Schneider Electric Supply Chain Security Program

ITU August 2023

Cassie Crossley, VP Supply Chain Security

Life Is On Schneider Electric

Who is Schneider Electric?

Schneider Electric provides energy and automation digital solutions for efficiency and sustainability

Key figures for 2022

5% of revenues devoted to R&D

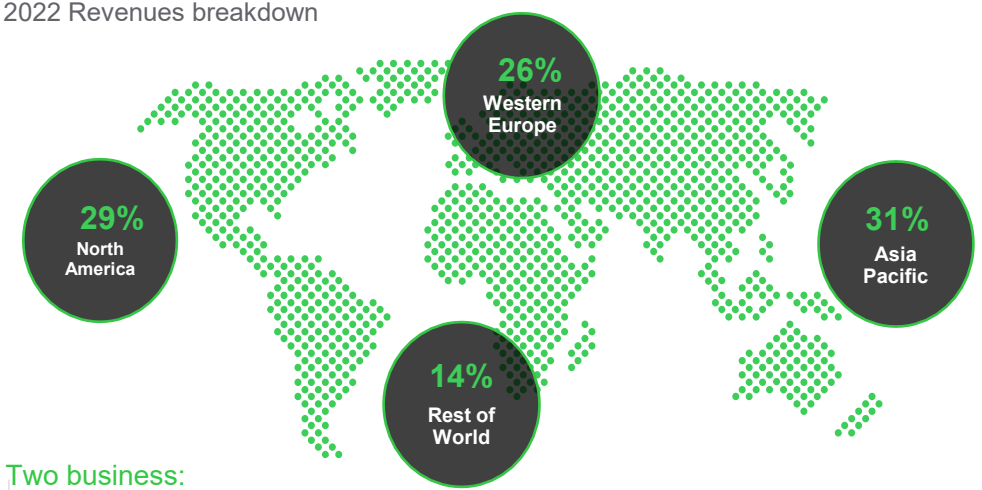
€34 billion
2022 revenues

43%
of revenues in new economies

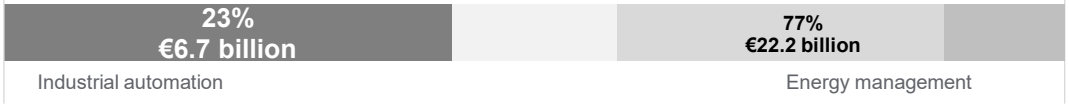
128,000+
Employees in over 100 countries

A well-balanced global presence

2022 Revenues breakdown



Two business:



We partner in everything we do

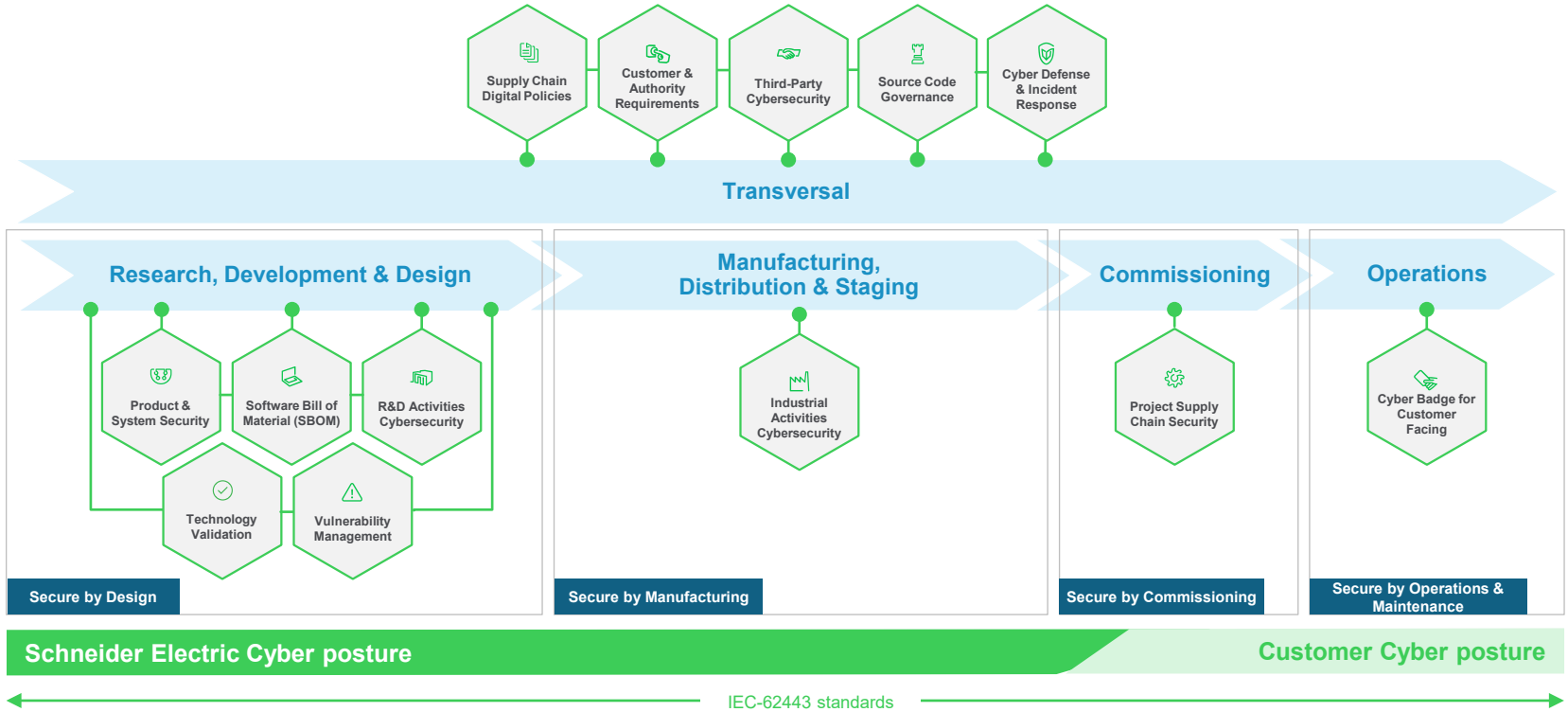
650k service providers & partners

42k+ system integrators & developers

52k+ unique suppliers

Schneider Electric’s Supply Chain Security

We seek to embrace the whole value chain from security by design to secure operations with a comprehensive set of programs…



SBOM Use Cases

Software Production: SBOM's can help SE decision what external software should be included in our code base

Reduce

- Unplanned/unscheduled work
- Code Bloat

Dependencies

Understand broader complex links across all code bases

Compliance

- License Obligations
- End of life

Monitor

Components for Vulnerabilities

Tracking

- Ease of code review
- Component usage: Banned/Allowed

Software Selection: SBOM can help Clients and Consumers select what products to purchase

Identify potential vulnerabilities

- Targeted Security analysis
- End-of-life component(s) awareness

- Verify Source
- Compliance with internal/regulatory policies
- Claims verification
- -

- Software integrations

Pre-purchase/installation planning

Market Signals

Software Operation: SBOM can help to install, configure, maintain, and administer software

Quickly evaluate if a component is in use

Independent mitigations

Make informed risk-based decisions

End of life alerts

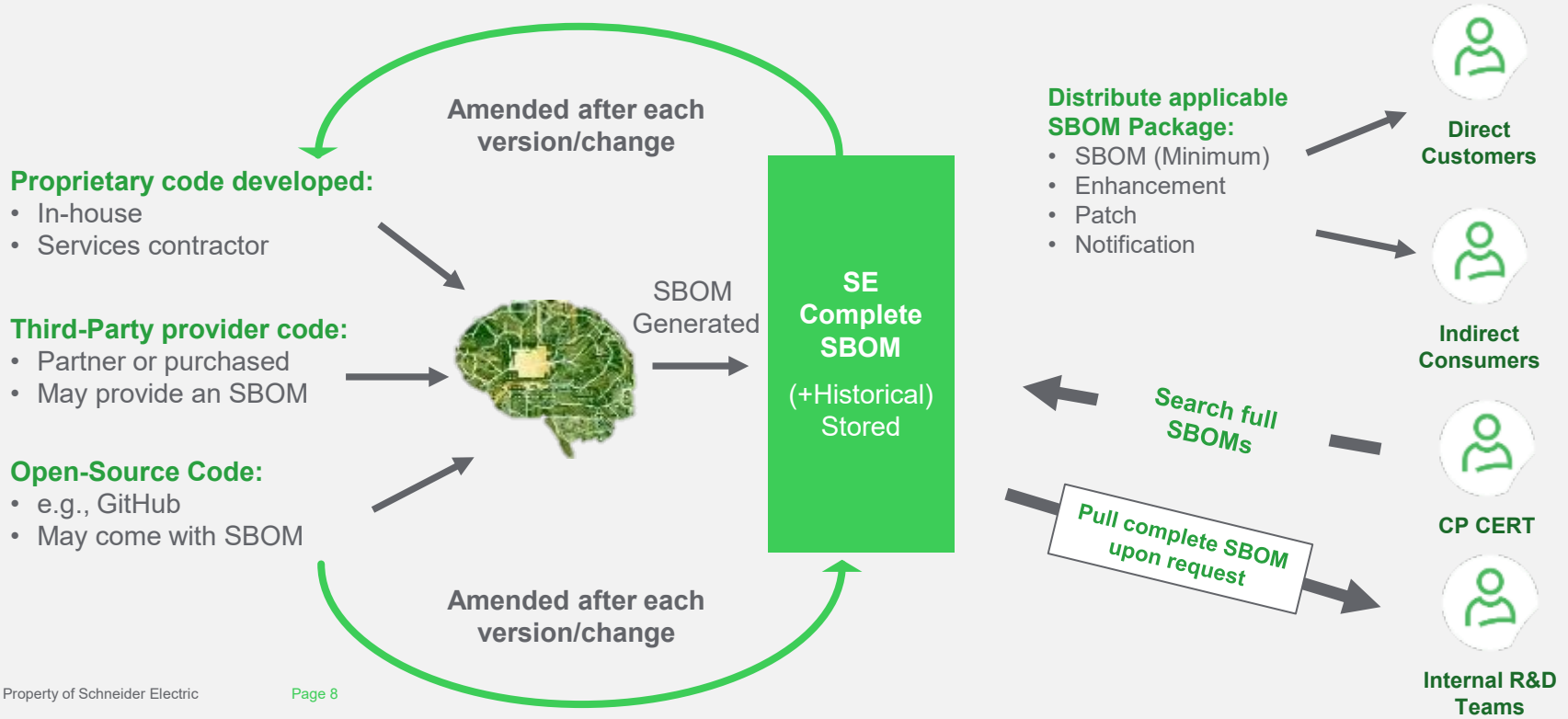
Support compliance and reporting requirements

Reduction in costs through streamlined and efficient administration

SBOM: Logical Flow

SBOM Processing and Construction: High-Level End-to-End Flow for each Product (Software and/or Firmware)

SE Product: Software and/or Firmware



Summary of our SBOM Journey

3+ years in our SBOM program – mandatory for all products since January 2021

Strengths

- 4000+ SBOMs for internal products
- Valuable learnings and **improved speed** to generate security notices by leveraging SBOMs during Log4j, OpenSSL, and other critical open-source CVEs
- Increased **awareness** in R&D teams regarding third party dependencies
- Stronger transparency and **trust** with customers

Opportunities

- Over half of active development projects don't have CI/CD pipelines → requires SBOM collection to be manual
- Binary scanning tools designed for open source; cannot identify commercial or proprietary libraries without additional information → requires manual creation of SBOMs and validation of all generated SBOMs
- Many suppliers not prepared yet to provide machine-readable SBOMs