CYBELLUM

The Product Security Maturity Model
Complying on another level

Table of Contents

Product Security is Maturing 3

The Four Pillars of Product Security Maturity 4

- Pillar 1: Asset Management 5
- Pillar 2: Assurance 6
- Pillar 3: Compliance 7
- Pillar 4: Risk Management 8

Product Security Maturity Levels in Action 9

- Level 0 9
- How do Level 0 teams begin product security activities? 9
- Level 1 10
- How do Level 1 teams conduct product security activities? 10
- Level 2 11
- How do Level 2 teams conduct product security activities? 11
- Level 3 12
- How do Level 3 teams conduct product security activities? 13
- Level 4 13
- Envisioning the future of product security 14

About us 15

Resources 16

Product Security is Maturing

We are in an era of regulatory catch-up, where best practices have been codified into law.

As long-anticipated regulations come into force, product security managers and executives are beginning to feel comfortable taking their hands off of the controls and allowing automation to conduct the menial tasks as they guide the ship. This maturing of practices that allowed for data sources to be reliable and reporting to be consistent came from years of trial and error in anticipation of this very moment.

Today's reality remains that most teams are still in the earlier days of their maturity journey– struggling to align sources and automate the tasks that impact a product's management, assurance levels, compliance standing, and overall risk.

Now, with so many product security regulations coming into force, those who are not progressing on their product security maturity are so buried under alerts (many of which are irrelevant or less than critical) and newly emerging crises, that they can't see the regulatory forest for the trees.

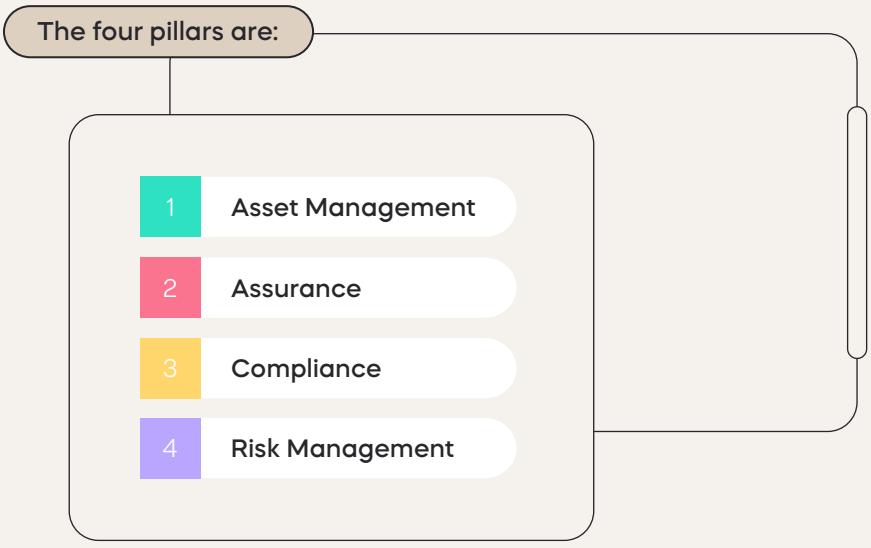
To address this challenge, we put together the Product Security Maturity Model, allowing companies to follow guidelines, that are based on regulations, best practices, and methods to secure products well into the future. Today, this model has helped teams understand where they can improve and the best practices to follow to reach the next level, including easing the path to compliance for R155, FDA PMA, NIS2, CRA, ISO 62443, and more.

Wherever you are on your product security maturity journey, we invite you for an inside look into how we encourage companies to systematically comply at scale.

The Four Pillars of Product Security Maturity

As the world of product security undergoes new challenges, solutions, and evolving regulations, understanding an organization's current security posture and delineating clear paths for improvement are paramount.

While compiling data from regulations, vulnerability assessments, and leaders in the field, we found that most product security activities fall into four buckets, which we call 'pillars'.



Just like pillars holding up a structure, the four product security maturity pillars can not function as standalone entities. Rather, they are deeply intertwined, ensuring a holistic approach to security.

It is critical to recognize that advancement in one area necessitates progression in others. For example, stagnation in asset management will undermine product security efforts related to assurance and vulnerability management.

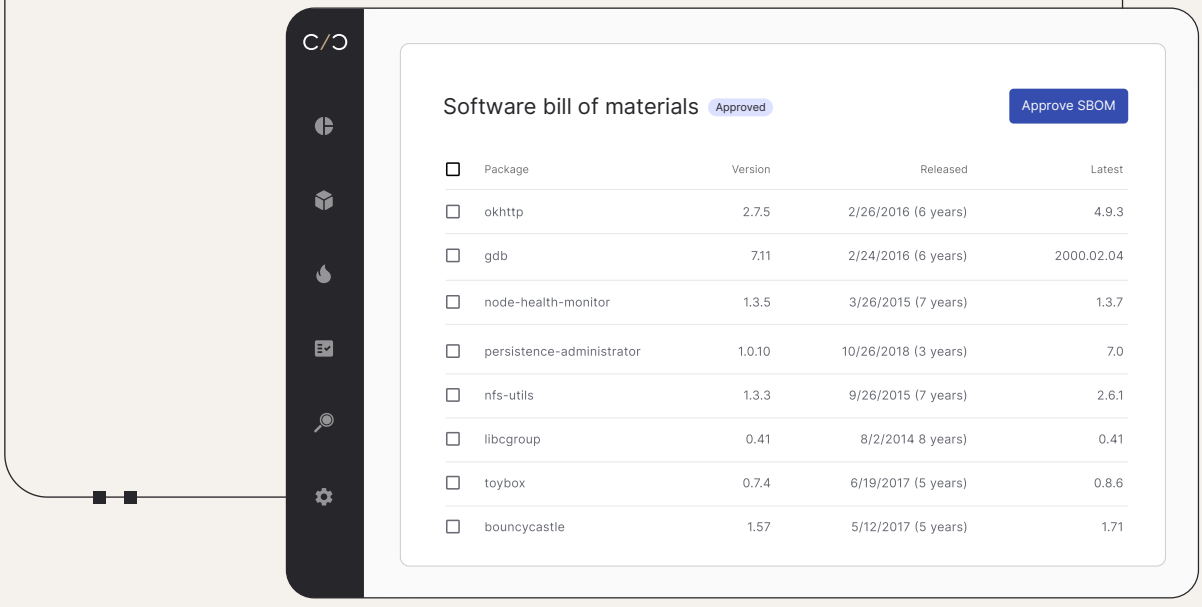
Achieving level three maturity in Asset Management, for instance, while remaining at level one in Assurance, is not only impractical but also counterproductive. Each pillar reinforces the others, creating a robust and resilient security posture. Let's delve into each pillar to understand its essence and the journey towards maturity.

1

Pillar 1: Asset Management

At the heart of any cybersecurity strategy lies a fundamental question: What are we protecting? This is where Asset Management comes into play. Initially, it's about defining your assets - identifying what is crucial for your operations and what could be potential targets for threats. As organizations mature in this pillar, they start incorporating an increasing number of data sources, enriching their understanding of the assets. High-level maturity involves leveraging detailed information from Hardware Bill of Materials (HBOMs), Software Bill of Materials (SBOMs), and Vulnerability Exposure and Evaluations (VEX)/ vulnerability reports. This comprehensive approach provides a detailed birds-eye view of all assets, especially those within development environments, ensuring nothing is overlooked.

The takeaway here is clear: from simplicity to comprehensive coverage, Asset Management provides the foundation of knowing what you have and what needs safeguarding.



Understanding assets begins with a managed repository of all internal components, also known as SBOM Management.

2

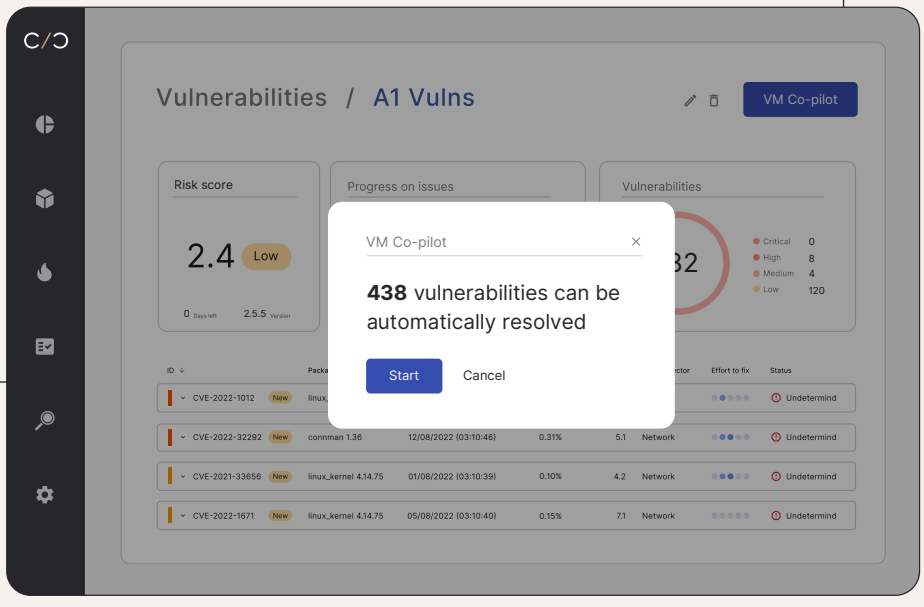
Pillar 2: Assurance

Assurance is about finding risks and vulnerabilities, coding weaknesses, and validating security measures so teams can manage product security without missing a beat. It starts with conducting assessments - how these are managed, triaged, and enriched with data from various sources, marks the maturity of this pillar.

For comparison, a company with level 1 maturity may collect data from the NVD and compare it to a list of components kept in a spreadsheet. Maturing this process will allow CPSOs to cut resources, improve operational efficiency, and begin conducting product security at scale. In practice, companies can add vulnerability sources to gain the full context of a threat beyond the limited NVD data, implement automation to create and manage SBOMs, and rely on this automation to better prioritize threats. The Product Security Platform does this with the VM-CoPilot by conducting vulnerability scans and relying on a contextualized automated engine to triage findings and allow teams to address risks accordingly.

As the ability to track and manage vulnerabilities grows, organizations can employ advanced testing methodologies such as fuzz and penetration testing, and post-production practices like incident response via well-prepared Product Security Incident Response Teams (PSIRT). Teams can remain confident that the data created by these activities is aggregated and merged to gain a bird's eye view of risk.

The key takeaway is that quality equates to security. The synchronization of quality assurance processes with security measures, often mandated by federal regulations, ensures not only compliance but also robust security.



Develop internal policies to ensure they meet other company needs

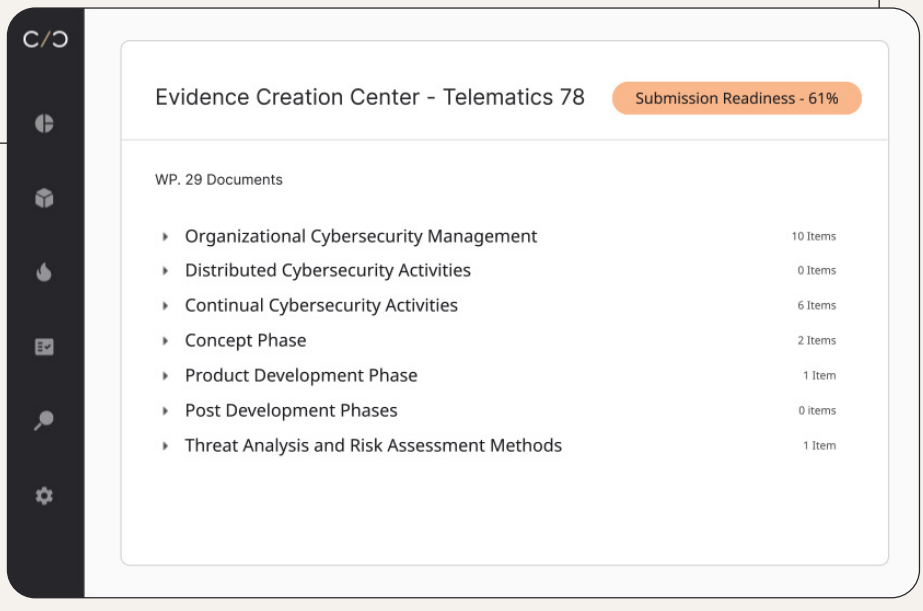
3

Pillar 3: Compliance

While quality products are top of mind for manufacturers, complying with regulations is what keeps connected devices on the market. A robust compliance program entails the organized collection, digestion, and production of documents that provide insight to auditors and a supplier's customer's auditors into how component vulnerabilities are discovered and managed.

Maturity in this pillar can be understood as a team's audit readiness. Moving away from ad hoc collections that risk sending teams into a resource-intensive reverse-engineering documentation frenzy, teams must take it upon themselves to embrace automation tools that help conduct activities and create the audit-relevant evidence needed with a few clicks. For example, a high maturity level means you can produce a full, up-to-date list of SBOMs and assets at any given time. It also means you have the ability to provide evidence into which vulnerabilities were fixed, how and when they were fixed, as well as showcase pen test results and threat models, all from one data system.

To streamline this process and give CPSOs the peace of mind needed for scheduled or even surprise audits, teams in automotive, medical devices, and other sectors must have a centralized data system in place that can ingest information from internal teams and external vendors for full evidence integration. An example of this is The Product Security Platform, which extracts data from any given point and generates evidence for auditors as mentioned above.



Review compliance status for each regulation then quickly develop reports to share with stakeholders and auditors.

4

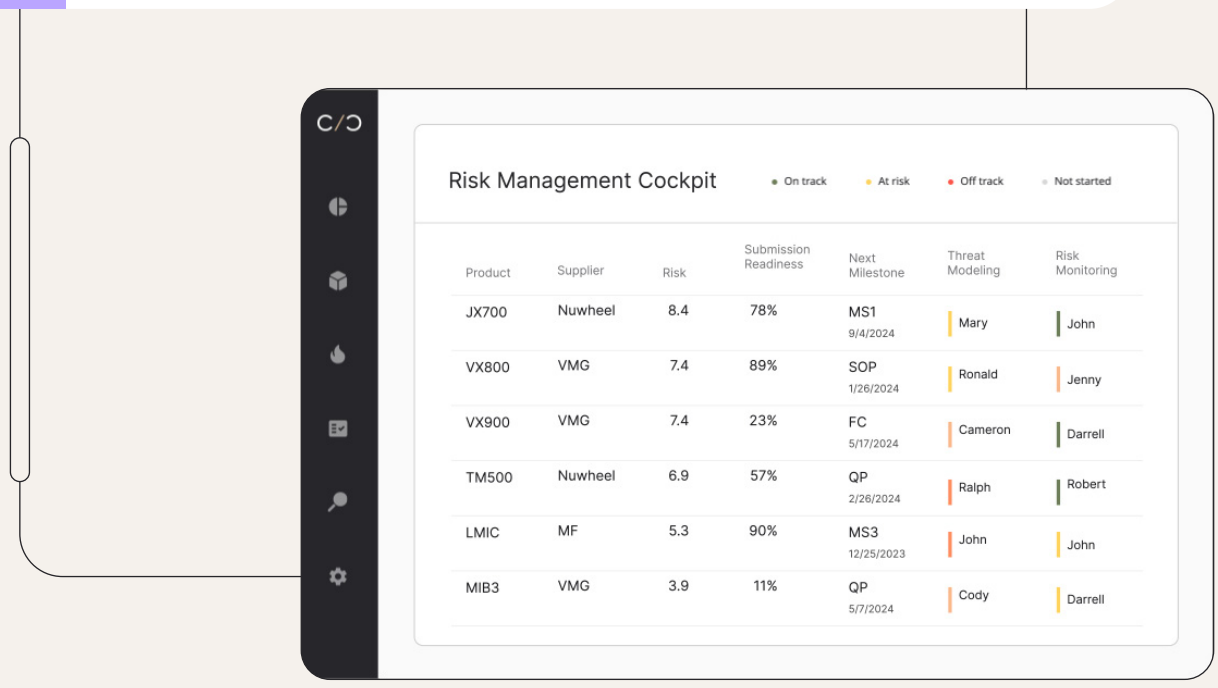
Pillar 4: Risk Management

Risk Management is the executive overview of how security products are managed across the board. It's about providing risk professionals and C-level executives with a clear picture of how security is being advanced within and across teams.

An organization's ability to track, manage, and govern its security practices measures the maturity of this pillar with automation and full risk management integration as its key cornerstone.

Relevant asset sources, such as CI/CD information and robust up-to-date SBOMs are accompanied by threat modeling feeds, PSIRT preparation, and pen test results are integrated into a centralized system. Once automation is implemented, teams can reduce their burden on manual tasks and implement real-time dashboards that offer critical alerts and insights.

The takeaway is straightforward: effective risk management demands putting processes into place that allow for a bird's eye view– allowing CPSOs to govern and direct the security posture organization-wide.



Investigate incidents and understand your product security posture to better balance risk and ensure continuity.

The Four Pillars of Product Security - Asset Management, Assurance, Compliance, and Risk Management - provide a structured framework for organizations to assess and improve their cybersecurity posture.

In the following sections, we'll explore each level, see examples of what teams look like at each stage, and understand the next steps.

Product Security Maturity Levels in Action

Level 0

The beginning is where we have traditionally all started. While CISA has provided a starter guide on how to begin with a security-first approach with their 6 SBOM types, nearly all product security professionals have worked in a situation where they have a product and must travel back in time to retroactively build a security system within it.

Assets- Non-specific knowledge of assets and variations

- No awareness of internal components
- Unable to compile an SBOM

Assurance- No cybersecurity steps taken

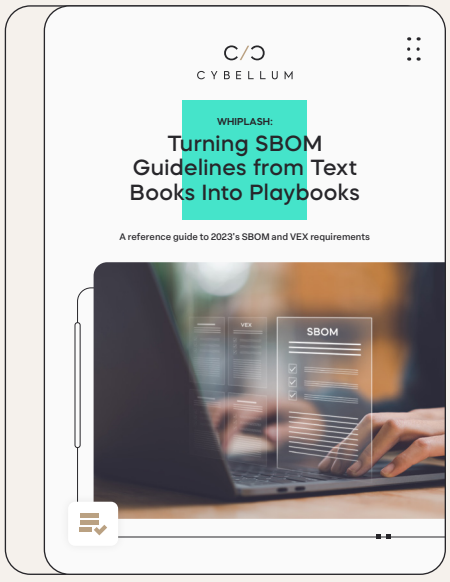
- Lack buy-in or are unaware of cybersecurity realities
- “We are so small, no one would think to attack us”

Compliance

- No one designated to compare development practices or product realities against local regulations
- Large liability

Risk- Manual data gathering and point-in-time report creation

- May carry out basic functions using tools intended for other environments
- Lack of awareness surrounding product security risks



How do Level 0 teams begin product security activities?

This team has found itself at the onset of a journey just like a classic coming-of-age story. They have a product that is functionally ready to hit the market or may even have one already deployed but they must secure their connected device in a way that has not yet been considered.

This can be due to new regulations or identifying a catastrophic vulnerability that must be mitigated.

They begin activities by deconstructing the product’s software piece by piece. Each discovered software component must be listed so it can be checked later against vulnerabilities or other known threats.

While beginning with a platform, such as The Product Security Platform will allow them to rapidly understand threats within the context of a product’s full internal system, many of them begin with spreadsheets that are doomed to become obsolete shortly after asessments are conducted, as new open source or unsecured components are added, discovered, or replaced regularly.

Level 1

Level one is defined by teams who are still exploring the realities of the threat landscape. This means they already fulfill the basic requirements of SBOMs and assurance, but do it in a mostly manual, and non-scalable way, which requires a lot of resources and is difficult to track.

Assets- Basic SBOM Generation

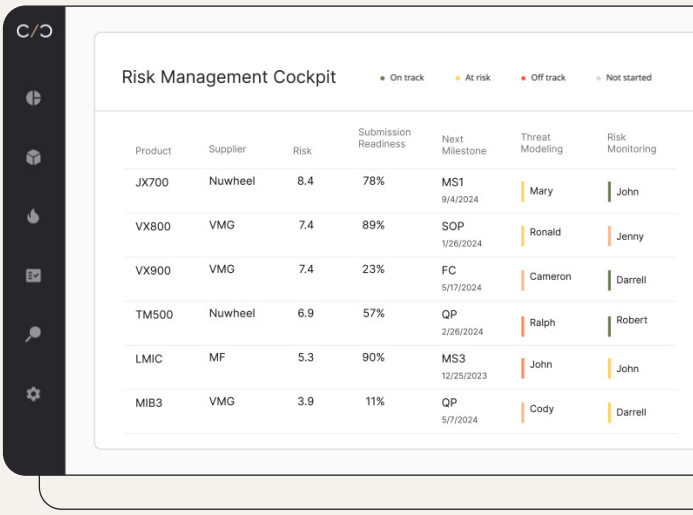
- Importing and creating SBOMs
- Reliance on one source for SBOMs (such as binary scanning)

Assurance- Basic Vulnerability Monitoring

- Mapping vulnerabilities and CVEs to SBOMs

Compliance- Ad-hoc compliance ("I'm surprised by an audit")

- Compliance reports exist but are disconnected, no consistent format or central repository
- Compliance is more reactive - less knowledge of where things are, so there's a need to actively look for the data, the security protocols



The Product Security Platform allows managers to understand their product's risk based on the latest data

Risk- Manual data gathering and point-in-time report creation

- No centralized destination for risk management
- Risk status has to be pieced together manually based on data from multiple sources

How do Level 1 teams conduct product security activities?

Teams who are at level 1 have begun the process of collecting and organizing data surrounding their products and the threats they hold. While their efforts may prove useful when dealing with individual queries, the lack of automation creates gaps in their efforts, straining resources during routine operations.

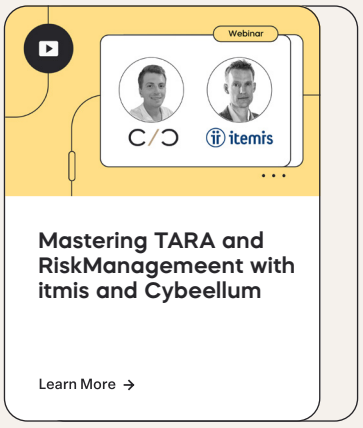
To reach Level 2, these companies must implement a product security system. The Product Security Platform, where workflows can be created based on NTIA minimum elements and other frameworks, collects accurate data on what's in their products via SBOM generation and management. With a centralized location, such as those created by The Product Security Platform, teams can maintain reports in a central repository and use dashboards to understand what challenges lay beyond immediate emergencies.

Level 2

Level 2 shows a greater awareness than Level 1 surrounding streamlined processes, better organization, and data collection. While still reactionary, teams can rely on SBOMs and contextualized analysis to gather information for reports or audits.

Asset- Broader Asset Definition & Introduction of Workflows

- Organizations are creating SBOM workflows that meet NTIA standards and include methods from other frameworks.
- Enhancing SBOM accuracy involves adding sources for precise package identification and detailing assets, including HBOMs, and distinguishing between product and component levels.
- Tracking multiple SBOM versions throughout a product's lifecycle is essential for maintaining accurate records of changes and updates.



Assurance- Reactive Contextual Analysis

- Smart filtering techniques are applied to prioritize vulnerabilities based on their context and impact on a company's specific products, incorporating both the context of the vulnerability and its exploitability (EPSS).
- The process predominantly relies on external information sources, resulting in a mostly reactive approach to vulnerability management.

Compliance- Centralized Evidence Creation and Management (“I’m half ready for an audit”)

- Some compliance evidence, like SBOMs, follows a consistent format or framework.
- A unified system exists for creating and compiling compliance evidence from various domains, including SBOMs, assets, vulnerabilities, and risk.
- Compliance efforts are guided by existing frameworks like internal policies, leading to a more proactive approach.
- There's a feature for uploading reports to a centralized repository.

Risk- Partial risk management

- Dashboards are available for certain risk management aspects, like tracking product vulnerabilities.
- The information on these dashboards is not frequently updated.
- There are no established playbooks akin to those used in Security Orchestration, Automation, and Response (SOAR).
- The system lacks real-time alert capabilities.

How do Level 2 teams conduct product security activities?

Level 2 teams conduct product security tasks with a general plan in mind. They utilize multiple data sources within a centralized platform, such as The Product Security Platform, and implement automated workflows to update reports as needed.

While still reactive, these teams have laid the foundation for more robust product security practices (such as those at Level 3) through data collection, contextualized vulnerability data, and a consistent framework for compiling reports.

To reach level 3, these teams must put that data into action by conducting threat analysis, developing playbooks, enriching vulnerability data into the asset repository, auto-generating reports, and more.

Watch: Asaf Atsmon discusses vulnerability Scoring with EPSS and how it helps product security make better risk-management decisions.

Level 3

Level 3 can be understood as the proactivity level. Working together with various stakeholders across an organization and leveraging numerous data sources, product security teams can generate the foundational data they need to meet internal and external demands while more easily producing compliance-relevant documentation.

Multi-type Asset Management, TARA and Sharing

- To enhance accuracy and depth, SBOMs are sourced from a broader range of inputs to and form a comprehensive multi-source overview, including Build SBOMs, Design SBOMs, Implementation SBOMs, offering insights into both product and component compositions rather than just a product-centric perspective.
- The integration of Threat Assessment & Remediation Analysis (TARA) involves importing data into the asset repository to enrich asset information.
- Basic activities related to SBOM sharing are implemented to facilitate information exchange.

Assurance- Proactive Enrichment

- Vulnerability data is enhanced by aligning it with both internal and external policies to provide a more comprehensive security posture.
- The inclusion of additional data sources such as private feeds, fuzz tests, Threat Assessment & Remediation Analysis (TARA), and penetration testing results further enriches the vulnerability analysis.

Compliance- Automated Evidence Management (“I’m fully ready for an audit”)

- Reports are automatically produced using existing data from within your systems, reflecting activities like Software Bill of Materials (SBOMs) and assurance measures.

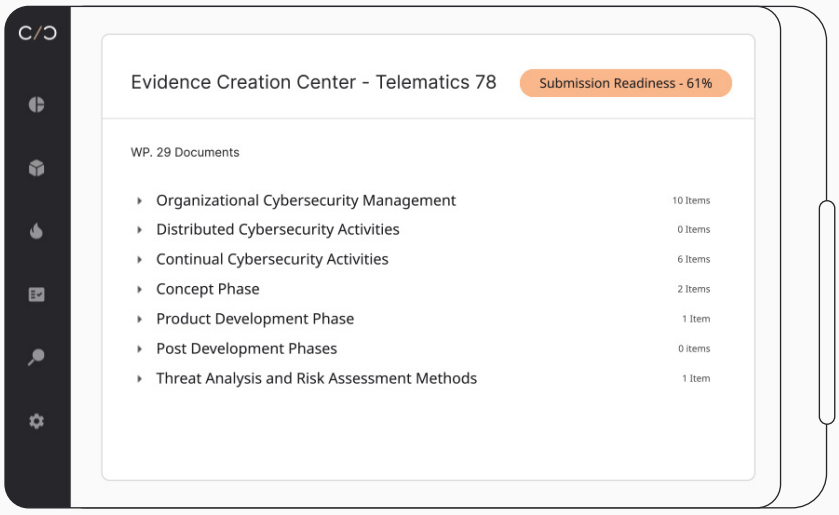
Risk- Risk management automation

- Dashboards receive automatic updates through integrations with asset, vulnerability, and risk data, ensuring current information.
- Real-time alerts are configured to notify of critical issues as they arise.
- Playbooks for responding to security incidents are established and accessible.
- A centralized system is in place to manage and monitor additional data sources, providing a cohesive view of security data.

How do Level 3 teams conduct product security activities?

Teams at this level are familiar with automation and continuously integrate new automation into their processes. Relying on robust data, SBOMs, and dashboards, they can look far into the future to plan their product security activities and have greater ease in keeping their devices secure and compliant throughout the full product lifecycle.

While Level 3 teams work continuously to absorb and integrate new data, Level 4 demands seamless activities between all four pillars. While relying on greater accuracy and depth to automatically share information, information from the full product lifecycle, from design to end of life fully integrated into the QMS, PLM/ALM, and other systems so they can proactively prepare what's needed to mitigate a new vulnerability or a surprise audit.



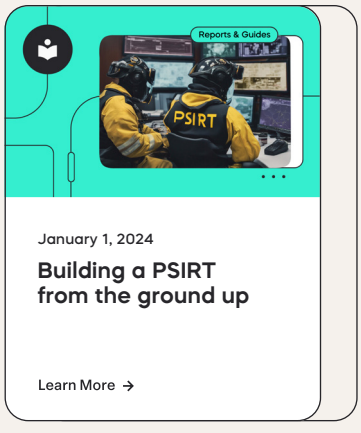
Centralizing data from both internal and external sources illuminates blind spots, allowing for an organized, knowledge-based approach.

Level 4

The highest level, level 4, represents a team that has fully automated their activities, integrating The Product Security Platform into their development lifecycle and contextualizing vulnerability data from multiple sources. This allows teams to take a birds-eye-view approach across all pillars, managing their product security with continuous reliability, greater accuracy, and using fewer resources.

Assets- Fully Automated Asset Management

- Workflows feature automation and scalability, with seamless integrations across various stages from design to build, facilitating easy import of asset data.
- There's comprehensive access to query any SBOM or asset, providing full control over asset data.
- A developed portal exists for the mature sharing of SBOMs with customers and/or suppliers.



Assurance- Fully Automated Asset Management

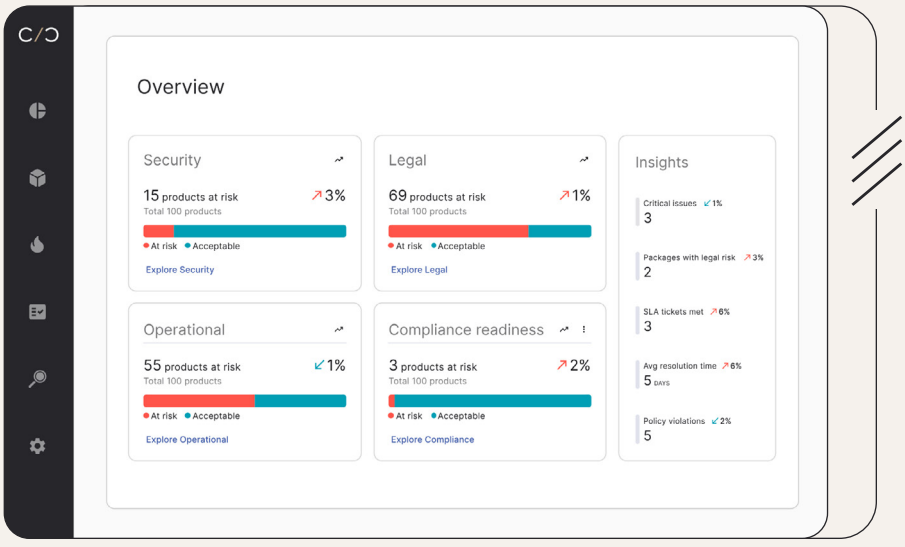
- Workflows are designed for automation and scalability, featuring seamless integrations at every juncture necessary for importing asset data, from the design phase to the build phase and beyond.
- There is complete capability to query any Software Bill of Materials (SBOM) or asset, providing full control over asset data.
- A well-developed SBOM sharing portal is available for use by customers and suppliers, facilitating efficient information exchange.

Compliance- Full Evidence Integration (“I’m ready for an audit even before the auditor comes”)

- Evidence data is fully integrated into Quality Management Systems (QMS), Product Lifecycle Management (PLM)/Application Lifecycle Management (ALM), and other relevant systems, ensuring comprehensive coverage.
- The approach to compliance is proactive, with it being seamlessly woven into the development lifecycle, ensuring readiness for audits well in advance of the auditor's arrival.

Risk- Fully Integrated Risk Management

- There is complete integration of risk and compliance data with enterprise and asset management systems, offering a comprehensive view of risk for each product at any moment.
- All pertinent sources of asset information, such as CI/CD pipelines and SBOMs, along with sources of findings like TARA, threat feeds, Product Security Incident Response Team (PSIRT) feeds, penetration testing outcomes, etc., are consolidated into a unified system.
- Response mechanisms are fully automated, ensuring swift action through real-time alerts and predefined playbooks.



With The Product Security Platform, managers can utilize robust platforms, bolstered by full lifecycle data.

Envisioning the future of product security

What future path does product security hold?

The hard unsurprising truth is that we don’t know. What is certain is that the future holds great challenges and opportunities ahead, demanding that we prepare for a landscape that pushes us repeatedly to review and revise our practices.

Just as we once learned to crawl at Level 0, run at Level 1, ride a bike at Level 2, get our first set of wheels at Level 3, and come of age in Level 4, we will have to remember that there is always more to learn, more to share, and more to secure.

About us

CYBELLUM IS WHERE TEAMS DO PRODUCT SECURITY.

Device manufacturers such as Jaguar Land Rover, Supermicro, Danaher, and Faurecia use Cybellum's Product Security Platform and services to manage cybersecurity risk and compliance across business units and lifecycle stages. From Asset & SBOM Management to Assurance & Vulnerability Management, Compliance Validation, and Incident Response, teams ensure their connected products are fundamentally secure and compliant – and stay that way.

Experience what product security can be. Book a demo.

Resources

Blogs

The VM Co-Pilot: An Automated Analyst for Product Vulnerability Management

EV Charging Stations: An Emerging Threat for Automotive OEMs

How to Keep the Software Supply Chain Accountable with SBOMs

Podcasts

Knowledge Base

Breaking Down the FDA's 2023 Premarket Cybersecurity Regulations

Learn More →

LG Vehicle Component Solutions Case Study

Learn More →

SBOM for Connected Devices: Getting it Right

Learn More →

More about the Product Security Platform