Vulnir

Online CRA Workshop 'Deep dive session: Vulnerability Handling'

22 July 2025 - SURVEY

Angelo D'Amato
Founder / Cybersecurity Expert
VULNIR

Meet your speaker

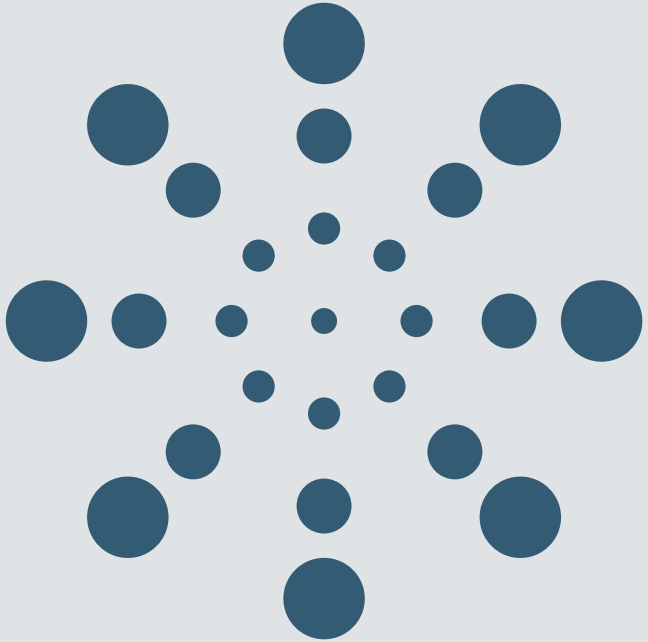
Angelo D'Amato
Founder / Cybersecurity Expert, Vulnir

Background

- With over fifteen years of experience, he is the subject matter expert for:
  - End-to-end cybersecurity assessments (Penetration testing, Security assessments)
  - Certifications (e.g., UL 2900, Common Criteria)
  - Regulatory compliance (e.g., Radio Equipment Directive, Cyber Resilience Act)
- I currently cover the role of rapporteur (*) for CRA as a CEN contractor within CEN/CLC/JTC 13/WG 9 for
  - PT2: Generic Security Requirements
  - PT3: Vulnerability handling requirements

* The European Union funds my activities within the STAN4CR project through the European Innovation Council and SMEs Executive Agency (EISMEA) under Grant Agreement No. 101196779.

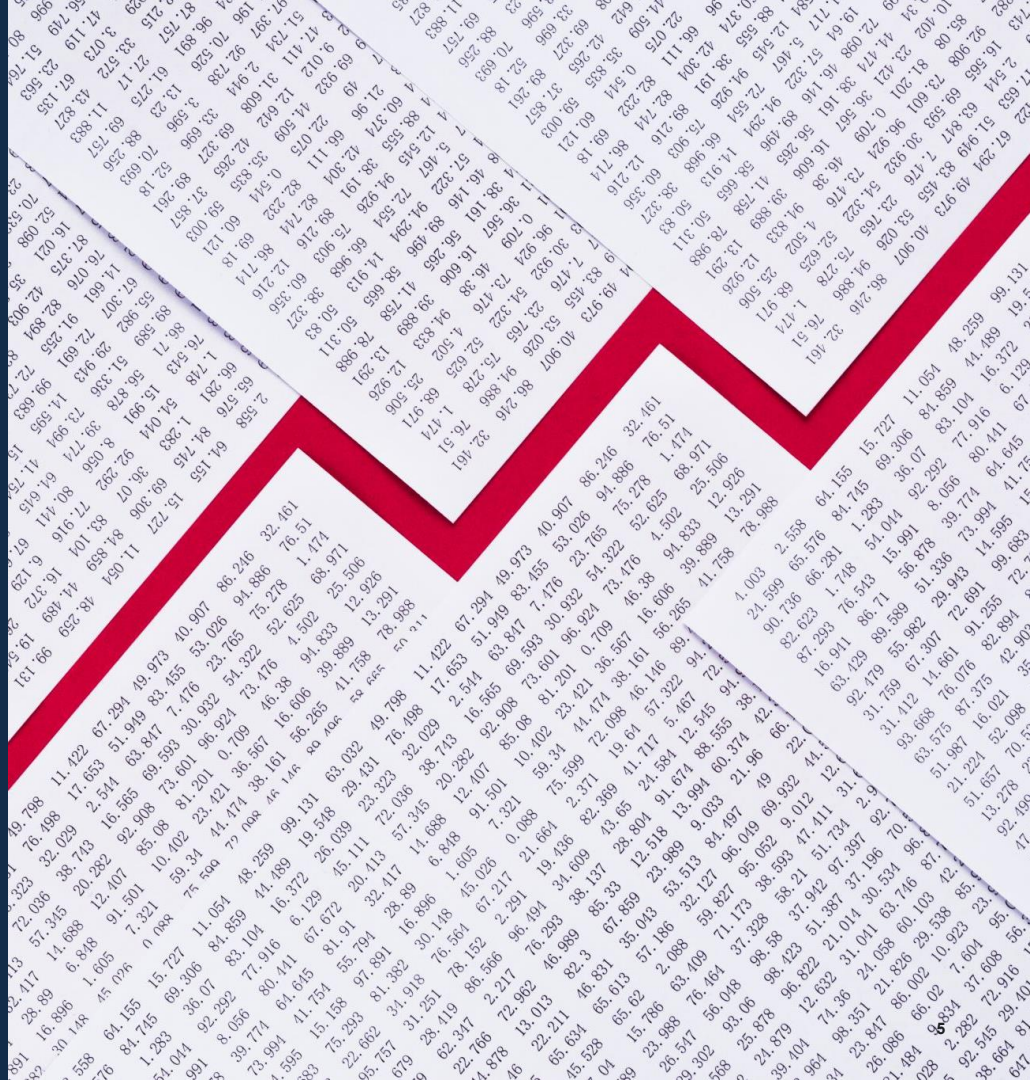
05 Vulnerability handling: Deep Dive Survey



Survey participant overview

NUMBER OF ANSWERS			
5.1	5.1 [PRE] PREPARATION	4.34 Average Rating	47
5.2	5.2 [RCP] RECEIPT	4.45 Average Rating	31
5.3	5.3 [VRF] VERIFICATION	4.37 Average Rating	27
5.4	5.4 [RMD] REMEDIATION	4.30 Average Rating	23
5.5	5.5 [RLS] RELEASE	4.35 Average Rating	23
5.6	5.6 [PRP] POST RELEASE	4.27 Average Rating	22
06	Post-Workshop Survey: Cyber Resilience Act - Vulnerability Handling	4.40 Average Rating	15

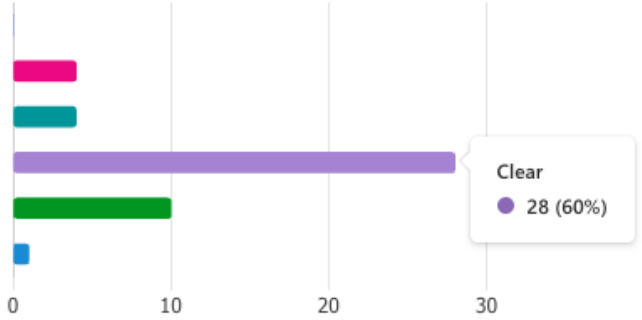
5.1 [PRE] PREPARATION



2. Clarity and Understandability: How clear and easy to understand is the proposed content for this section?

More details

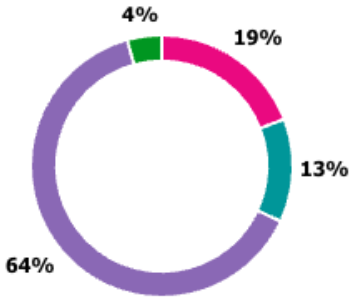
Not Clear	0
Somewhat clear	4
Neutral	4
Clear	28
Very Clear	10
Other	1



3. Practicality and Implementability: How practical and implementable do you find the requirements/guidance in this section for your organization or typical stakeholders?

More details

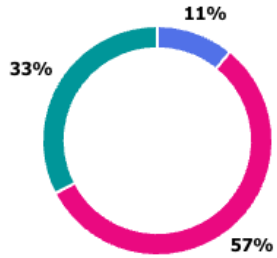
Not Practical	0
Somewhat practical	9
Neutral	6
Practical	30
Very Practical	2



4. Do you feel anything significant is missing from this section?

More details

Yes	5
No	26
Maybe	15



5. If you felt that something significant is missing please specify:

More details

14
Responses

Latest Responses
...

3 respondents (21%) answered identification for this question.

5.If you felt that something significant is missing please specify:

1	Cryptographic Bill of Materials
2	N/a
3	None
4	How can we help you developing the standard
5	Guidance on how to start already today e.g., using flow diagrams
6	The correlation to the existing legislation like EN Etsi 303 645 is Missing
7	I think it's in a good progress
8	Interplay with AI

5.If you felt that something significant is missing please specify:

9	I don’t think there is significant extra effort to expand the SBOM beyond top level, especially if automated tooling was used to get the top level information in the first place. Requiring more complete SBOMs that stop at certain sensible boundaries on a best effort basis should be reasonable.
10	Preparations for Inter-manufacturers (supply chain) reporting, coordinated disclosure and reporting to CSIRT, ENISA. Deduplication. In CRA, the PDE is bundled with the Remote Data Processing solution(s), which seem to complicate the reporting, identification, handling (RDP doesn't have a separate identifier). The RDP might also mostly come from a different manufacturer, in which case the vulnerability would have to be escalated. Not clear how the standard covers this.
11	Which would be the acceptance criteria for assessing the compliance to the requirements? Will it be included in the document? Or is it outside its scope?

5.If you felt that something significant is missing please specify:

12	Technical Detail: While there is a proper format for SBOM, component identification is not so clear. On the one hand, the established CPE naming scheme is ambigous and IMHO not really suited for large monitoring of components not-yet affected by a vulnerability. On the other hand the proposed PURL naming standard, addressing this issue is not widely adopted. Not sure where to address this problem (not in this session probably), but proper component identification seems like a crucial missing link in the whole vulnerability process right now.
13	The Ideal Case are well dealt with. Issues will Serie from the Compilation of HW, FW and SW from different parties.
14	Not super clear from this how we should acknowledge accepted vulnerabilities - example most of our products does not have encrypted communication as they are also designed to teach children how to code. Thus a replay is accepted by the toys, and will not lead to any harm. So we have mitigated the risks by not having any Personal identification risks (no PI and no mics etc.). This is allowed in EN 18031, and hope to see the same reflection of considering risk to the user.

6. Suggestions for Improvement: What specific changes or additions would you recommend for this section?

More details

14

Responses

Latest Responses

"- Hardware BOM really should be a great idea! - A SBOM is today also often referr... "

...

3 respondents (23%) answered Implementation for this question.

Update

6.Suggestions for Improvement: What specific changes or additions would you recommend for this section?

1	Chained requirements for SBOM. Server systems are depending on frequent updates - many mainly caused by security issues.
2	Handover material and slides
3	N/a
4	Ensure the "assessments" are not too generic, which could potentially result in a manufacturer complying without being secure (e.g. HTTPS doesn't mean it's securely configured).
5	None
6	Further detail conformity procedures
7	I am focusing on CRA with respect to AI interplay and i am a core team member of jtc21 wg5 and monitoring wg2 on risk
8	Not at this Stage - but in the Implementation Phase We need to Trigger some dry runs. So one can already familiarize with Process before the Stress Level rises

6.Suggestions for Improvement: What specific changes or additions would you recommend for this section?

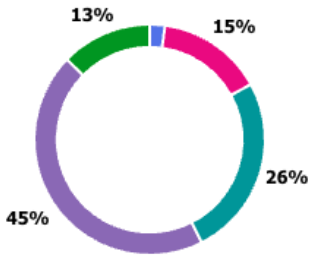
9	Non, very clear at this level
10	Performance review, ideally periodic, to ensure implementation of CVD process
11	SBOM content and dependency requirements represent a significant topic area. While NTIA's minimal elements for an SBOM provide a useful reference framework, my experience indicates that SMBs (Small and Medium Businesses) often struggle with implementation due to limited resources and technical expertise. However, I believe initiatives like CYBERFORT and the occtet.eu project can provide valuable assistance to bridge this gap. Regarding top-level dependency requirements, I recommend adopting a risk-based approach that varies by device type. For example: general devices might require top-level dependencies only, critical devices should include all-level dependencies, while Class I or Class II devices could require 2-3 dependency levels based on their risk profile and regulatory requirements. Hardware BOM has relatively less security impact compared to software components, since SBOM primarily encompasses software, firmware, and related digital components that pose greater cybersecurity risks.

6.Suggestions for Improvement: What specific changes or additions would you recommend for this section?

12	If possible less speed and more examples. Angelo is an excellent lecturer.
13	For the top level dependencies, then SDKs (software development kits) are a little bit of a nightmare. most of them support quite a lot of usage cases, and can have many vulnerabilities that are not relevant for your final product. So you end up having to justify why parts of third party software kit is not relevant to your product. For the secure communication, then I hope it will also be allowed to just keep a non-secure line of communication in parallel? example an email address - UK PSTI mandates us to be able to receive them without creating a user profile, and without collecting any PI, and we still somewhat respecting the intend of the law for it to be transparent and simple to do for the average user.
14	- Hardware BOM really should be a great idea! - A SBOM is today also often referred to as "System BOM" - which also makes sense to have a detailed listing for the whole system. - Software BOMs should be well specified to have a common format and to give tool vendors a chance to adapt properly.

7. In your opinion, is the proposed section proportionate to the cybersecurity risks it aims to address for organizations of all sizes, particularly Small and Medium-sized Enterprises (SMEs)? More details

Not at all proportionate/Excessive burden	1
Somewhat disproportionate/Significant burden for SMEs	7
Neutral/Unsure	12
Somewhat proportionate/Manageable for most SMEs	21
Very proportionate/Well-adapted for SMEs	6



8. Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME: More details

20
Responses

Latest Responses
"In my experience SME's may have only 1 or 2 software engineers especially with th... "
"The response time to handle incoming vulnerabilities will be almost impossible to ... "
...

8 respondents (44%) answered SME for this question. Update

8.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

1	I feel like the requirements for OSS should also be mentioned
2	well-prepared materials in an organised way
3	SME will have hard time to align and comply
4	To me the section was clear. It gave a good overview of the requirement and referenced plenty of other sources which someone could use to further educate themselves in the matter
5	Good insight, but need more time to digest and get input from my peers
6	A lot of paperwork and administrative burden with supply chain security
7	Practicality will depend on the level of detail/information required in the final specifications of SBOM and hardware bill of materials. Understanding that neither of these need to be made publicly available, or indeed down the supply chain, it could be burdonsome to require manufacturers to detail in their BOMs dependencies in their dependencies where there is no obligation for upstream suppliers to make that information available

8.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

8	Its a good basis
9	Generally you need to have small definitive steps to guide users through the process. Smaller organizations don't have the internal resources to develop their own strategies and it's helpful to have this guidance.
10	I find the maze of regulation a burden and hard to get across all the different domains, not specifically a CRA issue, but if CRA could consider the default domain outside of the verticals, then maybe SME’s may get more relevant guidance when experts have to perform multiple rolles
11	The Process is fine - but SMEs may really run through very Last Moment - some gamification can help
12	Doable, especially with software aimed to help SMEs
13	Even if considering it proportionate, it could impact considerably in investments needed for complying

8.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

14	There are quite many "new" security activities needed now (or at least that SMEs were not doing) but the tools and documention provided will help. The first months/years of adoption will reqyire additionnal efforts
15	As an SME, it seems like too much of a moving target. I.e. final specs are late to arrive in relation to the implementation deadline. Proper consulting/implementation help is not widely available. In reality, as a cybersecurity specialist at a SME I'm between a rock and a hard place: While one could argue that we can already start with the implementation of a vulnerability handling process, business deciders are not easily convinced due to draft standards of final documents. Big companies usually have spare ressources (i.e. trained manpower), at an SME there is always the decision to do business features instead.

8.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

16	Probably most of the organizations, including SMEs will prepare the CVD process according to CRA and the harmonized standards - on documents. I guess the difference will happen in the implementation: organizations with lacking resources in PSIRT and SDLC or awareness of cybersecurity in CxO / executive level could fail to deliver the expected level of quality in CVD process, leading to e.g. false SBOMs, ignored alerts, misjudged triage, and inadequate treatments
17	For the top level dependencies, then SDKs (software development kits) and open source software are a little bit of a nightmare. most of them support quite a lot of usage cases, and can have many vulnerabilities that are not relevant for your final product. So you end up having to justify quite extensively why parts of third party software kit is not relevant to your product.
18	The proposed section is very flexible. Even though the presenter displayed some advanced artefact, SME can still decide to go for a less "advance" way of vulnerability handling materials.
19	The response time to handle incoming vulnerabilities will be almost impossible to meet for (smaller) SMEs.

8.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

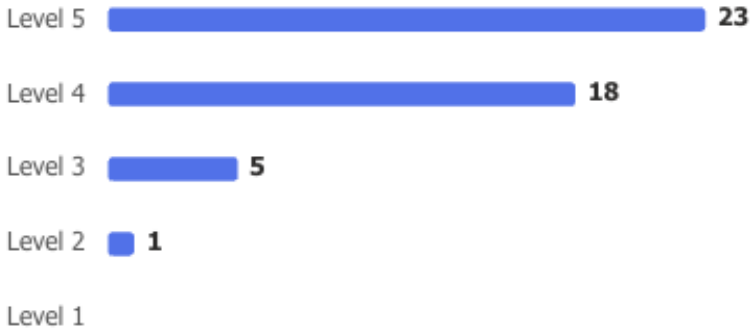
20	In my experience SME's may have only 1 or 2 software engineers especially with the smallest organizations of say < 10 and they will not be able to cope with this at all. Really needs a more minimalistic approach if possible under the CRA or an exemption for low volume or low risk products.

9. Overall, how satisfied are you with this section?

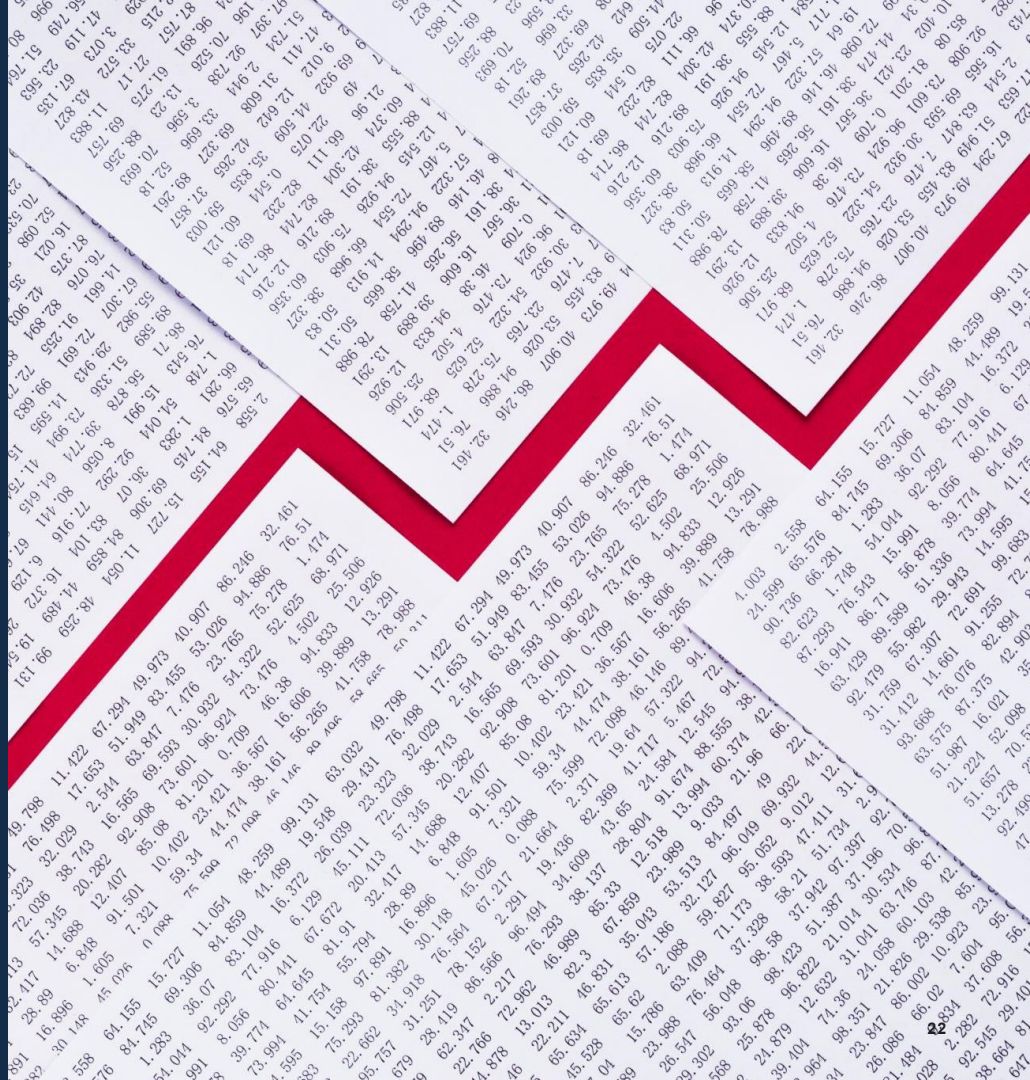
More details

4.34

Average Rating



5.2 [RCP] RECEIPT

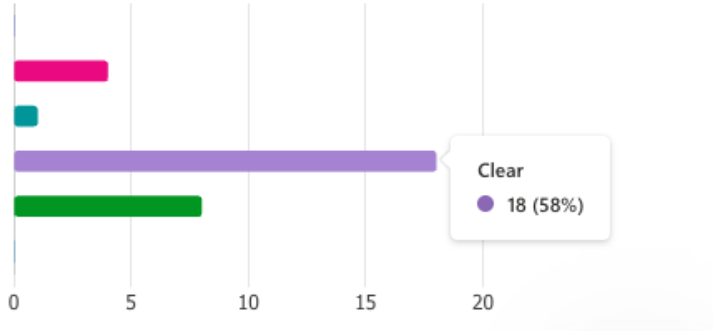


Vulnir

2. Clarity and Understandability: How clear and easy to understand is the proposed content for this section?

More details

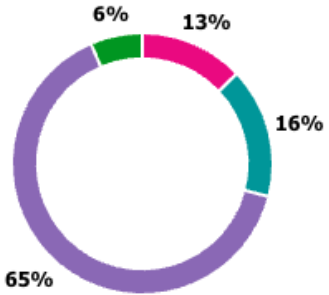
Not Clear	0
Somewhat clear	4
Neutral	1
Clear	18
Very Clear	8
Other	0



3. Practicality and Implementability: How practical and implementable do you find the requirements/guidance in this section for yo ur organization or typical stakeholders?

More details

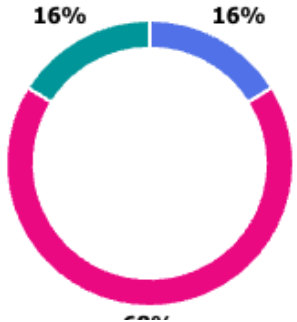
Not Practical	0
Somewhat practical	4
Neutral	5
Practical	20
Very Practical	2



4. Do you feel anything significant is missing from this section?

More details

Yes	5
No	21
Maybe	5



5. If you felt that something significant is missing please specify:

More details

8
Responses

Latest Responses

"It seems inefficient that users of software components should need to monitor for ..."

"The trend for complex software systems is to assemble components dynamically in..."

...

3 respondents (38%) answered components for this question.

5.If you felt that something significant is missing please specify:

1	More documentation and guidance
2	I think the Bills of Material should also reflect information about the build machine (OS, toolchain, etc.)
3	Risks (but not specific vulnerabilities) related to the software/hardware components, e.g. using end of life or not actively maintained components
4	details on how the SBoM monitoring would be proved? (similar to 21434 can we have some templates defined to fulfill the requirements? the HBoM sections needs more work and clarity similar to SBoM
5	SBOM
6	What Product Identifier to use when monitoring CVE streams? Is CPE good enough? Any guidelines here? I imagine this can be hard as might be specific to the industry.

5.If you felt that something significant is missing please specify:

7	The trend for complex software systems is to assemble components dynamically in real-time. In such situations, a SBOM, which is a static document that lists the components at a specific point in time, becomes more challenging to generate and maintain accurately. This highlights the limitation of SBOMs in dynamic environments where components change frequently. My doubt is how this will be handled concretely in the future
8	It seems inefficient that users of software components should need to monitor for included vulnerabilities, meaning maybe massive numbers of people all looking for the same thing. Surely the creators of these components should have the duty to inform all the users of their product. Then users only need to act when notified ?

6. Suggestions for Improvement: What specific changes or additions would you recommend for this section?

More details

9

Responses

Latest Responses

"If users of software components have registered their use with the supplier who th... "

...

3 respondents (33%) answered software components for this question.

6.Suggestions for Improvement: What specific changes or additions would you recommend for this section?

1	Risk level management for defining "appropriate" measures
2	Off topic but: If EUVD becomes mandatory database to monitor vulnerabilities, I kindly request inclusion of unique identifiers (cpe and/or purl) for the affected software and version range to each of the EUVD security advisory. Otherwise, SBOM tools/vulnerability monitoring tools will have a difficulty implementing automatic EUVD monitoring and matching to components on SBOM, which means manual operation is necessary.
3	Monitoring of EoL status of software components, this is for example already required when developming medical device software.
4	details on how the SBoM monitoring would be proved? (similar to 21434 can we have some templates defined to fulfill the requirements? the HBoM sections needs more work and clarity similar to SBoM

6.Suggestions for Improvement: What specific changes or additions would you recommend for this section?

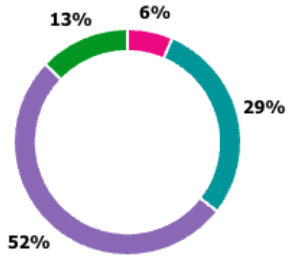
5	The HBOM should really be included. From the experiences with the RED DA as of today, we already know that your product needs to rely on specific revisions of hardware components to be compliant. This should be tracked properly in an HBOM. Also hardware often comes with firmware which is - same as above - part of a hardware component revision.
6	Regular testing requirement may be substituted with regular risk/threat analysis, and testing can be done if it is necessary according to its results.
7	For Supply Chain Cybersecurity Practices: considering the widespread reliance on open-source components in modern supply chains, it would be beneficial to reference ISO/IEC 18974, which specifically addresses open-source software security management. This standard provides comprehensive guidance on managing risks associated with open-source software components and strengthens overall cybersecurity within the supply chain ecosystem.

6.Suggestions for Improvement: What specific changes or additions would you recommend for this section?

8	Example of HBOM relevancy: kensington lock for a product (e.g. laptop). Vulnerability in how it was implemented. (extreme example but where it might be relevant).
9	If users of software components have registered their use with the supplier who then has the obligation to notify the user, then that should be sufficient to meet the requirement for identify vulnerabilities in the software component.

7. In your opinion, is the proposed section proportionate to the cybersecurity risks it aims to address for organizations of all sizes, particularly Small and Medium-sized Enterprises (SMEs)? More details

Not at all proportionate/Excessive burden	0
Somewhat disproportionate/Significant burden for SMEs	2
Neutral/Unsure	9
Somewhat proportionate/Manageable for most SMEs	16
Very proportionate/Well-adapted for SMEs	4



8. Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME: More details

9
Responses

Latest Responses
"SMC would likely struggle to have the resources to monitor all the various vulnera... "
...

4 respondents (44%) answered vulnerability for this question.

8.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

1	The information is clear and again plenty of resources are being shared as well.
2	It heavily depends on the threat model and use case
3	please be aware that we for many components have dual sourcing in order to lower the risk, and for some of the chinese Manufacturer see them changing names and ownership structure quite often, which make the practical tracking fairly hard to do.
4	Balances effort and risk
5	HBoM aspects how to handle vulnerability for supplier and internal stakeholders are unclear.
6	industrial collaboration

8.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

7	When using automated security scanning tools, organisations can become overwhelmed by the triage process of findings into qualified vulnerabilities. This can take a lot of effort in practice. Some practical guidance could be useful here. Also it should be mentioned that these tools don't provide vulnerabilities, only findings. They need to be qualified first.
8	SMEs might not have a CTI tool setup or a subscription to a Vulnerability Aggregator to receive a good coverage of publicly disclosed vulnerabilities. If the vulnerability is for a component they integrate this might be especially hard to monitor.
9	SMC would likely struggle to have the resources to monitor all the various vulnerability data bases for software components, whereas if they were always notified the task is easier.

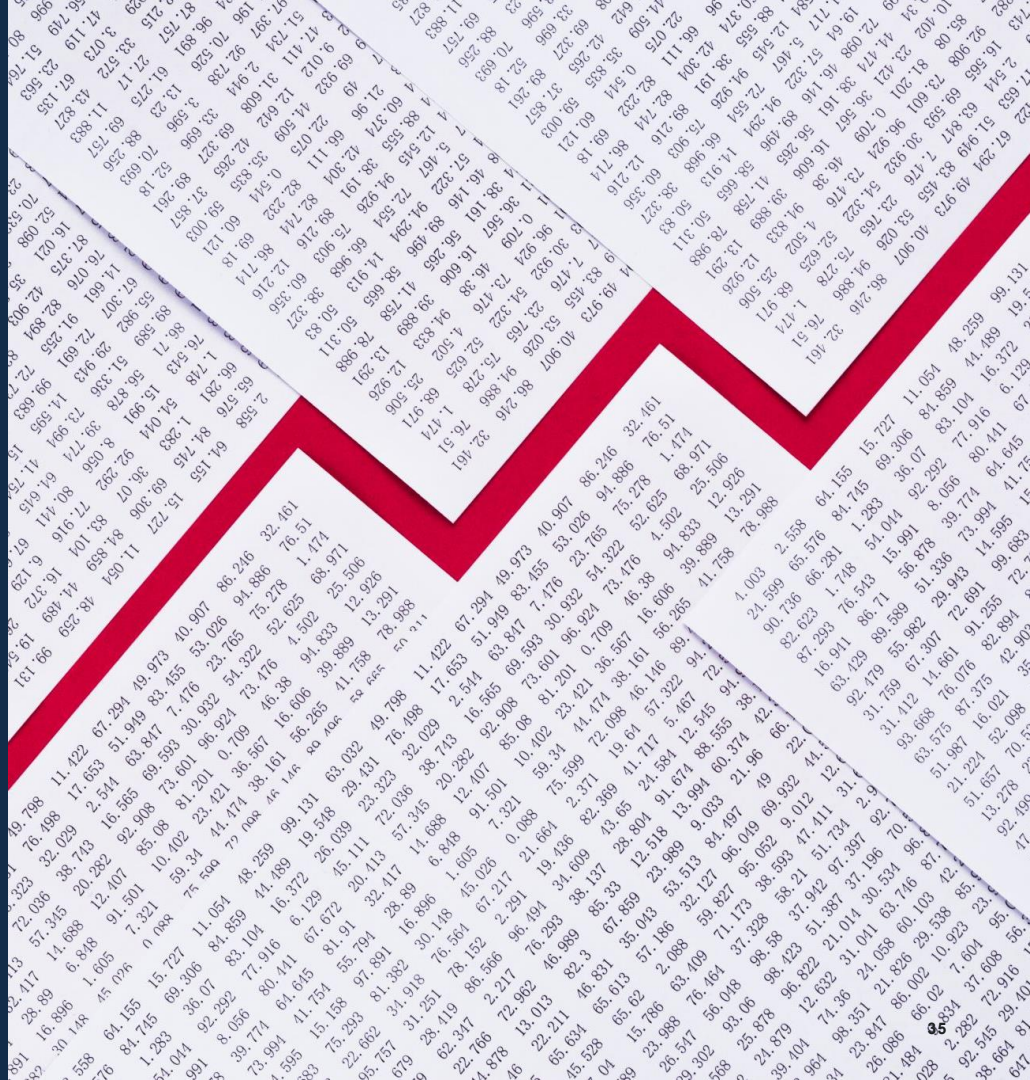
9. Overall, how satisfied are you with this section?

More details

4.45

Average Rating

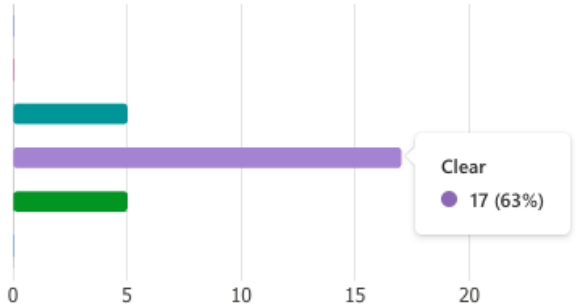
5.3 [VRF] VERIFICATION



2. Clarity and Understandability: How clear and easy to understand is the proposed content for this section?

More details

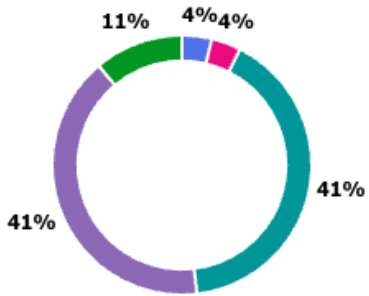
Not Clear	0
Somewhat clear	0
Neutral	5
Clear	17
Very Clear	5
Other	0



3. Practicality and Implementability: How practical and implementable do you find the requirements/guidance in this section for yo ur organization or typical stakeholders?

More details

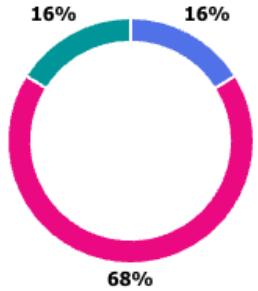
Not Practical	1
Somewhat practical	1
Neutral	11
Practical	11
Very Practical	3



4. Do you feel anything significant is missing from this section?

More details

Yes	5
No	21
Maybe	5



5. If you felt that something significant is missing please specify:

More details

5
Responses

Latest Responses

"Not missing but too much see 6."

"please specify if it is all suppliers that need to be in the security communication lo... "

...

2 respondents (40%) answered risk for this question.

5.If you felt that something significant is missing please specify:

1	How to handle all the frames of the known-unknowns risk matrix.
2	Risk acceptance is maybe not explicitly mentioned, does every vulnerability need to be remediated or only above a certain level that is higher than the risk appetite of the end-user / organization? Also, in legacy products sometimes significant gradual efforts over long periods of time are the only reasonable way to mitigate the risk, see for example memory safety concerns in memory unsafe programming languages like C/C++. Having a roadmap towards reducing the risk instead of spending massive effort towards fixing them completely could be useful here.
3	Guidelines for efficient coordination and communication with other parties in the supply chain to ensure no delays. Nothing mentioned about handling anonymous reports (the communication requirements).
4	please specify if it is all suppliers that need to be in the security communication loop or just proving it for one??

5.If you felt that something significant is missing please specify:

5	Not missing but too much see 6.

6. Suggestions for Improvement: What specific changes or additions would you recommend for this section?

More details

6

Responses

Latest Responses

"It is quite a simple requirement - address and remediate vulnerabilities - does in n... "

"Indeed, VRF4-6 seems more structural and could be shift to PRE"

"Proving the communication part seems a bit messy. How should it be handled for ... "

...

3 respondents (50%) answered Vulnerability for this question.

6.Suggestions for Improvement: What specific changes or additions would you recommend for this section?

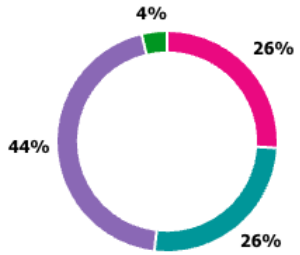
1	Interaction between Known Vulnerability, Actual Risk & the prohibition of products with "known exploitable vulnerability" from CRA.
2	Mentioning how this interplay with GDPR as well? The DPA would have to be involved in certain cases beside the CSIRT coordinator, correct?
3	I would recommend against specifically naming a ticketing system. A ticketing system is a method rather than an objective, and standards should focus on what needs to be achieved rather than how to achieve it. Companies should have the flexibility to use alternative methods to reach this goal.
4	Proving the communication part seems a bit messy. How should it be handled for a new product with new components without any known vulnerabilities? a bunch of emails to/from 50 subcomponent and software suppliers confirming everything is ok or ? and how to handle the ones where we are just asked to subscribe to a newsletter

6.Suggestions for Improvement: What specific changes or additions would you recommend for this section?

5	Indeed, VRF4-6 seems more structural and could be shift to PRE
6	It is quite a simple requirement - address and remediate vulnerabilities - does in need all these steps - VRF 1 confirm vulnerability and VRF X provide solution would seem enough.

7. In your opinion, is the proposed section proportionate to the cybersecurity risks it aims to address for organizations of all sizes, particularly Small and Medium-sized Enterprises (SMEs)? More details

Not at all proportionate/Excessive burden	0
Somewhat disproportionate/Significant burden for SMEs	7
Neutral/Unsure	7
Somewhat proportionate/Manageable for most SMEs	12
Very proportionate/Well-adapted for SMEs	1



8. Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME: More details

12
Responses

Latest Responses
"If a problem is reported the SW engineer in the SME will just make a fix and send i... "
"Proving the communication part seems a bit messy. How should it be handled for ... "
...

5 respondents (42%) answered SMEs for this question.

8.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

1	Straight Forward but complete
2	Any additional paywalled standard referenced increases the burdern for SMEs. Same would be for requiring a ticket system.
3	SME's and startups will have to make things process heavy , which as of today they like to keep light.
4	More easy to understand this section.
5	Liked the examples
6	Triage for individual SAST findings for example could be burdensome, perhaps mentioning triage in bulk (by finding type or software module) is useful.

8.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

7	While necessary, some measures like opsec for cvd may stretch ressources thin for SMEs. Tbh, I don't see how many SMEs with one or two IT persons can handle PGP.
8	It might be complicated for small company to address the VRF requirements as it may require the vendor to invest money and also time.
9	With specialized software this is manageable. Requiring a ticketing system might be too much.
10	SMEs typically do not have dedicated resources or personnel to handle triage, vulnerability risk assessments, and similar tasks, so we need to see if there are any projects that can provide assistance to SMEs.

8.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

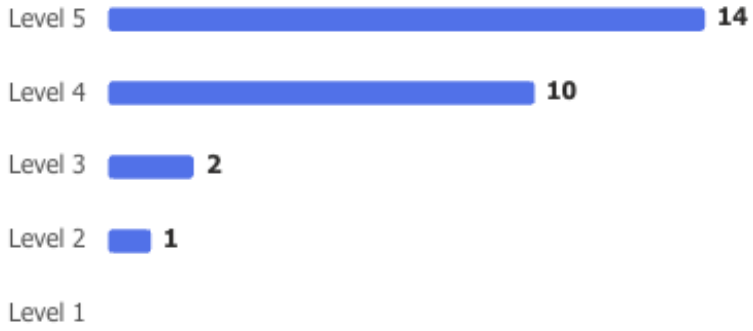
11	Proving the communication part seems a bit messy. How should it be handled for a new product with new components without any known vulnerabilities? a bunch of emails to/from 50 subcomponent and software suppliers confirming everything is ok or ? and how to handle the ones where we are just asked to subscribe to a newsletter
12	If a problem is reported the SW engineer in the SME will just make a fix and send it to the SME's customers with minimum administrative work.

9. Overall, how satisfied are you with this section?

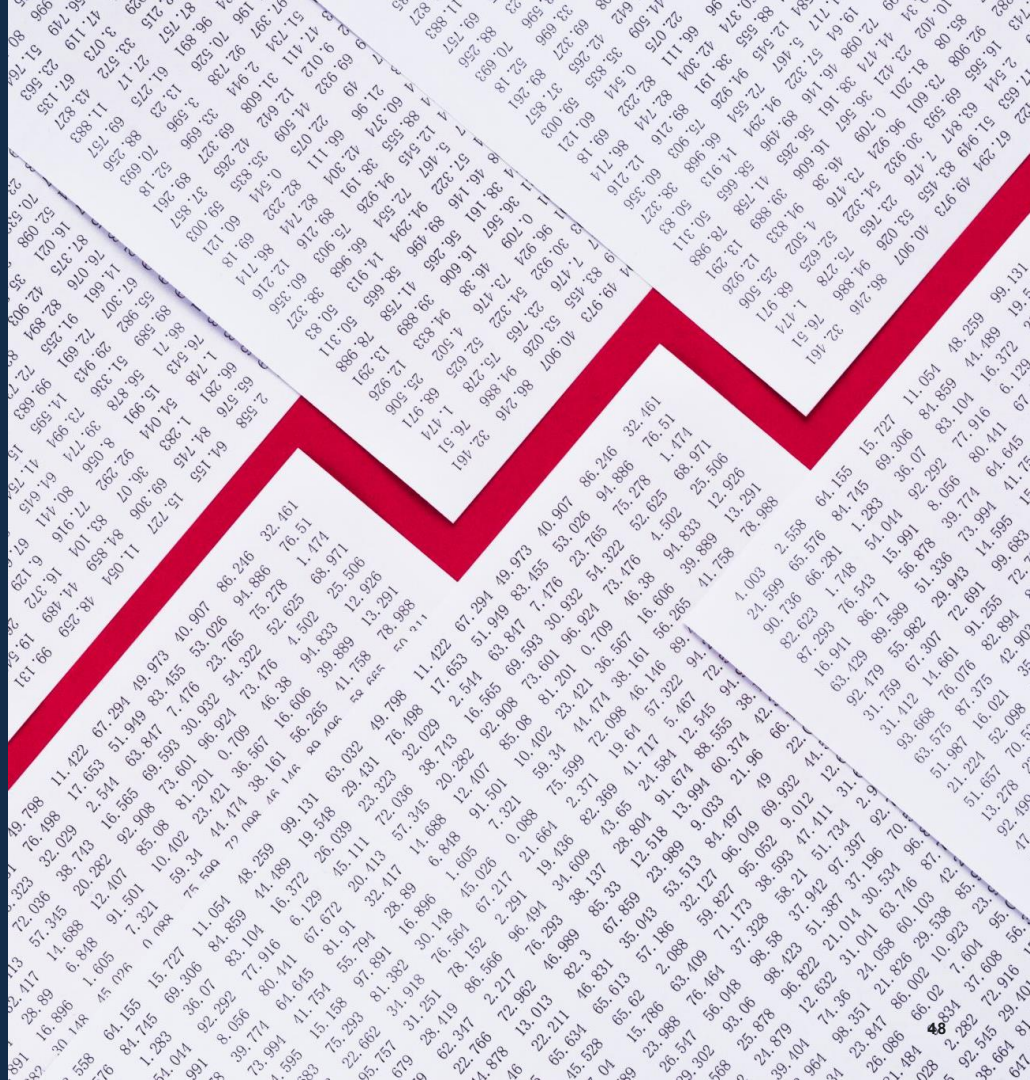
More details

4.37

Average Rating



5.4 [RMD] Remediation

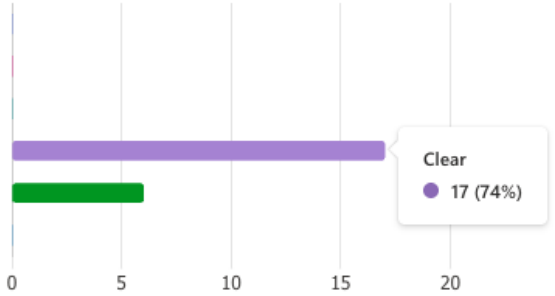


Vulnir

2. Clarity and Understandability: How clear and easy to understand is the proposed content for this section?

More details

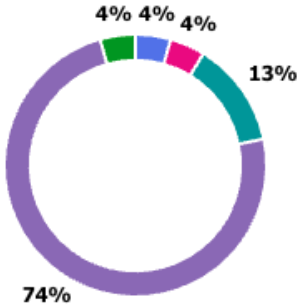
Not Clear	0
Somewhat clear	0
Neutral	0
Clear	17
Very Clear	6
Other	0



3. Practicality and Implementability: How practical and implementable do you find the requirements/guidance in this section for your organization or typical stakeholders?

More details

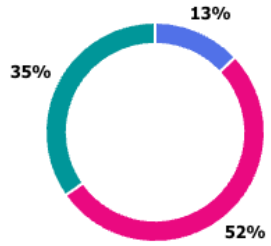
Not Practical	1
Somewhat practical	1
Neutral	3
Practical	17
Very Practical	1



4. Do you feel anything significant is missing from this section?

More details

Yes	3
No	12
Maybe	8



5. If you felt that something significant is missing please specify:

More details

8
Responses

Latest Responses

"how do you prove the remediation for a new product in a meaningful way ? you d... "

"The distinction between security and features updates is very important. As the Blu..."

...

4 respondents (50%) answered need for this question.

5.If you felt that something significant is missing please specify:

1	The Focus is on SW What Happens if the HW devices in the System are vulnerable.
2	To make it a little more specific, it could be mentioned that a simulated attack should be tested and that it should be verified that the remediation successfully blocked the attack.
3	As also highlight, the need for repeating of tests, could be hard for SMEs
4	[RMD-3] should be linked to PT1 on secure development - not sure if a specific requirement is needed in this standard, however I accept that validation of a fix is logical to "close the loop" on the remediation activity
5	Remediation across multiple product versions. The standard seems to focus on patching the latest version, which makes it difficult (or irrelevant) that you are separating the functional from the security patches if only the last version is supported.
6	The mentioned "without delay" and "new" security update need to be defined more clearly.

5.If you felt that something significant is missing please specify:

7	The distinction between security and features updates is very important. As the Blue Guide states, a feature update my lead to a whole new device, which then needs a re-assessment regarding compliance and even new standards. => A guidance on that and a real definition of feature updates is desperately needed.
8	how do you prove the remediation for a new product in a meaningful way ? you don't have any vulnerabilities and you cannot standardize a test for all scenarios. so this ends up being something where you end up having a process flow chart or similar piece of paper, that does not prove anything except that you understood the concept.

6. Suggestions for Improvement: What specific changes or additions would you recommend for this section?

More details

6

Responses

Latest Responses

"have it in the standard, but leave it out from the proof activities. it will be a copy p... "

...

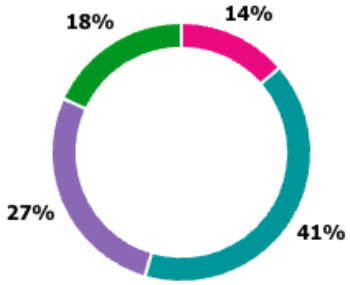
1 respondents (17%) answered security testing for this question.

6.Suggestions for Improvement: What specific changes or additions would you recommend for this section?

1	More specific testing please
2	Examöes were good
3	difference between remediation and mitigation
4	Suggest that ER on regular testing is probably more about regular vulnerability/penetration/security testing. I think this should be linked to the product risk assessment, and which defines the frequency, nature etc. of testing
5	Sometimes it's difficult to distinguish between bug fixes and security fixes, and some patches contain both, so separating them would be quite challenging.
6	have it in the standard, but leave it out from the proof activities. it will be a copy paste with no value for new producs.

7. In your opinion, is the proposed section proportionate to the cybersecurity risks it aims to address for organizations of all sizes, particularly Small and Medium-sized Enterprises (SMEs)? More details

Not at all proportionate/Excessive burden	0
Somewhat disproportionate/Significant burden for SMEs	3
Neutral/Unsure	9
Somewhat proportionate/Manageable for most SMEs	6
Very proportionate/Well-adapted for SMEs	4



8. Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME: More details

4
Responses

Latest Responses

"Seems to be the minimum needed, decide how to fix, make the fix, test the fix. Diff... "

"how to proof meaningfully without being a process diagram review."

"The amount and kind of Security testing might make a huge difference on the feas... "

...

8.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

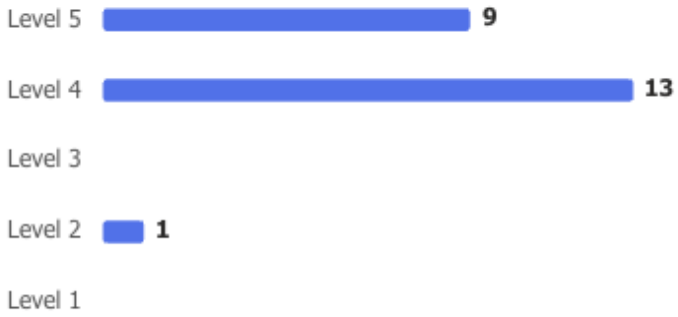
1	SMEs typically don't have capability and resources to meet the goal of the RMD, and therefore the additional assistance might be needed
2	The amount and kind of Security testing might make a huge difference on the feasibility for SMEs.
3	how to proof meaningfully without being a process diagram review.
4	Seems to be the minimum needed, decide how to fix, make the fix, test the fix. Difficulty would be judging how deeply to test the rest of the system to check for unintended consequences. A complete system test would be quite onerous and too much for some SMEs.

9. Overall, how satisfied are you with this section?

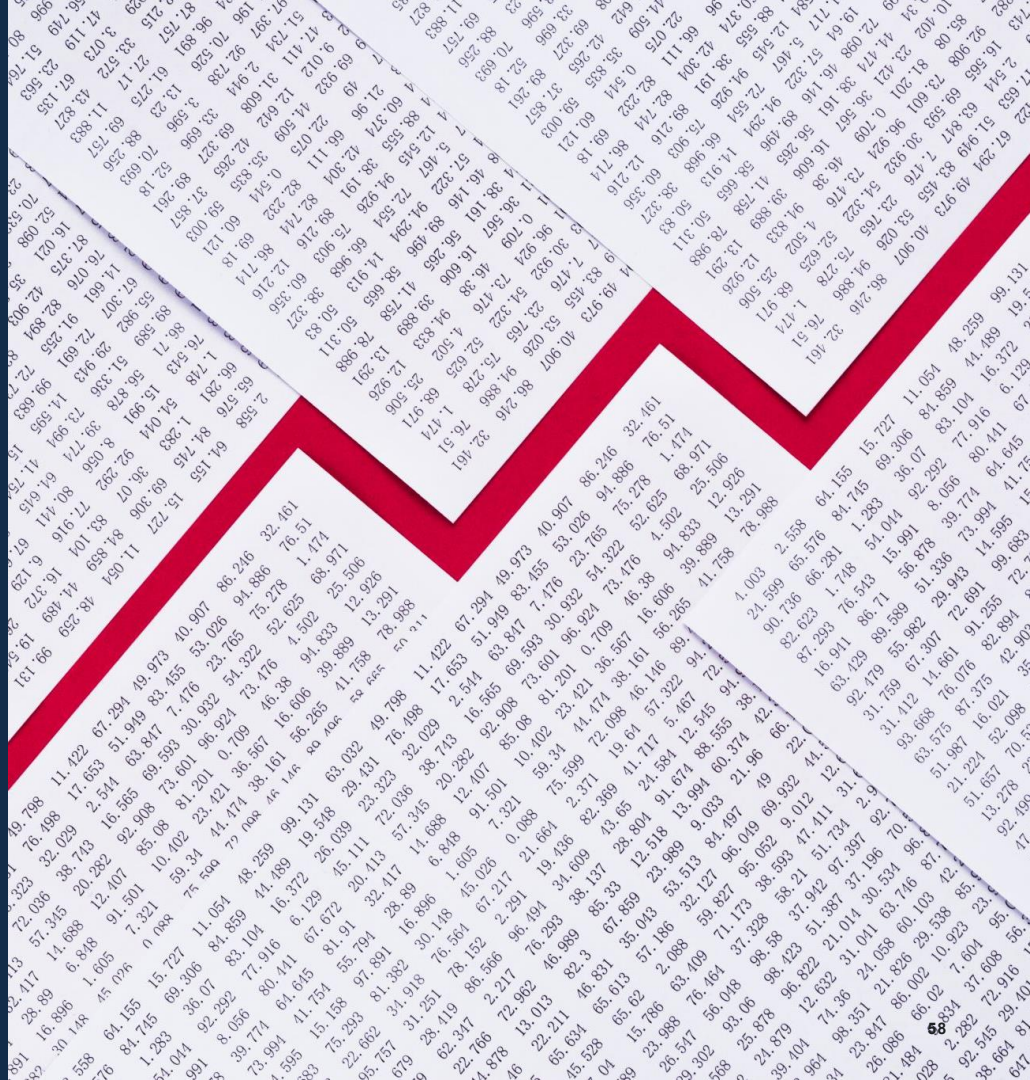
More details

4.30

Average Rating



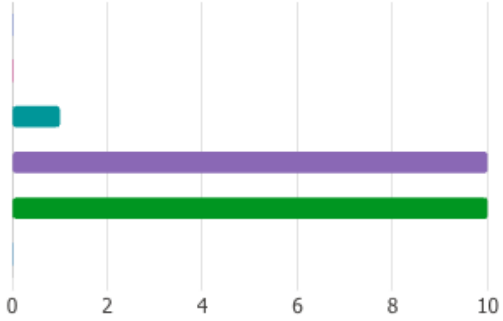
5.5 [RLS] Release



2. Clarity and Understandability: How clear and easy to understand is the proposed content for this section?

More details

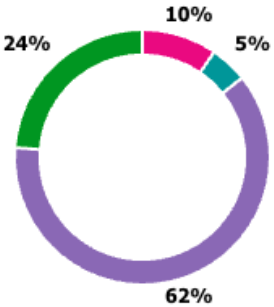
Not Clear	0
Somewhat clear	0
Neutral	1
Clear	10
Very Clear	10
Other	0



3. Practicality and Implementability: How practical and implementable do you find the requirements/guidance in this section for your organization or typical stakeholders?

More details

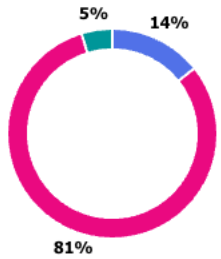
Not Practical	0
Somewhat practical	2
Neutral	1
Practical	13
Very Practical	5



4. Do you feel anything significant is missing from this section?

More details

Yes	3
No	17
Maybe	1



5. If you felt that something significant is missing please specify:

More details

3

Responses

Latest Responses

"A security update might not be suitable for older functionality versions, should use..."

...

5.If you felt that something significant is missing please specify:

1	Open Source Software as Reporter / Recipient of Reports from Downstream
2	What if it is not feasible to fix the vulnerability with an update? Other solutions e.g. product recall, isolation, etc.?
3	A security update might not be suitable for older functionality versions, should users be required to update to the latest functionality version to allow the security update ?

6. Suggestions for Improvement: What specific changes or additions would you recommend for this section?

More details

3

Responses

Latest Responses

"The cryptographic algorithms used in RLS-2 should be linked to the relevant sectio..."

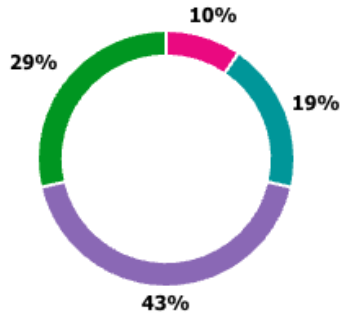
...

6.Suggestions for Improvement: What specific changes or additions would you recommend for this section?

1	There are all together very many points. Could it be reduced?
2	how to prove for new products without a track record as well as clear communication for how to handle in app stores, where it often is just one release.
3	The cryptographic algorithms used in RLS-2 should be linked to the relevant sections.RetryClaude can make mistakes. Please double-check responses.

7. In your opinion, is the proposed section proportionate to the cybersecurity risks it aims to address for organizations of all sizes, particularly Small and Medium-sized Enterprises (SMEs)? More details

Not at all proportionate/Excessive burden	0
Somewhat disproportionate/Significant burden for SMEs	2
Neutral/Unsure	4
Somewhat proportionate/Manageable for most SMEs	9
Very proportionate/Well-adapted for SMEs	6



8. Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME: More details

8
Responses

Latest Responses
"As above, having to provide a security update and validate it for many older functi... "
"The authenticity is typically achieved through digital signatures. In my experience, ... "
...

4 respondents (50%) answered SMEs for this question.

8.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

1	Straight Forward
2	Very common process, no need for anything fancy
3	Again SMEs are usually ressource constrained, and I don't see how a small business can handle all this.
4	OSS Unclarity
5	SME would be challenged not by this methodological framework but anyway with cybersecurity
6	testing is a bit hard if you allow to many versions to live in parallel
7	The authenticity is typically achieved through digital signatures. In my experience, digital signatures pose a significant challenge for SMEs, from key management all the way to production.

8.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

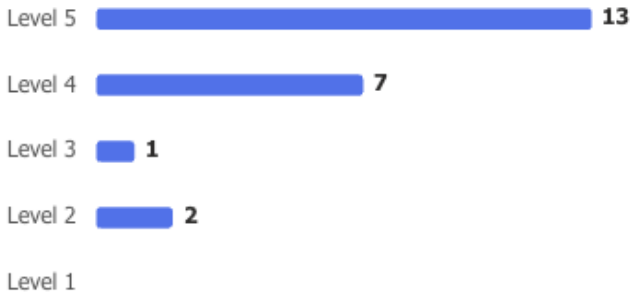
8	As above, having to provide a security update and validate it for many older functional versions would be a big burden for SMEs. Restricting security updates to only the latest functional version would significantly reduce the burden.

9. Overall, how satisfied are you with this section?

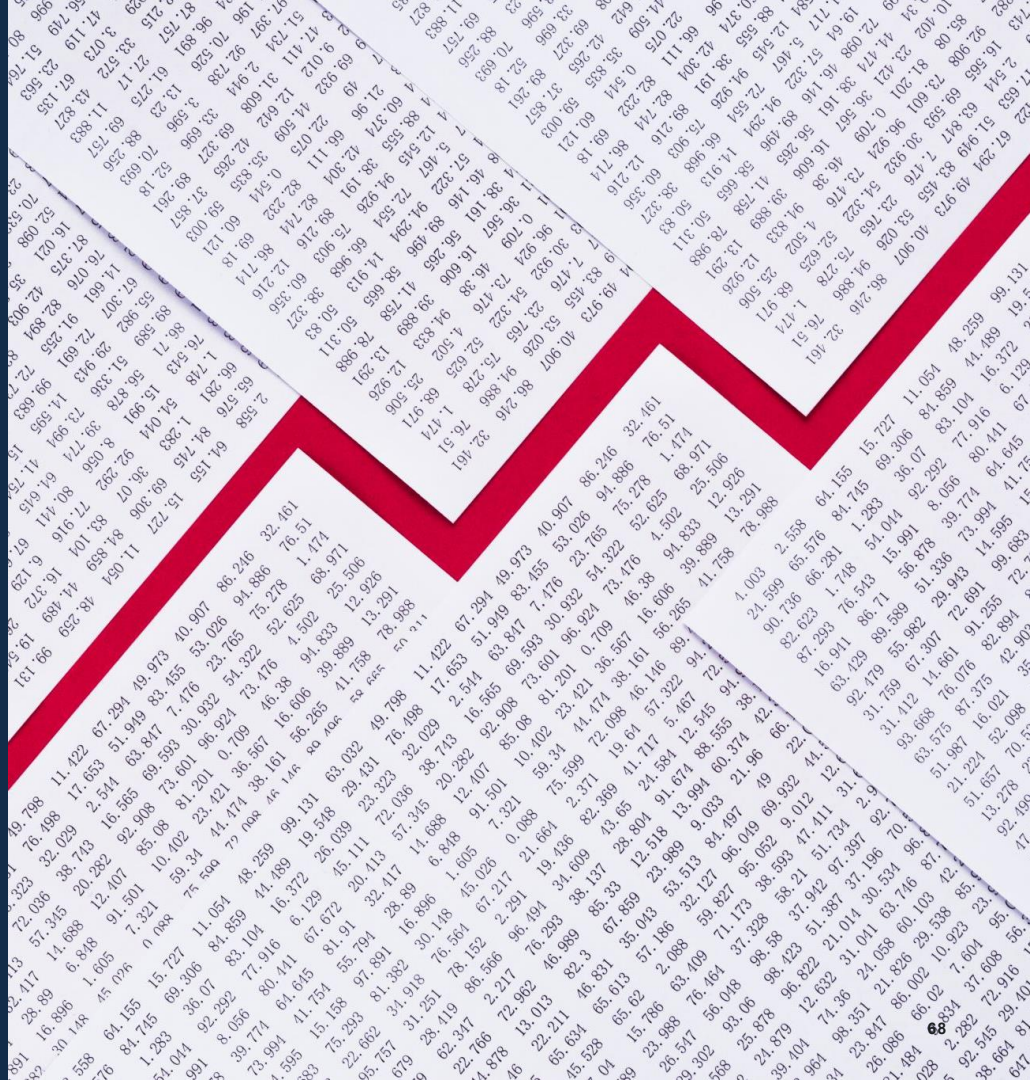
More details

4.35

Average Rating



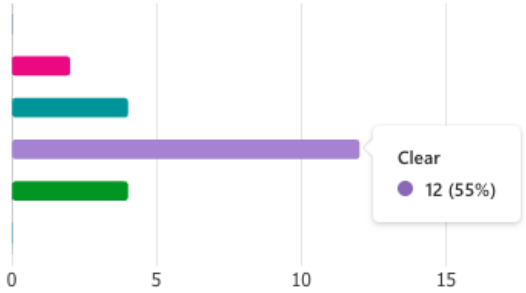
5.6 [PRP] Post Release



2. Clarity and Understandability: How clear and easy to understand is the proposed content for this section?

More details

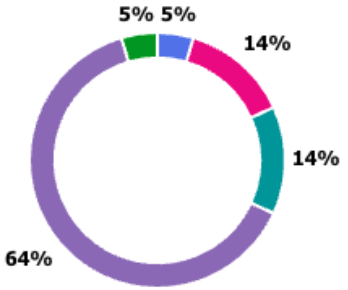
Not Clear	0
Somewhat clear	2
Neutral	4
Clear	12
Very Clear	4
Other	0



3. Practicality and Implementability: How practical and implementable do you find the requirements/guidance in this section for your organization or typical stakeholders?

More details

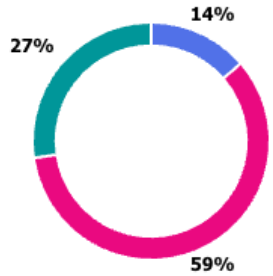
Not Practical	1
Somewhat practical	3
Neutral	3
Practical	14
Very Practical	1



4. Do you feel anything significant is missing from this section?

More details

Yes	3
No	13
Maybe	6



5. If you felt that something significant is missing please specify:

More details

7

Responses

Latest Responses

"Creation of vulnerability history file or database (for internal application software) ... "

"Monitoring update completion percentage and remediation status"

...

3 respondents (43%) answered vulnerability for this question.

5.If you felt that something significant is missing please specify:

1	Looking forward to reading the standard - material
2	Again, OSS is not treated at all here, and I think that needs to be considered.
3	If the exploited vulnerability, incident is in the Remote Data Processing bit, post remediation it feels like there could be updates to internal policies as well.
4	Examples or more specific activities for Post-Release Plan
5	There Stil Seen to be use cases related to HW changes and vulnerabilities
6	Monitoring update completion percentage and remediation status
7	Creation of vulnerability history file or database (for internal application software) should be required. So that new designers can learn from previous issues. Good cross referencing / indexing is essential

6. Suggestions for Improvement: What specific changes or additions would you recommend for this section?

More details

5

Responses

Latest Responses

...

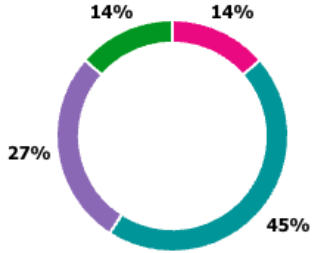
1 respondents (20%) answered OSS Expectations for this question.

6.Suggestions for Improvement: What specific changes or additions would you recommend for this section?

1	Straight Forward
2	OSS Expectations
3	Not sure this requirement that is not related to an ER belongs in a harmonised standard - while it is absolutely a good idea, the implications of it being in a harmonised standard means smaller organisations that may choose not to do this may be burdened with the need to engage a notified body
4	Showing typical examples of Post release activities would be very helpful.
5	maybe a baseline of a Plan

7. In your opinion, is the proposed section proportionate to the cybersecurity risks it aims to address for organizations of all sizes, particularly Small and Medium-sized Enterprises (SMEs)? More details

Not at all proportionate/Excessive burden	0
Somewhat disproportionate/Significant burden for SMEs	3
Neutral/Unsure	10
Somewhat proportionate/Manageable for most SMEs	6
Very proportionate/Well-adapted for SMEs	3



8. Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME: More details

2
Responses

Latest Responses

"be mindful of this being a process documentation exercise more than a practical a... "

...

8.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

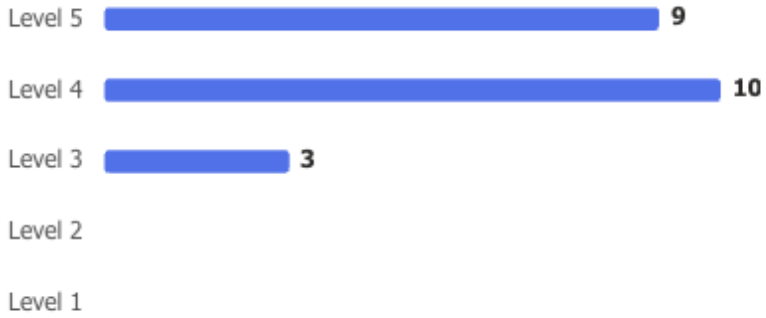
1	It doesn't address Open Source
2	be mindful of this being a process documentation exercise more than a practical approach or testing requirement.

9. Overall, how satisfied are you with this section?

More details

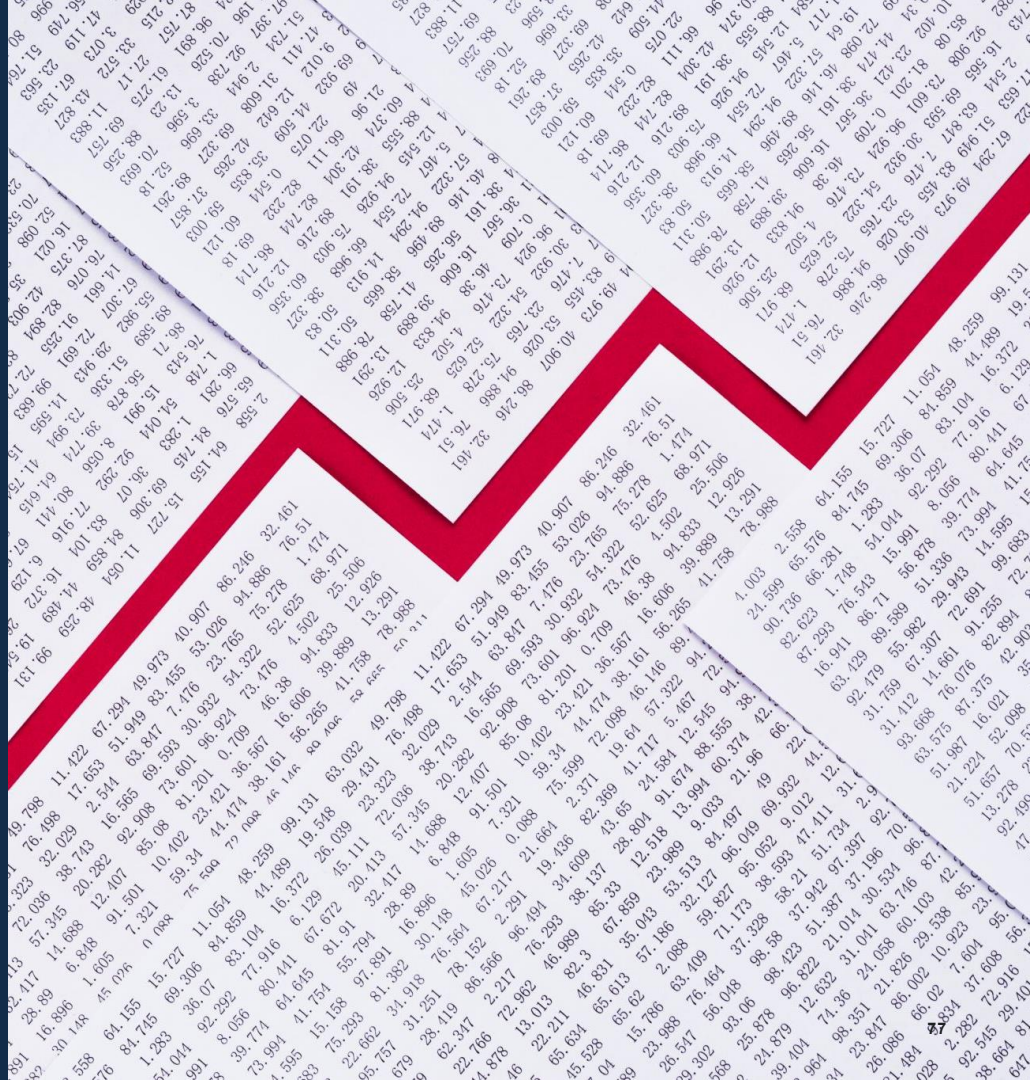
4.27

Average Rating



Conclusion

Post-Workshop Survey: Cyber Resilience Act - Vulnerability Handling

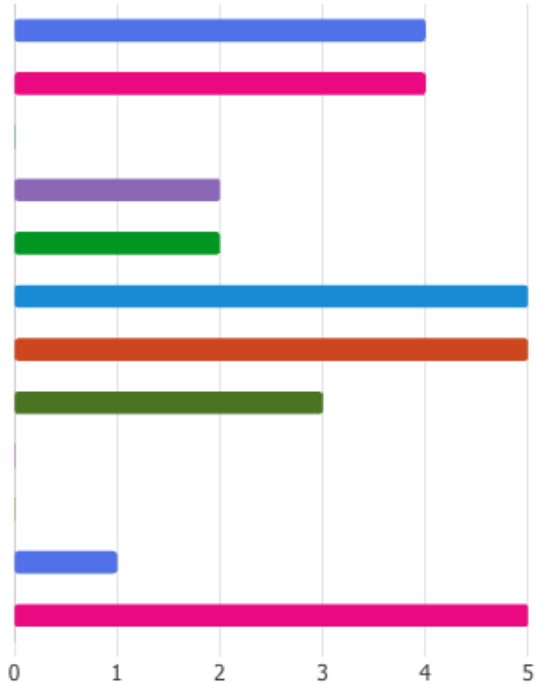


Vulnir

2. Which of the following best describes your primary affiliation? (Select all that apply)

More details

Open-source community member	4
Small and Medium-sized Enterprise (SME)	4
Large enterprise	0
Academic/Research institution	2
Government/Regulatory body	2
Cybersecurity consultant	5
Software developer/vendor	5
Hardware manufacturer	3
Legal professional	0
Importer	0
Distributor	1
Other	5



3. What is your primary role or area of expertise related to cybersecurity or product development?

More details

11
Responses

Latest Responses

"certification"

"Product Security Incident Response, Secure software development, cybersecurity e... "

"My work focuses on cybersecurity standardization, open source development, and ..."

...

4 respondents (36%) answered Cybersecurity for this question.

3.What is your primary role or area of expertise related to cybersecurity or product development?

1	Product management
2	Product Security Manager
3	Pentesting and vulnerability assessment
4	I'm project manager regarding the development of a vulnerability management platform. We will be building extra features to make the CRA requirements easier to comply by automating parts of the process.
5	Smart is an engineering service provider for embedded devices and also embedded product security. As port of this we provide consulting services regarding RED DA and CRA.
6	Presales - Cybersecurity Solution Architect
7	I wear many hats, open source, SME, rapporteur

3.What is your primary role or area of expertise related to cybersecurity or product development?

8	Enterprise Architect for Fire Safety Products, Cybersecurity Evangelist, CLC TC79 WG17 member
9	My work focuses on cybersecurity standardization, open source development, and industrial security standards. I am actively involved as a member of Taiwan's Standard Committee, contributing to the development of national cybersecurity standards and guidelines, working closely with government agencies on strategic directions, and supporting the practical implementation of cybersecurity standards across industries. Within the open source community, I serve as a Debian Developer, contributing to maintaining various security-related tools and packages within the Debian ecosystem. In addition, I actively participate in ISA and IEC standards committees, particularly focusing on the ISA/IEC 62443 series for industrial cybersecurity. Currently, I serve as the co-chair for the 62443-3-1 working group on industrial control systems security technical requirements, and as one of the editors for the 62443-4-1 standard, which addresses secure software development lifecycle practices and vulnerability handling processes. This standard is notably referenced in NIST SP 800-218 (Secure Software Development Framework).

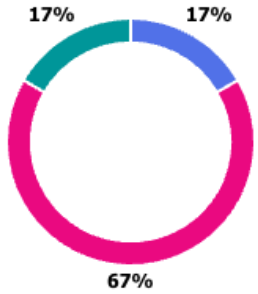
3.What is your primary role or area of expertise related to cybersecurity or product development?

10	Product Security Incident Response, Secure software development, cybersecurity education, coordinated vulnerability disclosure
11	certification

4. Does you organization aperate already a Product Security Incident Response Team (PSIRT)?

More details

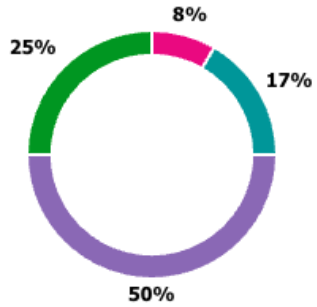
Yes	2
No	8
Maybe	2



5. Prior to this workshop, how familiar were you with the Cyber Resilience Act (CRA)?

More details

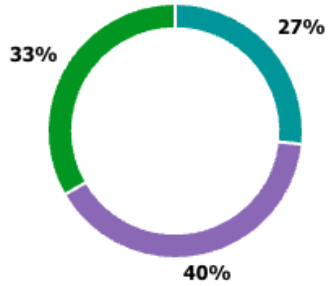
Not at all familiar	0
Slightly familiar	1
Moderately familiar	2
Very familiar	6
Expert	3



6. How familiar are you with Vulnerability management handling?

More details

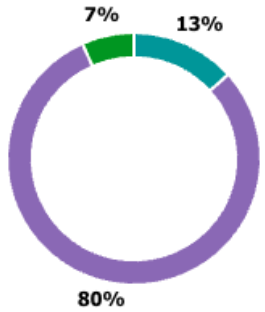
Not at all familiar	0
Slightly familiar	0
Moderately familiar	4
Very familiar	6
Expert	5



7. Do you believe the current draft adequately addresses the key challenges and needs related to digital product security, specificall y vulnerability handling?

More details

Strongly Disagree	0
Disagree	0
Neutral	2
Agree	12
Strongly Agree	1



8. Please elaborate on the previous answer (if you wish to highlight any point on the level of adequacy of PT3 draft standard)

More details

7

Responses

Latest Responses

"Some definitions and criteria within the draft could potentially benefit from further..."

...

3 respondents (43%) answered draft for this question.

8.Please elaborate on the previous answer (if you wish to highlight any point on the level of adequacy of PT3 draft standard)

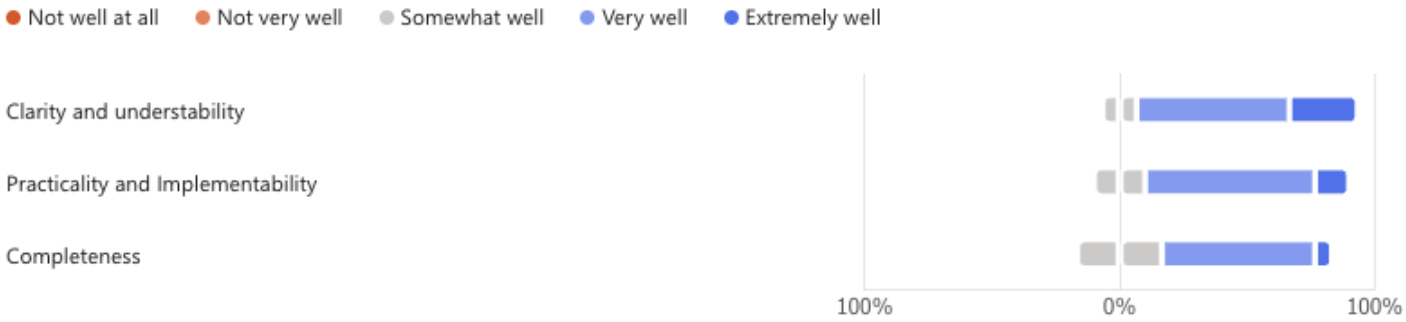
1	There are a few points which leave loopholes if a manufacturer is inclined to escape the obligations under the CRA.
2	It seems to provide pretty clear guideance
3	I think the draft covers the biggest requirements and also provides with extra materials to make it easier to educate yourself further.
4	This is a challenging standard and very important for manufacturers
5	The current draft provides a generic framework that can be applicable as is. The vendor shall adapt it to the criticity level of its product
6	- OSS is missing in many places. - SBOM, HBOM, CBOM - seems like it could be a challenge to adapt to market expectations

8.Please elaborate on the previous answer (if you wish to highlight any point on the level of adequacy of PT3 draft standard)

7	Some definitions and criteria within the draft could potentially benefit from further refinement to support more consistent interpretation across different organizations. This might help reduce implementation variations that could affect the intended security outcomes. Regarding the Software Bill of Materials (SBOM) requirements, there seems to be room for more specific guidance on content and scope boundaries. Areas that might warrant additional detail include component identification depth, dependency mapping requirements, and metadata specifications for software components. Implementers might benefit from clearer direction on handling transitive dependencies, dynamically linked libraries, and determining appropriate granularity levels.

9. How would you rate overall the presented draft standard on the following characteristics?

More details



10. Please explain your reasoning on your rate (at question n 9) if you have additional point to highlight

More details

5
Responses

Latest Responses
"The draft provides comprehensive coverage of vulnerability handling processes, in... "
...

1 respondents (20%) answered vulnerability management for this question.

10. Please explain your reasoning on your rate (at question n 9) if you have additional point to highlight

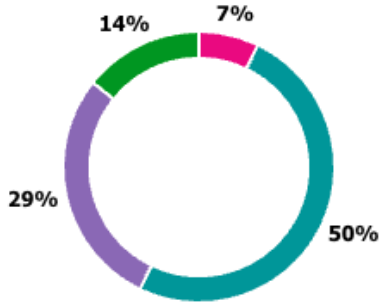
1	Regulatory capture is one of the dangers. The other danger is a wealth of exceptions to choose from.
2	Thank you for sharing all your insights and advancement on PT3, it was very rich in information.
3	Organisational view of strategic vulnerability management interplaying internal manufacturers is missing.
4	The presenter iterates over each requiremement and explain how to address them with set of examples.
5	The draft provides comprehensive coverage of vulnerability handling processes, including receiving, reviewing, assessing, addressing, disclosing, and post-release management.
6	

10. Please explain your reasoning on your rate (at question n 9) if you have additional point to highlight

6	Practices that the WG believes must be done in manufacturers to achieve the goal of CRA should be written in the harmonized standards as explicitely as possible. As far as I've engaged with manufacturers, they tend to attempt to minimize the impact of CRA by interpreting requirements, sometimes incorrectly, at the convenience of themselves. (e.g. "We already have IEC 62443 certification and our PSIRT so no additional work is required"). In fact, Management and product development teams often put strong pressure to do that to the divisions in charge of CRA implementation, such as security division or compliance division. In addition, requirements imposed by manufacturers but not explicitly written in the requirements or standards are often subject to rejection or additional claim of cost by suppliers, even if these are the established cybersecurity best practices. Explicit requirements definition helps such divisions to justify their budget requests to management and to communicate with product development team and suppliers for understanding and support in the additional processes/specifications to comply with CRA.

11. How well do you believe the proposed CRA Vulnerability Handling standard draft integrates with or builds upon existing standards like EN ISO/IEC 30111:2020 (Vulnerability Handling Processes) and EN ISO/IEC 29147:2020 (Vulnerability Disclosure)? More details

Poorly Integrated	0
Adequately Integrated	1
Neutral / Unsure	7
Well Integrated	4
Very Well Integrated	2



12. Suggestions for Improvement: What specific changes or additions would you recommend (in terms of relation with ISO 30111 and ISO 29147) More details

3
Responses

Latest Responses

"Generally, standards (ISO 30111 and ISO 29147) tend to focus on defining "what" r... "

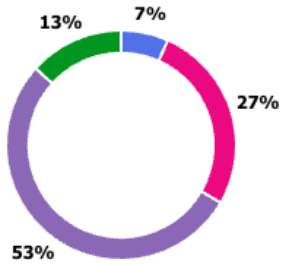
...

12.Suggestions for Improvement: What specific changes or additions would you recommend (in terms of relation with ISO 30111 and ISO 29147)

1	One of the problems I see here is that you are referring to proprietary standards with the expectation that the reader has access, when this is not necessarily the case.
2	I guess I have to go read 30111 and 29147 before I can answer that
3	Generally, standards (ISO 30111 and ISO 29147) tend to focus on defining "what" rather than "how," though for harmonized standards, there might be some consideration for including additional descriptive content and guidance, perhaps drawing from approaches used in standards like ISO/IEC 18031. Additionally, the SBOM supplementary requirements could potentially benefit from clearer specification regarding scope, content, and related requirements. The OpenChain project has developed some guidance that might be worth considering as a reference: https://github.com/OpenChain-Project/Telco-WG/blob/main/OpenChain-Telco-SBOM-Guide_EN.md This resource appears to offer practical perspectives on SBOM implementation that could potentially inform discussions around the standard's requirements definition, particularly when considering how to establish appropriate boundaries for SBOM content and compliance criteria.

13. In your opinion, is the proposed CRA Vulnerability Handling standard draft proportionate to the cybersecurity risks it aims to address for organizations of all sizes, particularly Small and Medium-sized Enterprises (SMEs)? More details

Not at all proportionate/Excessive burden	1
Somewhat disproportionate/Significant burden for SMEs	4
Neutral/Unsure	0
Somewhat proportionate/Manageable for most SMEs	8
Very proportionate/Well-adapted for SMEs	2



14. Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME: More details

8
Responses

Latest Responses
"Small Enterprises do not have the engagement with upstream open source creator... "
"Based on my experience with cybersecurity standards implementation, I would like... "
...

5 respondents (63%) answered SMEs for this question.

14.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

1	SMEs may not have the resources or knowledge at hand to exploit loopholes, but larger enterprises may pull that off.
2	There might be a huge burden regarding regular security testing, and the incident response time. Also - as we do currently experience with RED DA - the paperwork even for self assessment is huge and standards like 18031 is hard to understand for developers/companies with no security background.
3	Risk of products are equal to any sized enterprize. I believe industrial collboration of vulnerability collection and evaluation is needed especially for SME'S.
4	As indicated earlier, I see the proposed CRA Vulnerability Handling as a framework that can be adapted to products no matter the size of the company.
5	For SME's yes, for Open Source - that's totally questionable

14.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

6	Resource constraints for a lot of the stuff is a major topic, so a lot of the stuff seems a little bloated for small teams (i.e. 5-10 people). Also, it always feels like we still chase a moving target. This is fine for big corporations which can afford to put dedicated ressources on the topic, but leads to cognitive overload for SMEs.

14.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

7	Based on my experience with cybersecurity standards implementation, I would like to share some observations regarding potential challenges for SMEs. The comprehensive vulnerability handling process, while thorough in covering receiving, reviewing, assessing, addressing, disclosing, and post-release activities, might present resource allocation challenges for smaller organizations. SMEs often operate with limited cybersecurity personnel and may find it difficult to establish dedicated processes for each phase of vulnerability management without significant strain on their existing resources. Regarding SBOM requirements, if these demand extensive component identification and dependency mapping, this could prove resource-intensive for organizations with limited technical infrastructure. Smaller companies may lack access to automated tools necessary for generating and maintaining comprehensive SBOMs, potentially requiring manual processes that are both time-consuming and prone to errors. From an implementation perspective, SMEs might benefit from more scalable guidance that allows for proportionate responses based on organizational size and risk profile. The associated costs of compliance tools, third-party assessment services, and ongoing maintenance activities could disproportionately impact smaller organizations compared to larger enterprises with dedicated cybersecurity budgets. It might be worth considering whether the standard could incorporate risk-based approaches that allow SMEs to prioritize implementation based on their specific threat landscape and business context, while still maintaining the overall security objectives. This could help ensure that the standard remains accessible to organizations of varying sizes and capabilities.

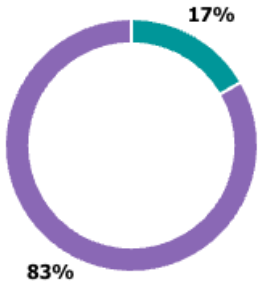
14.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

8	Small Enterprises do not have the engagement with upstream open source creators to effectively meet their Manufacturer obligations

15. Overall, how valuable was this deep-dive session for you?

More details

Extremely not useful	0
Somewhat not useful	0
Somewhat useful	2
Very useful	10
Extremely useful	0



16. What was the most valuable aspect of this workshop for you?

More details

8
Responses

Latest Responses
"Based on my participation in the workshop, the collaborative exchange of different..."
...

5 respondents (63%) answered requirement for this question.

16. What was the most valuable aspect of this workshop for you?

1	understanding the Standards approach
2	Clarification of the requirement and work advacement. Description of the process for vulnerability management and CRA application.
3	Getting a clear overview on all the requirements and also the extra materials / examples
4	I understood the structure of this standard.Overview
5	The explaination of each requirement and the examples
6	The slides helped me understand things better.
7	Getting a profound introduction into the requirements of vulnerability handling

16. What was the most valuable aspect of this workshop for you?

8	Based on my participation in the workshop, the collaborative exchange of different perspectives on implementation challenges was particularly valuable to me. The discussions around clarifying definitions and criteria in the draft standard helped me better understand areas where additional precision might be beneficial. I found the conversations about SBOM requirements and their practical implications for organizations of different sizes to be quite insightful. The workshop format provided a constructive environment for contributing to the refinement of important cybersecurity standards, which I found meaningful from both a learning and collaborative perspective.

17. What was the least valuable aspect, or what could be improved?

More details

5

Responses

Latest Responses

"Based on my experience in the workshop, there were a few areas that might benefi..."

...

2 respondents (40%) answered valuable for this question.

17.What was the least valuable aspect, or what could be improved?

1	Post-release activity is unclear
2	To inform overview of the standard is valuable and improve for operational view.
3	N/A
4	It could have been a couple hours longer, I feel that toward the end it was rusted.

17.What was the least valuable aspect, or what could be improved?

5	Based on my experience in the workshop, there were a few areas that might benefit from enhancement in future sessions. The time allocation for certain discussions seemed somewhat uneven, with some important technical details receiving limited exploration while other topics had extended coverage. This occasionally made it challenging to fully develop certain points that could have benefited from deeper examination. I observed that some discussions tended to focus more on high-level concepts rather than diving into specific implementation scenarios that organizations might encounter. Having more concrete examples or case studies could potentially help participants better understand how the standards would apply in practice. Additionally, it seemed that some technical nuances around SBOM requirements and vulnerability handling processes could have used more detailed exploration, particularly regarding how these requirements might scale across different organizational contexts. These are modest observations, and overall the workshop provided valuable collaborative opportunities. Future sessions might consider incorporating more time for detailed technical discussions.

18. Any additional comments or feedback you'd like to share regarding the CRA Vulnerability Handling standard or the workshop of today? More details

3

Responses

Latest Responses

...

18. Any additional comments or feedback you'd like to share regarding the CRA Vulnerability Handling standard or the workshop of today?

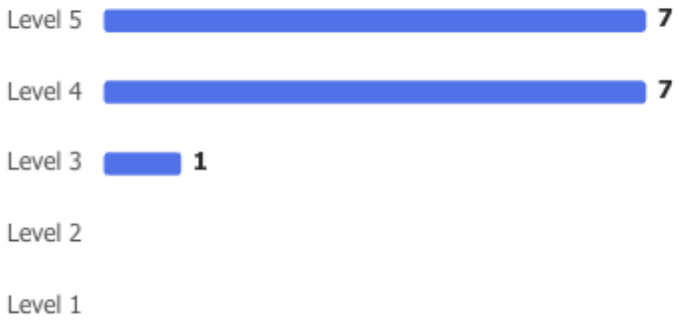
1	Good job, continue like that
2	Thanks for this!
3	Please share the presentation really soon

19. Overall, how satisfied are you with the PT3 draft as it is today?

More details

4.40

Average Rating



Thank you

VULNIR.com

info@vulnir.com