:WHIPLASH

from Guidelines SBOM Turning Playbooks Into Books Text

requirements VEX and SBOM s'2023 to guide reference A

Contents of Table

.Whiplash

- attestation software Secure 1: Section required now Automation

other or military be it whether ,government US the with work to looking companies Private .security national of matter a as deliver they products the for responsibility take must ,agencies

responsibility take companies how of example one is Form Attestation Software Secure s'CISA and security its to attesting ,government US the to provided be will that code own their for .activities government disrupting without operate to capability

security to attention great pay only not suppliers that demand form this in listed steps four The into dives one part While .so do to automation use but ,chain supply software the throughout happens what on expand four and ,three ,two parts ,environments secure in code developing .customers with share to enough developed is code the once

,reviews necessary for allow systems management vulnerability and SBOM Automating
while resources existing on strain reduces significantly It .approvals and ,updates
.compliance to time and market to time improving

code trustworthy Sourcing #2:

supply code source trusted maintain to effort faith-good a made has producer software The :by
chains

A
processes comparable or tools automated Employing

third of security the address to steps reasonable includes that process a Establishing
B
;vulnerabilities related manage and components party

.enough not is SBOM standalone a ,bill Omnibus 2022 December the in saw we like Just
the that ensure and suppliers their from SBOMs date to up request must Manufacturers
.vulnerabilities any carry not does devices embedded in used being code

and products their in code the for responsible ,ever than more ,now are Manufacturers

from avoided be must vulnerabilities ,snuff to up is product final the sure make To .devices .stages building through design the

code component device of history Known #3:

party-third and internal for data provenance maintains producer software The “states form The “.software the into incorporated code

the ,product ready-market a to components software individual from develops software As ,requirements form the meet and this address To .grow dependencies and complexities of list .device or product a inside software all regarding information detail should SBOMs

automation through resilience and Responsibility #4:

check that processes comparable or tools automated employed producer software The :states form The .vulnerabilities security for

A

at and basis ongoing an on operate processes these ensured producer software The .releases update or ,version ,product to prior ,minimum a

security discovered address to process or policy a has producer software The

B

.release product to prior vulnerabilities

,accepts and program disclosure vulnerability a operates producer software The

C

.fashion timely a in vulnerabilities software disclosed addresses and ,reviews

must also you but ,activities related-compliance of track keep to have only not you that means This

.mitigationthroughdiscoveryinit

ialfrom,vulnerabilitiesaddressthatpoliciesinternaldemonstrate

Platform Security Product single a within requirements regulatory and internal Meeting
.lifecycle product full the throughout redundancies out cuts

security product conducting and SBOMs date to up maintaining in part key a is Automation
can platform security product a ,truth of source single a as SBOM the using By .activities
.databases threat and vulnerability against referenced-cross when vulnerabilities identify

,vulnerabilities identifying automatically for process a have must manufacturer the ,addition In
,community developer the from vulnerabilities discovered newly addressing and
acknowledging
.(4 section see (report other or VEX a through them disclose and

Playbook The

to much too simply are requirements form the meet to needed tasks required the of Many
business all across run that variations and ,models ,products the all With .manually achieve .bear
to team any for great too burden a becomes management SBOM ,units

that process automation tuned-fine a adopt can field regulated any in operate that Organizations
single a in document VEX relevant a produces and ,SBOMs updates ,vulnerabilities for scans
ability the ,out on here From .documentation compliance for activity recording while all ,workflow as act
will repositories SBOM maintained properly via transparent remain to
.globally devices to spreading and contracts government with starting ,baseline a

types SBOM 6 s'CISA 2: Section

device full ,code trustworthy requires 1, Section in discussed as ,Form Attestation s'CISA While
.insights actionable into information that turn to process automated an and ,history meet to it
packaging and information this managing of way own their had has company each continuously are

organizations setting-standard and governments ,demands compliance .SBOM the adopting towards manufacturers steering

only was that SBOM an have you if ,all After .concept new a not is SBOMs Maintaining ,However .stage later a at truth of source a as viewed be exactly t'won it ,design at updated SBOM true for potential the holds that idea an is SBOMs of types categorizing and standardizing

seamlessly integrated be can materials of bill software s'component a where ,interoperability .system greater the into

of stages 6 into SBOMs down broke agency cybersecurity the ,CISA by out put draft recent a In .limitations and benefits with along entail should each what describing ,lifecycle s'product a

of Bill Software of Types :draft s'CISA in appears as written are 1-6 type SBOM in items Listed :Note Documents) SBOM (Material

,documents evolving-ever are SBOMs .recreated or to added continuously are and ,step next the

SBOM

entering before reviewed ,step each with approved being

Design - 1 Type SBOM

Definition

software planned ,intended of SBOM
included with product or project
not may which of some (components
.artifact software new a for) exist yet

Description Data

.use developer

know to need pros ProdSec
design a from derived Typically
.concept initial or ,RFP ,specification

Benefits

components incompatible Highlight -
or purchase licensing of ahead
.acquisition

recommended or approved Defines -
for list component included

Limitations

.generate to difficult very be may This -

as detail much as identify to Unlikely - .types SBOM
other in found

intend they that components software of list hypothetical a drafting begin should Companies
and vulnerabilities understand to simulated be can it ,compiled Once .project future a for use to
.development during required be will that techniques mitigation

component one for complications related-vulnerability or compliance many too find may Teams
.later headaches of hours countless them saving ,another using by solved is that

many changes to prone is that process intensive resource a be may it ,sounds this as great As
.unreliable and vague SBOM this making ,over times

Source - 2 Type SBOM

the into view a provide Can -
of hierarchy / tree dependency
.components included the

Definition

the from directly created SBOM
source ,environment development
dependencies included and ,files
.artifact product an build to used

know to need pros ProdSec

Description Data

software from generated Typically
,tooling) SCA (analysis composition
.clarifications manual with

Limitations

which (components highlight Can never that)
vulnerabilities have might deployed in out
compiled are or run .code

,ecosystem/language on Depending
or ,plugin ,runtime include not may appserver like
,components dynamic .libraries platform or

other to references require May .completeness for
SBOMs

Benefits

access without visibility Provides -
.process build the to

of remediation facilitate Can -
.source the at vulnerabilities

While .environment development the from taken is that document transitory a is SBOM Source A .status current s’project the of snapshot a only is it ,process build the into visibility allows this

with ,tooling) SCA (analysis composition software from generated typically “:states draft The guide internal general a as used be to likely more is SBOM its that means” clarifications manual .future the in used be can that something than

product allows it that is ,SBOM phase-design the to similar ,document of type this of benefit The it ensuring – days early s’project the in vulnerabilities remediate and identify to teams security .future the into threats any carry t’doesn

Build - 3 Type SBOM

Definition

the of part as generated SBOM
to software the building of process
.,g.e (artifact releasable a create
data from) package or executable
,dependencies ,files source as such
process build ,components built
.SBOMs other and ,data ephemeral

Benefits

the that confidence Increases -
the of representation SBOM
due correct is artifact product
the during available information to
Continuous or/and build
Deployment Continuous/Integration
.processes) CD/CI(

more into visibility Provides -

.code source just than components

signing enabling by trust Increased -
by artifact product and SBOM the of
.workflow build same the

know to need pros ProdSec

Limitations

build the change to have Potentially - .SBOM this
generate to process

build the on dependent Highly - is build the which
in environment
.executed

indirect capture to difficult be May - .dependencies
runtime or/and

correct the contain not May - linked dynamically of
versions
be may they as (dependencies
on depending runtime at replaced
.(ecosystem/language

Description Data

build a of part as generated Typically integrated
of consist May .process Source and Build
intermediate
artifact release final a for SBOMs
.SBOM

bill software usable a of aspects important many contain to enough mature are SBOMs 3 Type
the in critical are They .device the of life the throughout remain to likely are that materials of .milestone
crucial this at vulnerabilities identify they as process development
brings also It .dependents into transparency improve to process build the on relies stage This
source the on relying only not re'we as ,components hidden previously into visibility greater .code

into fits it how and itself of unsure bit a – adolescence its in still is SBOM This ,hand other the On
runtime or indirect capture to difficult be may it ,CISA to According .it around world the .future the in used
be may that versions software the reflect t'doesn and dependencies

Analyzed - 4 Type SBOM

,packages ,executables .,g.e (artifacts
(images machine virtual and ,containers
generally analysis Such .build its after
some In .heuristics of variety a requires
to referred be also may this ,contexts
.SBOM" party rd3 "a as

Definition

of analysis through generated SBOM

.tools creation type SBOM other by

know to need pros ProdSec

Description Data

analysis through generated Typically .tooling party rd3 by artifacts of

Benefits

active an without visibility Provides - as such ,environment development .artifacts firmware legacy

build the to access need not Does - .process

from data SBOM verify help Can - .sources other

missed dependencies hidden find May -

Limitations

,errors ,omissions to prone be May - is tool the if approximations or recognize or decompose to unable .precisely components software the

or heuristics on depend May - .factors risk specific-context

be can SBOM analyzed an ,development of stage final its to closer moves project the As as such artifacts and analysis through picture holistic a gain to party third a by optimized can it since beneficial is This .images machine virtual and ,containers ,packages ,executables .earlier detected not were that dependencies hidden find and SBOMs earlier validate

runtime and deployment identifying begin to these review should specialists security Product

.fleeting is relevance its that know but risks

Deployed - 5 Type SBOM

components software Highlights
other including ,system a on installed
components system and configurations
.application an run to used

know to need pros ProdSec

Definition

of inventory an provides SBOM
.system a on present is that software
other of assembly an be may This
of analysis combines that SBOMs
examination and ,options configuration
potentially (a in behavior execution of
.environment deployment) simulated

Description Data

the recording by generated Typically information
configuration and SBOMs installed been have that
artifacts of .systems on

Limitations

and install changing require May - .generate to
processes deploy

the reflect accurately not May - ,environment
runtime s'software
in reside may components as
.code inaccessible

Benefits

professionals security product to familiar are that SBOMs seeing begin we 5, Type SBOM With
begin can SBOM the ,system the in present s'that software of inventory an on Based .today .field
the in product the of use true the examining and variations configuration in taking

in common become mitigations and updates component as ,dynamic these keep to critical s'It the
reflect accurately not may "SBOMs these that warns draft the ,addition In .days early the ".code
inaccessible in reside may components as ,environment runtime s'software

Runtime - 6 Type SBOM

Definition

through generated SBOM
the running system the instrumenting
components only capture to ,software
as well as ,system the in present
dynamically or outs-call external
,contexts some In .components loaded
an as to referred be also may this
.SBOM" Dynamic "or" Instrumented"

Benefits

understand to visibility Provides -
is system the when use in is what
dynamically including ,running

external and components loaded .connections

information detailed include Can - are components whether about .used are parts what and active

record to system a with interacting

running a in present artifacts the been have that or/and environment .executed

know to need pros ProdSec

Limitations

analyzed be to system the Requires - require may which ,running while .overhead additional

may information detailed Some - system the after only available be until time of period a for run has has functionality complete the .exercised been

Description Data

tooling from generated Typically

.come to years for updates experience will product this ,SBOMs dynamic of age the Entering up remain must SBOM the ,memory distant a deployment and it behind far development With third ,versions ,outs-call external ,components latest the reflect continuously and date to .components loaded dynamically and ,tools party

operations time-real interrupting without SBOM this access to have will pros security Product full s'product the of representation digital a ,™Twins Digital Cyber on Relying .device the of against conducted be to tests allowing by stress this alleviate help can ,software and firmware .offline it taking of instead device whole the of replica digital a

must a is Automation

of thousands possibly and hundreds the for SBOMs of types varied six managing of idea The .overwhelming seems products across variations

work to need teams security product ,means this what down break truly to are we if ,However reflected be will approach first-security a ensure to project a of start the from developers with completes that machine a out plan to need developers ,beginning very the From .SBOM every in their on rely should professionals security Product .reliably functioning while hand at task the this on exist threats what understand ,SBOMs the scan to platform management vulnerability anything before recommendations alternative or mitigations suggest and ,device hypothetical

.forward moved is

a between difference the be can SBOMs ,field the in vulnerabilities managing When SBOM boosted who ,LG by recognized was This .mitigation missed a and response rapid address better to vulnerabilities new of 50% triaged automatically and X7 generation .needs security product

security industrial and automotive guides IMDRF 3: Section

of Bill Software for Practices and Principles IMDRF from are below sections and Quotes :Note .Cybersity Device Medical for Materials

of pieces allow that dependents and ,software ,versions component the all of list a are SBOMs .life a save and ,vehicle a protect ,on lights the keep securely to silicone and ,metal ,polymers ,developers of entourage its without much do t'can ,is it that socialite the being ,SBOM the However .others and ,documents compliance ,reports VEX ,teams PSIRT ,experts security product

a also is it ,However .to referred commonly s'it as ,'ingredients of list 'a is SBOM the ,own its On their protecting better into teams security product calibrate to used be can that truth of source .devices

Practices and Principles their out put) IMDRF (Forum Regulations Device Medical International The an offering– world medical the Cybersecurity Device Medical for Materials of Bill Software for and makers policy that doubt no s'There .sectors industrial and automotive the for opportunity .implementation and reactions on eye close a keeping are organizations standards

work for in punch SBOMs

.organizations to loss significant prevent to ability the is SBOMs for cases use best the of One is ecosystem medical The .on lights the keep to ability of loss a and ,reputation of loss ,life of Loss of support in uptime ensure) MDMs (s'Manufacturer Device Medical .mind in uptime with designed business the consider also must) HCPs (Providers Care Health .care for them on rely who people the .care on have will it impact the to addition in breach a of implications

Medical for Materials of Bill Software For Practices and Principles s'IMDRF the ,reason this For s'HCP and s'MDM the both from SBOMs for cases use the approaches Cybersecurity Device .perspective

Medical
Industrial

Automotive

Device Medical for Materials of Bill Software for Practices and Principles s'IMDRF The .field the in used be can SBOMs how into industries other for beacon a as acts Cybersecurity

lifecycle product total the throughout MDM by used be also may SBOMs ",states document The .decommissioning and support of end through stage design the from device medical a of) TPLC(stance security proactive more a take to organizations by used be can SBOMs ,Holistically SBOM an for cases use of examples provides section This .device a of cycle life entire the across :for tool adjunct an as

Management Incident management Vulnerability management Risk

Management Risk

Perspective s’MDM

house-in own their beyond look to have will IMDRF the by trusted be to want who Manufacturers software including ,chain supply software full the from information include to teams development and ,stacks IP / TCP ,systems operating ,libraries :include can dependencies These .dependencies .system a on software the run to required components other

:as such ,activities security product with assist to on aligned be should SBOMs that highlight also They

evaluation Risk -

control Risk -

monitoring and assessments Vulnerability -

future the into uptime ensure to management risk Lifecycle -

perspective s’HCP

their and devices medical of risks cyber and operational the understand adequately to need HDOs .components software

:should teams security product ,SBOM an from obtained information the With

SBOMs to linked inventory device Create -

vulnerabilities including assessments risk ongoing Conduct -

possible wherever devices medical to access manage and Identity -

communications device Monitor -

misconfigurations for device Monitor -

(OSS ,COS ,OS (components unsupported for SBOMs Monitor -

program update and management patch a Implement -

(.etc ,Whitepapers Security 2,MDS (artifacts security other and elements data SBOM manage and Ingest -

.precondition a as SBOMs date to up request must who ,procurement with begins process whole This can and another from device one purchasing of cons and pros full the weigh to purchasers allow will This .vulnerabilities minimize to take can they steps on manufacturer a with discussion a begin

Management Vulnerability

Perspective s’MDM

their to threats emerging compare can teams security product ,truth of source a as SBOM an Having the explain to created be then can document VEX A .™Twin Digital Cyber a through components field-in (4. section in requirements VEX CISA the in this on More (.recommendations mitigation and issue

Officers Security Product Chief for allowing ,multiplier force a as work can automation ,more s’What flexible or fixed a on ,variants their and products all across catalog SBOM entire their review to) CPSOs(.schedule

Perspective s’HCP

attacks cyber of impact the with familiar too all become have facilities their and providers care Health OT or IT secure a on dependent be not should security product ,reason this For .organizations their to .fold the into security product brings that approach holistic a on but ,alone system

they should consequences fatal potentially with entities own their as protected be to need Products using be should organizations that ways four identifies IMDRF ,reason this For .inoperable become :SBOMs

emerge they as vulnerabilities new against assets s’organization healthcare of Monitoring -

mitigations interim Driving -

management vulnerability Lifecycle -
activities security Proactive -

Management Incident

Managing .quickly act to need will HCPs and MDMs both ,discovered is incident an how of
Regardless quickly act to teams support enables lifecycle product full the throughout and types all across SBOMs .made be to need decisions critical when

and ,correlation ,collection systematic the improves repository] SBOM [The “states document The incident
improves ultimately which events relevant-cybersecurity detect to information of evaluation “.handling

takeaway Key

after well even ,do can SBOMs what for foundation the lays it as sectors all for critical is guide This
outdated or inaccurate of days the– hear to all for shot warning a sends it ,more Even .deployment nice
“from mindset SBOM their switch leaders team security product that time s'It .over are SBOMs .“critical “to"
have to

,time some for agencies regulatory many by discussed been has adoption SBOM widespread While
into theory this put to first the be will facilities care health and manufacturers device medical for allow
will ,serves sector a else whoever or ,operators ,drivers ,patients to benefits The .practice .follow to
teams security product for book play a and ,design safer ,products reliable more

revision SBOM up tighten to team their amongst steps active is do to need manufacturers What
.timelines

SBOMs Beyond 4: Section

from directly taken is text point-bullet below the of much ,clarity of sake the For :Note
.documents VEX CISA

that likely s’it ,SBOM an compiling Once
.device the within exist will vulnerabilities
,risk high be will others ,critical be will Some
.irrelevant be will many and

that those as such ,vulnerabilities Irrelevant
specific a with coupled when present only are
was that one or use t'didn you component
,supplier a by code custom using mitigated
customer a to reported be to need still may
quickly can this ,automation Using .agency or
a of development the through achieved be
,CISA to according which ,document VEX
details and vulnerability the down break must
.it surrounding

.story whole the tell t'don alone ingredients the ,salad a Like
need salad the Does? contained be components the will How
?publish to warnings allergy any there Are? dressing a

Requirements VEX Minimum s'CISA

requirements Minimum

more or one holding object .statements provide

container a is document VEX A VEX

MUST document VEX A VEX one least at contain .statement

and metadata document .data other provide MAY

MUST document VEX A VEX required

should document VEX a what for foundation a lays and obvious quite are two first the While
.document VEX recognized-CISA a define will that details into dives one third the ,contain

Elements Data VEX

document VEX

product allowing ,points data multiple of up made is Metadata
"lines the between read "quickly to PSIRT and teams security
teams and developers While .SBOM Runtime or Deployed a
of types SBOM in metadata and statements VEX including
be should operators or owners device ,)Analyzed through
Design from (1-4 as premature or incomplete be may these
that remember should .risk assess to truth of source a
metadata Document

N statement VEX

statements and document VEX 18

1 statement VEX

2 statement VEX

Data Document

*VEX ,possible extent greatest the To "*should metadata document VEX ,CISA to According
,necessary and appropriate When .level document VEX the at maintained and defined is metadata
synthesized be MAY metadata document VEX .level statement VEX the at defined is metadata
VEX least at be MUST] updated_last_time_doc [,example for; metadata statement VEX from
derived or accurately MUST metadata document VEX .]updated_last_time_statement [newest the
as recent as ".statements VEX contained all to apply

and conventions naming the ,documents legal other many like just is means this What
the stating ,document that only to connected remain should information identifying
all to apply and ,updated was it time last the ,to relates it component the ,purpose
s'document .review to about is reader the that information following

minimum the ,bodies federal other and ,FDA ,CISA from seen ve'we that documents many Like recommended strongly and" MUST "as identified ,information required of mix a is information
."MAY "or" SHOULD "as appearing ,guidelines

29. page on covered you got ve'We? terminology much Too

[id_doc [ID Document

ID document one include Must -

any if contact of point a as is author the who state should ID This -
.questions has lifecycle product the throughout stakeholder

[id_doc [/] author [as identified be will This -

takeaway ProdSec

according ,Instead .stakeholders all to identity true their out give to have not does author The for ID naming a choose ,convention naming document own their create should they ,CISA to .signatures digital using cryptographically and ,themselves

/ [author [or] id_doc[/]author [be will followed be to convention the that recommended is It .[id_statement [/] id_doc[

[version_doc [Version Document

number version one least at include must document The -

;and change document new each with updated be and change must Version -

change incremental positive convey Must -

takeaway ProdSec

the as important as even and ID document the as important as is number version The ,attention needs that product exact the for beacon a as Used .document the within information on down cut and management vulnerability streamline will accuracy version document

.crisis of time a during remediation

[role_author [Role Author

author the of role the specify may document The -

,coordinator as such ,category identifying an use to choose may author The -
2.0. CSAF by defined as others or ,vendor ,user ,translator ,other ,discoverer

takeaway ProdSec

teams PSIRT as ,peacetime during useful most be will author the from authority of level The
.occur threat a should action of course best the deem teams security product and

[tooling [Tooling

VEX ,documents VEX generate that mechanisms automated or tools specify May -
.information VEX other or ,statements

takeaway ProdSec

,However .]role_author [contradiction acceptable an is report VEX the generate to tool a Using
.generated was document the how state must report VEX the

[issued_first_time_doc [issued first Timestamp

.issued first was document VEX the that time and date the provide must document VEX A

included all of] issued_first_time_statement [oldest the equal must] isued_first_time_doc[
.statements VEX

takeaway ProdSec

(1 Section (form attestation the to back goes document a of age the understand to able Being
.military and government US the for services provide who suppliers software by required is that
trustworthiness the determines also origins earliest its to document the back trace to able Being with line
in forward point that from updated continuously be then should It .document the of .[version_doc[

Statement VEX

[status [single a convey must that declaration a is statement VEX A -
.s]id_product [more or one for] id_vul [single a to applies that

.document VEX a within contained logically be must statement VEX A -

,is that ,document VEX one within only exist must statement VEX A -
.document VEX containing their to local logically are statements VEX

takeaway ProdSec

a into insight containing ,document VEX the of part is statement This
specific the to applies only and addressed being vulnerability specific
to teams allows confusion minimized This .addressed being vulnerability
is statement the if confirm to trying of instead hand at matter the on focus .vulnerability specific a to applicable

created be should] id_statement [- .[id_statement [/] id_doc [/] author [,example for ,information VEX other from generated

.[id_doc [of scope the within statements VEX of index an

Metadata VEX

the to specific be will ideally and document VEX the within be minimally may] id_statement [- **takeaway ProdSec** stored best is metadata VEX .statement VEX relevant

[id_statement [ID Statement

statement VEX metadata Statement

.document VEX a within statement VEX a identifies uniquely] id_statement [- .document VEX a within referenced specifically be to able be must statement VEX A - .[id_statement [one provide should statement VEX A - be may and namespaces] id_doc [and] author [the within

Status

details Vulnerability

details Product

was as Just .game the of name the is activities of records keeping ,]id_document [with as Just who ,is problem the what of record a have should statement the ,document entire the for done .from came statement the that document VEX original the reference and ,it addressing is

[version_statement [Version Statement

.statement VEX the of version the indicates] version_statement [-

.[version_statement [one provide must statement VEX A -

.change incremental positive convey clearly must] version_statement [-

.changes statement VEX the within content any when incremented be must] version_statement [-

.[version_document [to related be otherwise or from derived be may] version_statement [-

version which knowing ,versions document regarding above mentioned was what to Similar to relation in point reference a as especially ,important is read being s'that statement the of .[updated_last_time_statement [and] issued_first_time_statement[

[issued_first_time_statement [issued first Timestamp

.issued first was statement VEX the that time and date the provide must statement VEX A -

.[issued_first_time_doc [to related otherwise or from derived be may] issued_first_time_statement [-

[time_statement_impact [to related otherwise or from derived be may] issued_first_time_statement [-
.[time_statement_action [or

takeaway ProdSec

as issue first of time s'document the from different be may issue first s'statement A
Identifying .discovery similar another or date later a at found but related be may vulnerabilities over progress track to teams security product for timeline a creates statement issued first the .devices their across appearing are vulnerabilities new how understand and time

[updated_last_time_statement [updated last Timestamp

.modified last was statement VEX the that time and date the provide must statement VEX A -

.[issued_first_time_statement [to equivalent be initially must] updated_last_time_statement [-

[time_statement_impact [to related otherwise or from derived be may] updated_last_time_statement [-
.[time_statement_action [or

_impact [recent most the than newer or to equivalent be must] updated_last_time_statement [-
.[time_statement_action [or] time_statement

takeaway ProdSec

information that ensuring ,statement VEX the of iteration each with updated be should This needed without used be to ready and date to up is teams maintenance or PSIRT by pulled .statement date to up an is it confirm to on later verification

sea digital a in component small A

pre created are that SBOMs Unlike .product whole a surrounding VEX a for guidelines the are Below a

w
it
hi
n
r
el
e
v
a
n
c
e
s'
v
ul
n

erability the towards point to able be must SBOMs stage-later, deployment

.system product greater

the ,statements VEX and documents VEX of statements" should "and ,"must ","may "the to Similar .information below the contain will details product

details Product

.statement VEX a in components or products the describes and identifies details Product -

more or one include may and] id_product [more or one include must details Product -
.[id_subcomponent[

.identifiers known-well and existing use should] id_subcomponent [and] id_product [-

.identifiers SBOM existing reference should] id_subcomponent [and id_product [-

current and reasonable to conform should] id_subcomponent [and] id_product [-
.construct" version/product/supplier "a follow ,example for ,conventions

,versions ,IDs commit ,hashes ,URLs ,URIs be may] id_subcomponent [and] id_product [-
.system identification other any or ,ranges date ,dates ,ranges version

.[author [the by created arbitrarily be may] id_subcomponent [and] id_product [-

:example for ,components or products of sets specify may] id_subcomponent [and] id_product [- supplier a
by owned component or product Every -
line product or family product A -
ranges Version -
branch specific A -

[id_product [identifier Product

.to applies] status [and] id_vul [that component or product the identify must] id_product [-

:of one least at specify MUST and components or products of set a specify may] id_product [-
[id_subcomponent [-
(product a of component-sub a often (component A -
assembled good final a ,example for ,product A -
family or line product a ,example for ,components or products of set A -
(supplier the from components or products all of set the indicating (supplier A -

[id_subcomponent [identifier Subcomponent

with associated subcomponents for identifiers more or one include may statement VEX A - .details
vulnerability

.[id_vul [to respect with] id_product [of] status [the asserts statement VEX A -

.[id_product [in included is] id_subcomponent [that convey also may statement VEX A -

_product [while] id_vul [by" affected "is] id_subcomponent [that convey to is case use VEX common A - .[id_vul
[by" affected_not "is] id

with associated is] id_product [if particularly ,]id_product [from derived be may] id_subcomponent [-
.dependencies convey that references other or SBOM

.[description_vul [or] id_vul [from derived be may] id_subcomponent [-

[supplier [Supplier

.[id_subcomponent [or] id_product [of] supplier [the identify should details Product -

.applies] supplier [which to] id_subcomponent [or] id_product [the indicate clearly must] supplier [- :example
For
[id_product [/] supplier [-
[id_subcomponent [/] supplier [-

details Vulnerability

.statement VEX a in vulnerability the about information provide and identify details Vulnerability -

.statement VEX a in vulnerability the identifies] id_vul] [id_vul [identifier Vulnerability - .[id_vul [one specify must statement VEX A -

Global the ,CVE :as such identifiers known-well and ,available readily ,existing use SHOULD] id_vul [- that expected is It .system identification vulnerability s'supplier a or ,)GSD (Database Security .VEX from separately maintained and to external are systems identification vulnerability

.URLs or URIs be may] id_vul [-

A] description_vul [Description 2.6.2 .]author [the by created be MAY and arbitrary be may] id_vul [- .[id_vul [to corresponds that] description_vul [one reference or include must statement VEX

VEX to available made or statement VEX the in included be either must] description_vul [- .(URL a through ,example for (consumers

takeaway ProdSec

be can it if valuable only is ,statements and documents for necessary as such ,Documentation common use must teams ,happen to this for order In .parties-third by digested and shared easily .available readily reports VEX the make and identifiers GSD or CVE as such ,references

in updated be can it so online available report VEX dynamic and living a keep to recommended is It .stakeholder each to documents new delivering about worrying without time real

status Vulnerability

for ability the requires reports actionable to documents alone stand from reports VEX Turning the Is ".with faced are they vulnerability the of state the understand immediately to stakeholders are?" product my to mean it does what and component the is active How "and?" relevant vulnerability .answered wants CISA that questions two just

:either state must report The

1. not does vulnerability The .required is mitigation or remediation No -") affected_not ("affected Not s]id_product [listed the affect
2. otherwise or ,mitigate ,remediate to] author [by recommended are Actions -") affected ("Affected .s]id_product [listed the affects vulnerability The .]id_vul [address describe should that] statement_action [one include must statement VEX a ,"affected "status For .[id_vul [mitigate or remediate to actions
3. .[id_vul [for fixes contain s]id_product [listed The -") fixed ("Fixed
4. relevant other or statement VEX the of] author [The -") investigation_under ("Investigation Under .[status [final a declared yet not have and investigating are parties investigation the once change will" investigation_under] "status [that expected is It - .conclusion a reached has

[statement_impact [statement Impact

an provide MUST statement VEX a then ,provided not is] justification [if ,"affected_not] "status [For by" affected_not "are s]id_product [listed the why or how explains further that] statement_impact[.[id_vul[

.[statement_impact [an provide MAY statement VEX a then ,provided is] justification [If

[time_statement_impact [statement impact of Timestamp

_impact [the when recording ,]time_statement_impact [include MAY] statement_impact[.issued was] statement

[justification [Justification

.[justification [provide should statement VEX a ,"affected_not] "status [For -

.provided be must] statement_impact [then provided not is] justification [If -

:values following the of one be MUST] justification [-

.[id_product [in included not is] id_subcomponent [vulnerable The -"present_not_Component "-

but] id_product [in included is] id_subcomponent [vulnerable The -"present_not_code_Vulnerable "- or configured is code source when occurs case this ,Typically .present not is code vulnerable the .code vulnerable the excludes that way a in built

cannot]) id_subcomponent [in likely (code vulnerable The -"path_execute_in_not_code_Vulnerable "- [id_product [when occurs case this ,Typically .]id_product [by used is it way the to due executed be .it use otherwise or call not does but code vulnerable the includes

by used and present is code vulnerable The -"adversary_by_controlled_be_cannot_code_Vulnerable "- .vulnerability the exploit to attacker an by controlled be cannot but] id_product[

prevent that features or protections in-built includes] id_product [-"exist_already_mitigations_Inline "- and attacker the by subverted be cannot protections in-built These .vulnerability the of exploitation exploitation prevent completely mitigations These .user the by disabled or configured be cannot .vectors attack known on based

amongst information sharing or requirements management vulnerability government meeting Whether a with begins tool security product a as SBOMs to concept from journey smoothest the ,customers .mindset design-by-secure

being is code as soon as loop the in members team ProdSec having prioritize that Organizations business greater and ,trust of reputation a ,products quality better from benefit will prepared .opportunities

Platform Security Product The 5: Section

to has someone ,standards specific-industry the of all manage and understand to trying Above to them enable and teams security on pressure reduce To .aspects all oversee and manage actually security product dedicated a ,scale at manage to impossible nearly already are that tasks perform .required is solution

Management SBOM

and ,tracked ,verified be to need SBOMs ,policies external and internal with comply To

including teams multiple across ,version and ,component ,product each for approved

...security course of and ,compliance ,QA ,development

detection from go you so ,process management SBOM entire the automates Cybellum .time no in management vulnerability and approval to

rd3 ,chain supply your into visibility deep Gain **- place one in SBOMs all Manage**

,products ,components across code proprietary and ,components software party

.units business and

with continuously SBOMs manage and Create **- time through versions SBOM Track**

.time through changes the see and ,version new every

you so ,quickly reports generate and validate ,Create **- easier much compliance Make**

.others and ,ISO ,IMDRF ,FDA ,CISA the of likes the from standards industry meet easily

your with integrations Seamless **- workflows existing into generation SBOM Integrate** all for support and ,systems update software and ,CD/CI ,PLM as such system existing .export and import including ,SPDX and CycloneDX as such ,format VEX and SBOM

,SBOM simple the beyond risks associated all Expose **- SBOMs simple Beyond** .more and ,configuration OS ,PII ,passwords ,cryptography ,BOM HW as such

costly the Without **- validation SBOM on less ,research security on more Focus** time your focus to able be will you ,audits manual of hassle consuming time and .vulnerabilities critical remediating and risk reducing on ,counts it where

you so ,exported or shared rapidly be can SBOMs ready-Compliance **:ready-Audit** .next comes whatever securing on focus can

Management Vulnerability

,detail incredible in software device your analyzes Cybellum **.impact risk real the Understand** which understand Clearly .database vulnerability product dedicated a with it matches then .so less ones which and products your to threat immediate an post vulnerabilities

with risks priority-low and positive false by caused noise the Reduce **- Cancellation Noise** .prioritization vulnerability manual removes that platform a

each ,sector industrial or ,device medical ,automotive the in Whether **- Focused Industry** industry s'Cybellum on based insights contextualized Gain .ecosystem unique a has field .demands regulatory and vulnerabilities prioritize better to solutions specific

VEX ,management SBOM Automate **- Mitigation to SBOM from ,loop the Close** .time no in fixed to found from get you so ,orchestration mitigation and ,generation

software new mitigate and Analyze **- Assessments Production Post Continuous** .line the down updates

existing and new Meet **- Regulations Cybersecurity with Compliance Rapid** .regulations

Management Compliance

by gaps compliance cyber identify Rapidly **.process compliance cyber entire the Automate**
.automatically all ,assessments vulnerability with requirements regulatory mapped-pre matching
.clicks few a only in reports ready-regulator generate to you allows visibility Better

and historical for data regulatory relevant and evidence all of register a Keep **- Document**
.units business and lines product all across ,purposes auditing

and standards ,regulations existing and new with up Keep **- standards new of top on Stay**
.workflow your into policies these integrating automatically by practices best

violations highlights validation regulatory Automated **- certified get and faster Comply**
generate then ,open remains what see to you allowing ,reports compiled-auto delivers and
.structure s'standard each match perfectly that reports detailed

across approval and oversight compliance improve and up Ramp **- scale at Comply**
.teams and products

engine same the using validation policy internal Automate **- policies internal govern Easily**
.requirements external and internal both with comply products all sure make to

(PSIRT (Response Incident Product

their to risks relevant most your See **.roof one under investigation to detection from Go**
.location central one in all - investigations detailed facilitate then ,products production-post

clear Quickly **- investigations thorough on focus can you so work grunt PSIRT Automate**
with seamlessly Integrate .vulnerabilities urgent most' products your identify and noise through
.incidents mitigate quickly can you so ,systems operational other and ,SOAR ,SIEM your

the against steps decisive Take **- events related-security all of pulse the on finger your Keep**
time Slash .systems and products specific your of context the in all ,risks cyber relevant most
continuously products production-post keeping towards steps critical take and remediation to .secure

intelligence threat of monitoring and aggregation Automated **- intelligence threat Automate**
.products specific your to relevant s'what identify sources

,investigations managing and creating for workbench a Get **- investigations entire**
Facilitate ,Then .tickets relevant opening and ,analysis the formulating to ,info relevant comprising
from .stakeholder individual each for reports customized generate

saves software s'product your about data existing-pre Leveraging **- times remediation Reduce**
.activities mitigation and ,investigations ,monitoring threat on time you

product all of collection data Ongoing **- standards production post with faster Comply**

.others and ,ISO ,IMDRF ,FDA ,CISA from standards meet to you allow activities security

place one in all it manage can Managers And

that vulnerabilities widespread most the Discover **.action for ready ,issues pressing most Your** even and ,now right faced violations compliance biggest the uncover ,products your of many affect .supplier riskiest the identify

of percentage the as such ,time over progress Track **- time over trends See**
.more and ,times resolution average ,met tickets SLA ,risk at products

are risks which exactly See **- chain supply your over control unprecedented Achieve**
.suppliers or components riskiest the pinpointing ,vendor or supplier which from coming

compliance ,risks security crucial most the Highlight **- angle every from insights Gain**
.moment given any at challenges licensing and ,gaps

each at have you products many how Identify **- visibility lifecycle full Have**
.posture security their on in zero then ,stage lifecycle

measure and activities security product to KPIs Put **- progress the Quantify**
.ROI department

Untangling
Chaos Terminological

,Standards of Glossary Security Product
More and ,Regulations

Terms Key Defining

compliance of blocks Building

Standards

,organizations recognized by established practices best or Guidelines :Definition - groups industry or ,bodies professional

,products of consistency and ,reliability ,safety ,quality Ensure :Purpose - industries across processes or ,services

Compliance

,regulations ,rules established following or to adhering of act The :Definition - standards or ,policies

or ,policies internal ,standards industry ,requirements legal to Conform :Purpose - organizations or ,bodies industry ,authorities regulatory by set practices ethical

Compliance Regulatory

by forth set regulations and ,rules ,laws to Conformance :Definition - authorities regulatory or governmental

such ,business a of aspects various governing requirements to Adhere :Purpose - to ,protection environmental and financials ,privacy ,safety ,security product as action legal and ,penalties ,fines avoid

Differences

Landscape Regulatory and ,Compliance ,Standards Exploring :Compliance of ABCs The

covers compliance while ,industries or areas specific on focus Standards **:Scope** .requirements regulatory including ,standards or ,policies ,rules of range broader a .specifically regulations imposed-government targets compliance Regulatory

on based ,mandatory or voluntary be can Standards **:Mandatory .vs Voluntary** compliance regulatory while ,expected generally is Compliance .industry and context .regulations governmental to due mandatory is

and reputation harm may standards with compliance-Non **:Consequences**
,penalties legal in result can compliance-non regulatory while ,competitiveness
.revocations or suspensions license and ,fines

industry or organizations professional by developed are Standards **:Authority** to adherence by driven are compliance regulatory and compliance while ,bodies .regulations and rules organizational or ,industry ,governmental
A

Standards

Standards of Landscape the Navigating

Standards International

(Standardization for Organization International (ISO :Example
countries and industries across applicable guidelines Global :Scope

Standards National

States United the in) Institute Standards National American (ANSI :Example
organizations setting-standard national by developed guidelines specific-Country :Scope

Standards specific-Industry

healthcare for) Act Accountability and Portability Insurance Health (HIPAA :Example
industries specific of practices and requirements unique the to tailored Standards :Scope

Standards specific-Company

to organizations individual by developed practices best and guidelines Internal :Scope
goals and needs specific their meet
partners chain supply its for Conduct of Code Supplier s'Apple :Example

Standards of Benefits

Standards to Adherence of Rewards the Reaping

Reliability and ,Safety ,Security ,Quality Product Improved

experience customer better and performance Consistent -
failures or ,defects ,accidents ,compromises of Reduction -

Competitiveness Market and Trust Consumer Increased

credibility and reputation brand Enhanced -
practices best to adherence through advantage Competitive -

Collaboration and Trade International Facilitated

countries across industries and organizations for language Common -
requirements regulatory global with compliance Simplified -

Fines of Avoidance and Mitigation Risk

loss financial and penalties legal to exposure Reduced -
liabilities and risks potential of management Proactive -

Management Compliance

Management Compliance Effective of Pillars Four The

Assessment Risk

risk compliance potential of evaluation and Identification -

likelihood and impact their on based risks of Prioritization -

Monitoring Compliance

standards or ,policies ,rules to adherence ensure to reviews and audits Regular -

updates and changes regulatory of Tracking -

Education and Training

programs training employee of implementation and Development -

practices best and requirements compliance of awareness Building -

Documentation and Reporting

data related-compliance of analysis and Collection -

efforts compliance demonstrate to reporting and keeping-Record -

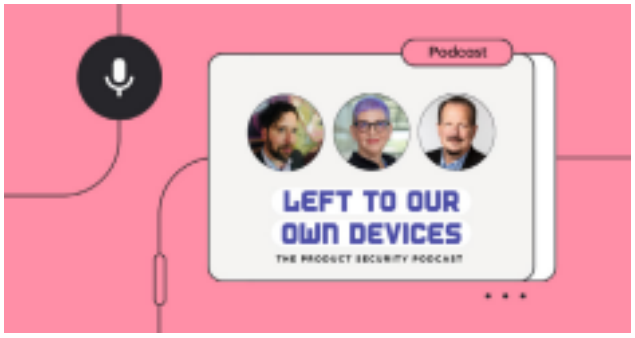
us About

com.cybellum.www visit more learn To

about more
Learn

Security Product

Blogs



Base Knowledge

Podcasts

Getting :Devices
Right

Overview

Vehicle LG

Solutions Component
Study Case

the about More

Medical Your Making Cyber Devices
the for Compliant
from :Omnibus
Practice to Theory
Connected for SBOM it

Platform Security Product

com.Cybellum