bluepinksecurity

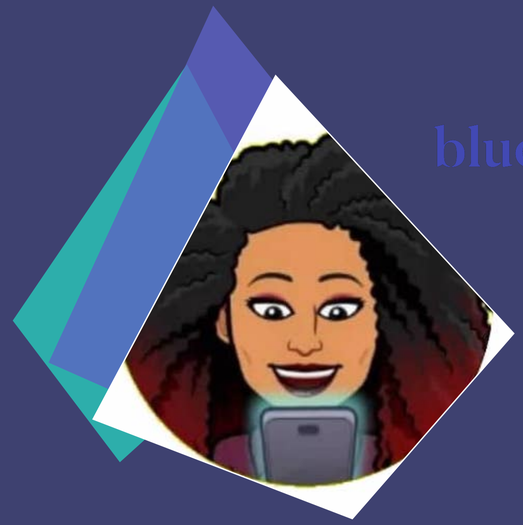
Comment la sécurité dès la conception des applications constitue une bonne réponse aux incidents?

DevSecops - SOC

Présentée par Baka Diop

next >

bluepinksecurity



Baka Diop

Experte sécurité applicative

Senior Cybersecurity Architect Automotive chez Thales - Squad

CEO BLUEPINKSECURITY (SARL)

Conférencière et influenceuse DevSecOps

Team Leader application Security

Podcaster « welcome ladies cybersecurity » BluePinkSecurity

Membre et Mentor CEFCYS

bluepinksecurity

Sommaire

bluepinksecurity

Définitions

ISO27034
SDLC
Audits de sécurité
Piliers fondamentaux de la sécurité de l'information
SOC

Norme ISO 27034

bluepinksecurity

➢Extrait de la norme

ISO 27034 ISO/CEI 27034- 1 (2011) Section 6.1 “Application Security is a process performed to apply controls and measurements to an organization’s applications in order to manage the risk of using them.” “Controls and measurements can be applied to the application itself (its processes, components, software and results), to its data (configuration data, user data, organization data), and to all technology, processes and actors involved in the application’s life cycle.”

SDLC : Software Development LifeCycle

bluepinksecurity

➢Les étapes standards du SDLC

Audits de sécurité

bluepinksecurity

01 WhiteBox

02 GreyBox

03 BlackBox

04 Scanneur de vulnérabilités

Piliers fondamentaux de la sécurité de l'information

bluepinksecurity

SOC

bluepinksecurity

Modèles de sécurité

S2DLC
Security by Design (SbD)
Privacy by Design

S2DLC : Secure Software Development LifeCycle

bluepinksecurity

1 Phase de prérequis	2 Phase de spécifications	3 Phase de développement	4 Phase de tests	5 Phase de Maintenance
FORMATION	Revue de l'architecture	Scans statiques	**Scans dynamiques**	**Plans de maintenance**
Définition des exigences	Revue du design	Revue de code	**Gestion des vulnérabilités**	**Veille de vulnérabilités**
Analyse de risques	Workflow des menaces	Automatisation des tests	**Phase de Validation**	**Déploiement des correctifs**
Politiques de sécurité				

➢Un modèle du S2DLC

Security by Design SbD (Sécurité dès la conception)

bluepinksecurity

➢Définition

L'architecture, la conception et l'implémentation des logiciels doivent répondre aux exigences en protégeant les applications et les informations traitées, et en résistant aux attaques.

➢Bénéfices

- Réduction du temps de traitement des vulnérabilités,
- De la surface d'attaque
- réduction considérable des risques avec la défense en profondeur

Exemples :

Sopra Steria a déjoué l'attaque par ransomware qui la visait, révèle l'Anssi

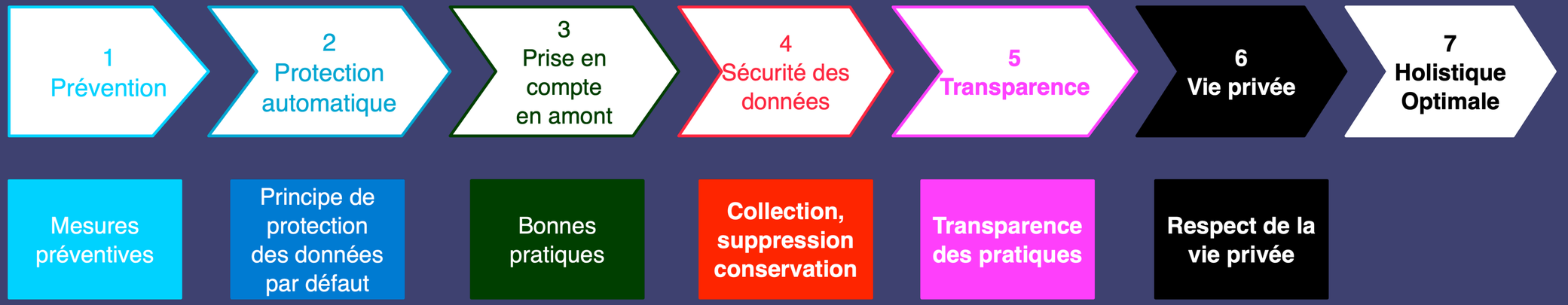
COMMENT LE RANSOMWARE EST ENTRÉ DANS L'ENTREPRISE	NB D'INCIDENTS	% D'INCIDENTS
Via un fichier te´le´charge´/email avec PJ malveillante	741	29%
Via une attaque a` distance du serveur	543	21%
Via un email avec pie`ce jointe malveillante	401	16%
Instances de Cloud public mal configure´es	233	9%
Via le protocole RDP (Remote Desktop Protocol)	221	9%
Via un prestataire avec qui nous collaborons	218	9%
Via une cle´ USB/support amovible	172	7%
Autre	0	0%
Ne sait pas	9	0%
Total	2 538	100%

Techniques d'attaque des ransomwares

Source : https://www.sophos.com

Privacy by Design - PbD

bluepinksecurity



➢Bénéfices

Empêcher de potentielles fuites de données et des sanctions RGPD à hauteur de 4% du Chiffres d'affaires

Exemples : sanction de 60 millions d'euros à l'encontre de GOOGLE LLC et de 40 millions d'euros à l'encontre de GOOGLE IRLANDE LIMITED

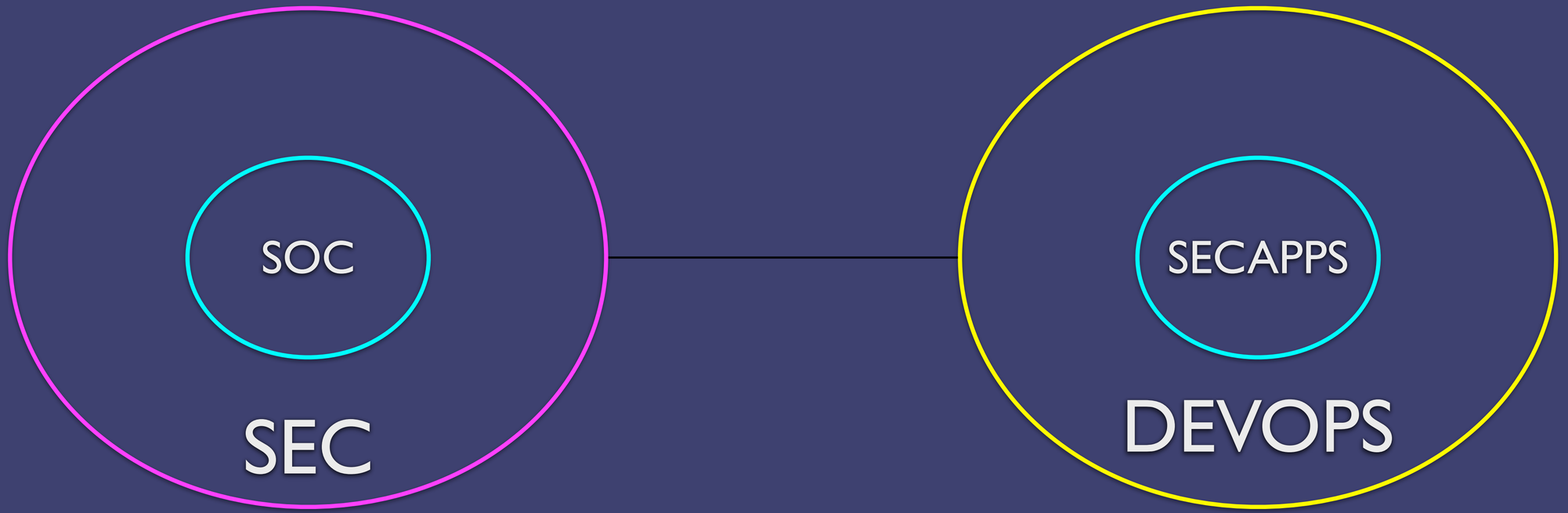
Source : https://donnees-rgpd.fr/definitions/privacy-by-design/

Retex suite à des interventions

Cas 1 : Niveau 0
Cas 2 : Niveau 1
Cas 3 : Niveau 2

Cas 1 : Niveau 0

bluepinksecurity



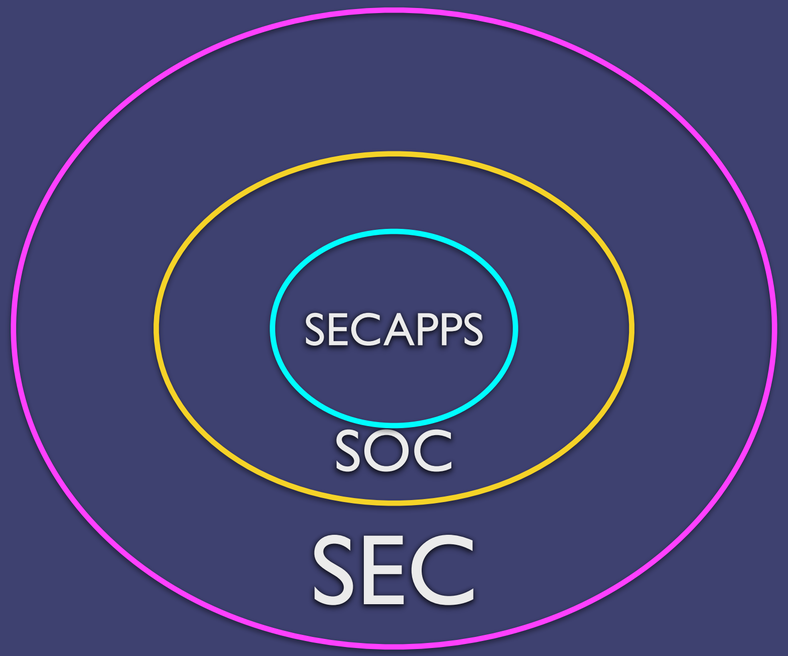
Cas 1 : Situation

bluepinksecurity

- Périmètre d’action SecApp limité
- Echanges uniquement dans le cadre des pentests
- L’activité SecApp(Tools, stratégies etc) n’est pas piloté dans son ensemble
- L’activité SecApp est considéré comme une charge supplémentaire
- Surmenage de l’équipe SOC

Cas 2 : Niveau 1

bluepinksecurity



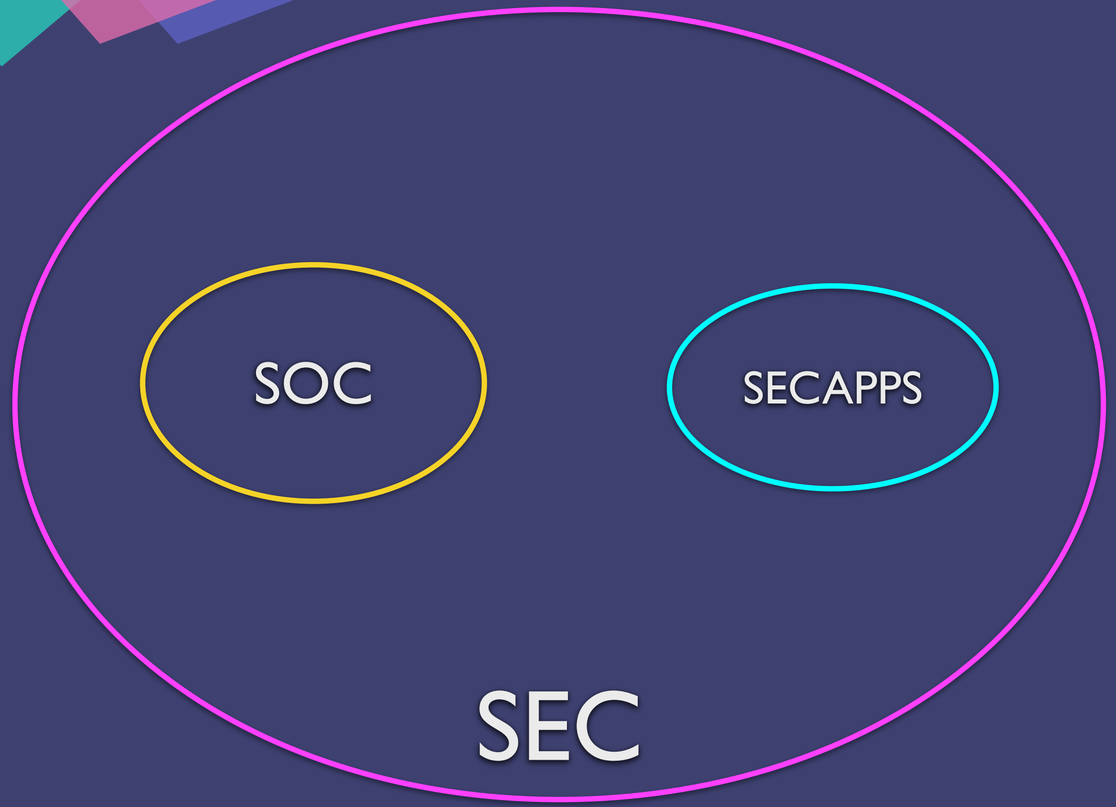
Cas 2 : Situation

bluepinksecurity

- Intervention de l’équipe SecApp en cas de suspicion d’attaque
- Gestion de vulnérabilités et indicateurs des vulnérabilités
- Surmenage de l’équipe SecApp !!!

Cas 3 : Niveau 2 Meilleur solution

bluepinksecurity



Cas 3 : Situation

bluepinksecurity

- Répartition des tâches
- Equipe dédiée en SecApp
- Collaboration étroite entre SOC(CERT) et la SecAPP

Recommendations

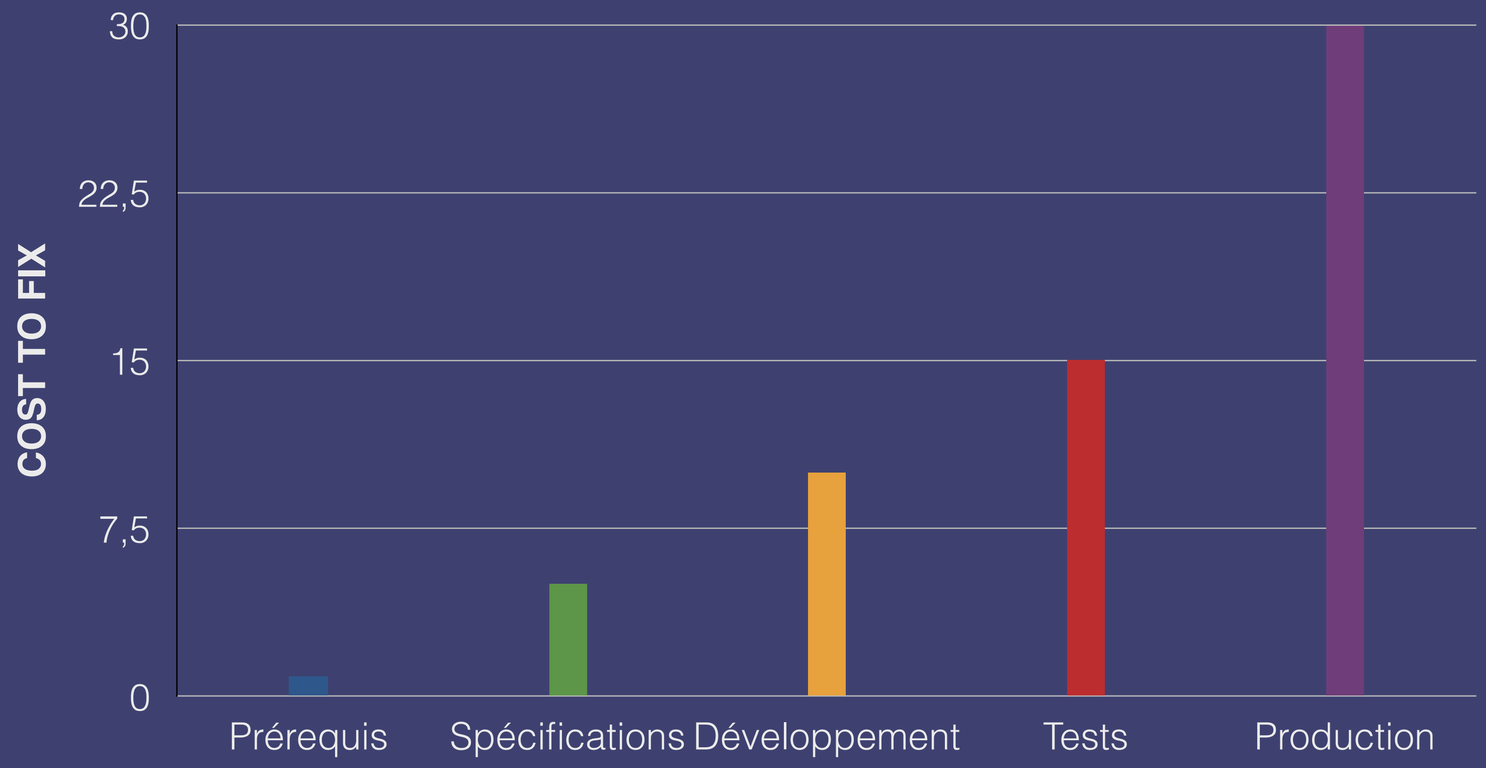
Formations et sensibilisations
Adoption des modèles SecApp
Anticipations des menaces

Formations et sensibilisations

bluepinksecurity

Adoption des modèles SecApp

bluepinksecurity



S2DLC

SECURITY BY DESIGN

PRIVACY BY DESIGN

ZERO TRUST

Anticipation des menaces

bluepinksecurity

Coût moyen pour remédier à une attaque de ransomware

bluepinksecurity

Merci !!!

Questions

Réponses

@baka-d-818019164

@cobadisec

< previous