Title: Leveraging SBOMs for Vulnerability Management

Session Length: 30 minutes

Presenter: Cassie Crossley, VP Supply Chain Security, Schneider Electric

Abstract: There is some debate as to how SBOMs can enhance vulnerability management practices, and some believe that collecting SBOMs from internal teams or suppliers is too difficult and time-consuming. Learn how Schneider Electric has collected thousands of our product SBOMs and how we are leveraging the SBOMs as part of our corporate product CERT to quickly analyze and focus our attention when time is of importance. This presentation describes how we modified our policies and processes to collect, generate, and store thousands of SBOMs. You will hear how we have leveraged SBOMs during the Log4j and OpenSSL vulnerability events. Then we will conclude with key learnings, suggestions, and opportunities for improvement.

Session Outline:

- Introduce presenter and Schneider Electric
- How we modified our process to require SBOMs as part of the secure development lifecycle (SDL)
    - Policy and process change: leveraged requirement already in ISA/IEC 62443 to track software components
    - SBOMs mandatory as of January 2021 for any production releases
    - SBOM Collection:
        - Used our process for tracking releases to request binaries for SBOM generation
        - Generated SBOMs using software composition analysis (SCA) tools. Using APIs to take CI/CD built SBOMs directly into our SBOM storage tool.
        - Stored in SBOM repository: originally was a corporate document repository, now in a tool specifically designed for SBOM storage and sharing
- Case studies
    - Log4j - Dec 2021: First major time leveraging SBOMs. Lessons learned: SBOMs were stored in various repositories. Only had SBOMs for products which had released that year. Helped pinpoint which products were known to have Log4j so immediate contact to those teams could be prioritized.
    - OpenSSL – Nov 2022: Companies were alerted that two vulnerabilities were going to be announced on Nov 1. Lessons learned: Had nearly two years of SBOMs. Advanced warning allowed us to identify products with OpenSSL for prioritization.
- Key learnings and suggestions for other CERTs
    - Implement SBOM requirement into the SDLC.
    - Leverage current tools and open source projects to generate SBOMs.
    - Store collected SBOMs into single repository.
    - Revise CERT processes to use SBOM tools (commercial or open source) to quickly query and prioritize vulnerabilities.

    - Integrate relevant tools to automate querying SBOM to detect the vulnerabilities.
- Opportunities for improvement / Items of note:
    - SCA tools primarily identify open source packages. Enhance SBOMs with commercial and proprietary packages (e.g., commercial crypto library or your company's reusable inner source)
    - Collection of SBOMs from suppliers. Leverage cyber agreements, laws, and regulations to require suppliers to provide transparency (e.g., US FDA, US EO 14028, EU Cyber Resilience Act).
    - Cloud-native architectures – Cloud platform tools can generate SaaSBOMs.

Take-aways:

- SBOM collection is important to CERTs. Update policies and procedures to collect them.
- SBOMs can speed up analysis and prioritization when time is of the essence.
- Suppliers are hesitant to give SBOMs, partially because they aren't being used. It is encouraging to see the benefits from SBOMs.
- SBOMs aren't perfect, but even so they are useful (in other words, a little light in the darkness is better than nothing)

Presenter Bio:

Cassie Crossley, Vice President, Supply Chain Security in the global Cybersecurity & Product Security Office at Schneider Electric, is an experienced cybersecurity technology executive in Information Technology and Product Development and author of "Software Supply Chain Security: Securing the End-to-End Supply Chain for Software, Firmware, and Hardware." She has many years of business and technical leadership experience in supply chain security, cybersecurity, product/application security, software/firmware development, program management, and data privacy.

LinkedIn: https://www.linkedin.com/in/cassiecrossley/