Vulnerability DEX Pack Story

Background: Customer Experience Engineers requested positioning information to share with clients on one of our "Digital Experience (DEX) Packs. The Vulnerability DEX Pack is a curated collection of dashboards displaying data pertaining to specific cyber threats our software could detect and to alert to mitigate risk.

Introduction

The Vulnerability DEX Pack detects, informs, and quantifies your enterprise's vulnerability to specific cyber threats.

Detect

The log4j code is a simple data logging tool used in several popular cloud storage systems and other software. Because of the ease and accessibility, log4j is the perfect instrument for a cyber-attack. According to the Washington Post, "Huge swaths of the computer code that modern life runs on use Java and contain log4j." [1] Windows, Linux, Apple, and operating systems are all vulnerable to log4j breaches. What the threat does is attach a bug to the log4j code allowing systems throughout an enterprise to be breached.

Inform

There are fixes and patches to defend against said attacks. Knowing where the vulnerabilities are in your enterprise can help to mitigate against these risks and are prepared for possible future cyber threats. The Vulnerability DEX Pack informs you of what systems, files, and software are still at risk.

Quantify

With SysTrack's data analysis, we pinpoint the specific systems that are still vulnerable to the log4j attack. Your cyber security team can patch or update those systems before it spreads. We also reveal the path and the file in which the log4j threat entered. With our resolve tool, when a system is online, we can see which software still needs patches, the last use, and how many systems are still using the vulnerable software. Dell Insyde H20 UEFI and WinVerifyTrust Signature are two software packages that were particularly affected by log4j. SysTrack assesses which systems are secured and those that are still vulnerable. For WinVerify Trust, it quantifies which systems are still vulnerable, the last trigger date, and whether the sensor is currently active.

---

[1] Hunter, T., & Vynck, G. D. (2021, December 21). *The 'most serious' security breach ever is unfolding right now. here's what you need to know.* The Washington Post. Retrieved May 6, 2022, from https://www.washingtonpost.com/technology/2021/12/20/log4j-hack-vulnerability-java/