CYBELLUM

CUSTOMER CASE STUDY

Networking OEM selects Cybellum to strengthen product cybersecurity

About the Customer: A multi-national vendor headquartered in APAC, developing networking and telecom equipment for large enterprises and communications service providers.

THE CHALLENGE

Streamline secure software development and enhance adherence to internal security policies

THE OUTCOME

DevSecOps
transformation

20x
faster assessments

POLICY
compliance validation

SECURITY
status transparency

"Cybellum's enterprise-grade platform minimized manual efforts and enabled us to scale our vulnerability management program across dozens of teams, while facilitating development workflows and respecting strict security requirements. **Director of Product Security, Leading Networking OEM**

THE CHALLENGE

In recent years, numerous cyber attacks targeted enterprise and consumer networking equipment, increasing customer awareness of the importance of cybersecurity and driving demand for secure devices.

To remain competitive and maintain its global leadership, the vendor decided to double-down their efforts to build cyber secure devices. Following an internal evaluation and a joint discovery process with Cybellum, the vendor identified the following key challenges and requirements:

- Existing security assessment processes for product firmware are predominantly manual and thus not scalable
- Current tools and methodologies yield many false-positives
- No centralized view of product security risk and insufficient tracking of vulnerability analysis progress
- Lack of adherence to corporate security policies related to coding standards, open-source license conflicts, cryptography guidelines and privacy rules prohibited continuous improvement of its secure posture
- Product security operations are separate from the standard SDLC workflow, making it difficult for development teams and product security to cooperate and resolve security issues
- Emerging cybersecurity standards must eventually be supported so any new solution must be flexible enough to accommodate those (detecting relevant violations, tracking and documenting user decisions, supporting auditing processes etc.)
- Any new solution must support Linux and Android - the two main OSs they use
- Internal security guidelines mandated on-premise deployment within its datacenter

Last but not least, the vendor required an expert grade platform that had previously been vetted and had proved itself in real world deployments.

THE SOLUTION

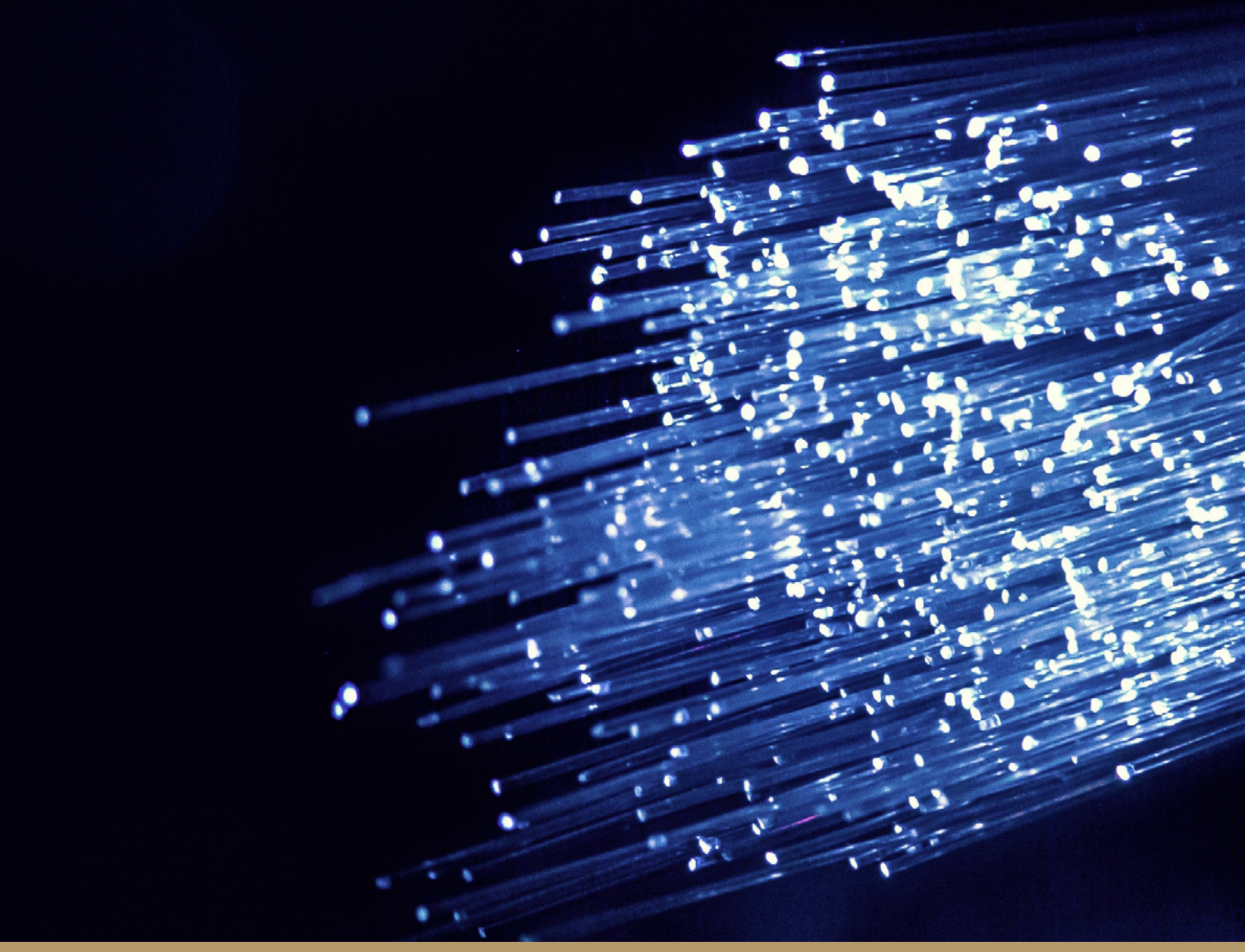
Following a proof-of-concept project, the Cybellum Cyber Digital Twins™ platform was deployed at the vendor's datacenter:

- On-premise deployment of a centralized vulnerability management platform serving dozens of development teams - from threat-intelligence collection to CVE and zero-day detection within device firmware, to mitigation recommendations
- Daily threat intelligence updates delivered via a disconnected server, adhering to strict corporate security guidelines
- Automated assessment of vulnerabilities and internal policy violations integrated within the vendor's standard SDLC using Cybellum's RESTful API
- Automated alerts are provided for any open-source licensing conflicts
- Context-based prioritization and remediation guidelines optimized resource utilization and cut time-to-mitigation
- 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 (Cyber Security for Consumer IoT devices - Baseline Requirements) and the ability to easily create custom policies as needed

THE RESULTS

The vendor went live within three months of signing with Cybellum, and the results were quick to follow:

- **20x faster vulnerability management process with fewer false-positives thanks to a frictionless DevSecOps workflow**
- **The product security team and R&D executives have clear visibility into the security status of every development program**
- **Internal security policies are rigorously enforced enhancing the vendor's overall security resilience**
- **The vendor is able to validate adherence to FOSS licensing policies, reducing further legal risk**



KEY BENEFITS

COMPLETE COVERAGE

Manage vulnerabilities and security gaps in vehicle components and companion apps, protecting them from CVEs and zero-days. All via binary analysis. No source code needed.

SHIFT TO AUTOMATIC

Scale up vulnerability management across development programs with minimal manual effort, so you can meet and beat deadlines and prevent security risks.

FRICTIONLESS DevSecOps

Robust integrations with PLM, SDLC, asset-management and other backend systems streamline development processes.

About Cybellum

Cybellum empowers OEMs and their suppliers to develop and maintain secure automotive products at scale. Our Cyber Digital Twins™ platform unifies pre-SOP Product Security Assessments with post-development Product Security Operations, providing you the visibility, context and agility needed to secure vehicles across their lifespan.