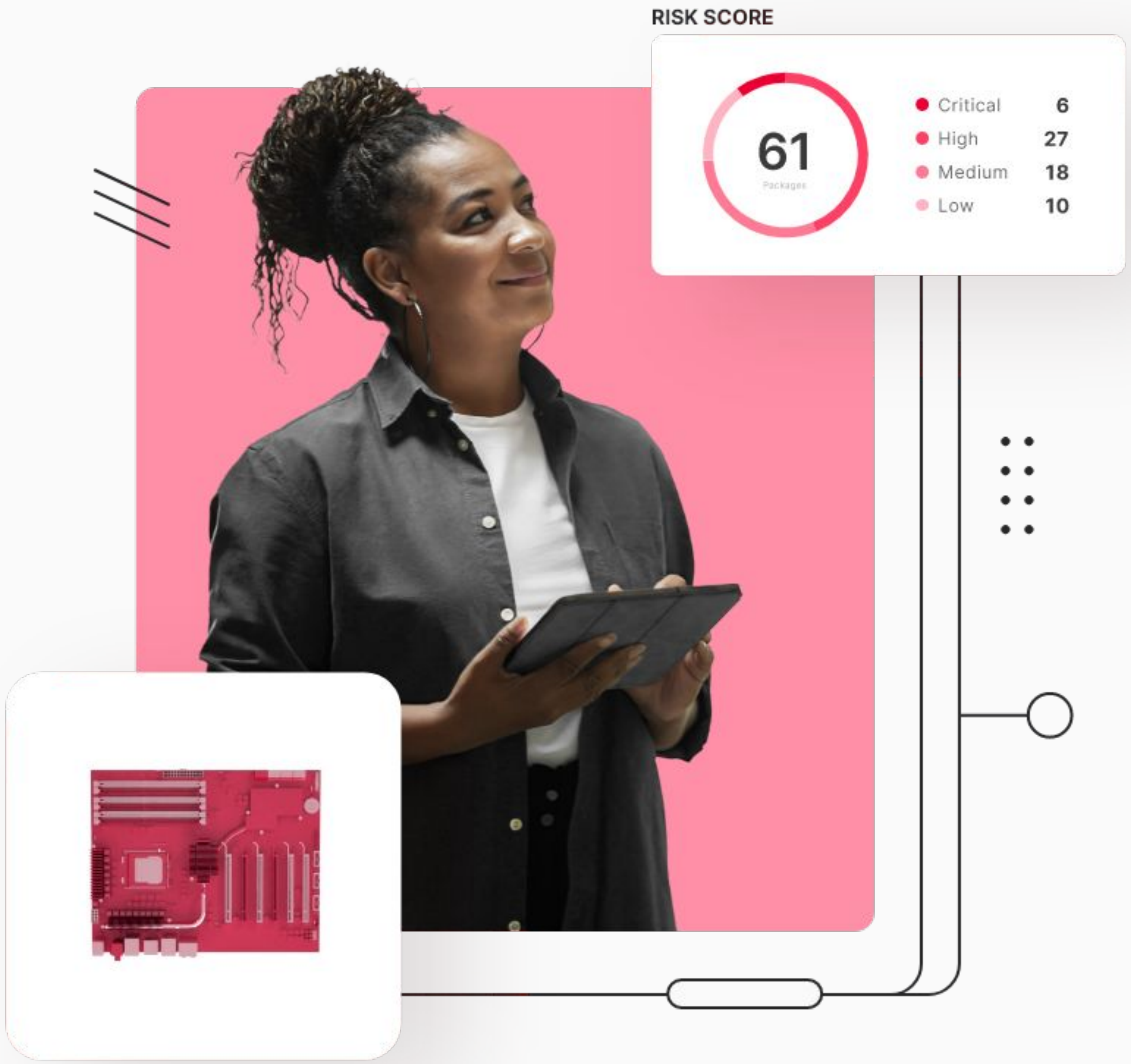
ASUS & Cybellum

New Product Security Management Process

Eddie Lazebnik

VP Sales and Strategy APAC

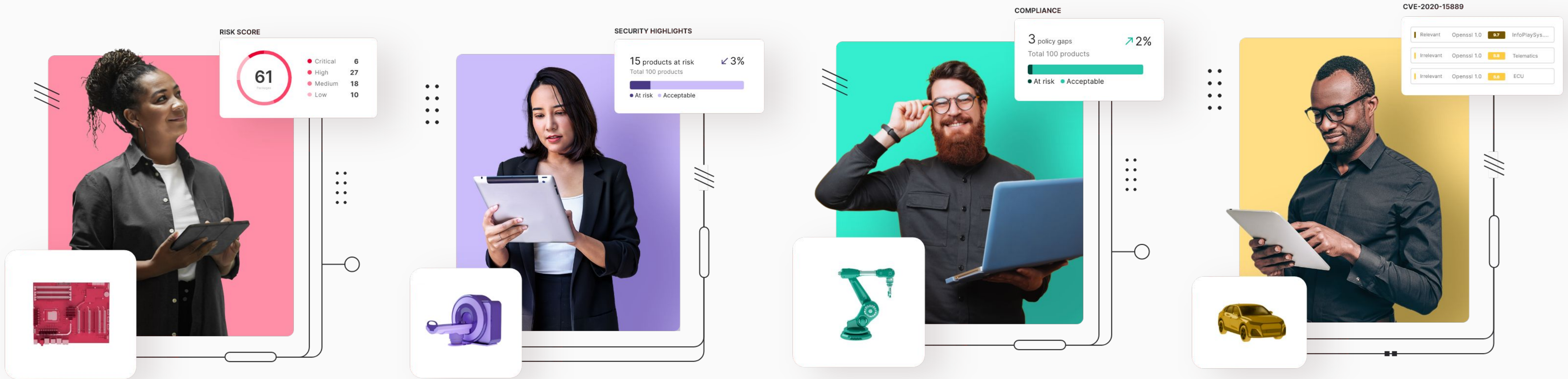
September 12th, 2023



A little bit about us

Our mission
Since 2016

To make the connected products we all rely on fundamentally secure, by creating a whole new standard for product security worldwide



Helping Product Security Teams on Their Journey

NISSAN
Audi
Arthrex®
RENAULT NISSAN MITSUBISHI
JAGUAR
LAND ROVER
FORVIA faurecia
DANAHER
SUPERMICRO®
Dräger
veoneer
HARMAN A SAMSUNG COMPANY
CATARC
ROLLS RR ROYCE
SIEMENS
Great Wall
BMW
stryker®
DENSO
HOZON 合众汽车
mobileye™
LG

Helping product security teams on their journey

Working with the world's leading manufacturers and partners

JAGUAR · LAND ROVER · NISSAN · mobileye

Arthrex · Dräger · FORVIA faurecia

ROLLS ROYCE · Audi · HARMAN · SUPERMICRO

Actively involved in product cybersecurity standards & alliances

ISO · SAE INTERNATIONAL · iamts · NTIA

EcoMotion Smart Mobility Community · STARTUPAUTOBAHN powered by PLUG AND PLAY · Health-ISAC NAVIGATOR PROGRAM

CVE · ioXt internet of secure things · OPENCHAIN · 医療ISAC認証 Medical ISAC Japan

AUTO-ISAC Automotive Information Sharing and Analysis Center · ASRG Automotive Security Research Group · DRIVE FUTURE MOBILITY NOW

Helping develop the global product security community

Living and breathing Product Security

An R&D team experienced with the systems, architectures, and regulations of the Medical Device, Automotive, and Industrial Manufacturing industries

Backed by market leaders

Cybellum is fully backed by LG Electronics

LG

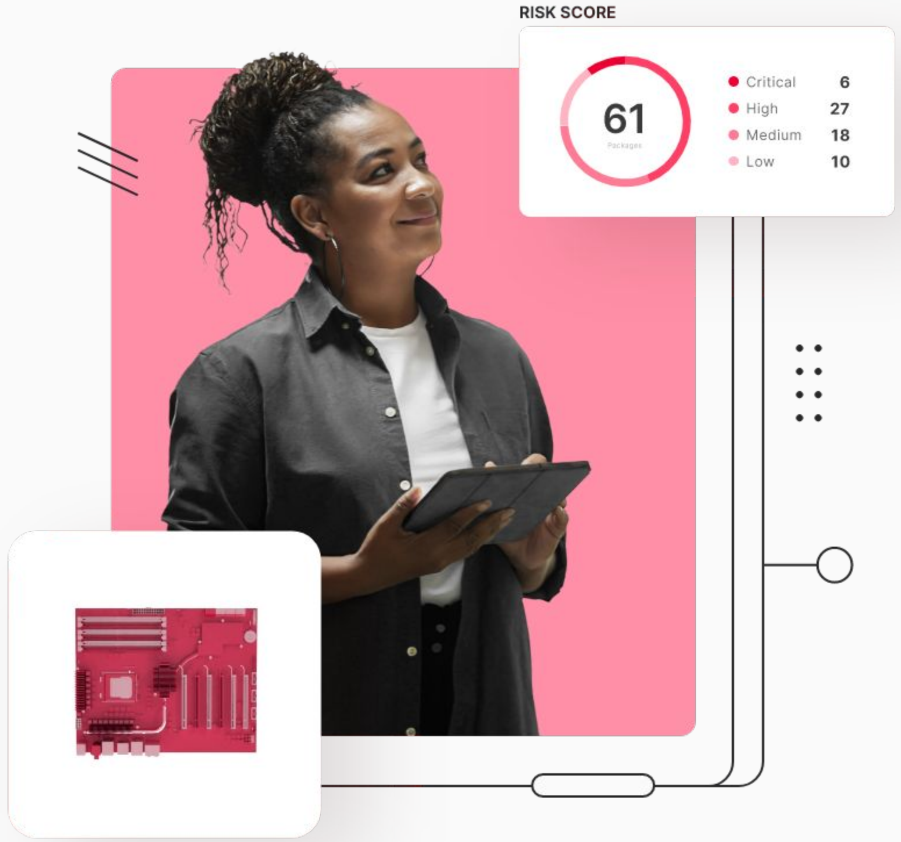
Why now?

Product Security Has Become the Biggest Challenge for Device OEMs and Their Suppliers

More software and complexity as devices become software-defined

FDA EU WP29 ISO

More cybersecurity regulations and standards introduced



LOG4J Ripple20

Device software vulnerabilities are more frequent (>26K a year), and the supply chain is becoming a huge risk

Time to market is suffering, security is under enormous pressure to keep up with development

UNECE

WP.29 R155

"Processes in a CSMS should ensure security is adequately considered:

- Inside the organization for managing cybersecurity
- Risk identification
- Assessment, categorization and treatment of risks
- Verify that identified risks are managed
- Test cybersecurity of vehicle types
- Ensure that risk assessment is kept current
- Monitor, detect and respond to cyber issues

"Should cover these phases: Development, Production, Post-production

EU Cyber Resilience Act

> *Products with digital elements shall be designed, developed and produced in a way that ensures an appropriate level of cybersecurity based on the risks*

> *Products with digital elements shall ensure that vulnerabilities can be addressed through security updates*

> *Identify and document vulnerabilities & components contained in the product, including by drawing up an SBOM in a commonly used and machine-readable format*

> *In relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates*

The current approach is not sufficient

Manual
and unscalable

Infrequent and
done too late

Limited by general-purpose IT
security tools

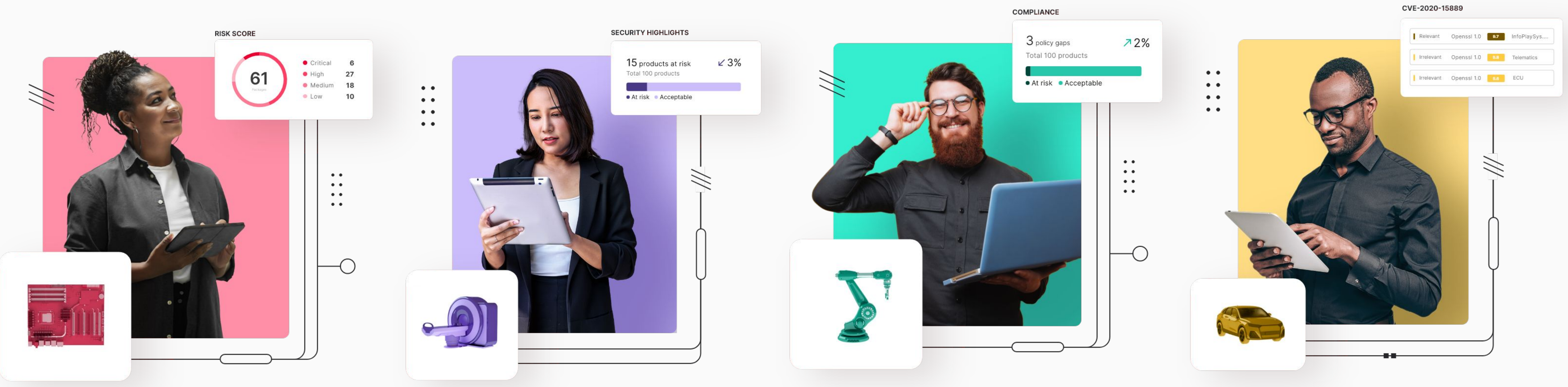
Prevents us from seeing the full picture
and doing proper risk *management*

Complex, relies on
too many different tools

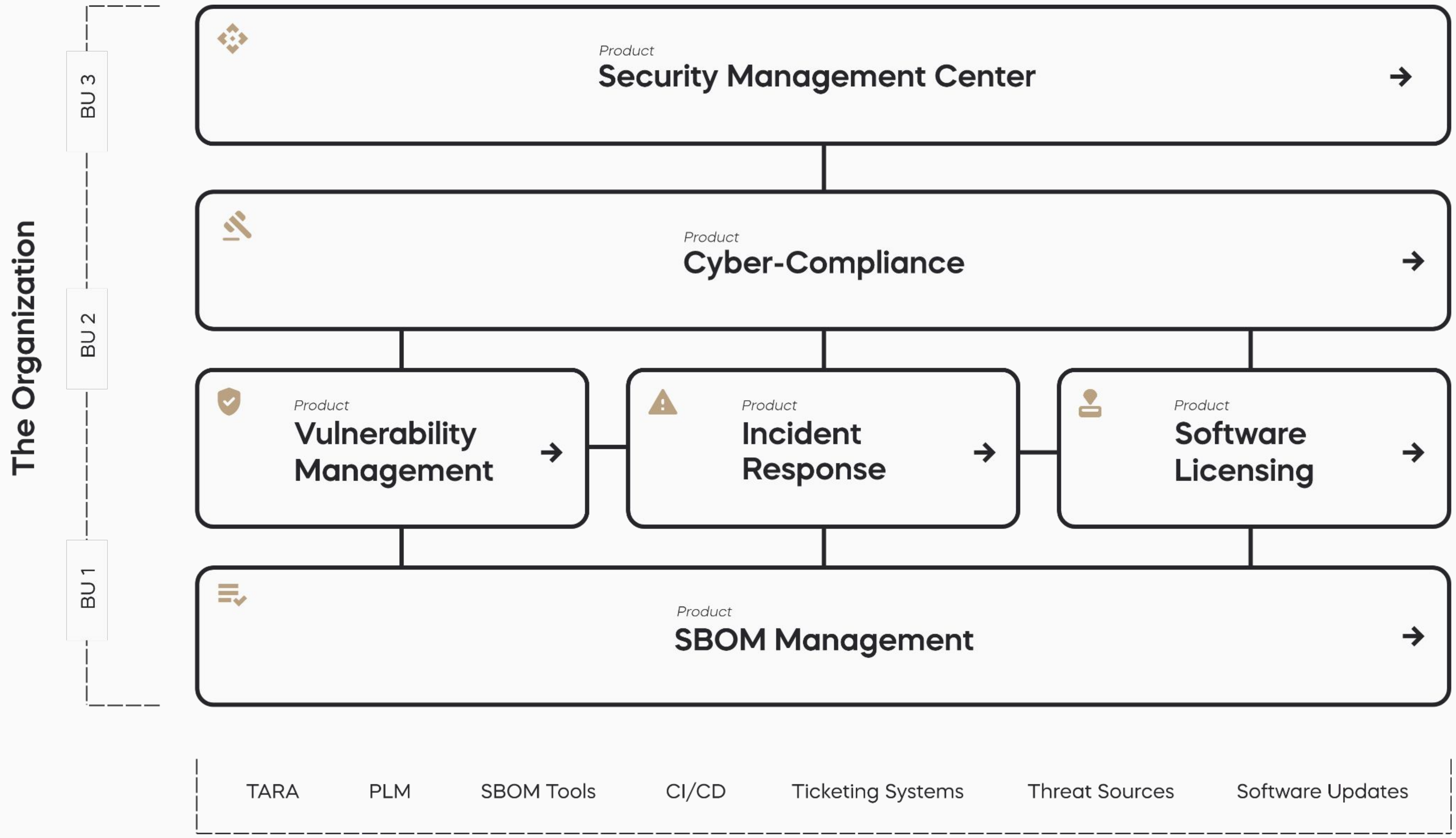
The New Approach - Product Security Management System (PSMS)

The Vision

To empower all teams involved in product security
to efficiently manage and execute their tasks,
by building a unified management system for product security
that's perfectly integrated into the product lifecycle



The product Security Management System



How the PSMS Benefits Your Organization (Case-studies)

IAI Elta
Drones, IoT and Defense rate testing

Customer Profile

- Israel's major aerospace and aviation manufacturer,
- Producing aerial and astronautic systems for both military and civilian usage.

- IAI designs, develops, produces and maintains civil aircraft, drones, fighter aircraft, missile, avionics, and space-based systems.

- Also manufactures military systems for ground and naval forces.

Challenges

- Clearing and approving the code for each component, project, system - the scale is beyond manageable

- Unique architectures, OSs, needs of the industry - general tools just not good enough

- Findings must be filtered, prioritized and actionable - manpower shortage

- Accuracy - being the Israeli Governmental military organization - their reports can't contain false positives

- Customization - reports, analysis, findings - must be done their way

Modern jets are flying data center everything is computerized and accordingly the Cyber risk is increasing hence all components have to be tested
– Esti Peshin, VP, General Manager, Cyber Division at Israel Aerospace Industries

LG Electronics SBOM Management & CSMS

Customer Profile

LG Vehicle Solutions (VS)
An LGE company headquartered in Seoul
7,500 employees, 13 countries

Products
Advanced automotive parts including cockpit electronics, connectivity and vision systems

Background
LGE VS Cybersecurity Development department performs all security activities required by the UN R155 regulation across their lifecycle - creation of 100% validated SBOMs, vulnerability analysis and management, incident response, security mitigations and OS hardening.
This activity involves regular progress reporting to OEMs, and managing the security processes required by the CSMS regulation.

Challenges

- **Growing number of projects** - tens of projects must be managed concurrently by the cyber security department at different stages of development and post production.
- **Projects getting more complex** - some with over 1,000 software components
- **Highly manual processes** - manual tracking, analysis, reporting, lack of governance across products, no consolidated policies
- **Cyber security activities are very slow**:
  - Takes days to complete a vulnerability analysis of a single product-version
  - Takes days to prepare a vulnerability incident report
  - Takes days to prepare an incident response monitoring report

Solution

- **Cybellum Platform** - onboarded tens of development projects
- **Analysis Services** - a team of analysts that are constantly analyzing and optimizing results

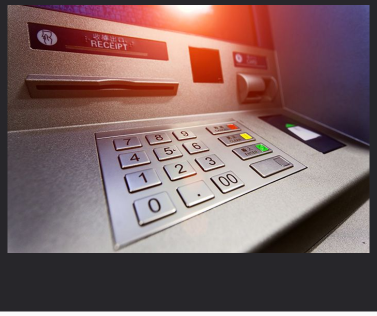
SBOM
Created automatically from binaries & validated by Cybellum analysts.

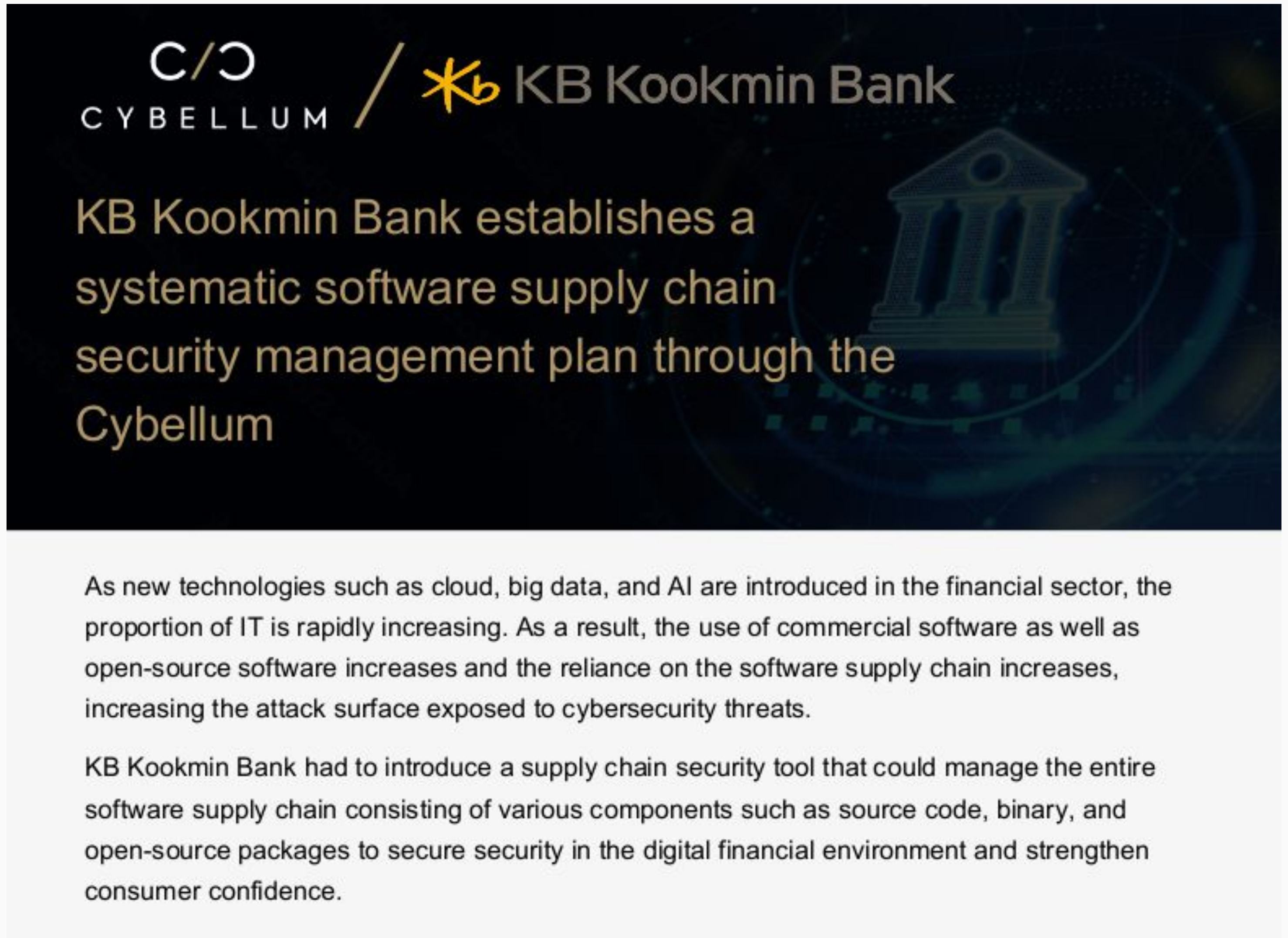
Vulnerabilities

- Automatically triaged based on firmware context and configurations as part of CI/CD pipelines
- Software revisions are evaluated using Cybellum's multi-version CDTs and assessments, tracking SW component version changes and impact on vulnerabilities
- Reports to OEMs are created directly from the system
- OEM security requirements are automatically validated using policies technology.

Using Cybellum, LG VS are managing SBOMs and vulnerabilities 3x faster with 25% more accurate than their previous methodology and tools

Banking Sector South Korea
Regulation and Security Hygiene





KB Kookmin Bank establishes a systematic software supply chain security management plan through the Cybellum

As new technologies such as cloud, big data, and AI are introduced in the financial sector, the proportion of IT is rapidly increasing. As a result, the use of commercial software as well as open-source software increases and the reliance on the software supply chain increases, increasing the attack surface exposed to cybersecurity threats.

KB Kookmin Bank had to introduce a supply chain security tool that could manage the entire software supply chain consisting of various components such as source code, binary, and open-source packages to secure security in the digital financial environment and strengthen consumer confidence.

Challenges

- **New technologies** such as, AI, machine learning and cloud
- More **Mobile Application** usage
- Usage of **Open Source** Software
- They need to manage SBOM management, licenses and vulnerabilities
- Product security elements are fundamental: Encryption, Privacy, Authentication, Vulnerabilities.

- New regulations:
  - Local Financial Compliance
  - Executive Order of President Joe Biden - EO 14028 : National Cybersecurity Improvement

- No centralized view of product security risk and insufficient tracking of analysis progress

> ***Cybellum's product security platform generates and manages SBOMs using Cyber Digital Twin™ technology.***
> ***Implementing automated SBOM generation has given us visibility into our complex and vast supply chain, allowing us to better manage prioritization and mitigation of various security vulnerabilities.***
> -
> - ***KIWOONG KIM, Deputy General Manager, KB Kookmin Bank***

Market-leading Medical Device Manufacturer SBOM Management & Post Market Monitoring

Customer Profile

- Based in NA, with global operations
- Multiple product-lines with 00s of products
- Corporate focus on safety and quality - a top priority for R&D and product security

Challenges

- Difficulties meeting FDA regulatory requirements for 510(K)/PMA and Post-market continuous monitoring
- Existing solutions don't quite cut it
- Lack of management capabilities
  - Generation + verification, editing, approval, distribution
  - For both SBOM & HW BOM
- Scale
  - 100s of products with proprietary and 3rd party software
  - SBOMs of different origin and format (from source code, firmware, SPDX, CycloneDX, manifest files)

Solution

- Partnership model with Cybellum for commitment on roadmap and vision
- Cybellum's Product Security Platform:
  - Digital Twin generation (SBOM, hardware profile, cryptography, APIs etc.)
  - Transitive dependencies exposure
  - SBOM import (OSS, COTS, SOUP)
  - SBOM/HBOM mgmt. (verify, edit, approve)
  - Customized SBOM report distribution
  - Management dashboard
  - Basis for future expansion to post-market security requirements (Incident Response)
- Cybellum Services
  - Extraction of SBOMs for post-market products
  - SBOM consolidation, verification and repository

The company quickly ramped-up its SBOM and Product Security program, enhancing visibility and control over the entire process across the organization, and meeting regulatory quality requirements

US-based Networking and Telecom OEM

Customer Profile

- OEM headquartered in APAC, developing networking and telecom equipment for large enterprises and communications service providers

Challenges

- No centralized view of product security risk and insufficient tracking of analysis progress
- Product security operations are separate from the standard SDLC workflow, making it difficult for R&D and Product Security to cooperate and resolve security issues in a timely manner
- Lack of adherence to corporate security policies related to coding standards, open-source license conflicts, cryptography guidelines
- Existing security assessment processes for are mostly manual and not scalable
- Current tools yield too many false-positives
- Internal security guidelines mandated on-premise deployment within its datacenter

Solution

- On-prem deployment of Cybellum's Product Security Platform
- CVE and zero-day detection within device firmware, mitigation recommendations
- Daily threat intelligence updates delivered via a disconnected server, adhering to corporate security guidelines
- Automated assessment of CVEs and internal policy violations through integration with the SDLC, using Cybellum's RESTful API
- Alerts for any open-source licensing conflicts
- Automated exploit analysis and triaging, through VM CoPilot
- Dashboards track the security status of different programs, assisting R&D and the security team to meet development timelines
- Support for ETSI EN 303 645 and the ability to easily create custom policies as needed

> ***"** Cybellum's enterprise-grade platform enabled us to scale our vulnerability management program across dozens of teams, while speeding-up development workflows and adhering to strict security requirements.***
> ***– Director of Product Security, APAC Networking & Telco OEM***

The OEM was able to achieve DevSecOps transformation, improve assessments time x20, facilitate policy complaince and get orgnizational visibility into its security poosture

The White Paper Proposal

Background

ASUS, one of the world's leading electronics manufacturers, views product security as a strategic innovative value and therefore is constantly researching new ways to improve their new product security process.

Would like to write a white paper research report about creating and implementing new product security management best practices and analyze their impact on ASUS. To that end, they would like to work with Cybellum, the leading provider of the Product Security Platform, for the creation of the white paper, which will include:

- A new methodology for product security management that will be developed by ASUS and Cybellum,
- The methodology will combine a measurable KPI model, as well as a plan to use new automation and AI capabilities to improve the product security activities at ASUS
- The white paper will detail the needs coming from the ASUS team, the methodology, the implementation plan, and the benefits for ASUS stakeholders across the organization

Suggested Plan (Part A)

Discovery sessions

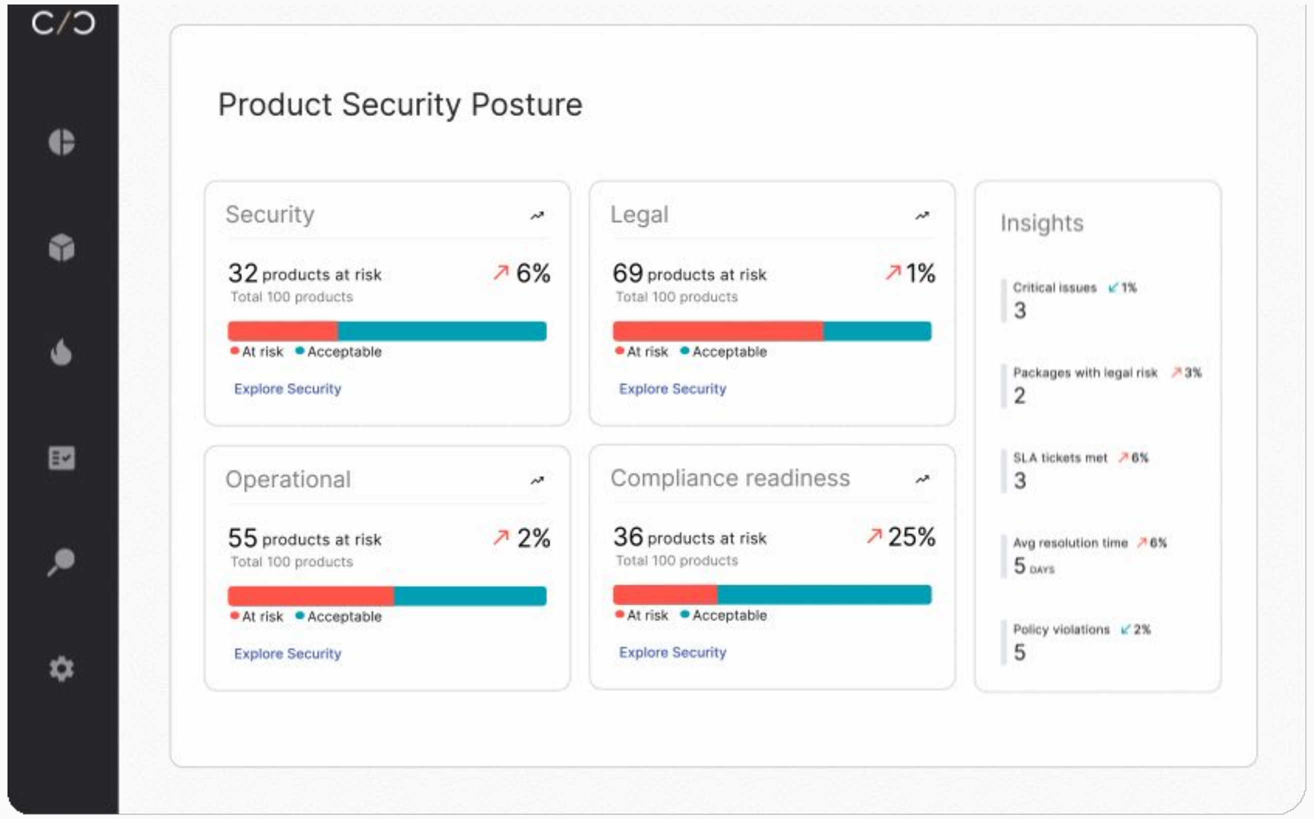
- A task force of ASUS and Cybellum representatives will be chosen
- Structured discovery sessions between Cybellum & ASUS will take place, where the taskforce will uncover:
    i. The main goals of ASUS's product security activities,
    ii. The main areas for improvement,
    iii. The relevant products/business units to be involved in the process,
    iv. The relevant technological details (architectures, OSs, APIs, etc.)

Research and interviews

- The Cybellum and ASUS task force will interview key personnel at ASUS and Cybellum, and will analyze data from the Cybellum Product Security Platform to incorporate the analysis to the white paper in addition to the focused discovery sessions

Methodology and plan creation

- The task force will create a detailed plan for an uplifted product security management process at ASUS:
    i. Which will incorporate new KPIs,
    ii. New technologies (such as automation tools and AI capabilities),
    iii. Implementation plan at ASUS



Suggested Plan (Part B)

White paper creation

- The white paper will detail the new management process
- It will also focus on the main benefits of the new management process, such as:
  i. Board level visibility into organizational product security status,
  ii. Improved cyber defects treatment by reducing the time to prioritization and mitigation of vulnerabilities,
  iii. Improved SBOM management process,
  iv. Improved customer SLA results,
  v. Crips Internal KPIs performance
- The white paper will also detail the "before" and "after" state of the product security process and will highlight potential benefits for the main stakeholders at ASUS, including the leadership team, the product quality teams, cybersecurity teams, R&D teams, compliance teams, and executives
- In addition, the white paper will include the main achievements of the ASUS product security team and the main technologies used
- The research will also include recommended KPIs for measuring the performance of product security, and how these KPIs improved following the POC
- One of the work products would be dashboards, reports and general abstraction to board level of: General organization product security risk, different programs and their security risk, Different BUs compliance status, vendors product security evaluation and management. Examples and potential insights would be presented.

Additional publication options

- Webinar / Podcast
- 2 pager teaser
- Research walkthrough video

Thank You

eddie@cybellum.com