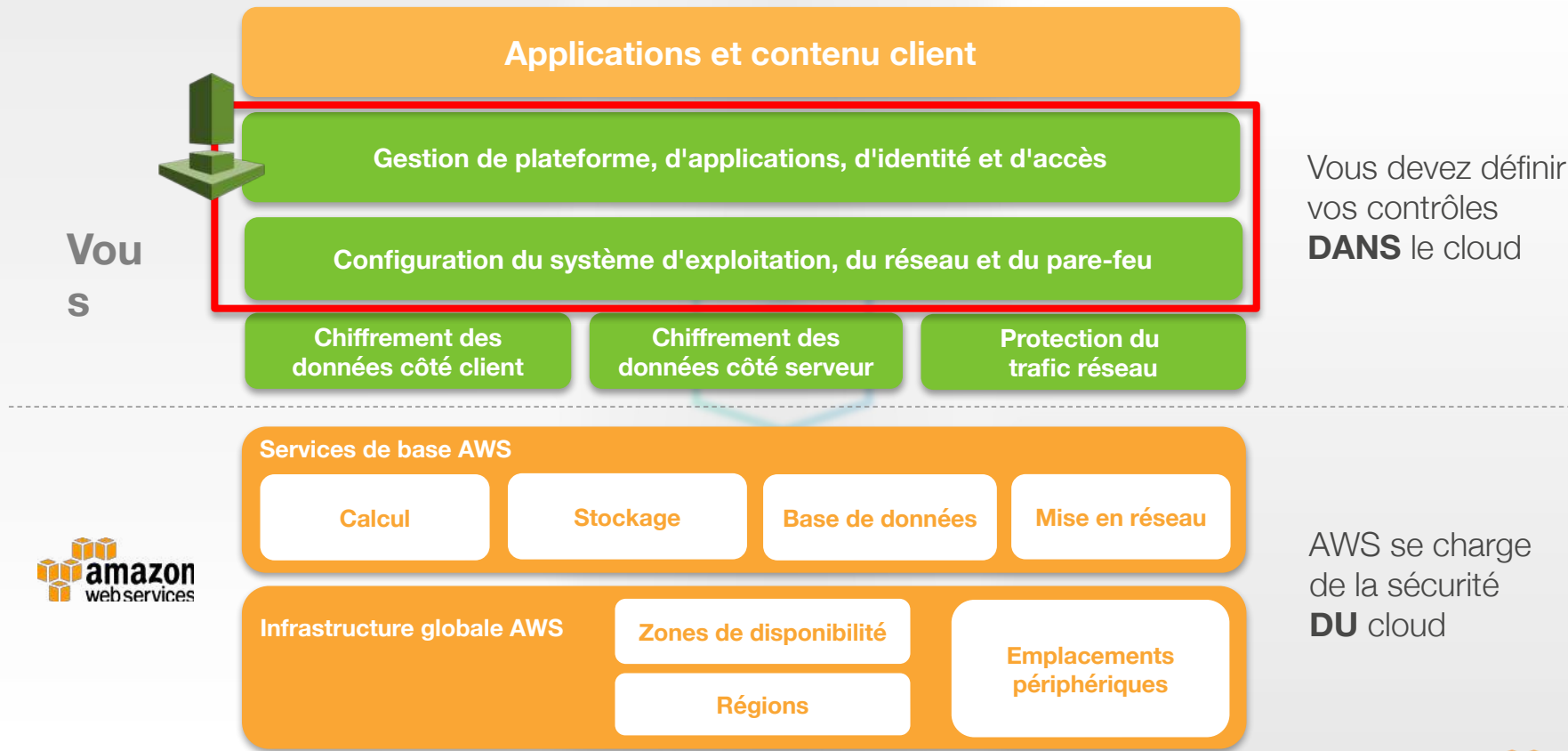
Amazon Inspector

Inspector vous permet d'**analyser** vos instances EC2 et d'**identifier** des failles de sécurité.

1. Définissez **la liste des instances** avec un *tag*
2. Déployez **l'agent Inspector** sur les instances concernées
3. Lancez une **évaluation**, basée sur une liste de **règles** pré-établie.
4. Analysez les **résultats**.

Note : Inspector ne change rien au modèle de sécurité partagée.

AWS Inspector vous aide à sécuriser votre plate-forme



Terminologie Inspector

Evaluation (*Assessment*)

- Analyse d'une application afin de détecter les failles de sécurité

Cible d'évaluation (*Assessment Target*)

- Ensemble d'instances EC2 que vous voulez évaluer

Groupe de règles (*Rule Package*)

- Ensemble de vérifications de sécurité (« règles »)

Modèle d'évaluation (*Assessement Template*)

- Cible + groupe de règles + durée

Résultats (*Findings*)

- Problème de sécurité potentiel dans votre application
- Les données collectées lors de l'évaluation correspondent à une règle
- Description détaillée, contexte et étapes de résolution

Groupes de règles

- **Common Vulnerabilities and Exposures**
 - Vulnérabilités CVE <http://cve.mitre.org>
 - <https://s3-us-west-2.amazonaws.com/rules-engine/CVEList.txt> (43,819)
- **CIS Operating System Security Configuration Benchmarks**
 - Vulnérabilités du Center for Internet Security <http://cisecurity.org>
 - <http://benchmarks.cisecurity.org>
- **Security Best Practices**
 - Bonnes pratiques SSH, mots de passe, etc. (Linux uniquement)
 - https://docs.aws.amazon.com/fr_fr/inspector/latest/userguide/inspector_security-best-practices.html
- **Runtime Behavior Analysis**
 - Comportement des instances pendant l'évaluation (protocoles réseau, etc.)
 - https://docs.aws.amazon.com/fr_fr/inspector/latest/userguide/inspector_runtime-behavior-analysis.html

Disponibilité et prix

- Inspector est disponible dans les régions suivantes :
 - US: Oregon, N. Virginia
 - EU: Irlande
 - Asia Pacific: Corée du Sud, Inde, Japon, Australie
- Tarif dégressif : de \$0.30 à \$0.05 par évaluation
- Niveau d'usage gratuit : 250 évaluations pendant 90 jours

Agent Inspector – Linux

- Amazon Linux (>= 2015.03), Ubuntu (14.04 LTS), RHEL (7.2), CentOS (7.2)
- Versions de noyau Linux supportées : https://s3.amazonaws.com/aws-agent.us-east-1/linux/support/supported_versions.json

```
$ wget https://d1wk0tztpsntt1.cloudfront.net/linux/latest/install
```

```
$ sudo bash install
```

```
$ sudo /opt/aws/awsagent/bin/awsagent status
```

```
$ sudo /etc/init.d/awsagent [ stop | start ]
```

Attention : l'agent dépend du noyau. Il est prudent de le mettre à jour après chaque mise à jour du noyau

Agent Inspector – Windows

- Windows Server 2008 R2, Windows Server 2012 et 2012 R2
- Téléchargez et exécutez le fichier suivant :

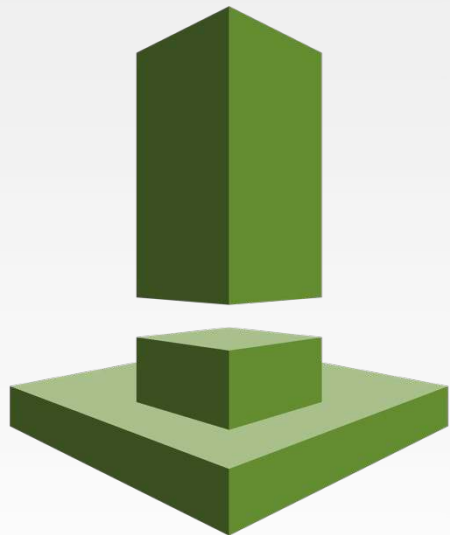
<https://d1wk0tztpsntt1.cloudfront.net/windows/installer/latest/AWSAgentInstall.exe>

- Lancement et arrêt via *services.msc* :
 - *AWS Agent Service*
 - *AWS Agent Updater Service*

Utiliser Inspector

- Console AWS (uniquement en Anglais)
- Ligne de commande AWS <https://docs.aws.amazon.com/cli/latest/reference/inspector/index.html>
- SDK AWS <https://aws.amazon.com/tools>
 - Java <https://docs.aws.amazon.com/AWSJavaSDK/latest/javadoc/com/amazonaws/services/inspector/AmazonInspector.html>
 - Python <https://boto3.readthedocs.org/en/latest/reference/services/inspector.html>
 - Documentation de l'API <https://docs.aws.amazon.com/inspector/latest/APIReference/Welcome.html>

Démonstration



3 instances Linux

- Ubuntu 14.04.02 LTS (Avril 2014)
- Amazon Linux 2015.03
- Amazon Linux 2016.09

→ Packages PHP, MySQL, Java, Apache, Bind, etc.

1 instance Windows Server 2012

Pré-requis

Amazon Inspector prerequisites



Create a role

Create a role to allow Amazon Inspector to access your AWS account. [Learn more.](#)

Amazon Inspector role*

<role not created or selected>

Choose or create role

Tag your EC2 instances

Amazon Inspector runs security assessments for your resources that run on AWS EC2 infrastructure. To get started, you must first tag the EC2 instances that you want to include in your assessment target. [Learn more.](#)

[Tag your EC2 instances](#)

Install AWS agent on your EC2 instances

The AWS agent monitors the behavior of the EC2 instance that you install it on. You must install the AWS agent on each EC2 instance that you want to include in your assessment target.

[Install AWS agent](#)

***Required**

Cancel

Next

Définir une cible d'évaluation

Define an assessment target



An assessment target represents a collection of AWS resources that help you accomplish your business goals. [Learn more.](#)

Name*

Webinar-001

Tags*

Key	Value	
InspectorTag	Assessment001	
Add a new key		

*Required

[Cancel](#)

[Preview](#)

[Previous](#)

[Next](#)

Définir un modèle d'évaluation

Define an assessment template



An assessment template allows you to specify various properties for an assessment run, including rules packages, duration, SNS notifications, and how to label any findings. [Learn more.](#)

Name*

Webinar-001-commonVulns

Rules packages*

Common Vulnerabilities and Exposures-1.1



Select an Inspector rules package



Amazon Inspector runs assessments for the assessment target against selected rules package(s). [Learn more.](#)

Duration*

1 hour (Recommended)



The default Amazon Inspector assessment template duration is 1 hour. You can modify the duration, but note that assessment templates with longer durations can deliver fuller sets of findings.

***Required**

[Cancel](#)

[Previous](#)

[Next](#)

Récapitulatif du modèle d'évaluation

Amazon Inspector - Assessment Templates

An assessment template allows you to specify various properties for an assessment run, including rules packages, duration, SNS notifications, and how to label any findings. [Learn more](#).

CreateRunStopDeleteClone

Last updated on December 15, 2016 4:28:44 PM (0m ago)

Filter

1 selected

« < Viewing 1-1 of 1 > »

<input type="checkbox"/>	Name	Duration	Target name	Last run	All runs
<input checked="" type="checkbox"/>	Webinar-001-commonVulns	1 Hour	Webinar-001	none	0

Assessment Template - Webinar-001-commonVulns

Name

Webinar-001-commonVulns

ARN

arn:aws:inspector:us-west-2:[REDACTED]:target/0-aiPGypOn/template/0-BLQMAkoU

Target name

[Webinar-001](#)

Rules packages

[Common Vulnerabilities and Exposures-1.1](#)

Duration

1 Hour

Lancer l'évaluation

Amazon Inspector - Assessment Runs

An assessment run is the process of discovering potential security issues through the analysis of your assessment target's behavior against selected rules packages. [Learn more.](#)

RunStopDelete

Last updated on December 15, 2016 4:29:15 PM (0m ago)

« < Viewing 1-1 of 1 > »

<input type="checkbox"/>	Start time	Status	Template name	Findings
<input type="checkbox"/>	Today at 4:29 PM (GMT+1) (a few sec...	Collecting data	Webinar-001-commonVulns	0

Assessment - Run - Webinar-001-commonVulns - 2016-12-15T15:29:01.800Z

ARN `arn:aws:inspector:us-west-1:[redacted]:target/0-aiPGypOn/template/0-BLQMAkoU/run/0-6e7dOXgG`

Start Today at 4:29 PM (GMT+1) (a few seconds ago)

Target name [Webinar-001](#)

Template name [Webinar-001-commonVulns](#)

Rules packages [Common Vulnerabilities and Exposures-1.1](#)

Duration 1 Hour

Status Collecting data

Findings 0

Show AWS agentsShow status

Pendant l'évaluation

Run - Webinar-001-commonVulns - 2016-12-15T15:29:01.800Z

Last updated on December 15, 2016 4:29:44 PM (0m ago)

Filter

Viewing 1-3 of 3

Instance	Name	Matche...	AWS age...	Status	Message...
i-02c89c...	AMZ201503	InspectorTa...	HEALTHY	Collecting ...	1127
i-04e963...	Ubuntu	InspectorTa...	HEALTHY	Collecting ...	1863
i-0c8c9f...	AMZ201609	InspectorTa...	HEALTHY	Collecting ...	1045

OK

Run - Webinar-001-commonVulns - 2016-12-15T15:29:01.800Z

Amazon Inspector has been analyzing **Webinar-001** for **5 minutes 41 seconds**.

Amazon Inspector has received **4458** telemetry messages in total from **3** agents.

RefreshClose

Lister les résultats dans la console

Amazon Inspector - Findings

Findings are potential security issues discovered after Amazon Inspector runs an assessment against a specified assessment target. [Learn more](#).

[Add/Edit attributes](#)

Last updated on December 15, 2016 8:48:11 PM (1m ago)



Filter

Viewing 1-25 of 420

<input type="checkbox"/>	Severity ⓘ	Date	Finding	Target	Template	Rules Package	AWS agent ID
<input type="checkbox"/>	High	Today at 5:31 PM (GMT+1)...	Instance i-04e963f9395279434 is vuln...	Webinar-001	Webinar-001...	Common Vulnerabilities and Exposur...	I-04e963f9395279434
<input type="checkbox"/>	High	Today at 5:31 PM (GMT+1)...	Instance i-04e963f9395279434 is vuln...	Webinar-001	Webinar-001...	Common Vulnerabilities and Exposur...	I-04e963f9395279434
<input type="checkbox"/>	High	Today at 5:31 PM (GMT+1)...	Instance i-04e963f9395279434 is vuln...	Webinar-001	Webinar-001...	Common Vulnerabilities and Exposur...	I-04e963f9395279434
<input type="checkbox"/>	High	Today at 5:31 PM (GMT+1)...	Instance i-02c89c928eb8f3a62 is vuln...	Webinar-001	Webinar-001...	Common Vulnerabilities and Exposur...	I-02c89c928eb8f3a62

Finding for assessment target 'Webinar-001' and template 'Webinar-001-commonVulns'

ARN [arn:aws:inspector:us-west-2:██████████:at/0-aiPGypOn/template/0-BLQMAkoU/run/0-6e7dOXgG/finding/0-gkvqfuGM](#)

Run name [Run - Webinar-001-commonVulns - 2016-12-15T15:29:01.800Z](#)

Target name [Webinar-001](#)

Template name [Webinar-001-commonVulns](#)

Start Today at 4:29 PM (GMT+1) (4 hours ago)

End Today at 5:31 PM (GMT+1) (3 hours ago)

Status Analysis complete

Rules package [Common Vulnerabilities and Exposures-1.1](#)

AWS agent ID [i-02c89c928eb8f3a62](#)

Finding Instance i-02c89c928eb8f3a62 is vulnerable to CVE-2015-3143

Severity High ⓘ

Description cURL and libcurl 7.10.6 through 7.41.0 does not properly re-use NTLM connections, which allows remote attackers to connect as other users via an unauthenticated request, a similar issue to CVE-2014-0015.

Recommendation Use your Operating System's update feature to update package curl, curl-0:7.40.0-1.49.amzn1, libcurl-0:7.40.0-1.49.amzn1. For more information see <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3143>

Lister les résultats avec la ligne de commande AWS

```
$ aws inspector list-assessment-runs
```

```
{
  "assessmentRunArns": [
    "arn:aws:inspector:us-west-2:ACCOUNT:target/0-aiPGyp0n/template/0-BLQMAkoU/run/0-6e7d0XgG"
  ]
}
```

```
$ aws inspector list-findings --assessment-run-arns "arn:aws:inspector:us-west-2:ACCOUNT:target/0-aiPGyp0n/template/0-BLQMAkoU/run/0-6e7d0XgG"
```

```
...
  "findingArns": [
    "arn:aws:inspector:us-west-2:ACCOUNT:target/0-aiPGyp0n/template/0-BLQMAkoU/run/0-6e7d0XgG/finding/0-01Eg2Ug0",
  ]
}
```

```
$ aws inspector describe-findings --finding-arns "arn:aws:inspector:us-west-2:ACCOUNT:target/0-aiPGyp0n/template/0-BLQMAkoU/run/0-6e7d0XgG/finding/0-01Eg2Ug0"
```

Le résultat de notre évaluation

Ubuntu 14.04.02

```
aws inspector list-findings --assessment-run-arns "arn:aws:inspector:us-west-2:ACCOUNT:target/0-aiPGyp0n/template/0-BLQMAkoU/run/0-6e7d0XgG" --filter '{"severities":["High"], "agentIds":["i-04e963f9395279434"]}' --max-results 1000 --output text | grep FINDINGARNs | wc -l
```

242

Amazon Linux 2015.03

```
aws inspector list-findings --assessment-run-arns "arn:aws:inspector:us-west-2:ACCOUNT:target/0-aiPGyp0n/template/0-BLQMAkoU/run/0-6e7d0XgG" --filter '{"severities":["High"], "agentIds":["i-02c89c928eb8f3a62"]}' --max-results 1000 --output text | grep FINDINGARNs | wc -l
```

69

Amazon Linux 2016.09

```
aws inspector list-findings --assessment-run-arns "arn:aws:inspector:us-west-2:ACCOUNT:target/0-aiPGyp0n/template/0-BLQMAkoU/run/0-6e7d0XgG" --filter '{"severities":["High"], "agentIds":["i-0c8c9f709dd7f7cfd"]}' --max-results 1000 --output text | grep FINDINGARNs | wc -l
```

4

CVE-2015-8325 (OpenSSH)

CVE-2016-7039 / CVE-2016-8666 / CVE-2016-9083 (Linux kernel)



Comment corriger les problèmes ?

Mettez à jour vos instances **régulièrement** !

\$ sudo yum update --cves=... -y

\$ sudo yum update --security -y

\$ sudo yum update -y

```
Last login: Thu Dec 15 15:08:55 2016 from 205.251.233.50
```

```
  _I_  _I_  )  
 _I_ (  /   Amazon Linux AMI  
_I_\_I_\_I_
```

```
https://aws.amazon.com/amazon-linux-ami/2016.09-release-notes/  
6 package(s) needed for security out of 11 available  
Run "sudo yum update" to apply all updates.  
[ec2-user@ip-172-31-40-254 ~]$
```

```
Downloading packages:
```

```
(1/11): aws-cli-1.11.17-1.43.amzn1.noarch.rpm  
(2/11): curl-7.47.1-9.66.amzn1.x86_64.rpm  
(3/11): kernel-4.4.35-33.55.amzn1.x86_64.rpm  
(4/11): libcurl-7.47.1-9.66.amzn1.x86_64.rpm  
(5/11): openssh-6.6.1p1-31.62.amzn1.x86_64.rpm  
(6/11): openssh-clients-6.6.1p1-31.62.amzn1.x86_64.rpm  
(7/11): openssh-server-6.6.1p1-31.62.amzn1.x86_64.rpm  
(8/11): python27-boto-1.4.74-1.60.amzn1.noarch.rpm  
(9/11): system-release-2016.09-0.8.noarch.rpm  
(10/11): tzdata-2016i-1.66.amzn1.noarch.rpm  
(11/11): tzdata-java-2016i-1.66.amzn1.noarch.rpm
```

Evaluons à nouveau l'instance Amazon Linux 2016.09

Amazon Inspector - Findings

Findings are potential security issues discovered after Amazon Inspector runs an assessment against a specified assessment target. [Learn more.](#)

✖ Filters: {"assessmentRunArns":["arn:aws:inspector:us-west-2:██████████:target/0-Rzum75K3/template/0-ehW3Sr9a/run/0-gTrUJAxQ"]}

[Add/Edit attributes](#)

Filter

<input type="checkbox"/>	Severity ⓘ	Date ▾	Finding	Target	Template	Rules Package
<input type="checkbox"/>	Informa...	Today a...	No potential security issues found	Webinar-002	Webinar-002...	Common Vulnerabilities and Exposur...

Finding for assessment target 'Webinar-002' and template 'Webinar-002-commonVulns-amzlinux201609'

ARN [arn:aws:inspector:us-west-2:██████████:target/0-Rzum75K3/template/0-ehW3Sr9a/run/0-gTrUJAxQ/finding/0-EwQfQu82](#)

Run name [Run - Webinar-002-commonVulns-amzlinux201609 - 2016-12-15T18:57:56.555Z](#)

Target name [Webinar-002](#)

Template name [Webinar-002-commonVulns-amzlinux201609](#)

Start Today at 7:57 PM (GMT+1) (an hour ago)

End Today at 8:59 PM (GMT+1) (7 minutes ago)

Status Analysis complete

Rules package [Common Vulnerabilities and Exposures-1.1](#)

Finding No potential security issues found

Severity Informational ⓘ

Description Amazon Inspector did not find any potential security issues during this assessment.

Recommendation No remediation needed.

Après mise à jour et scan de 24 heures ☺

Ubuntu 14.04.02

```
aws inspector list-findings --assessment-run-arns "arn:aws:inspector:us-west-2:ACCOUNT:target/0-aiPGyp0n/template/0-KQ1FrZu6/run/0-Ixqaicyh" --filter '{"severities":["High"], "agentIds":["i-04e963f9395279434"]}' --max-results 1000 --output text | grep FINDINGARNs | wc -l
```

52

Amazon Linux 2015.03

```
aws inspector list-findings --assessment-run-arns "arn:aws:inspector:us-west-2:ACCOUNT:target/0-aiPGyp0n/template/0-KQ1FrZu6/run/0-Ixqaicyh" --filter '{"severities":["High"], "agentIds":["i-02c89c928eb8f3a62"]}' --max-results 1000 --output text | grep FINDINGARNs | wc -l
```

0

Amazon Linux 2016.09

```
aws inspector list-findings --assessment-run-arns "arn:aws:inspector:us-west-2:ACCOUNT:target/0-aiPGyp0n/template/0-KQ1FrZu6/run/0-Ixqaicyh" --filter '{"severities":["High"], "agentIds":["i-0c8c9f709dd7f7cfd"]}' --max-results 1000 --output text | grep FINDINGARNs | wc -l
```

0

Quelques conseils

- Attention aux **vieilles AMI** et à leurs **vieux packages**
 - Amazon Linux est bien mise à jour, mais pensez à utiliser la dernière AMI en date
- Scannez **régulièrement** vos instances
 - Comparez la liste des instances scannées avec la liste des instances qui tournent !
- Appliquez **systématiquement** les mises à jour de sécurité
 - Au redémarrage (script d'initialisation)
 - Attention : Pas dans User Data, qui n'est exécuté qu'à la création de l'instance
 - Tâche *cron* sur l'instance
 - Événements CloudWatch programmés
 - EC2 Systems Manager
- Mettez à jour l'agent Inspector **à chaque changement de noyau**
 - Au redémarrage (script d'initialisation)
- Intégrez Inspector dans votre pipeline de **déploiement continu**

Ressources complémentaires

Livres blancs AWS

<https://aws.amazon.com/whitepapers/auditing-security-checklist-for-use-of-aws/>

<https://aws.amazon.com/blogs/security/new-whitepaper-security-at-scale-logging-in-aws/>

<https://aws.amazon.com/whitepapers/overview-of-risk-and-compliance/>

AWS re:Invent 2015 | (SEC324) New! Introducing Amazon Inspector

https://www.youtube.com/watch?v=HjuEtMrWc_w

<https://aws.amazon.com/fr/blogs/aws/scale-your-security-vulnerability-testing-with-amazon-inspector/>

<https://aws.amazon.com/fr/about-aws/whats-new/2016/12/amazon-ec2-systems-manager-now-offers-patch-management/>

Slides et vidéos des webinaires : <http://bit.ly/2hKPihB>

Merci !

Julien Simon

Principal Technical Evangelist, AWS

julsimon@amazon.fr

@julsimon

Webinaires 2017 : <https://attendee.gotowebinar.com/register/7239291589398918401>

Lundi

- Bonnes pratiques d'authentification avec AWS IAM
- Chiffrez vos données avec AWS

Mardi

- Fireside chat avec Matthieu Bouthors et Julien Simon
- Re:Invent update 1

Mercredi

- Deep dive : Amazon Virtual Private Cloud
- Bonnes pratiques anti-DDoS

Jeudi

- Re:Invent update 2
- Gérez les incidents de sécurité avec AWS CloudTrail

Vendredi

- Automatisez vos audits de sécurité avec Amazon Inspector
- Bonnes pratiques de sécurité sur AWS

Slides et vidéos des webinaires : <http://bit.ly/2hKPiHB>