

 **Tech-Hub** • SOFLO DEVCON 2024  
SOUTHFLORIDATECHHUB.ORG

Saturday • May 4, 2024 • DAVIE, FL • 8:00AM – 8:00PM

**SCA**

**Software Composition Analysis**

**3:40PM – 4:40PM**

College of Computing  
and Engineering  
NOVA SOUTHEASTERN UNIVERSITY

**NSU**  
Florida



# EUGENIO ALVAREZ



A South Florida software engineering professional. Experienced in organizational design, software design, construction, and deployment. Extensive knowledge of Java. Proponent of Unit testing. An advocate for Agile Software Engineering methods using Kanban and Scrum.

[www.linkedin.com/in/ealvarez](https://www.linkedin.com/in/ealvarez)

# INTRODUCTION

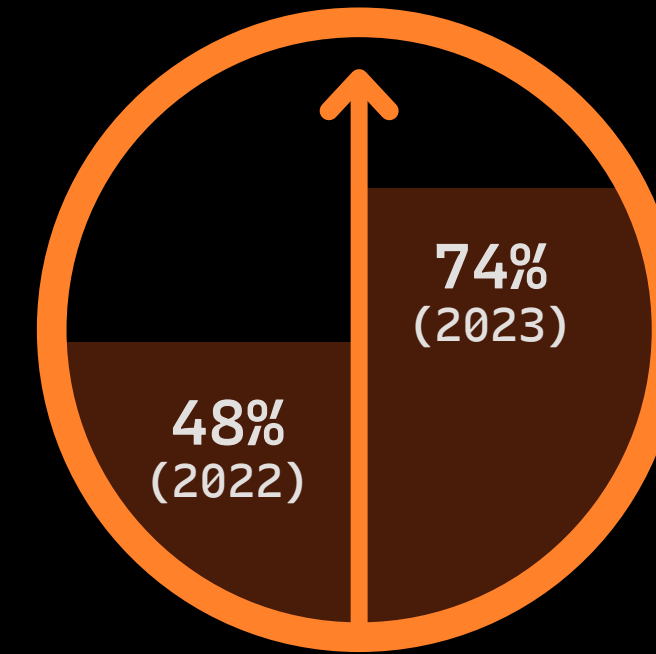
- Market forces are driving companies to develop secure software faster to gain a competitive advantage.
- The software development community has found that Software Component Analysis tooling can improve the competitive need for increased security and speed.
- Software Composition Analysis tooling provides an efficient way to reduce security threats from open-source software components.

# OPEN SOURCE EXPOSURE



96%

of the total  
codebases  
contained  
open source



54% increase in codebases  
containing **high-risk**  
**vulnerabilities** in the  
past year

84%

of codebases assessed for risk contained **vulnerabilities**

74%

of codebases assessed for risk contained **high-risk vulnerabilities**

Source: Synopsys Open Source Security and Risk Report 2024



# OPEN SOURCE COMPONENTS PER APPLICATION (2016-2024)



*Source: Meta-analysis from Synopsys BlackDuck Open Source Security and Risk Reports 2016-2024*

# WHY SO MANY OPEN SOURCE COMPONENTS

**AVERAGE OF 526**

*Source: Synopsys BlackDuck Open Source Security and Risk Reports 2024*

**AVERAGE OF 148  
FOR JAVA APPLICATIONS  
(EST. 90% OF THAT IS OPEN SOURCE)**

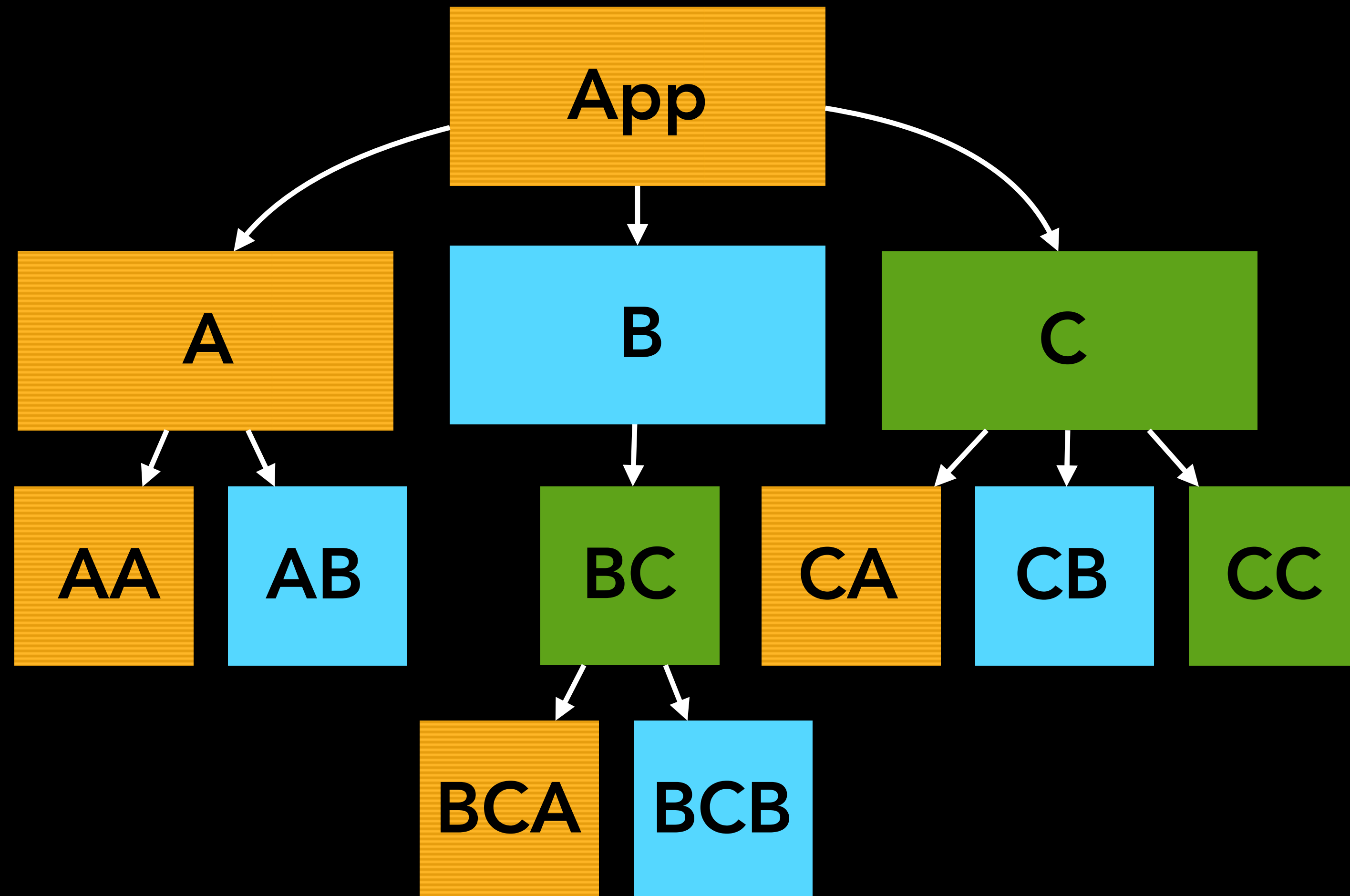
*Source: Sonatype 9th Annual State of the Software Supply Chain Report, Nov 2023*

**MEDIAN OF 683  
FOR JAVASCRIPT APPLICATIONS  
(FROM A MEDIAN OF 10 DIRECT)**

*Source: GitHub Octoverse Report, Dec 2020*

# TRANSITIVE DEPENDENCIES

“Do you realize how many dependencies?”



**"A JEDI USES THE FORCE FOR KNOWLEDGE  
AND DEFENSE, NEVER FOR ATTACK."**



Source: <https://www.starwars.com/news/the-starwars-com-10-best-yoda-quotes>  
<https://www.starwars.com/databank/the-force>



# SECURE CODING TOOL CHEST



- SAST: Static Application Security Testing
- DAST: Dynamic Application Security Testing
- SCA: Software Composition Analysis

# SCA USE-CASES

- Identify open source components
- Identify security issues in open source components
- Identify license issues in open source components
- Mitigate open-source issues
- Manage open-source quality
- Audits for M&A (Mergers and Acquisitions)
- Monitor vendor software



# SOFTWARE COMPOSITION ANALYSIS COMBINED WITH STATIC APPLICATION SCAN

- Some SCA tools use SAST to confirm that code is vulnerable
- Be careful with false negatives
  - Dynamic code can only be confirmed with runtime analysis



# JUST A SIMPLE UPDATE?



- H2 database
- JUnit4 vs JUnit5
- Spring Framework
- Angular JS
- Apache Struts

# MAYBE OR MAYBE NOT

# CVE

## (COMMON VULNERABILITIES AND EXPOSURES)

- Publicly released list of known cybersecurity vulnerabilities
  - Issued by vendors and researchers
  - Each CVE has an identification number “identifier”
  - A CVE does not include technical data
- Databases of public disclosed CVEs (multiple)
  - NVD (National Vulnerabilities Database) USA

Source: <https://www.cve.org/>

# SBOM FORMATS (SOFTWARE BILL OF MATERIALS)

- CycloneDX
  - Open source machine-readable by OWASP
- SPDX® (Software Package Data Exchange)
  - Open standard ISO/IEC 5692:2021 by Linux Foundation

Source: <https://cyclonedx.org/>

Source: <https://spdx.dev/>



# EXAMPLE SBOM?

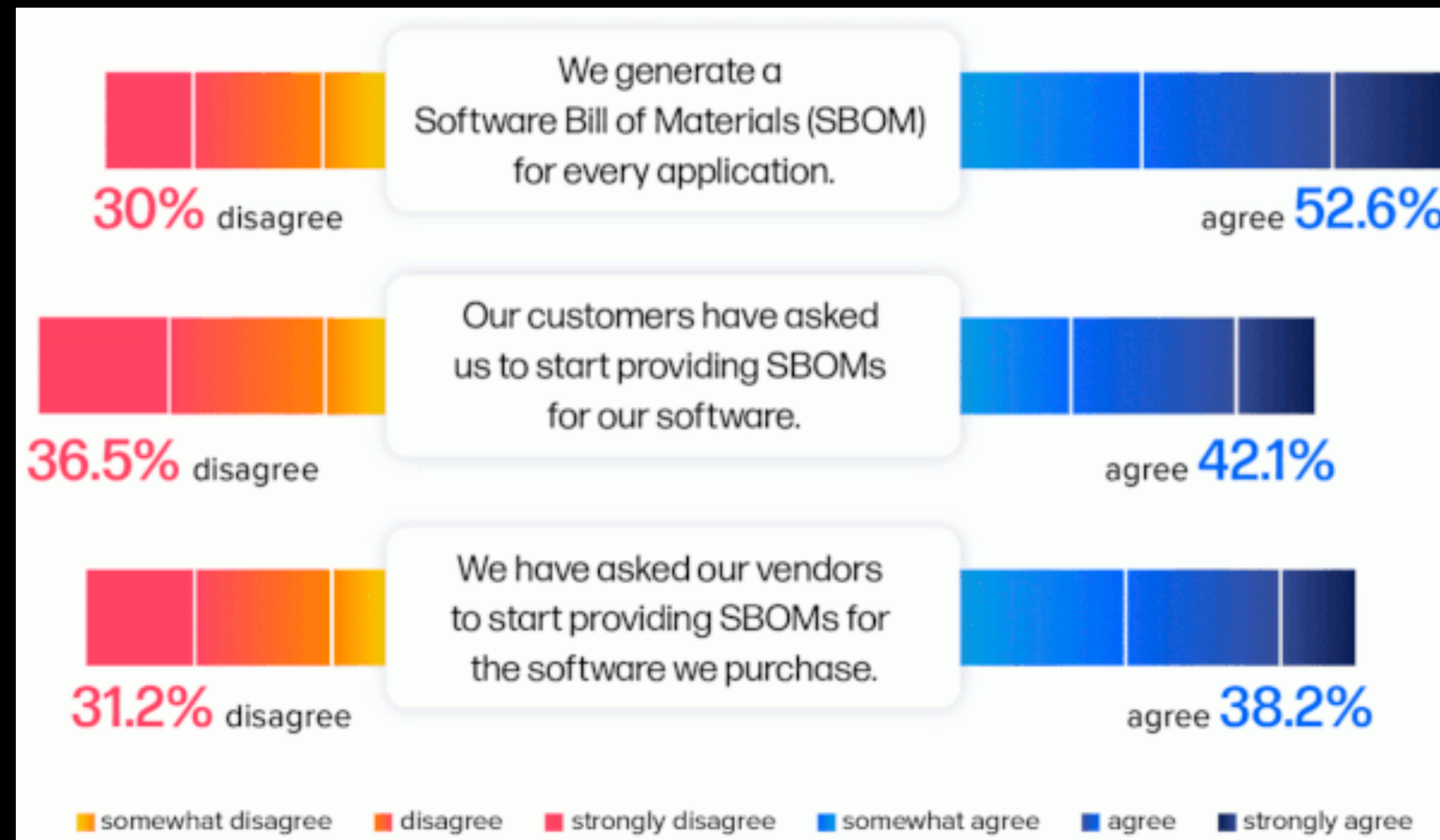
**SPDX Example of an SBOM**

```
SPDXVersion: SPDX-2.1
DataLicense: CC0-1.0
DocumentNamespace: http://www.spdx.org/spdxdocs/8f141b09-1138-4fc5-aecb-
fc10d9ac1eed
DocumentName: SpdxDoc for GNU Time
SPDXID: SPDXRef-DOCUMENT

## Creation Information
Creator: Person: Gary O'Neill
Created: 2018-08-17T11:29:46Z
LicenseConcluded: GPL-2.0-or-later AND GPL-3.0-or-later
## Relationships
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-1

## Package Information
PackageName: GNU Time
PackageVersion: 1.9
PackageSupplier: Organization: GNU
PackageOriginator: Organization: GNU
PackageDownloadLocation: https://ftp.gnu.org/gnu/time/
PackageVerificationCode: 8ee8abb8bc16a33a4444bb6384fa
PackageChecksum: SHA1: 75068c26abbed3ad3980685bae21d7202d288317
PackageHomePage: https://www.gnu.org/software/time/
PackageLicenseConcluded: (GFDL-1.3 AND GPL-3.0-or-later AND LicenseRef-1)
## License Information from files
PackageLicenseInfoFromFiles: X11
PackageLicenseInfoFromFiles: GPL-2.0-or-later WITH libtool-exception
PackageLicenseInfoFromFiles: GPL-3.0-or-later
PackageLicenseInfoFromFiles: LicenseRef-1
PackageLicenseInfoFromFiles: GFDL-1.3
PackageLicenseDeclared: GPL-3.0-or-later
PackageLicenseComments: <text>Several files contained a GPL 2.0 or later
license. Since they were linked to a GPL 3.0
text>
PackageCopyrightText: <text>Copyright (C) 1989, 1991, 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026, 2027, 2028, 2029, 2030, 2031, 2032, 2033, 2034, 2035, 2036, 2037, 2038, 2039, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2054, 2055, 2056, 2057, 2058, 2059, 2060, 2061, 2062, 2063, 2064, 2065, 2066, 2067, 2068, 2069, 2070, 2071, 2072, 2073, 2074, 2075, 2076, 2077, 2078, 2079, 2080, 2081, 2082, 2083, 2084, 2085, 2086, 2087, 2088, 2089, 2090, 2091, 2092, 2093, 2094, 2095, 2096, 2097, 2098, 2099, 2100, 2101, 2102, 2103, 2104, 2105, 2106, 2107, 2108, 2109, 2110, 2111, 2112, 2113, 2114, 2115, 2116, 2117, 2118, 2119, 2120, 2121, 2122, 2123, 2124, 2125, 2126, 2127, 2128, 2129, 2130, 2131, 2132, 2133, 2134, 2135, 2136, 2137, 2138, 2139, 2140, 2141, 2142, 2143, 2144, 2145, 2146, 2147, 2148, 2149, 2150, 2151, 2152, 2153, 2154, 2155, 2156, 2157, 2158, 2159, 2160, 2161, 2162, 2163, 2164, 2165, 2166, 2167, 2168, 2169, 2170, 2171, 2172, 2173, 2174, 2175, 2176, 2177, 2178, 2179, 2180, 2181, 2182, 2183, 2184, 2185, 2186, 2187, 2188, 2189, 2190, 2191, 2192, 2193, 2194, 2195, 2196, 2197, 2198, 2199, 2200, 2201, 2202, 2203, 2204, 2205, 2206, 2207, 2208, 2209, 2210, 2211, 2212, 2213, 2214, 2215, 2216, 2217, 2218, 2219, 2220, 2221, 2222, 2223, 2224, 2225, 2226, 2227, 2228, 2229, 2230, 2231, 2232, 2233, 2234, 2235, 2236, 2237, 2238, 2239, 2240, 2241, 2242, 2243, 2244, 2245, 2246, 2247, 2248, 2249, 2250, 2251, 2252, 2253, 2254, 2255, 2256, 2257, 2258, 2259, 2260, 2261, 2262, 2263, 2264, 2265, 2266, 2267, 2268, 2269, 2270, 2271, 2272, 2273, 2274, 2275, 2276, 2277, 2278, 2279, 2280, 2281, 2282, 2283, 2284, 2285, 2286, 2287, 2288, 2289, 2290, 2291, 2292, 2293, 2294, 2295, 2296, 2297, 2298, 2299, 2300, 2301, 2302, 2303, 2304, 2305, 2306, 2307, 2308, 2309, 2310, 2311, 2312, 2313, 2314, 2315, 2316, 2317, 2318, 2319, 2320, 2321, 2322, 2323, 2324, 2325, 2326, 2327, 2328, 2329, 2330, 2331, 2332, 2333, 2334, 2335, 2336, 2337, 2338, 2339, 2340, 2341, 2342, 2343, 2344, 2345, 2346, 2347, 2348, 2349, 2350, 2351, 2352, 2353, 2354, 2355, 2356, 2357, 2358, 2359, 2360, 2361, 2362, 2363, 2364, 2365, 2366, 2367, 2368, 2369, 2370, 2371, 2372, 2373, 2374, 2375, 2376, 2377, 2378, 2379, 2380, 2381, 2382, 2383, 2384, 2385, 2386, 2387, 2388, 2389, 2390, 2391, 2392, 2393, 2394, 2395, 2396, 2397, 2398, 2399, 2400, 2401, 2402, 2403, 2404, 2405, 2406, 2407, 2408, 2409, 2410, 2411, 2412, 2413, 2414, 2415, 2416, 2417, 2418, 2419, 2420, 2421, 2422, 2423, 2424, 2425, 2426, 2427, 2428, 2429, 2430, 2431, 2432, 2433, 2434, 2435, 2436, 2437, 2438, 2439, 2440, 2441, 2442, 2443, 2444, 2445, 2446, 2447, 2448, 2449, 2450, 2451, 2452, 2453, 2454, 2455, 2456, 2457, 2458, 2459, 2460, 2461, 2462, 2463, 2464, 2465, 2466, 2467, 2468, 2469, 2470, 2471, 2472, 2473, 2474, 2475, 2476, 2477, 2478, 2479, 2480, 2481, 2482, 2483, 2484, 2485, 2486, 2487, 2488, 2489, 2490, 2491, 2492, 2493, 2494, 2495, 2496, 2497, 2498, 2499, 2500, 2501, 2502, 2503, 2504, 2505, 2506, 2507, 2508, 2509, 2510, 2511, 2512, 2513, 2514, 2515, 2516, 2517, 2518, 2519, 2520, 2521, 2522, 2523, 2524, 2525, 2526, 2527, 2528, 2529, 2530, 2531, 2532, 2533, 2534, 2535, 2536, 2537, 2538, 2539, 2540, 2541, 2542, 2543, 2544, 2545, 2546, 2547, 2548, 2549, 2550, 2551, 2552, 2553, 2554, 2555, 2556, 2557, 2558, 2559, 2560, 2561, 2562, 2563, 2564, 2565, 2566, 2567, 2568, 2569, 2570, 2571, 2572, 2573, 2574, 2575, 2576, 2577, 2578, 2579, 2580, 2581, 2582, 2583, 2584, 2585, 2586, 2587, 2588, 2589, 2590, 2591, 2592, 2593, 2594, 2595, 2596, 2597, 2598, 2599, 2600, 2601, 2602, 2603, 2604, 2605, 2606, 2607, 2608, 2609, 2610, 2611, 2612, 2613, 2614, 2615, 2616, 2617, 2618, 2619, 2620, 2621, 2622, 2623, 2624, 2625, 2626, 2627, 2628, 2629, 2630, 2631, 2632, 2633, 2634, 2635, 2636, 2637, 2638, 2639, 2640, 2641, 2642, 2643, 2644, 2645, 2646, 2647, 2648, 2649, 2650, 2651, 2652, 2653, 2654, 2655, 2656, 2657, 2658, 2659, 2660, 2661, 2662, 2663, 2664, 2665, 2666, 2667, 2668, 2669, 2670, 2671, 2672, 2673, 2674, 2675, 2676, 2677, 2678, 2679, 2680, 2681, 2682, 2683, 2684, 2685, 2686, 2687, 2688, 2689, 2690, 2691, 2692, 2693, 2694, 2695, 2696, 2697, 2698, 2699, 2700, 2701, 2702, 2703, 2704, 2705, 2706, 2707, 2708, 2709, 2710, 2711, 2712, 2713, 2714, 2715, 2716, 2717, 2718, 2719, 2720, 2721, 2722, 2723, 2724, 2725, 2726, 2727, 2728, 2729, 2730, 2731, 2732, 2733, 2734, 2735, 2736, 2737, 2738, 2739, 2740, 2741, 2742, 2743, 2744, 2745, 2746, 2747, 2748, 2749, 2750, 2751, 2752, 2753, 2754, 2755, 2756, 2757, 2758, 2759, 2760, 2761, 2762, 2763, 2764, 2765, 2766, 2767, 2768, 2769, 2770, 2771, 2772, 2773, 2774, 2775, 2776, 2777, 2778, 2779, 2780, 2781, 2782, 2783, 2784, 2785, 2786, 2787, 2788, 2789, 2790, 2791, 2792, 2793, 2794, 2795, 2796, 2797, 2798, 2799, 2800, 2801, 2802, 2803, 2804, 2805, 2806, 2807, 2808, 2809, 2810, 2811, 2812, 2813, 2814, 2815, 2816, 2817, 2818, 2819, 2820, 2821, 2822, 2823, 2824, 2825, 2826, 2827, 2828, 2829, 2830, 2831, 2832, 2833, 2834, 2835, 2836, 2837, 2838, 2839, 2840, 2841, 2842, 2843, 2844, 2845, 2846, 2847, 2848, 2849, 2850, 2851, 2852, 2853, 2854, 2855, 2856, 2857, 2858, 2859, 2860, 2861, 2862, 2863, 2864, 2865, 2866, 2867, 2868, 2869, 2870, 2871, 2872, 2873, 2874, 2875, 2876, 2877, 2878, 2879, 2880, 2881, 2882, 2883, 2884, 2885, 2886, 2887, 2888, 2889, 2890, 2891, 2892, 2893, 2894, 2895, 2896, 2897, 2898, 2899, 2900, 2901, 2902, 2903, 2904, 2905, 2906, 2907, 2908, 2909, 2910, 2911, 2912, 2913, 2914, 2915, 2916, 2917, 2918, 2919, 2920, 2921, 2922, 2923, 2924, 2925, 2926, 2927, 2928, 2929, 2930, 2931, 2932, 2933, 2934, 2935, 2936, 2937, 2938, 2939, 2940, 2941, 2942, 2943, 2944, 2945, 2946, 2947, 2948, 2949, 2950, 2951, 2952, 2953, 2954, 2955, 2956, 2957, 2958, 2959, 2960, 2961, 2962, 2963, 2964, 2965, 2966, 2967, 2968, 2969, 2970, 2971, 2972, 2973, 2974, 2975, 2976, 2977, 2978, 2979, 2980, 2981, 2982, 2983, 2984, 2985, 2986, 2987, 2988, 2989, 2990, 2991, 2992, 2993, 2994, 2995, 2996, 2997, 2998, 2999, 3000, 3001, 3002, 3003, 3004, 3005, 3006, 3007, 3008, 3009, 3010, 3011, 3012, 3013, 3014, 3015, 3016, 3017, 3018, 3019, 3020, 3021, 3022, 3023, 3024, 3025, 3026, 3027, 3028, 3029, 3030, 3031, 3032, 3033, 3034, 3035, 3036, 3037, 3038, 3039, 3040, 3041, 3042, 3043, 3044, 3045, 3046, 3047, 3048, 3049, 3050, 3051, 3052, 3053, 3054, 3055, 3056, 3057, 3058, 3059, 3060, 3061, 3062, 3063, 3064, 3065, 3066, 3067, 3068, 3069, 3070, 3071, 3072, 3073, 3074, 3075, 3076, 3077, 3078, 3079, 3080, 3081, 3082, 3083, 3084, 3085, 3086, 3087, 3088, 3089, 3090, 3091, 3092, 3093, 3094, 3095, 3096, 3097, 3098, 3099, 3100, 3101, 3102, 3103, 3104, 3105, 3106, 3107, 3108, 3109, 3110, 3111, 3112, 3113, 3114, 3115, 3116, 3117, 3118, 3119, 3120, 3121, 3122, 3123, 3124, 3125, 3126, 3127, 3128, 3129, 3130, 3131, 3132, 3133, 3134, 3135, 3136, 3137, 3138, 3139, 3140, 3141, 3142, 3143, 3144, 3145, 3146, 3147, 3148, 3149, 3150, 3151, 3152, 3153, 3154, 3155, 3156, 3157, 3158, 3159, 3160, 3161, 3162, 3163, 3164, 3165, 3166, 3167, 3168, 3169, 3170, 3171, 3172, 3173, 3174, 3175, 3176, 3177, 3178, 3179, 3180, 3181, 3182, 3183, 3184, 3185, 3186, 3187, 3188, 3189, 3190, 3191, 3192, 3193, 3194, 3195, 3196, 3197, 3198, 3199, 3200, 3201, 3202, 3203, 3204, 3205, 3206, 3207, 3208, 3209, 3210, 3211, 3212, 3213, 3214, 3215, 3216, 3217, 3218, 3219, 3220, 3221, 3222, 3223, 3224, 3225, 3226, 3227, 3228, 3229, 3230, 3231, 3232, 3233, 3234, 3235, 3236, 3237, 3238, 3239, 3240, 3241, 3242, 3243, 3244, 3245, 3246, 3247, 3248, 3249, 3250, 3251, 3252, 3253, 3254, 3255, 3256, 3257, 3258, 3259, 3260, 3261, 3262, 3263, 3264, 3265, 3266, 3267, 3268, 3269, 3270, 3271, 3272, 3273, 3274, 3275, 3276, 3277, 3278, 3279, 3280, 3281, 3282, 3283, 3284, 3285, 3286, 3287, 3288, 3289, 3290, 3291, 3292, 3293, 3294, 3295, 3296, 3297, 3298, 3299, 3300, 3301, 3302, 3303, 3304, 3305, 3306, 3307, 3308, 3309, 3310, 3311, 3312, 3313, 3314, 3315, 3316, 3317, 3318, 3319, 3320, 3321, 3322, 3323, 3324, 3325, 3326, 3327, 3328, 3329, 3330, 3331, 3332, 3333, 3334, 3335, 3336, 3337, 3338, 3339, 3340, 3341, 3342, 3343, 3344, 3345, 3346, 3347, 3348, 3349, 3350, 3351, 3352, 3353, 3354, 3355, 3356, 3357, 3358, 3359, 3360, 3361, 3362, 3363, 3364, 3365, 3366, 3367, 3368, 3369, 3370, 3371, 3372, 3373, 3374, 3375, 3376, 3377, 3378, 3379, 3380, 3381, 3382, 3383, 3384, 3385, 3386, 3387, 3388, 3389, 3390, 3391, 3392, 3393, 3394, 3395, 3396, 3397, 3398, 3399, 3400, 3401, 3402, 3403, 3404, 3405, 3406, 3407, 3408, 3409, 3410, 3411, 3412, 3413, 3414, 3415, 3416, 3417, 3418, 3419, 3420, 3421, 3422, 3423, 3424, 3425, 3426, 3427, 3428, 3429, 3430, 3431, 3432, 3433, 3434, 3435, 3436, 3437, 3438, 3439, 3440, 3441, 3442, 3443, 3444, 3445, 3446, 3447, 3448, 3449, 3450, 3451, 3452, 3453, 3454, 3455, 3456, 3457, 3458, 3459, 3460, 3461, 3462, 3463, 3464, 3465, 3466, 3467, 3468, 3469, 3470, 3471, 3472, 3473, 3474, 3475, 3476, 3477, 3478, 3479, 3480, 3481, 3482, 3483, 3484, 3485, 3486, 3487, 3488, 3489, 3490, 3491, 3492, 3493, 3494, 3495, 3496, 3497, 3498, 3499, 3500, 3501, 3502, 3503, 3504, 3505, 3506, 3507, 3508, 3509, 3510, 3511, 3512, 3513, 3514, 3515, 3516, 3517, 3518, 3519, 3520, 3521, 3522, 3523, 3524, 3525, 3526, 3527, 3528, 3529, 3530, 3531, 3532, 3533, 3534, 3535, 3536, 3537, 3538, 3539, 3540, 3541, 3542, 3543, 3544, 3545, 3546, 3547, 3548, 3549, 3550, 3551, 3552, 3553, 3554, 3555, 3556, 3557, 3558, 3559, 3560, 3561, 3562, 3563, 3564, 3565, 3566, 3567, 3568, 3569, 3570, 3571, 3572, 3573, 3574, 3575, 3576, 3577, 3578, 3579, 3580, 3581, 3582, 3583, 3584, 3585, 3586, 3587, 3588, 3589, 3590, 3591, 3592, 3593, 3594, 3595, 3596, 3597, 3598, 3599, 3600, 3601, 3602, 3603, 3604, 3605, 3606, 3607, 3608, 3609, 3610, 3611, 3612, 3613, 3614, 3615, 3616, 3617, 3618, 3619, 3620, 3621, 3622, 3623, 3624, 3625, 3626, 3627, 3628, 3629, 3630, 3631, 3632, 3633, 3634, 3635, 3636, 3637, 3638, 3639, 3640, 3641, 3642, 3643, 3644, 3645, 3646, 3647, 3648, 3649, 3650, 3651, 3652, 3653, 3654, 3655, 3656, 3657, 3658, 3659, 3660, 3661, 3662, 3663, 3664, 3665, 3666, 3667, 3668, 3669, 3670, 3671, 3672, 3673, 3674, 3675, 3676, 3677, 3678, 3679, 3680, 3681, 3682, 3683, 3684, 3685, 3686, 3687, 3688, 3689, 3690, 3691, 3692, 3693, 3694, 3695, 3696, 3697, 3698, 3699, 3700, 3701, 3702, 3703, 3704, 3705, 3706, 3707, 3708, 3709, 3710, 3711, 3712, 3713, 3714, 3715, 3716, 3717, 3718, 3719, 3720, 3721, 3722, 3723, 3724, 3725, 3726, 3727, 3728, 3729, 3730, 3731, 3732, 3733, 3734, 3735, 3736, 3737, 3738, 3739, 3740, 3741, 3742, 3743, 3744, 3745, 3746, 3747, 3748, 3749, 3750, 3751, 3752, 3753, 3754, 3755, 3756, 3757, 3758, 3759, 3760, 3761, 3762, 3763, 3764, 3765, 3766, 3767, 3768, 3769, 3770, 3771, 3772, 3773, 3774, 3775, 3776, 3777, 3778, 3779, 3780, 3781, 3782, 3783, 3784, 3785, 3786, 3787, 3788, 3789, 3790, 3791, 3792, 3793, 3794, 3795, 3796, 3797, 3798, 3799, 3800, 3801, 3802, 3803, 3804, 3805, 3806, 3807, 3808, 3809, 3810, 3811, 3812, 3813, 3814, 3815, 3816, 3817, 3818, 3819, 3820, 3821, 3822, 3823, 3824, 3825, 3826, 3827, 3828, 3829, 3830, 3831, 3832, 3833, 3834, 3835, 3836, 3837, 3838, 3839, 3840, 3841, 3842, 3843, 3844, 3845, 3846, 3847, 3848, 3849, 3850, 3851, 3852, 3853, 3854, 3855, 3856, 3857, 3858, 3859, 3860, 3861, 3862, 3863, 3864, 3865, 3866, 3867, 3868, 3869, 3870, 3871, 3872, 3873, 3874, 3875, 3876, 3877, 3878, 3879, 3880, 3881, 3882, 3883, 3884, 3885, 3886, 3887, 3888, 3889, 3890, 3891, 3892, 3893, 3894, 3895, 3896, 3897, 3898, 3899, 3900, 3901, 3902, 3903, 3904, 3905, 3906, 3907, 3908, 3909, 3910, 3911, 3912, 3913, 3914, 3915, 3916, 3917, 3918, 3919, 3920, 3921, 3922, 3923, 3924, 3925, 3926, 3927, 3928, 3929, 3930, 3931, 3932, 3933, 3934, 3935, 3936, 3937, 3938, 3939, 3940, 3941, 3942, 3943, 3944, 3945, 3946, 3947, 3948, 3949, 3950, 3951, 3952, 3953, 3954, 3955, 3956, 3957, 3958, 3959, 3960, 3961, 3962, 3963, 396
```

# SBOM USAGE SURVEY SAYS



Source: Sonatype 9th Annual State of the Software Supply Chain Report, Nov 2023

# SBOM ADOPTION DRIVERS

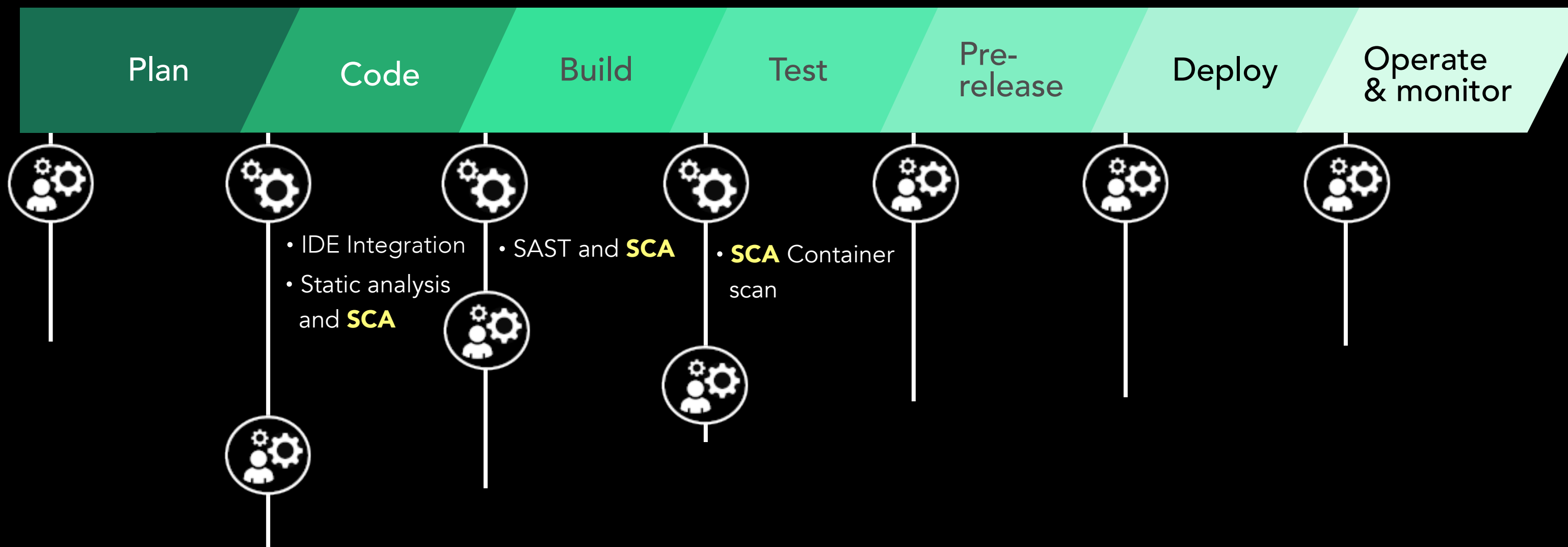
- Presidential Executive order 14028 (Cybersecurity)
  - An SBOM as part of Secure Development
- Regulatory Compliance
- Risk management via CI/CD supply chain monitoring
- Customer Assurance

Source: <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>



# WHERE IS SCA IN BUILD PIPELINE

## Application Security Pipeline



Source: <https://vulcan.io/blog/ci-cd-security-5-best-practices/>

# OPEN SOURCE LICENSE IDENTIFICATION AND MANAGEMENT

- MIT License
- Apache License 2.0
- BSD License variants
- Mozilla Public License 2.0
- Public Domain
- GNU Lesser (As long as the code is unmodified)
- **GNU GPL (License conflict)**

Source: <https://www.gnu.org/licenses/gpl-3.0.en.html>

# WHY GPL CAUSES A CONFLICT

- Copyleft Requirement: Any derivative work created from a GPL licensed code must be distributed under the GPL which includes the source code of the entire derivative work.
- Examples:
  - Linksys/Cisco WRT54G
  - Samsung Smart TVs

Source: <https://www.fsf.org/news/2008-12-cisco-suit>



# OPEN SOURCE VERSION MANAGEMENT

91%



of the codebases assessed for risk contained components that were **10 versions** or more **behind the most current version** of the component

*Source: Synopsys Open Source Security and Risk Report, Feb 2024*

96%



of the component downloads with known **vulnerabilities** could be **avoided** as a better, **fixed version** is already available

*Source: Sonatype 9th Annual State of the Software Supply Chain Report, Nov 2023*

- SCA Tools recommend the latest version

# OPEN SOURCE QUALITY MANAGEMENT

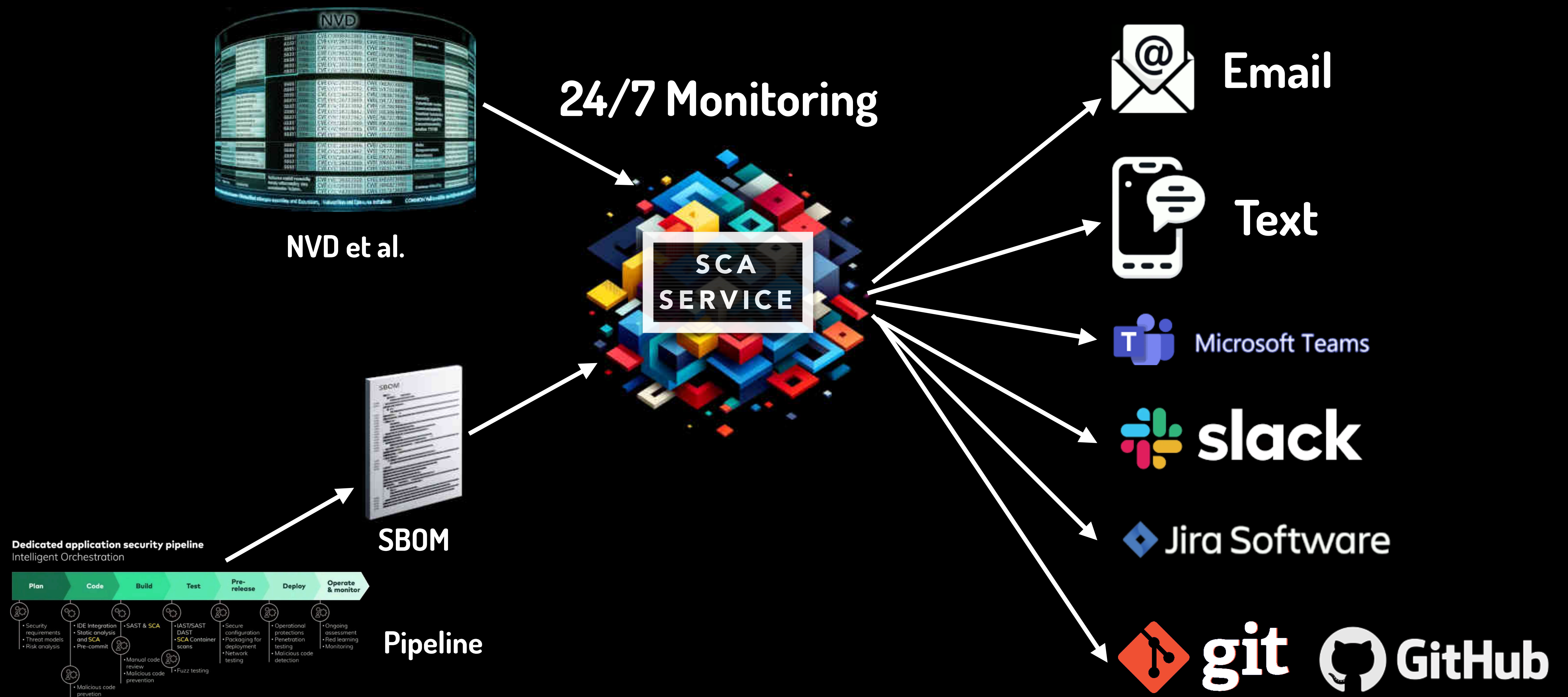
“The fact that 18.6% of [open source] projects stopped being maintained in the last year highlights the need to not only choose good dependencies, but monitor those dependencies for changes in their quality.” \*

*Source: Sonatype 9th Annual State of the Software Supply Chain Report, Nov 2023*

\* maintained as defined by the OpenSSF (Open Source Security Foundation) scorecard



# CONTINUOUS MONITORING AND NOTIFICATION



# SCA SCAN FOR VENDOR SOFTWARE



*Source: DALL·E*

# SBOM FOR VENDOR SOFTWARE RECOMMENDED



# THIRD-PARTY RISK MANAGEMENT (TPRM)

**"98% of organizations have a relationship with a third party that has been breached."**

*Source: SecurityScoreCard Global Third-Party Cybersecurity Breaches Report, Feb 2024*

**Third-party breaches by industry:**

**43% Technology & Telecommunications**

**30% Financial Services**

**29% Overall cross-industry rate**



*Source: SecurityScoreCard Global Third-Party Cybersecurity Breaches Report, Feb 2024*

- Stop depending on a questionnaires for TPRM
- Vendor SBOMs can be monitored 24/7 by SCA Tooling

# M&A USE-CASE


- Searching for code vulnerabilities
- Searching for licensing conflicts
- Experience
  - Scan and correct before initial engagement
  - Third-party software will be used to audit
  - Do not expect to explain any risk assessment

# AI HALLUCINATIONS



## AI hallucinates software packages and devs download them – even if potentially poisoned with malware

Simply look out for libraries imagined by ML and make them real, with actual malicious code.  
No wait, don't do that

 [Thomas Claburn](#) Thu 28 Mar 2024 // 07:01 UTC

**IN-DEPTH** Several big businesses have published source code that incorporates a software package previously hallucinated by generative AI.

Not only that but someone, having spotted this reoccurring hallucination, had turned that made-up dependency into a real one, which was subsequently downloaded and installed thousands of times by developers as a result of the AI's bad advice, we've learned. If the package was laced with actual malware, rather than being a benign test, the results could have been disastrous.

Source: [https://www.theregister.com/2024/03/28/ai\\_bots\\_hallucinate\\_software\\_packages/](https://www.theregister.com/2024/03/28/ai_bots_hallucinate_software_packages/)

# SCA TOOLS



# SCA IDE PLUGINS

The screenshot displays the IntelliJ IDEA interface with a project named 'WebGoat-develop'. The main editor shows a Docker Compose file 'goat-with-reverseproxy.yml'. The 'Code Analysis' tab is active, showing a list of issues. The first issue is 'Container allows filesystem write' at line 23. The right-hand pane provides details for this issue, including a description, status, and remediation steps.

**Issue: Container allows filesystem write**

The docker service container is configured to permit writing to the root filesystem. This makes some security attack vectors such as privilege escalation, denial-of-service or authorization bypass possible since the container instance's filesystem can be tampered with.

Status: Open

WebGoat-develop > goat-with-reverseproxy.yml: Line 23

Contributing code events (1) - Open

**Remediation:**

Explicitly set the "read-only" attribute of the service to "true" to create a service container with a read-only filesystem.

**Checker:**

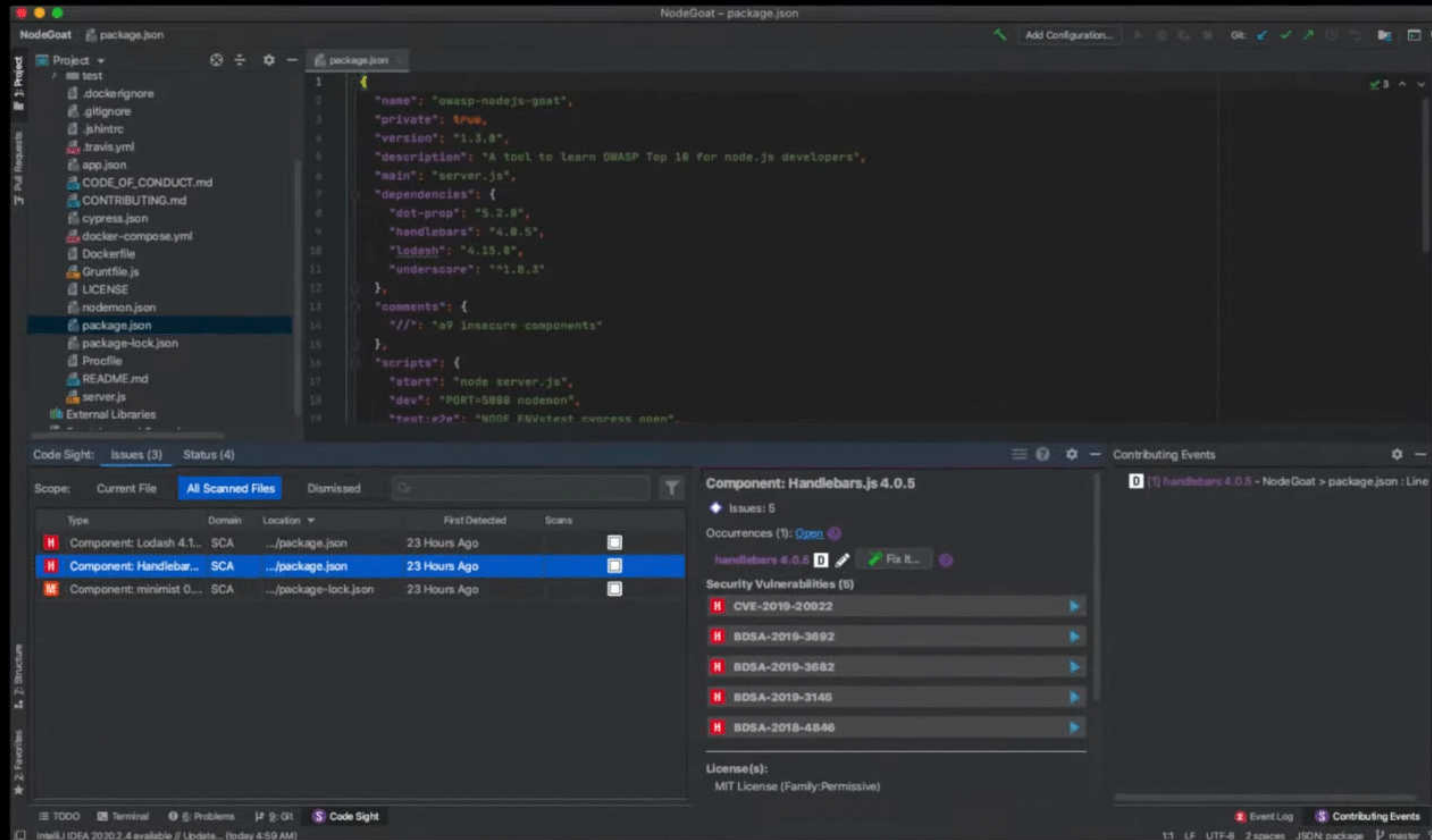
container\_filesystem\_write\_docker\_compose

Type	Location	Scans	First Detected
Container allows filesystem write	.../goat-with-reverseproxy.yml:23	1	16 Minutes Ago
Container allows filesystem write	.../goat-with-reverseproxy.yml:36	1	16 Minutes Ago
Container allows filesystem write	.../goat-with-reverseproxy.yml:6	1	16 Minutes Ago
Container privilege escalation allowed	.../goat-with-reverseproxy.yml:6	1	16 Minutes Ago
Container privilege escalation allowed	.../goat-with-reverseproxy.yml:36	1	16 Minutes Ago
Container privilege escalation allowed	.../goat-with-reverseproxy.yml:23	1	16 Minutes Ago
Container requests ability to craft raw...	.../goat-with-reverseproxy.yml:36	1	16 Minutes Ago
Container requests ability to craft raw...	.../goat-with-reverseproxy.yml:6	1	16 Minutes Ago
Container requests ability to craft raw...	.../goat-with-reverseproxy.yml:23	1	16 Minutes Ago

Source: <https://youtu.be/6cxi96CJB14>

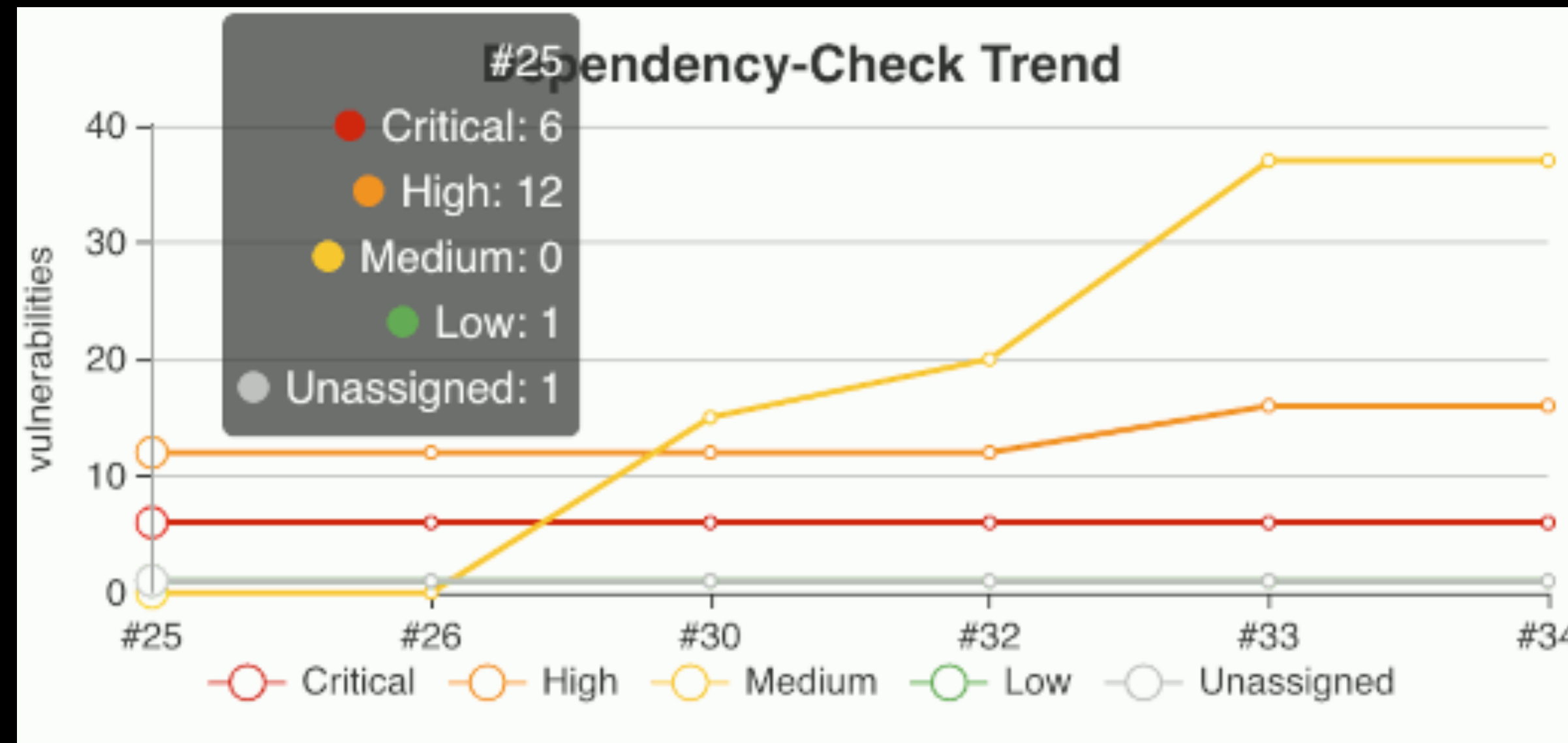


# SCA IDE PLUGINS



Source: <https://youtu.be/W9BHyXYw3vQ>

# DEPENDENCY CHECK



### Dependency-Check Results

SEVERITY DISTRIBUTION

6	16	37	1
---	----	----	---

Search

File Name	Vulnerability	Severity	Weakness
+ jackson-databind-2.8.11.3.jar	NVD CVE-2018-19360	Critical	CWE-502
+ jackson-databind-2.8.11.3.jar	NVD CVE-2018-19361	Critical	CWE-502
- jackson-databind-2.8.11.3.jar	NVD CVE-2018-19362	Critical	CWE-502

File Path	/Users/steve/.m2/repository/com/fasterxml/jackson/core/jackson-databind/2.8.11.3/jackson-databind-2.8.11.3.jar
SHA-1	844df5aba5a1a56e00905b165b12bb34116ee858
SHA-256	5582d55d615ea5ec09563558144c22cac46a06739a8561d7db4ff5c41532d6bc
Description	FasterXML jackson-databind 2.x before 2.9.8 might allow attackers to have unspecified impact by leveraging failure to block the jboss-common-core class from polymorphic deserialization.

+ jackson-databind-2.8.11.3.jar	NVD CVE-2019-12086	High	CWE-200
+ jquery-2.1.4.min.js	NVD CVE-2019-11358	Medium	CWE-79
+ jquery-2.2.4.min.js	NVD CVE-2015-9251	Medium	CWE-79
+ jquery-2.2.4.min.js	NVD CVE-2019-11358	Medium	CWE-79

3 of 7

Source: <https://plugins.jenkins.io/dependency-check-jenkins-plugin/>

# DEPENDENCY TRACK



Source: <https://www.dependencytrack.org/>



# DEPENDENCY TRACK DEMO OVERVIEW

- Step 1: Download application code from GitHub
- Step 2: Create SBOM from project
- Step 3: Upload SBOM to Dependency Track
- Step 4: Observe project's CVEs in Dependence Track

# RUNNING DEPENDENCY TRACK

- Step 1: Requirements
  - Windows/Mac/Linux with
    - Memory: Recommend 16 gigabytes
- Step 2: Download/install Docker
- Step 3: Download/install Dependency Track Docker image
  - `curl -LO https://dependencytrack.org/docker-compose.yml`
  - `docker-compose up -d`
- Step 4: Download/install git
- Step 5: Download/install npm
- Step 6: Download/install cdxgen
  - `npm install -g @cyclonedx/cdxgen`

# WHAT HAPPENS WHEN DEPENDENCY TRACK IS STARTED THE FIRST TIME

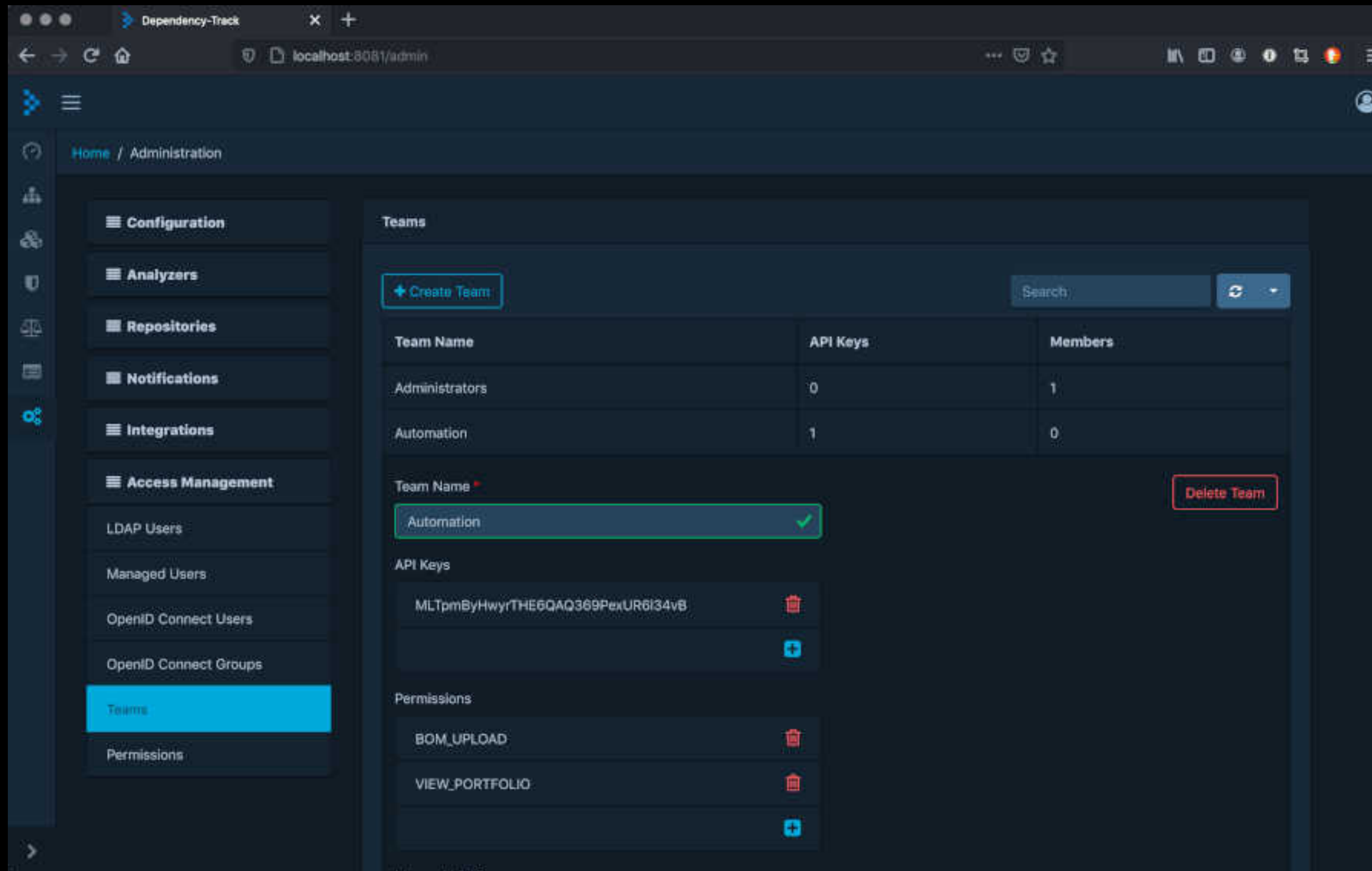
- Downloading the Docker compose file
  - `curl -LO https://dependencytrack.org/docker-compose.yml`
- Starts Docker container
  - `docker-compose up -d`
- An embedded H2 database is the default
  - Options: PostgreSQL or Microsoft SQL Server
- Initial startup downloads CVE database
  - Database download takes at least 30 mins.



# DEPENDENCY TRACK API SETUP

- Step 1: Login with user/password: admin/admin
  - <http://localhost:8080/>
  - Default: admin/admin
- Step 2: Dependency Track needs time to download DB (min. 30 mins)
- Step 3: Change admin password
- Step 4: Retrieve API key
  - Home / Administration / Access Management / Teams / Automation
- Note: UI: localhost:8080 / API: localhost:8081

# DEPENDENCY TRACK API RETRIEVE API KEY



- Note: Add "PROJECT\_CREATION\_UPLOAD" permission

# CREATING THE SBOM

- Why use cdxgen?
  - Multi-language support:
    - Python, C/C++, Java, JavaScript, Go, Ruby, Rest and more..
- Command line:
  - `cdxgen -o bom.json`
- Maven plugin (Java maven based projects):
  - `mvn cyclonedx:makeAggregateBom`
- Chose random Java application
  - `git clone https://github.com/neo-nico-neiman/fullstack-booking.git`



# SENDING SBOM VIA CURL

```
curl -X "POST" "http://localhost:8081/api/v1/bom" ^  
-H "Content-Type: multipart/form-data" ^  
-H "X-API-Key: odt_mt3zaRUX48bKPt82IBlQyhzluk7YRknG" ^  
-F "autoCreate=true" ^  
-F "projectName=fullstack-booking-cdxgen" ^  
-F "projectVersion=2.9" ^  
-F "bom=@bom.json"
```

\* Window batch file example

# DEPENDENCY TRACK

DEMO TIME!

# SOFTWARE COMPOSITION ANALYSIS

**South Florida Developer Conference (SoFlo Dev Con)**

# Thank You



[www.linkedin.com/in/ealvarez](https://www.linkedin.com/in/ealvarez)



# REFERENCES

- Synopsys 2024 Open Source Security and Risk Analysis Report (OSSRA)
  - <https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/rep-ossra-2024.pdf>
- Sonatype 2023 9th Annual State of the Software Supply Chain Report
  - [https://www.sonatype.com/hubfs/2023 Sonatype- 9th Annual State of the Software Supply Chain- Update.pdf](https://www.sonatype.com/hubfs/2023%20Sonatype-9th%20Annual%20State%20of%20the%20Software%20Supply%20Chain-Update.pdf)
- GitHub Octoverse Report 2020
  - <https://octoverse.github.com/2020/>
- The StarWars.com 10: Best Yoda Quotes
  - <https://www.starwars.com/news/the-starwars-com-10-best-yoda-quotes>
- CVE (Common Vulnerabilities and Exposures)
  - <https://www.cve.org>
- OWASP CycloneDX Software Bill of Materials (SBOM) Standard
  - <https://cyclonedx.org/>

# REFERENCES

- System Package Data Exchange (SPDX®) (SBOM) Standard
- <https://spdx.dev/>
- SBOM: An Up-Close Look at a Software Bill of Materials
- <https://www.thesslstore.com/blog/sbom-an-up-close-look-at-a-software-bill-of-materials/>
- Executive order 14028 (Cybersecurity)
- <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>
- CI/CD security - 5 best practices
- <https://vulcan.io/blog/ci-cd-security-5-best-practices/>
- GNU General Public License
- <https://www.gnu.org/licenses/gpl-3.0.en.html>
- GPL Violation law suit
- <https://www.fsf.org/news/2008-12-cisco-suit>

# REFERENCES

- The Register: AI hallucinates software packages
- [https://www.theregister.com/2024/03/28/ai\\_bots\\_hallucinate\\_software\\_packages/](https://www.theregister.com/2024/03/28/ai_bots_hallucinate_software_packages/)
- SecurityScoreCard Global Third-Party Cybersecurity Breaches Report, Feb 2024
- <https://securityscorecard.com/wp-content/uploads/2024/02/Global-Third-Party-Cybersecurity-Breaches-Final-1.pdf>
- Code Sight IDE Plugin for Application Security Testing | Synopsys
- <https://youtu.be/6cxi96CJB14>
- Secure and manage open source risks in applications and containers with Black Duck SCA
- <https://youtu.be/W9BHyXYw3vQ>
- OWASP Dependency Check
- <https://owasp.org/www-project-dependency-check/>
- <https://plugins.jenkins.io/dependency-check-jenkins-plugin/>
- OWASP Dependency Track
- <https://owasp.org/www-project-dependency-track/>
- <https://www.dependencytrack.org/>
- CycloneDX: A multi-language tool that can create SBOM (Bill of Materials) in CycloneDX format.
- <https://cyclonedx.github.io/cdxgen/>