# 1000100110613D0110016T



# MOABI

Supply Chain : Software Continuous Improvement

Control Software delivery

Measure Software Security via KPIs

Facilitate Continuous Software Improvement

TNRP deployment - 02/02/2022

Jonathan.brossard@moabi.com



## **Moabi Solution** Automated security audits for product and supply chain cybersecurity







#### **KEY PERFORMANCE INDICATORS**

Define a security policy across the Moabi platform thanks to Key Performance Indicators

CLOBAL SCORE Objective between 0 and 100 2 75	LEGACY Objective between 0 and 10	COMPLIANCE Objective between 0 and 10	HARDENING Objective between 0 and 10 8
CRYPTOGRAPHY Objective between 0 and 10	VULNERABILITIES Objective between 0 and 10	ZERO DAYS Objective between 0 and 10	MALWARE Objective between 0 and 10
CRYPTOGRAMY CRYPTOGRAMY LEGACY ULINERABILITIES COMPLIANCE	rdennic RDENNIC	0 1 2 3 4 5 6 7 8 9 10 0 1 2 3 4 5 6 7 8 9 10 0 1 2 3 4 5 6 7 8 9 10 0 1 2 3 4 5 6 7 8 9 10 2 2 3 4 5 6 7 8 9 10 MALWARE 0 1 2 3 4 5 6 7 8 9 10 MALWARE 0 1 2 3 4 5 6	0       1       2       3       4       5       6       7       8       9       10         0       1       2       3       4       5       6       7       8       9       10         0       1       2       3       4       5       6       7       8       9       10         0       1       2       3       4       5       6       7       8       9       10         7       8       9       10



i

## Moabi : KPI and criteria to improve product security 7 metrics 7 steps



	odays✓Detect potential oDays and class of vulnerability with symbolic execution (taint analysis)Compliance✓API calls : Enforce rules and standardsSecurity Standards✓Replace dangerous/deprecated functions		
	<b>Cryptography</b> Strengths of Ciphers	<ul> <li>Ensure privacy-by-design and GDPR</li> <li>Calcat strange sink are</li> </ul>	
	<b>Hardening</b> Defense in Depth	<ul> <li>✓ Activate all defense in depth features</li> <li>✓ Reduce Attack Surface</li> </ul>	
	<b>Legacy</b> Technical Debt	<ul> <li>Identify supported OS, architecture, toolchains and compilation dates</li> </ul>	_
	<b>Vulnerabilities</b> Known CVEs	<ul> <li>Spot existing CVEs with severity / remediation prioritie</li> </ul>	es
Known Ma	Malware alware or probability of	✓ <b>Detect Malware or probability of an unknown Mal</b>	ware

# **Baseline : Status and Evolution** Follow up Security posture changes









#### Status and cybersecurity posture

- Global score
- Per metric

Compare new posture

2

- Changes between releases
- Impact of continuous improvement

## **USE CASE** Product security and SSDLC





1 Selection of components for Integration



Development and CI/CD integration:

- Assess and test security of components (OSS, subsystems, ad'hoc development)
- Challenge suppliers to raise cybersecurity awareness and posture

- Assess new build
- Amend and correct identified issues (compliance, hardening, cryptography, CVEs....)

Before deployment and launch :

3

- Assess product deliverables : Application + OS + Firmware
- Check compliance with requirements and give assurance to customers

# **Product offering**



SaaS	SaaS - Pod	Appliance	Appliance - Air gap
Public CLoud	Dedicated HW IP Whitelisting	On premise Dedicated HW	On premise Dedicated HW No network connection
	Single Tenant Moabi and Customer Admin	Customer Admin	Customer Admin
<b>Subscription Model</b> License with Maintenance and Support	<b>Subscription Model</b> License with Maintenance and Support	<b>Subscription Model</b> License with Maintenance and Support	<b>Subscription Model</b> License with Maintenance and Support Updates with USB keys
Fast Start	Dedicated Resource on Cloud	Full Ownership	Highest Confidentiality and Privacy Level

# Multi x Architecture x Environment x Format



OS	CPU	File Format / Archive / Disk Image
Microsoft	Intel x86 / Intel x86 – 64	File format :
iPhone/iPad (iOS)	ARM 32 / Aarch64 / including ARM Thumb/Thumb2.	ELF, PE, COFF, a.out, Mach-O, Microsoft COM. Archive :
Mac OS / OSX	MIPS / MIPS64	APM, ARJ, CAB, CHM, Cpio, DEB, ISO (ISO 9660),
Android	Sparc 32 / Sparc 64	LZH, LZMA, MSI, NSIS (NullSoft installer), RAR, RPM, XAR, tar, .tar.bz2, .tb2, .tbz, .tbz2, .tz2, .tar.gz,
GNU Linux OpenBSD/FreeBSD/ NetBSD/Solaris	PowerPC Risc V	.taz, .tgz, .tar.lz, .tar.lzma, .tlz, .tar.lzo, .tar.xz, .txz, .tar.Z, .tZ, .taZ, .tar.zst, .tzst , 7z, BZIP2, GZIP, XZ, ZIP,
	Motorola 68000	Z, self-extracting executables.
VxWorks	Languages	Disk image format:
RTOS	C / C++	Ext2, Ext3, Ext4, SquashFS, JFFS2, Ubiquity, Yaffs, fat/vfat, NTFS, HFS, CramFS, VHD, UDF, DMG
	GO	(Apple Disk image), Vmware vmdk, WIN (Windows Imaging Format)
	ADA / Cobol / Fortran	intraging Format/
		Android apk and iOS ipa applications.

# **Conclusion Cybersecurity is a Process**



Continuous improvement





Procure secure 3<sup>rd</sup> party products



**Risk assessment and compliance process** 

## 0100001001100100100100100100100



## THANK YOU

#### More information

jonathan.brossard@moabi.com

