



MOABI

**ATTAQUES CONTRE LES SUPPLY CHAINS,
RANSOMWARE :
DE LA NECESSITE DE NOUVEAUX PROCESSUS**

Pr. Jonathan Brossard, CTO at MOABI
Jonathan.brossard@moabi.com

**CYBER@
STATION F**

**THALES
DIGITAL
FACTORY**

le cnam

Qui suis-je ?



- **Activités**

CTO, Fondateur de MOABI (Paris)

Professeur des Universités Associé en Cyber Sécurité au CNAM (Paris)

- **Activités passées**

Ingénieur Principal de la Sécurité Produit, Directeur de la Sécurité

Offensive, chez Salesforce (San Francisco)

CISO chez Change.org (San Francisco)



Prix, reconnaissance, etc.



Qui suis-je ?

x



MOABI

▪ *Chercheur en Cyber Sécurité...*

- Brossard Jonathan, Keynote, RoadSec 2020 (Sao Paolo, Brazil)
- Brossard Jonathan, Hardware Backdooring is Practical : 7 years review, Nullcon 2019 (Goa, India)
- Brossard Jonathan, Silent Protest, Shakacon 2016 (Hawaii)
- Brossard Jonathan, the Witchcraft Compiler collection (WCC), Intel ISec 2016 (Hillsborrow, USA)
- Brossard Jonathan, the Witchcraft Compiler collection (WCC), Blackhat Europe 2016 (London)
- Brossard Jonathan, Introduction to the Witchcraft Compiler collection (WCC), Bsidess SF 2016 (San Francisco)
- Brossard Jonathan, Introduction to the Witchcraft Compiler collection (WCC), DEFCON 2015 (Las Vegas)
- Brossard Jonathan, Introduction to the Witchcraft Compiler collection (WCC), H2HC 2015 (Sao Paolo)
- Brossard Jonathan & Hormazd Billimoria, SMBv2 : Sharing More than just your files, Blackhat Briefings 2015 (Las Vegas)
- Brossard Jonathan & Xiaoran Wang, Filecry : the new age of XXE, Blackhat Briefings 2015 (Las Vegas)
- Brossard Jonathan & Sergey Gorbaty, Java JDK Defenseless against XML Parsers, Blackhat Briefings 2015 (Las Vegas)
- Brossard Jonathan, Malware, Sandboxing and you, Ruxcon 2013 (Melbourne, Australia)
- Brossard Jonathan, Sandoxing is the ..., Syscan 360 2013 (Beijing)
- Brossard Jonathan, Hardware Backdooring is Practical, AusCert 2013 (Gold Coast, Australia)
- Brossard Jonathan, Hardware Backdooring is Practical, Nullcon 2012 (Goa)
- Brossard Jonathan, Rakshasa : Hardware Backdooring is Practical, H2HC 2013 (Sao Paolo)
- Brossard Jonathan, Hardware Backdooring is Practical, Intel ISec 2013 (Hillsborrow)
- Brossard Jonathan, Hardware Backdooring is Practical, NoSuchCon 2012 (Paris)
- Brossard Jonathan, Hardware Backdooring is Practical, DEFCON 2012 (Las Vegas)
- Brossard Jonathan, Rakshasa : Hardware Backdooring is Practical, Blackhat Briefings 2012 (Las Vegas)
- Brossard Jonathan, Post Memory Corruption Memory Analysis, Kiwicon 2011 (New Zealand)
- Brossard Jonathan, Post Memory Corruption Memory Analysis, Ruxcon 2011 (Melbourne)
- Brossard Jonathan, Post Memory Corruption Memory Analysis, Chaos Communication congress 2012 (Berlin)
- Brossard Jonathan, Post Memory Corruption Memory Analysis, Blackhat Briefings 2011 (Las Vegas)
- Brossard Jonathan, Breaking Virtualization by any means, HITB 2011 (Kuala Lumpur)
- Brossard Jonathan, Breaking Virtualization by switching the cpu to 8088 mode, HES 2010 (Paris)
- Brossard Jonathan, Breaking Virtualization by switching the cpu to 8088 mode, H2HC 2010 (Sao Paolo)
- Brossard Jonathan, Breaking Virtualization by switching the cpu to 8088 mode, Ruxcon 2010 (Melbourne)
- Brossard Jonathan, Breaking Virtualization by any means, HITB 2010 (Amsterdam)
- Brossard Jonathan, Practical brute-force against pre-boot authentication passwords, H2HC 2009 (Sao Paolo)
- Brossard Jonathan, Reverse Engineering for Exploit writers, ClubHack 2008 (Pune, India)
- Brossard Jonathan, Bypassing Pre-boot authentication passwords by instrumenting the BIOS keyboard buffer, DEFCON 2008 (Las Vegas)





CONTEXTE : REVUE DE L'ANNEE 2020/2021

Revue : Nouvelles du mois

Compétition de hacking "Tianfu" (Chine)



100% Binaires

Forbes

iPhone 13 Pro Hacked: Chinese Hackers Suddenly Break iOS 15.0.2 Security



Davey Winder Senior Contributor @
Cybersecurity
Straight Talking Cyber


[Follow](#)

- Windows 10 – hacked 5 times
- Adobe PDF Reader – 4 times
- Ubuntu 20 – 4 times
- Parallels VM – 3 times
- iOS 15 – 3 times
- Apple Safari – 2 times
- Google Chrome – 2 times
- ASUS AX56U router – 2 times
- Docker CE – 1 time
- VMWare ESXi – 1 time
- VMWare Workstation – 1 time
- qemu VM – 1 time
- Microsoft Exchange – 1 time

DARKReading The Edge DR Tech Sections Events Resources

China's Hackers Crack Devices at Tianfu Cup for \$1.5M in Prizes

China's premier hackers will target web browsers, operating systems, mobile devices, and even a car at Tianfu Cup.



Dark Reading Staff
Dark Reading

October 16, 2021



x

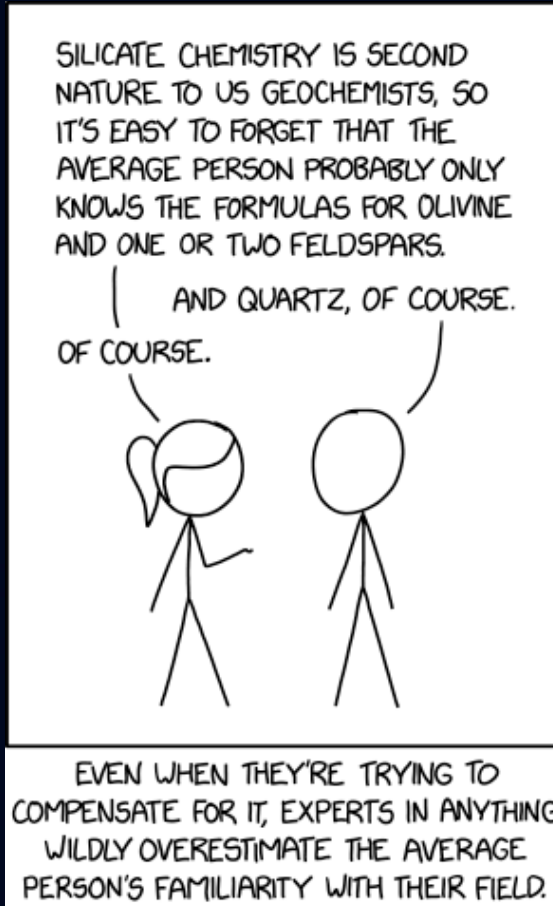
PETITE PARENTHÈSE

En limite de compétence technique ?

x



- *Le niveau de technicité des attaques devient très significatif*



- *Une solution possible*



Source: XKCD.com

Revue : Nouvelles de l'année

Attaques de Supply chains



100% Binaires

Piratage SolarWinds : les États-Unis parlent d'un hack de haut niveau nécessitant l'aide d'un pays

Par Mathieu Chartier (@chartier_mat) | Publié le 18/12/20 à 16h54

Kaseya hack floods hundreds of companies with ransomware

A screenshot of a French cybersecurity website. The header includes "CYBERGUERRE" and navigation links for "(GÉO)POLITIQUE", "HACK", "SÉCURITÉ", "PHISHING", and "ENQUÊTE". The main headline reads "Les hackers de SolarWinds ont infiltré son système dès septembre 2019". Below the headline is a small circular profile picture and the author's name "François Manens" with the date "13 janvier 2021".

CYBERGUERRE (GÉO)POLITIQUE HACK SÉCURITÉ PHISHING ENQUÊTE par Numer

Les hackers de SolarWinds ont infiltré son système dès septembre 2019

François Manens - 13 janvier 2021

A screenshot of a ZDNet article. The header features the ZDNet logo and a search icon. Navigation links include "CENTRAL EUROPE", "MIDDLE EAST", "SCANDINAVIA", "AFRICA", "UK", and "ITALY". A "MUST READ" section highlights "Tech skills: Four ways you can get the right mix". The main headline is "France: Russian state hackers targeted Centreon servers in years-long campaign". The sub-headline reads "New ANSSI report exposes new Sandworm APT attacks targeting IT companies using Centreon servers."

ZDNet

CENTRAL EUROPE MIDDLE EAST SCANDINAVIA AFRICA UK ITALY

MUST READ: Tech skills: Four ways you can get the right mix

France: Russian state hackers targeted Centreon servers in years-long campaign

New ANSSI report exposes new Sandworm APT attacks targeting IT companies using Centreon servers.

Revue : Nouvelles de l'année L'opinion des Gouvernements



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Alerts and Tips Resources Industrial Control Systems

National Cyber Awareness System > Alerts > Top Routinely Exploited Vulnerabilities

Alert (AA21-209A)

Top Routinely Exploited Vulnerabilities

Original release date: July 28, 2021 | Last revised: August 20, 2021

90% Binaires



Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques

PUBLICATIONS - SCANS ARCHIVES - RÉSEAU DES CSIRT - RECRUTEMENT CONTACT À PROPOS

« précédent

le 15 février 2021

BULLETIN D'ACTUALITÉ DU CERT-FR

Objet: Top 10 des vulnérabilités les plus marquantes de 2020

GESTION DU DOCUMENT

Référence	CERTFR-2021-ACT-008
Titre	Top 10 des vulnérabilités les plus marquantes de 2020
Date de la première version	15 février 2021
Date de la dernière version	15 février 2021
Source(s)	
Pièce(s) jointe(s)	Aucune(s)

Tableau 1: Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

TOP 10 DES VULNÉRABILITÉS LES PLUS MARQUANTES DE 2020

**Ransomware :
100% Binaires**

ÉTAT DE LA MENACE RANÇONGICIEL

À L'ENCONTRE DES ENTREPRISES ET DES INSTITUTIONS

43
2021-09-01





SUPPLY CHAIN versus LOGISTIQUE

Distinction "Supply Chain" versus "Logistique"

x



- *Supply chain*

Développement interne

- *Logistique*

Développement interne + externe



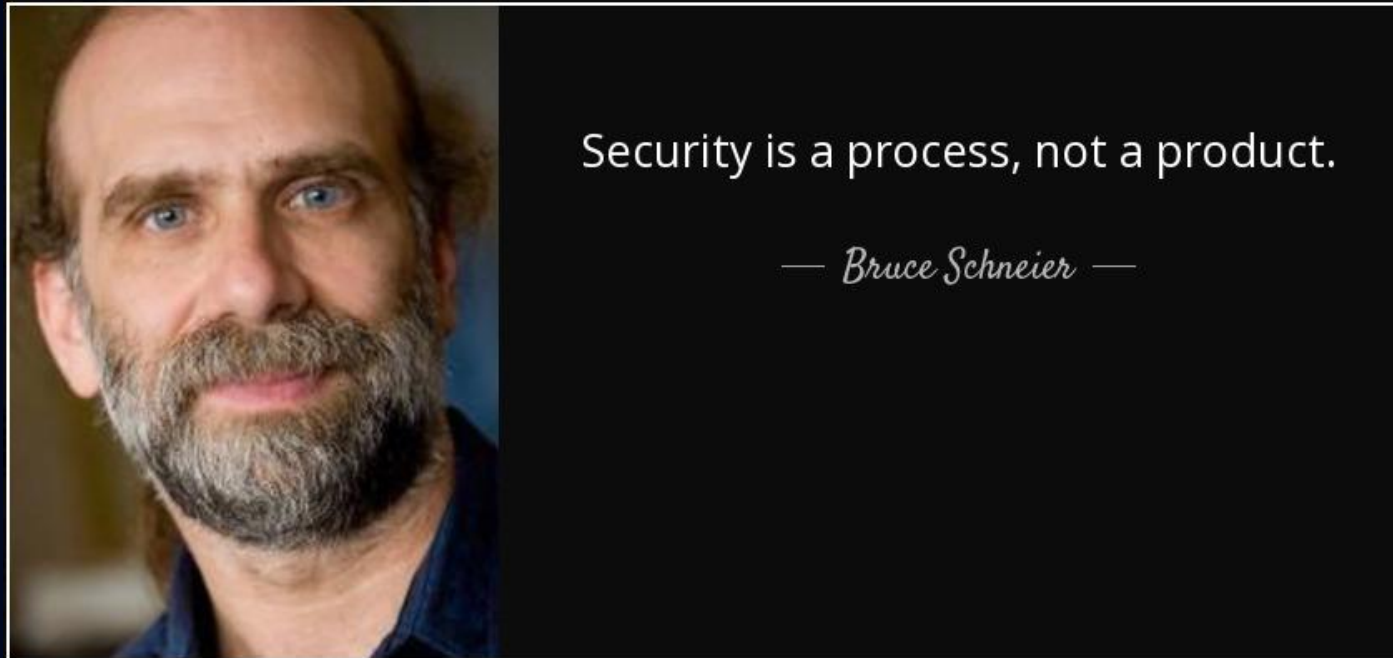
SECURISER SA SUPPLY CHAIN (DEVELOPPEMENT INTERNE)

La solution passe par de nouveaux Processus

x



- *La Sécurité, ce sont des Processus*



Nouveaux Problèmes = Nouveaux Processus



MOABI



National Cyber Security Centre
a part of GCHQ

10 Steps to Cyber Security

This collection is designed for security professionals and technical staff as a summary of NCSC advice for medium to large organisations. We recommend you start by reviewing your approach to risk management, along with the other nine areas of cyber security below, to ensure that technology, systems and information in your organisation are protected appropriately against the majority of cyber attacks and enable your organisation to best deliver its business objectives.

➤ **Risk management**
Take a risk-based approach to securing your data and systems.

➤ **Engagement and training**
Collaboratively build security that works for people in your organisation.

➤ **Asset management**
Know what data and systems you have and what business need they support.

➤ **Architecture and configuration**
Design, build, maintain and manage systems securely.

➤ **Vulnerability management**
Keep your systems protected throughout their lifecycle.



➤ **Identity and access management**
Control who and what can access your systems and data.

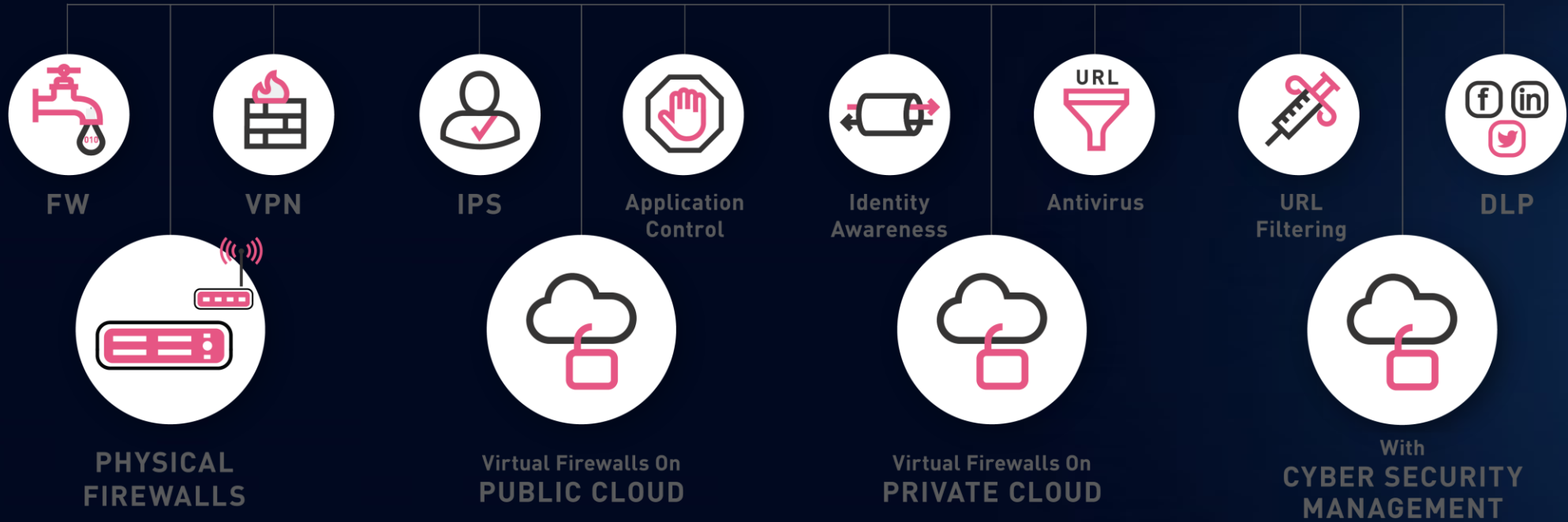
➤ **Data security**
Protect data where it is vulnerable.

➤ **Logging and monitoring**
Design your systems to be able to detect and investigate incidents.

➤ **Incident management**
Plan your response to cyber incidents in advance.

➤ **Supply chain security**
Collaborate with your suppliers and partners.

Corollaire : Comment ne PAS sécuriser sa Supply Chain



Nouveaux Problèmes = Nouveaux Processus



MOABI



National Cyber Security Centre
a part of GCHQ

10 Steps to Cyber Security

This collection is designed for security professionals and technical staff as a summary of NCSC advice for medium to large organisations. We recommend you start by reviewing your approach to risk management, along with the other nine areas of cyber security below, to ensure that technology, systems and information in your organisation are protected appropriately against the majority of cyber attacks and enable your organisation to best deliver its business objectives.

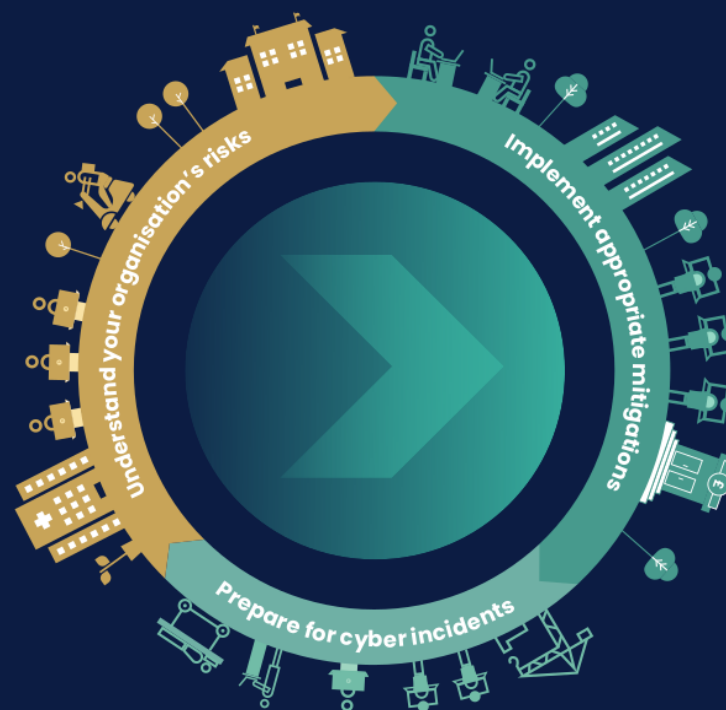
➤ **Risk management**
Take a risk-based approach to securing your data and systems.

➤ **Engagement and training**
Collaboratively build security that works for people in your organisation.

➤ **Asset management**
Know what data and systems you have and what business need they support.

➤ **Architecture and configuration**
Design, build, maintain and manage systems securely.

➤ **Vulnerability management**
Keep your systems protected throughout their lifecycle.



➤ **Identity and access management**
Control who and what can access your systems and data.

➤ **Data security**
Protect data where it is vulnerable.

➤ **Logging and monitoring**
Design your systems to be able to detect and investigate incidents.

➤ **Incident management**
Plan your response to cyber incidents in advance.

➤ **Supply chain security**
Collaborate with your suppliers and partners.

Dessine moi le cycle de vie d'un logiciel ...

x



- *Théorème de Magritte*



Astuce: Ceci n'est pas un Cycle (!!)



RETEX : SECURISER SALESFORCE

SSDLC : Secure Software Development Life Cycle



- *Microsoft (2001, source: microsoft.com)*



Après une itération, on boucle et on recommence : **Progrès continu**

SSDLC : Secure Software Development Life Cycle



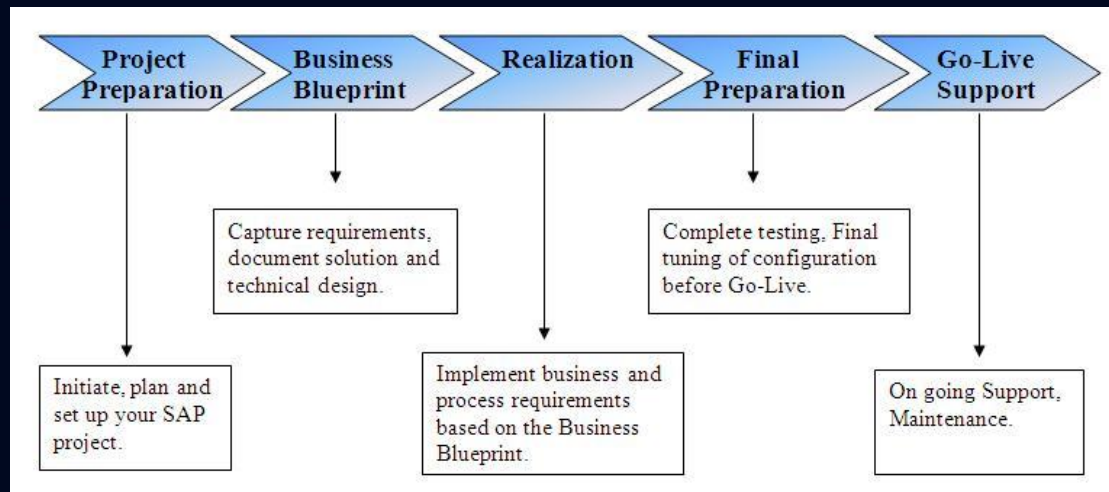
- *Salesforce*



Après une itération, on boucle et on recommence : **Progrès continu**

SSDLC : Secure Software Development Life Cycle

- *SAP (source: <https://blogs.sap.com>)*

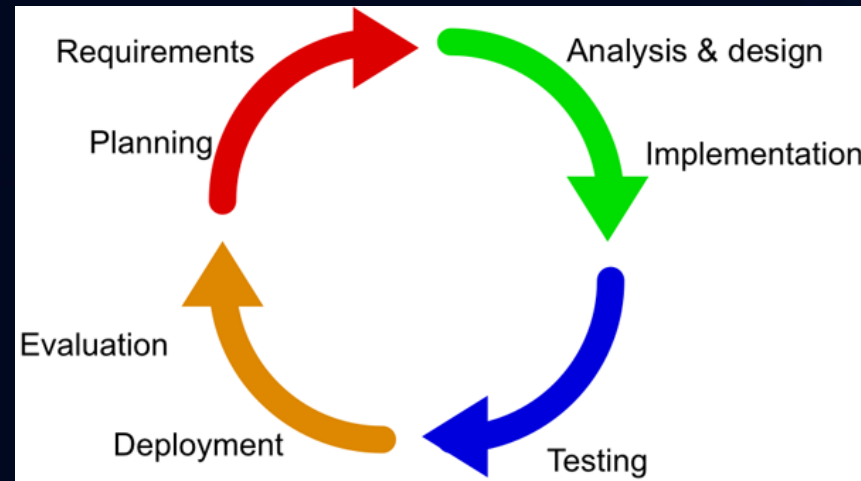


Après une itération, on boucle et on recommence : **Progrès continu**

SSDLC : Secure Software Development Life Cycle



- *IBM (source: <https://developer.ibm.com/articles/cc-cognitive-big-brained-data-pt2/>)*



Après une itération, on boucle et on recommence : **Progrès continu**

SSDLC : Secure Software Development Life Cycle



- *Apple (source: Apple.com)*



Après une itération, on boucle et on recommence : **Progrès continu**



SECURISER LA CHAINE LOGISTIQUE

Sécuriser la chaîne logistique (externe)



- *Les challenges*

- Pas d'accès au code source
- Les développeurs ne sont pas nos salariés
- Big code : la quantité de logiciels est exponentielle
- Les auto diagnostics des vendeurs sont fatalement biaisés
- Pas de visibilité sur les processus fournisseurs

Sécuriser la chaîne logistique

x



- *Solution : Due Diligence des logiciels fournis, release après release*



**TRUST BUT
VERIFY**

Après une itération, on boucle et on recommence : **Progrès continu**

Sécuriser la chaîne logistique



- *Bénéfices*

- Les fournisseurs font partie de la chaîne de valeur de l'entreprise.
- Investir sur ses fournisseurs et créer un écosystème de confiance (souverain ?) participe à augmenter la valeur de l'entreprise
- Les fournisseurs ne font pas exprès de livrer des logiciels non sécurisés : les aider à monter en compétence
- Responsabilité partagée



RETEX : DETECTION DE MALWARES PAR SANDBOXING

Détection de Ransomwares



- *Stagiaire (Ingénieur des Mines, 3mois)*

Sandboxing : Detection automatique de maze, megacortex, revil, ryuk, wannacry, etc.

```
{
  "Version of the Analyzer": "1.5.16",
  "Scan_Time": "2021-07-09 14:11:39",
  "Installer_name": "97D3C7CB2E8159FCB0AC0783611B.EXE",
  "Installer_files": [
    { "path": "C:\\Users\\Moabi\\Desktop\\CANARY1.PDF", "status": "deleted" },
    { "path": "C:\\Users\\Moabi\\Desktop\\CANARY1.PDF.IE4m", "status": "added" },
    { "path": "C:\\Users\\Moabi\\Desktop\\CANARY2.DOCX", "status": "deleted" },
    { "path": "C:\\Users\\Moabi\\Desktop\\CANARY2.DOCX.jgbVpg", "status": "added" },
    { "path": "C:\\Users\\Moabi\\Desktop\\CANARY3.PDF", "status": "deleted" },
    { "path": "C:\\Users\\Moabi\\Desktop\\CANARY3.PDF.RfAe4m", "status": "added" },
    { "path": "C:\\Users\\Moabi\\Desktop\\CANARY4.PPTX", "status": "deleted" },
    { "path": "C:\\Users\\Moabi\\Desktop\\CANARY4.PPTX.RfAe4m", "status": "added" },
    { "path": "C:\\Users\\Moabi\\Desktop\\CANARY5.PDF", "status": "deleted" },
    { "path": "C:\\Users\\Moabi\\Desktop\\CANARY5.PDF.ZIHQ35a", "status": "added" },
    { "path": "C:\\Users\\Moabi\\Desktop\\DECRYPT-FILES.txt", "status": "added" }
  ],
  "Certificates": [],
  "Vulnerabilities": [
    { "path": "C:\\Users\\Moabi\\Desktop\\CANARY1.PDF", "CWE": "506", "comment": "The application contains code that appears to be malicious in nature. Potential ransomware attack.", "impact": "10" },
    { "path": "C:\\Users\\Moabi\\Desktop\\CANARY2.DOCX", "CWE": "506", "comment": "The application contains code that appears to be malicious in nature. Potential ransomware attack.", "impact": "10" },
    { "path": "C:\\Users\\Moabi\\Desktop\\CANARY3.PDF", "CWE": "506", "comment": "The application contains code that appears to be malicious in nature. Potential ransomware attack.", "impact": "10" },
    { "path": "C:\\Users\\Moabi\\Desktop\\CANARY4.PPTX", "CWE": "506", "comment": "The application contains code that appears to be malicious in nature. Potential ransomware attack.", "impact": "10" },
    { "path": "C:\\Users\\Moabi\\Desktop\\CANARY5.PDF", "CWE": "506", "comment": "The application contains code that appears to be malicious in nature. Potential ransomware attack.", "impact": "10" }
  ],
  "Status": "Success"
}
```

INSTALLER CONFIGURATION KPI PASSED

INSTALLER CERTIFICATES

FRIENDLY NAME	THUMBPRINT	SUBJECT	NOT BEFORE	NOT AFTER	ALGORITHM
	9028EDF8D44509852119016D02183938AC34	CN=evil.com, O	6/29/2021 8:10:43 AM	12/31/2039 3:59:59 PM	SHA1RSA

INSTALLER FILES

PATH	STATUS
C:\ProgramData\Microsoft\Windows Defender\Scans\History\Results\Resource\12BE86493-sEEB-4976-9A79-95E03F8215d4	+ ADDED
C:\ProgramData\Microsoft\Windows Defender\Scans\History\Store\48BD1617DE3198926CAB1A7998B1c0	+ ADDED
C:\ProgramData\Microsoft\Windows Defender\Scans\History\Store\BC67886C6f4D4237A446ED447F62d18B	+ ADDED
C:\ProgramData\Microsoft\Windows Defender\Scans\History\Store\F30F00a2a0E27C0245A682D7776485	+ ADDED
C:\ProgramData\USOShare\Log\System\MoJocCoreWorker.g28864f0-4c38-49f4-8bb3-48e3122a6ee.s.etl	+ ADDED
C:\ProgramData\USOShare\Log\System\MoJocCoreWorker.g482c27f-46e3-45ba-b3ce-f296de37b12c.s.etl	- DELETED
C:\ProgramData\USOShare\Log\System\NotificationXBroker.44782177-95bf-4c67-828a-9aa718364540.1.etl	+ ADDED
C:\ProgramData\USOShare\Log\System\UpdateSessionOrchestration.158312c0-8b41-4e08-b239-0d5b7b2d5e4.s.etl	+ ADDED
C:\ProgramData\USOShare\Log\System\WuProvider.04d2f08-fa01-4b22-8936-99b3ab9d6105.1.etl	+ ADDED
C:\ProgramData\USOShare\Log\System\WuProvider.81d95f93-8320-4843-931b-689dfacc57.1.etl	- DELETED
C:\ProgramData\USOShare\Log\User\Notifications\Xs8cf550-d870-4d9c-8f2e-b083be1f4ee1.s.etl	+ ADDED
C:\Users\All Users\Microsoft\Windows Defender\Scans\History\Results\Resource\12BE86493-sEEB-4976-9A79-95E03F8215d4	+ ADDED

Bloquer tous les Ransomwares de manière générique

x



- ~~*Antivirus, EDR, XDR, application blacklisting*~~

- *Application Whitelisting*

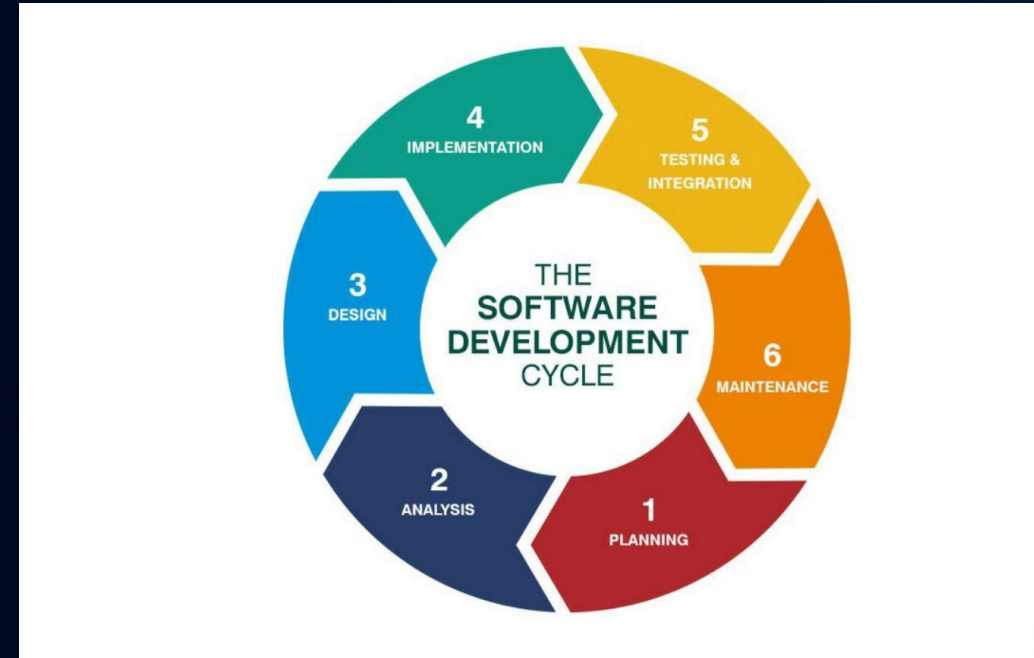
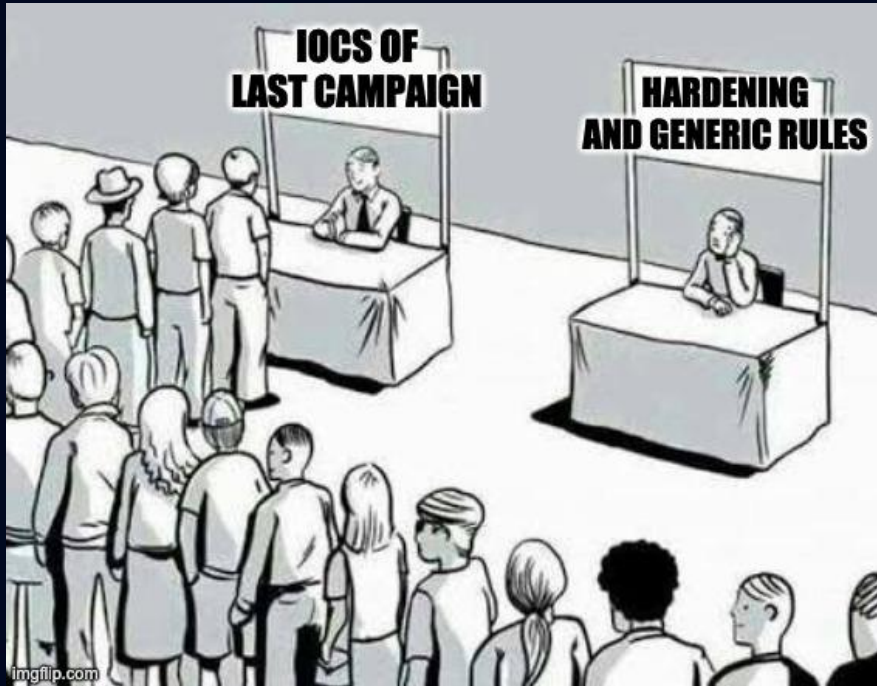
Absolument possible : implémenté chez Salesforce



x

CONCLUSION

Conclusion : nouveaux processus + progrès continu



Après une itération, on boucle et on recommence : **Progrès continu**



MOABI

Merci pour votre invitation

jonathan.brossard@moabi.com

