# SECURING CRITICAL INFRASTRUCTURES BY DISCOVERING HIDDEN VULNERABILITIES

Talha Siddiqui — Senior Data Scientist, aDolus Technology Inc.

Like most IT software, today's Operational Technology (OT) software is often composed of externally-developed packages and subcomponents, typically from a variety of open source and proprietary sources. These 3rd-party subcomponents can contain vulnerabilities that remain hidden from the user of this software, leaving OT users no means of determining if the product they are deploying in a mission critical system is at risk.

In contrast, most OT practitioners assume that by searching the National Vulnerability Database (NVD)[1], they will find all the vulnerabilities associated with a given OT software product or device. Sadly, this is not the case: the NVD is far from a complete set of vulnerabilities with some sources claiming that 76% of all OT vulnerabilities are missing from the NVD[2] and that an average vulnerability is "in the wild" for 5.3 years[3]. Furthermore, the NVD and manufacturer vulnerability notices rarely map vulnerabilities in software components back to the OT packages that contain those components. In addition, mergers and acquisitions mean that the vendor name on the product in use often doesn't match the vendor name seen in the NVD disclosure details. Finally, when OT suppliers issue vulnerability notices, they are typically in the form of human-legible reports that are not machine-readable and do not adhere to any industry standards.

The size of the typical OT system and the complexity of software makes it extremely difficult for a security analyst to manually aggregate vulnerability information, identify the affected subcomponents, and assess the impact to the typical OT system. An intelligent system is needed to automate these steps while conforming to the industry standards being set by the International Organization for Standardization (ISO), the US National Telecommunications and Information Administration (NTIA)[4], and others. For example, the OASIS-open Common Vulnerability Reporting Framework (CVRF) V1.1 standard[5] referenced in ISO/IEC 29147[6] and the newer OASIS-open Common Security Advisory Framework (CSAF)[7] outline machine-friendly vulnerability advisory structures that automated systems must be designed to interpret or future vulnerability coverage will be reduced as these machine-friendly formats become more prevalent.

This video will discuss how a variety of Artificial Intelligence (AI) techniques can help address these challenges. Specifically, we will discuss how applied research in Natural Language Processing (NLP) for vulnerability notices is enriching the metadata regarding software components and then tying vulnerability information to those files. We then use a Software Bill of Materials (SBOM)[8] analysis to identify components in OT products and associate vulnerabilities determined to impact those components to software and device products recognizable to OT end users. The predicted matches are then audited by software manufacturers and subject matter experts who create a yes-no answer key that is then used for optimization of AI model parameters. This combination of SBOM analysis and NLP allows both asset owners and suppliers of software to be informed of vulnerabilities hidden deep inside these mission critical products in a more timely manner

**REFERENCES**

[1] https://nvd.nist.gov/

[2] https://ics.kaspersky.com/media/ics-conference-2019/04-Artem-Zinenko-Nedostatki-publichnyh-baz-uyazvimostey.pdf

[3] Richard J. Thomas, Joseph Gardiner, Tom Chothia, Emmanouil Samanis, Joshua Perrett, Awais Rashid. Catch Me If You Can: An In-Depth Study of CVE Discovery Time and Inconsistencies for Managing Risks in Critical Infrastructures. In Proceedings of the 2020 Joint Workshop on CPS&IoT Security and Privacy, Pages 49–60, 2020.

[4] https://www.ntia.doc.gov/report/2021/minimum-elements-software-bill-materials-sbom

[5] https://www.icasi.org/the-common-vulnerability-reporting-framework-cvrf-v1-1/

[6] https://www.iso.org/standard/72311.html

[7] https://oasis-open.github.io/csaf-documentation/

[8] ISO/IEC 5962:2021 information technology — SPDX® Specification V2.2.1