

Supply Chain Security Frameworks

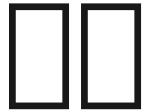
Press Space for next page →



- **SBOM** / Software Bill of Materials
- **SDLC** / Software Development Life Cycle



- **Dependency Management**
 - **Dependency Injection**
 - **Dependency Resolution**

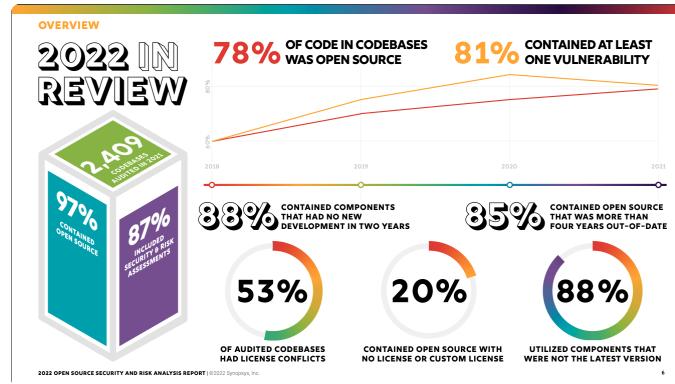




A horizontal row of 20 empty rectangular boxes, each with a thin black border, intended for children to practice writing their names.

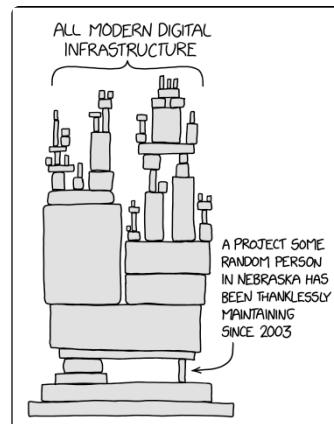
- 97% ████████████████████
 - ████ ████ ████ ████ 78% ██████████████████

ref: 2022 OPEN SOURCE SECURITY AND RISK ANALYSIS REPORT - Synopsys

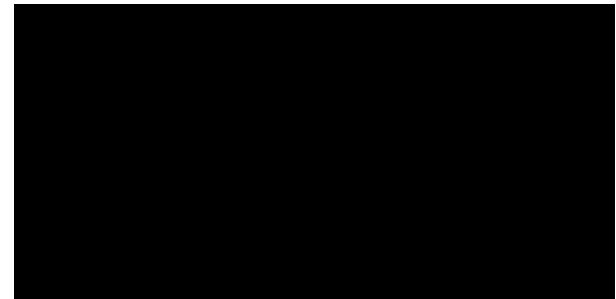


A horizontal row of 20 empty rectangular boxes, each with a thin black border, intended for handwritten responses.

*“The chain is only as strong as its **weakest link**, for if that fails the chain fails and the object that it has been holding up falls to the ground.”* - Thomas Reid (1785)



refs: 2347: Dependency - explain xkcd



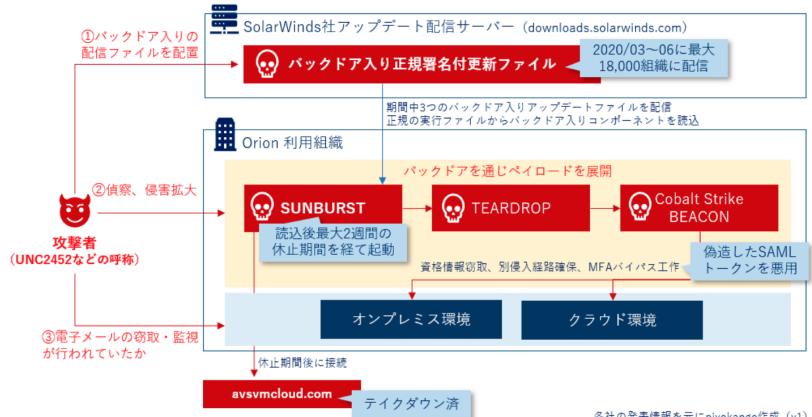
npm install...



ソラーワンズのオリオンプラットフォーム

Solar Winds×Orion Platform サイバーアクセス

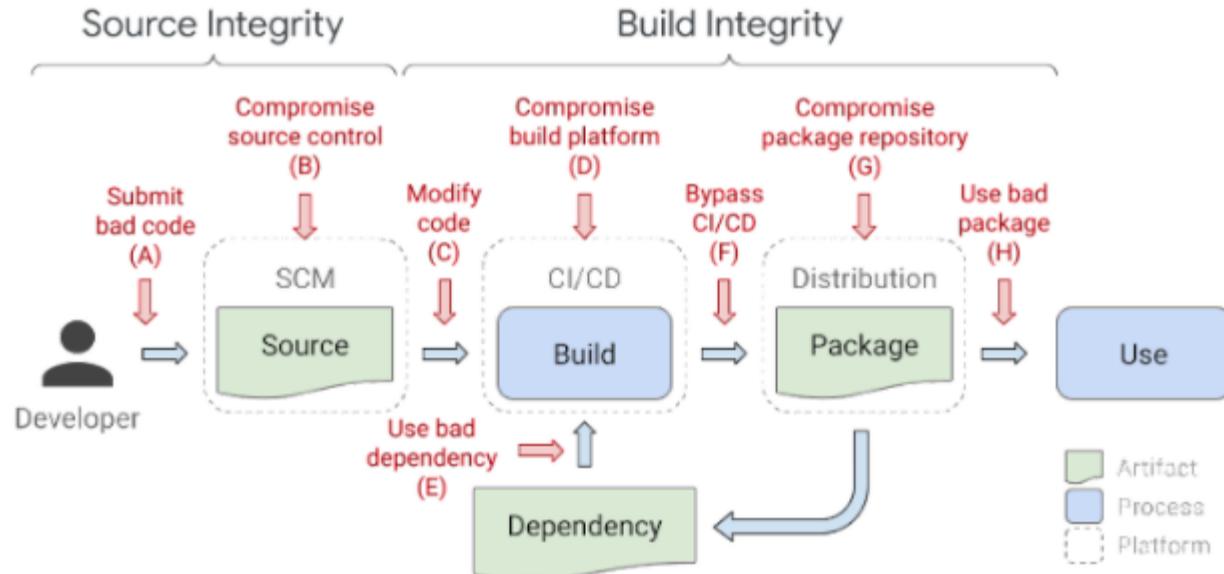
- Orion、オーリオンプラットフォーム
- Orion、オーリオンプラットフォーム、ソラーワンズ、DLL注入、
exploit
 - フィルタリング機能、監視機能、分析機能
- 2020年3~6月にかけて18,000組織
- Microsoft, Nvidia, Intelなど



※: SolarWinds オリオンプラットフォーム××××××××××\ - piyolog



Supply Chain Attacking Surface



ref: Protect your open source project from supply chain attacks | Google Open Source Blog

Executive Order 14028

EO-14028

EO-14028

* XX: `SBOM` EO-14028XXXXXX2XXXX

Sec. 4. Enhancing Software Supply Chain Security.

...

(e) ... (NIST) issue guidance identifying practices that enhance the security of the software supply chain...

_(vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;

...

(f) Within 60 days of the date of this order,... and the Administrator of the National Telecommunications and Information Administration, shall publish minimum elements for an SBOM.

【米国】国家のサイバーセキュリティの改善に係る米国大統領令の署名

- 2021年5月12日、バイデン大統領は、連邦政府機関におけるサイバーセキュリティ改善に係る大統領令に署名。
- 官民での脅威情報の共有、ソフトウェアサプライチェーンセキュリティ対策の強化、ゼロトラストアーキテクチャへの移行等を通じて、連邦政府機関のサイバーセキュリティ対応能力の向上を図っている。

本大統領令における主な指示事項

- | | |
|---|--|
| 1
官民の脅威情報共有における障害の除去 (Section 2) | ● ITサービスプロバイダーが連邦政府と確実に脅威情報を共有できるようにして、特定のインシデント情報の共有を義務づける。 |
| 2
連邦政府におけるより強力な標準の近代化と導入 (Section 3) | ● FedRAMP改定等を通じて、 <u>連邦政府が安全なクラウド及びゼロトラストアーキテクチャに移行することを支援</u> し、多要素認証と暗号化の導入を義務づける。 |
| 3
ソフトウェア・サプライチェーンのセキュリティ向上 (Section 4) | ● NISTを通じて政府が調達するソフトウェアの開発に関するセキュリティ基準（ <u>安全な開発環境の確保や構成要素に関する詳細（SBOM）の開示等を含む</u> ）を確立し、特に <u>重要なソフトウェアに対して一定の対策を義務づける</u> 。 |
| 4
サイバー安全審査委員会の創設 (Section 5) | ● 商務省は、既存のラベル表示などを参考にして、消費者向けの情報提供に関するパリオット制度を開始する。 |
| 5
インシデント対応のための標準フレイムックの策定 (Section 6, 7) | ● 国土安全保障省は、 <u>重大なインシデントが生じた際に政府と民間事業者が共同議長を務めるサイバー安全審査委員会</u> を設置し、サイバーセキュリティ向上に向け具体的な提言を行う権限を与える。 |
| 6
調査及び修復能力の向上 (Section 8) | ● 国土安全保障省は、連邦政府機関によるインシデント対応のためのフレイムックを策定する。
● 連邦政府機関は、エンドポイント検知・対応(EDR)イニシアチブを展開し、インシデントの検知、積極的なサイバーハンティング、有事対応をサポートする。
● 連邦政府機関に対してセキュリティイベントログの要件を設け、侵入を検知し、対処する組織能力の向上を支援する。 |

(出典) 各種公開情報より作成

XX: EO-14028XXXXXX2XXXXXX \- XXXXX

Supply Chain Security Frameworks

Supply Chain Security Frameworks

Abbr	Name	Org	Published	Descriptions
SSDF	Secure Software Development Framework v1.1	NIST	2022/02/03	ISO/IEC 21827-1, ISO/IEC 21827-2, EO14028
SLSA	Supply chain Levels for Software Artifacts	Google	2021/06/21	Integrity, End-to-End
-	Software Supply Chain Best Practices	CNCF	2021/05/14	Open Container Initiative
S2C2F	Secure Supply Chain Consumption Framework	OpenSSF (Microsoft)	2022/08/01	OSS

SSDF (SP 800-218)

NIST - Secure Software Development Framework

XXX/XXX

Software producer

Group	Tasks
Prepare the Organization (PO)	13
Protect the Software (PS)	4
Produce Well-Secured Software (PW)	16
Respond to Vulnerabilities (RV)	9

NIST Special Publication 800-218

Secure Software Development Framework (SSDF) Version 1.1:

Recommendations for Mitigating the Risk of Software Vulnerabilities

Practices	Tasks	National Implementation Examples	References
Prepare the Program (PD)			
Define Security Requirements for Software Development	PD.1.1. Identify and document all security requirements for the organization's software development infrastructure and processes, and measure the requirements over time.	<p>Example 1: Create policies for securing software development infrastructures and their components, including development endpoints. Investigate the SDLC and any relevant security standards to identify requirements.</p> <p>Example 2: Define policies for securing software development environments through the SDLC and maintaining the security, including for open-source and third-party components.</p> <p>Example 3: Review and update security requirements at least annually, or sooner if there are significant changes in the organization's business objectives (e.g., the organization's policies, business objectives, or management structure), or if new security incidents targeting software development infrastructure have occurred.</p> <p>Example 4: Develop audit checklists on pending changes in requirements.</p>	<p>BSI-SPM-1-G1_581-1_K2</p> <p>BSI-SPM-1-CP1_3P1_581-2_K82_562</p> <p>ECDM-4x4-1</p> <p>MISTCF-10_G-V3</p> <p>OWASP-ASVS-1.0</p> <p>OWASP-ASVS-1.1</p> <p>OWASP-ASVS-1.2</p> <p>OWASP-ASVS-1.3</p> <p>OWASP-ASVS-1.4</p> <p>OWASP-ASVS-1.5</p> <p>OWASP-ASVS-1.6</p> <p>OWASP-ASVS-1.7</p> <p>OWASP-ASVS-1.8</p> <p>OWASP-ASVS-1.9</p> <p>OWASP-ASVS-1.10</p> <p>OWASP-ASVS-1.11</p> <p>OWASP-ASVS-1.12</p> <p>OWASP-ASVS-1.13</p> <p>OWASP-ASVS-1.14</p> <p>OWASP-ASVS-1.15</p> <p>OWASP-ASVS-1.16</p> <p>OWASP-ASVS-1.17</p> <p>OWASP-ASVS-1.18</p> <p>OWASP-ASVS-1.19</p> <p>OWASP-ASVS-1.20</p> <p>OWASP-ASVS-1.21</p> <p>OWASP-ASVS-1.22</p> <p>OWASP-ASVS-1.23</p> <p>OWASP-ASVS-1.24</p> <p>OWASP-ASVS-1.25</p> <p>OWASP-ASVS-1.26</p> <p>OWASP-ASVS-1.27</p> <p>OWASP-ASVS-1.28</p> <p>OWASP-ASVS-1.29</p> <p>OWASP-ASVS-1.30</p> <p>OWASP-ASVS-1.31</p> <p>OWASP-ASVS-1.32</p> <p>OWASP-ASVS-1.33</p> <p>OWASP-ASVS-1.34</p> <p>OWASP-ASVS-1.35</p> <p>OWASP-ASVS-1.36</p> <p>OWASP-ASVS-1.37</p> <p>OWASP-ASVS-1.38</p> <p>OWASP-ASVS-1.39</p> <p>OWASP-ASVS-1.40</p> <p>OWASP-ASVS-1.41</p> <p>OWASP-ASVS-1.42</p> <p>OWASP-ASVS-1.43</p> <p>OWASP-ASVS-1.44</p> <p>OWASP-ASVS-1.45</p> <p>OWASP-ASVS-1.46</p> <p>OWASP-ASVS-1.47</p> <p>OWASP-ASVS-1.48</p> <p>OWASP-ASVS-1.49</p> <p>OWASP-ASVS-1.50</p> <p>OWASP-ASVS-1.51</p> <p>OWASP-ASVS-1.52</p> <p>OWASP-ASVS-1.53</p> <p>OWASP-ASVS-1.54</p> <p>OWASP-ASVS-1.55</p> <p>OWASP-ASVS-1.56</p> <p>OWASP-ASVS-1.57</p> <p>OWASP-ASVS-1.58</p> <p>OWASP-ASVS-1.59</p> <p>OWASP-ASVS-1.60</p> <p>OWASP-ASVS-1.61</p> <p>OWASP-ASVS-1.62</p> <p>OWASP-ASVS-1.63</p> <p>OWASP-ASVS-1.64</p> <p>OWASP-ASVS-1.65</p> <p>OWASP-ASVS-1.66</p> <p>OWASP-ASVS-1.67</p> <p>OWASP-ASVS-1.68</p> <p>OWASP-ASVS-1.69</p> <p>OWASP-ASVS-1.70</p> <p>OWASP-ASVS-1.71</p> <p>OWASP-ASVS-1.72</p> <p>OWASP-ASVS-1.73</p> <p>OWASP-ASVS-1.74</p> <p>OWASP-ASVS-1.75</p> <p>OWASP-ASVS-1.76</p> <p>OWASP-ASVS-1.77</p> <p>OWASP-ASVS-1.78</p> <p>OWASP-ASVS-1.79</p> <p>OWASP-ASVS-1.80</p> <p>OWASP-ASVS-1.81</p> <p>OWASP-ASVS-1.82</p> <p>OWASP-ASVS-1.83</p> <p>OWASP-ASVS-1.84</p> <p>OWASP-ASVS-1.85</p> <p>OWASP-ASVS-1.86</p> <p>OWASP-ASVS-1.87</p> <p>OWASP-ASVS-1.88</p> <p>OWASP-ASVS-1.89</p> <p>OWASP-ASVS-1.90</p> <p>OWASP-ASVS-1.91</p> <p>OWASP-ASVS-1.92</p> <p>OWASP-ASVS-1.93</p> <p>OWASP-ASVS-1.94</p> <p>OWASP-ASVS-1.95</p> <p>OWASP-ASVS-1.96</p> <p>OWASP-ASVS-1.97</p> <p>OWASP-ASVS-1.98</p> <p>OWASP-ASVS-1.99</p> <p>OWASP-ASVS-1.100</p> <p>OWASP-ASVS-1.101</p> <p>OWASP-ASVS-1.102</p> <p>OWASP-ASVS-1.103</p> <p>OWASP-ASVS-1.104</p> <p>OWASP-ASVS-1.105</p> <p>OWASP-ASVS-1.106</p> <p>OWASP-ASVS-1.107</p> <p>OWASP-ASVS-1.108</p> <p>OWASP-ASVS-1.109</p> <p>OWASP-ASVS-1.110</p> <p>OWASP-ASVS-1.111</p> <p>OWASP-ASVS-1.112</p> <p>OWASP-ASVS-1.113</p> <p>OWASP-ASVS-1.114</p> <p>OWASP-ASVS-1.115</p> <p>OWASP-ASVS-1.116</p> <p>OWASP-ASVS-1.117</p> <p>OWASP-ASVS-1.118</p> <p>OWASP-ASVS-1.119</p> <p>OWASP-ASVS-1.120</p> <p>OWASP-ASVS-1.121</p> <p>OWASP-ASVS-1.122</p> <p>OWASP-ASVS-1.123</p> <p>OWASP-ASVS-1.124</p> <p>OWASP-ASVS-1.125</p> <p>OWASP-ASVS-1.126</p> <p>OWASP-ASVS-1.127</p> <p>OWASP-ASVS-1.128</p> <p>OWASP-ASVS-1.129</p> <p>OWASP-ASVS-1.130</p> <p>OWASP-ASVS-1.131</p> <p>OWASP-ASVS-1.132</p> <p>OWASP-ASVS-1.133</p> <p>OWASP-ASVS-1.134</p> <p>OWASP-ASVS-1.135</p> <p>OWASP-ASVS-1.136</p> <p>OWASP-ASVS-1.137</p> <p>OWASP-ASVS-1.138</p> <p>OWASP-ASVS-1.139</p> <p>OWASP-ASVS-1.140</p> <p>OWASP-ASVS-1.141</p> <p>OWASP-ASVS-1.142</p> <p>OWASP-ASVS-1.143</p> <p>OWASP-ASVS-1.144</p> <p>OWASP-ASVS-1.145</p> <p>OWASP-ASVS-1.146</p> <p>OWASP-ASVS-1.147</p> <p>OWASP-ASVS-1.148</p> <p>OWASP-ASVS-1.149</p> <p>OWASP-ASVS-1.150</p> <p>OWASP-ASVS-1.151</p> <p>OWASP-ASVS-1.152</p> <p>OWASP-ASVS-1.153</p> <p>OWASP-ASVS-1.154</p> <p>OWASP-ASVS-1.155</p> <p>OWASP-ASVS-1.156</p> <p>OWASP-ASVS-1.157</p> <p>OWASP-ASVS-1.158</p> <p>OWASP-ASVS-1.159</p> <p>OWASP-ASVS-1.160</p> <p>OWASP-ASVS-1.161</p> <p>OWASP-ASVS-1.162</p> <p>OWASP-ASVS-1.163</p> <p>OWASP-ASVS-1.164</p> <p>OWASP-ASVS-1.165</p> <p>OWASP-ASVS-1.166</p> <p>OWASP-ASVS-1.167</p> <p>OWASP-ASVS-1.168</p> <p>OWASP-ASVS-1.169</p> <p>OWASP-ASVS-1.170</p> <p>OWASP-ASVS-1.171</p> <p>OWASP-ASVS-1.172</p> <p>OWASP-ASVS-1.173</p> <p>OWASP-ASVS-1.174</p> <p>OWASP-ASVS-1.175</p> <p>OWASP-ASVS-1.176</p> <p>OWASP-ASVS-1.177</p> <p>OWASP-ASVS-1.178</p> <p>OWASP-ASVS-1.179</p> <p>OWASP-ASVS-1.180</p> <p>OWASP-ASVS-1.181</p> <p>OWASP-ASVS-1.182</p> <p>OWASP-ASVS-1.183</p> <p>OWASP-ASVS-1.184</p> <p>OWASP-ASVS-1.185</p> <p>OWASP-ASVS-1.186</p> <p>OWASP-ASVS-1.187</p> <p>OWASP-ASVS-1.188</p> <p>OWASP-ASVS-1.189</p> <p>OWASP-ASVS-1.190</p> <p>OWASP-ASVS-1.191</p> <p>OWASP-ASVS-1.192</p> <p>OWASP-ASVS-1.193</p> <p>OWASP-ASVS-1.194</p> <p>OWASP-ASVS-1.195</p> <p>OWASP-ASVS-1.196</p> <p>OWASP-ASVS-1.197</p> <p>OWASP-ASVS-1.198</p> <p>OWASP-ASVS-1.199</p> <p>OWASP-ASVS-1.200</p> <p>OWASP-ASVS-1.201</p> <p>OWASP-ASVS-1.202</p> <p>OWASP-ASVS-1.203</p> <p>OWASP-ASVS-1.204</p> <p>OWASP-ASVS-1.205</p> <p>OWASP-ASVS-1.206</p> <p>OWASP-ASVS-1.207</p> <p>OWASP-ASVS-1.208</p> <p>OWASP-ASVS-1.209</p> <p>OWASP-ASVS-1.210</p> <p>OWASP-ASVS-1.211</p> <p>OWASP-ASVS-1.212</p> <p>OWASP-ASVS-1.213</p> <p>OWASP-ASVS-1.214</p> <p>OWASP-ASVS-1.215</p> <p>OWASP-ASVS-1.216</p> <p>OWASP-ASVS-1.217</p> <p>OWASP-ASVS-1.218</p> <p>OWASP-ASVS-1.219</p> <p>OWASP-ASVS-1.220</p> <p>OWASP-ASVS-1.221</p> <p>OWASP-ASVS-1.222</p> <p>OWASP-ASVS-1.223</p> <p>OWASP-ASVS-1.224</p> <p>OWASP-ASVS-1.225</p> <p>OWASP-ASVS-1.226</p> <p>OWASP-ASVS-1.227</p> <p>OWASP-ASVS-1.228</p> <p>OWASP-ASVS-1.229</p> <p>OWASP-ASVS-1.230</p> <p>OWASP-ASVS-1.231</p> <p>OWASP-ASVS-1.232</p> <p>OWASP-ASVS-1.233</p> <p>OWASP-ASVS-1.234</p> <p>OWASP-ASVS-1.235</p> <p>OWASP-ASVS-1.236</p> <p>OWASP-ASVS-1.237</p> <p>OWASP-ASVS-1.238</p> <p>OWASP-ASVS-1.239</p> <p>OWASP-ASVS-1.240</p> <p>OWASP-ASVS-1.241</p> <p>OWASP-ASVS-1.242</p> <p>OWASP-ASVS-1.243</p> <p>OWASP-ASVS-1.244</p> <p>OWASP-ASVS-1.245</p> <p>OWASP-ASVS-1.246</p> <p>OWASP-ASVS-1.247</p> <p>OWASP-ASVS-1.248</p> <p>OWASP-ASVS-1.249</p> <p>OWASP-ASVS-1.250</p> <p>OWASP-ASVS-1.251</p> <p>OWASP-ASVS-1.252</p> <p>OWASP-ASVS-1.253</p> <p>OWASP-ASVS-1.254</p> <p>OWASP-ASVS-1.255</p> <p>OWASP-ASVS-1.256</p> <p>OWASP-ASVS-1.257</p> <p>OWASP-ASVS-1.258</p> <p>OWASP-ASVS-1.259</p> <p>OWASP-ASVS-1.260</p> <p>OWASP-ASVS-1.261</p> <p>OWASP-ASVS-1.262</p> <p>OWASP-ASVS-1.263</p> <p>OWASP-ASVS-1.264</p> <p>OWASP-ASVS-1.265</p> <p>OWASP-ASVS-1.266</p> <p>OWASP-ASVS-1.267</p> <p>OWASP-ASVS-1.268</p> <p>OWASP-ASVS-1.269</p> <p>OWASP-ASVS-1.270</p> <p>OWASP-ASVS-1.271</p> <p>OWASP-ASVS-1.272</p> <p>OWASP-ASVS-1.273</p> <p>OWASP-ASVS-1.274</p> <p>OWASP-ASVS-1.275</p> <p>OWASP-ASVS-1.276</p> <p>OWASP-ASVS-1.277</p> <p>OWASP-ASVS-1.278</p> <p>OWASP-ASVS-1.279</p> <p>OWASP-ASVS-1.280</p> <p>OWASP-ASVS-1.281</p> <p>OWASP-ASVS-1.282</p> <p>OWASP-ASVS-1.283</p> <p>OWASP-ASVS-1.284</p> <p>OWASP-ASVS-1.285</p> <p>OWASP-ASVS-1.286</p> <p>OWASP-ASVS-1.287</p> <p>OWASP-ASVS-1.288</p> <p>OWASP-ASVS-1.289</p> <p>OWASP-ASVS-1.290</p> <p>OWASP-ASVS-1.291</p> <p>OWASP-ASVS-1.292</p> <p>OWASP-ASVS-1.293</p> <p>OWASP-ASVS-1.294</p> <p>OWASP-ASVS-1.295</p> <p>OWASP-ASVS-1.296</p> <p>OWASP-ASVS-1.297</p> <p>OWASP-ASVS-1.298</p> <p>OWASP-ASVS-1.299</p> <p>OWASP-ASVS-1.300</p> <p>OWASP-ASVS-1.301</p> <p>OWASP-ASVS-1.302</p> <p>OWASP-ASVS-1.303</p> <p>OWASP-ASVS-1.304</p> <p>OWASP-ASVS-1.305</p> <p>OWASP-ASVS-1.306</p> <p>OWASP-ASVS-1.307</p> <p>OWASP-ASVS-1.308</p> <p>OWASP-ASVS-1.309</p> <p>OWASP-ASVS-1.310</p> <p>OWASP-ASVS-1.311</p> <p>OWASP-ASVS-1.312</p> <p>OWASP-ASVS-1.313</p> <p>OWASP-ASVS-1.314</p> <p>OWASP-ASVS-1.315</p> <p>OWASP-ASVS-1.316</p> <p>OWASP-ASVS-1.317</p> <p>OWASP-ASVS-1.318</p> <p>OWASP-ASVS-1.319</p> <p>OWASP-ASVS-1.320</p> <p>OWASP-ASVS-1.321</p> <p>OWASP-ASVS-1.322</p> <p>OWASP-ASVS-1.323</p> <p>OWASP-ASVS-1.324</p> <p>OWASP-ASVS-1.325</p> <p>OWASP-ASVS-1.326</p> <p>OWASP-ASVS-1.327</p> <p>OWASP-ASVS-1.328</p> <p>OWASP-ASVS-1.329</p> <p>OWASP-ASVS-1.330</p> <p>OWASP-ASVS-1.331</p> <p>OWASP-ASVS-1.332</p> <p>OWASP-ASVS-1.333</p> <p>OWASP-ASVS-1.334</p> <p>OWASP-ASVS-1.335</p> <p>OWASP-ASVS-1.336</p> <p>OWASP-ASVS-1.337</p> <p>OWASP-ASVS-1.338</p> <p>OWASP-ASVS-1.339</p> <p>OWASP-ASVS-1.340</p> <p>OWASP-ASVS-1.341</p> <p>OWASP-ASVS-1.342</p> <p>OWASP-ASVS-1.343</p> <p>OWASP-ASVS-1.344</p> <p>OWASP-ASVS-1.345</p> <p>OWASP-ASVS-1.346</p> <p>OWASP-ASVS-1.347</p> <p>OWASP-ASVS-1.348</p> <p>OWASP-ASVS-1.349</p> <p>OWASP-ASVS-1.350</p> <p>OWASP-ASVS-1.351</p> <p>OWASP-ASVS-1.352</p> <p>OWASP-ASVS-1.353</p> <p>OWASP-ASVS-1.354</p> <p>OWASP-ASVS-1.355</p> <p>OWASP-ASVS-1.356</p> <p>OWASP-ASVS-1.357</p> <p>OWASP-ASVS-1.358</p> <p>OWASP-ASVS-1.359</p> <p>OWASP-ASVS-1.360</p> <p>OWASP-ASVS-1.361</p> <p>OWASP-ASVS-1.362</p> <p>OWASP-ASVS-1.363</p> <p>OWASP-ASVS-1.364</p> <p>OWASP-ASVS-1.365</p> <p>OWASP-ASVS-1.366</p> <p>OWASP-ASVS-1.367</p> <p>OWASP-ASVS-1.368</p> <p>OWASP-ASVS-1.369</p> <p>OWASP-ASVS-1.370</p> <p>OWASP-ASVS-1.371</p> <p>OWASP-ASVS-1.372</p> <p>OWASP-ASVS-1.373</p> <p>OWASP-ASVS-1.374</p> <p>OWASP-ASVS-1.375</p> <p>OWASP-ASVS-1.376</p> <p>OWASP-ASVS-1.377</p> <p>OWASP-ASVS-1.378</p> <p>OWASP-ASVS-1.379</p> <p>OWASP-ASVS-1.380</p> <p>OWASP-ASVS-1.381</p> <p>OWASP-ASVS-1.382</p> <p>OWASP-ASVS-1.383</p> <p>OWASP-ASVS-1.384</p> <p>OWASP-ASVS-1.385</p> <p>OWASP-ASVS-1.386</p> <p>OWASP-ASVS-1.387</p> <p>OWASP-ASVS-1.388</p> <p>OWASP-ASVS-1.389</p> <p>OWASP-ASVS-1.390</p> <p>OWASP-ASVS-1.391</p> <p>OWASP-ASVS-1.392</p> <p>OWASP-ASVS-1.393</p> <p>OWASP-ASVS-1.394</p> <p>OWASP-ASVS-1.395</p> <p>OWASP-ASVS-1.396</p> <p>OWASP-ASVS-1.397</p> <p>OWASP-ASVS-1.398</p> <p>OWASP-ASVS-1.399</p> <p>OWASP-ASVS-1.400</p> <p>OWASP-ASVS-1.401</p> <p>OWASP-ASVS-1.402</p> <p>OWASP-ASVS-1.403</p> <p>OWASP-ASVS-1.404</p> <p>OWASP-ASVS-1.405</p> <p>OWASP-ASVS-1.406</p> <p>OWASP-ASVS-1.407</p> <p>OWASP-ASVS-1.408</p> <p>OWASP-ASVS-1.409</p> <p>OWASP-ASVS-1.410</p> <p>OWASP-ASVS-1.411</p> <p>OWASP-ASVS-1.412</p> <p>OWASP-ASVS-1.413</p> <p>OWASP-ASVS-1.414</p> <p>OWASP-ASVS-1.415</p> <p>OWASP-ASVS-1.416</p> <p>OWASP-ASVS-1.417</p> <p>OWASP-ASVS-1.418</p> <p>OWASP-ASVS-1.419</p> <p>OWASP-ASVS-1.420</p> <p>OWASP-ASVS-1.421</p> <p>OWASP-ASVS-1.422</p> <p>OWASP-ASVS-1.423</p> <p>OWASP-ASVS-1.424</p> <p>OWASP-ASVS-1.425</p> <p>OWASP-ASVS-1.426</p> <p>OWASP-ASVS-1.427</p> <p>OWASP-ASVS-1.428</p> <p>OWASP-ASVS-1.429</p> <p>OWASP-ASVS-1.430</p> <p>OWASP-ASVS-1.431</p> <p>OWASP-ASVS-1.432</p> <p>OWASP-ASVS-1.433</p> <p>OWASP-ASVS-1.434</p> <p>OWASP-ASVS-1.435</p> <p>OWASP-ASVS-1.436</p> <p>OWASP-ASVS-1.437</p> <p>OWASP-ASVS-1.438</p> <p>OWASP-ASVS-1.439</p> <p>OWASP-ASVS-1.440</p> <p>OWASP-ASVS-1.441</p> <p>OWASP-ASVS-1.442</p> <p>OWASP-ASVS-1.443</p> <p>OWASP-ASVS-1.444</p> <p>OWASP-ASVS-1.445</p> <p>OWASP-ASVS-1.446</p> <p>OWASP-ASVS-1.447</p> <p>OWASP-ASVS-1.448</p> <p>OWASP-ASVS-1.449</p> <p>OWASP-ASVS-1.450</p> <p>OWASP-ASVS-1.451</p> <p>OWASP-ASVS-1.452</p> <p>OWASP-ASVS-1.453</p> <p>OWASP-ASVS-1.454</p> <p>OWASP-ASVS-1.455</p> <p>OWASP-ASVS-1.456</p> <p>OWASP-ASVS-1.457</p> <p>OWASP-ASVS-1.458</p> <p>OWASP-ASVS-1.459</p> <p>OWASP-ASVS-1.460</p> <p>OWASP-ASVS-1.461</p> <p>OWASP-ASVS-1.462</p> <p>OWASP-ASVS-1.463</p> <p>OWASP-ASVS-1.464</p> <p>OWASP-ASVS-1.465</p> <p>OWASP-ASVS-1.466</p> <p>OWASP-ASVS-1.467</p> <p>OWASP-ASVS-1.468</p> <p>OWASP-ASVS-1.469</p> <p>OWASP-ASVS-1.470</p> <p>OWASP-ASVS-1.471</p> <p>OWASP-ASVS-1.472</p> <p>OWASP-ASVS-1.473</p> <p>OWASP-ASVS-1.474</p> <p>OWASP-ASVS-1.475</p> <p>OWASP-ASVS-1.476</p> <p>OWASP-ASVS-1.477</p> <p>OWASP-ASVS-1.478</p> <p>OWASP-ASVS-1.479</p> <p>OWASP-ASVS-1.480</p> <p>OWASP-ASVS-1.481</p> <p>OWASP-ASVS-1.482</p> <p>OWASP-ASVS-1.483</p> <p>OWASP-ASVS-1.484</p> <p>OWASP-ASVS-1.485</p> <p>OWASP-ASVS-1.486</p> <p>OWASP-ASVS-1.487</p> <p>OWASP-ASVS-1.488</p> <p>OWASP-ASVS-1.489</p> <p>OWASP-ASVS-1.490</p> <p>OWASP-ASVS-1.491</p> <p>OWASP-ASVS-1.492</p> <p>OWASP-ASVS-1.493</p> <p>OWASP-ASVS-1.494</p> <p>OWASP-ASVS-1.495</p> <p>OWASP-ASVS-1.496</p> <p>OWASP-ASVS-1.497</p> <p>OWASP-ASVS-1.498</p> <p>OWASP-ASVS-1.499</p> <p>OWASP-ASVS-1.500</p> <p>OWASP-ASVS-1.501</p> <p>OWASP-ASVS-1.502</p> <p>OWASP-ASVS-1.503</p> <p>OWASP-ASVS-1.504</p> <p>OWASP-ASVS-1.505</p> <p>OWASP-ASVS-1.506</p> <p>OWASP-ASVS-1.507</p> <p>OWASP-ASVS-1.508</p> <p>OWASP-ASVS-1.509</p> <p>OWASP-ASVS-1.510</p> <p>OWASP-ASVS-1.511</p> <p>OWASP-ASVS-1.512</p> <p>OWASP-ASVS-1.513</p> <p>OWASP-ASVS-1.514</p> <p>OWASP-ASVS-1.515</p> <p>OWASP-ASVS-1.516</p> <p>OWASP-ASVS-1.517</p> <p>OWASP-ASVS-1.518</p> <p>OWASP-ASVS-1.519</p> <p>OWASP-ASVS-1.520</p> <p>OWASP-ASVS-1.521</p> <p>OWASP-ASVS-1.522</p> <p>OWASP-ASVS-1.523</p> <p>OWASP-ASVS-1.524</p> <p>OWASP-ASVS-1.525</p> <p>OWASP-ASVS-1.526</p> <p>OWASP-ASVS-1.527</p> <p>OWASP-ASVS-1.528</p> <p>OWASP-ASVS-1.529</p> <p>OWASP-ASVS-1.530</p> <p>OWASP-ASVS-1.531</p> <p>OWASP-ASVS-1.532</p> <p>OWASP-ASVS-1.533</p> <p>OWASP-ASVS-1.534</p> <p>OWASP-ASVS-1.535</p> <p>OWASP-ASVS-1.536</p> <p>OWASP-ASVS-1.537</p> <p>OWASP-ASVS-1.538</p> <p>OWASP-ASVS-1.539</p> <p>OWASP-ASVS-1.540</p> <p>OWASP-ASVS-1.541</p> <p>OWASP-ASVS-1.542</p> <p>OWASP-ASVS-1.543</p> <p>OWASP-ASVS-1.544</p> <p>OWASP-ASVS-1.545</p> <p>OWASP-ASVS-1.546</p> <p>OWASP-ASVS-1.547</p> <p>OWASP-ASVS-1.548</p> <p>OWASP-ASVS-1.549</p> <p>OWASP-ASVS-1.550</p> <p>OWASP-ASVS-1.551</p> <p>OWASP-ASVS-1.552</p> <p>OWASP-ASVS-1.553</p> <p>OWASP-ASVS-1.554</p> <p>OWASP-ASVS-1.555</p> <p>OWASP-ASVS-1.556</p> <p>OWASP-ASVS-1.557</p> <p>OWASP-ASVS-1.558</p> <p>OWASP-ASVS-1.559</p> <p>OWASP-ASVS-1.560</p> <p>OWASP-ASVS-1.561</p> <p>OWASP-ASVS-1.562</p> <p>OWASP-ASVS-1.563</p> <p>OWASP-ASVS-1.564</p> <p>OWASP-ASVS-1.565</p> <p>OWASP-ASVS-1.566</p> <p>OWASP-ASVS-1.567</p> <p>OWASP-ASVS-1.568</p> <p>OWASP-ASVS-1.569</p> <p>OWASP-ASVS-1.570</p> <p>OWASP-ASVS-1.571</p> <p>OWASP-ASVS-1.572</p> <p>OWASP-ASVS-1.573</p> <p>OWASP-ASVS-1.574</p> <p>OWASP-ASVS-1.575</p> <p>OWASP-ASVS-1.576</p> <p>OWASP-ASVS-1.577</p> <p>OWASP-ASVS-1.578</p> <p>OWASP-ASVS-1.579</p> <p>OWASP-ASVS-1.580</p> <p>OWASP-ASVS-1.581</p> <p>OWASP-ASVS-1.582</p> <p>OWASP-ASVS-1.583</p> <p>OWASP-ASVS-1.584</p> <p>OWASP-ASVS-1.585</p> <p>OWASP-ASVS-1.586</p> <p>OWASP-ASVS-1.587</p> <p>OWASP-ASVS-1.588</p> <p>OWASP-ASVS-1.589</p> <p>OWASP-ASVS-1.590</p> <p>OWASP-ASVS-1.591</p> <p>OWASP-ASVS-1.592</p> <p></p>

SSDF (SP 800-218)

NIST - Secure Software Development Framework

v1.1 [REDACTED] (XXXXXXXXXX)

Section Title

PO.1.2 [REDACTED]

PO.5.1 [REDACTED] XX/XX

PO.5.2 [REDACTED]

PS.3.2 [REDACTED]

PW.1.2 [REDACTED]

Appendix A—The SSDF and Executive Order 14028

The President's Executive Order (EO) on "Improving the Nation's Cybersecurity (14028)" issued on May 12, 2021 [[EO14028](#)], charged multiple agencies – including NIST – with enhancing cybersecurity through a variety of initiatives related to the security and integrity of the software supply chain.

Section 4 of the EO directed NIST to solicit input from the private sector, academia, government agencies, and others and to identify existing or develop new standards, tools, best practices, and other guidelines to enhance software supply chain security. Table 2 maps the subsections from Section 4e of the EO to SSDF practices and tasks that can help address each subsection as part of a risk-based approach.

Table 2: SSDF Practices Corresponding to EO 14028 Subsections

EO 14028 Subsection	SSDF Practices and Tasks
4e(i)(A)	PO.5.1
4e(i)(B)	PO.5.1
4e(i)(C)	PO.5.1, PO.5.2
4e(i)(D)	PO.5.1
4e(i)(E)	PO.5.2
4e(i)(F)	PO.3.2, PO.3.3, PO.5.1, PO.5.2
4e(ii)	PO.3.2, PO.3.3, PO.5.1, PO.5.2
4e(iii)	PO.3.1, PO.3.2, PO.5.1, PO.5.2, PS.1.1, PS.2.1, PS.3.1, PW.4.1, PW.4.4
4e(iv)	PO.4.1, PO.4.2, PS.1.1, PW.2.1, PW.4.4, PW.5.1, PW.6.1, PW.6.2, PW.7.1, PW.7.2, PW.8.2, PW.9.1, PW.9.2, RV.1.1, RV.1.2, RV.2.1, RV.2.2, RV.3.3
4e(v)	PO.3.2, PO.3.3, PO.4.1, PO.4.2, PO.5.1, PO.5.2, PW.1.2, PW.2.1, PW.7.2, PW.8.2, RV.2.2
4e(vi)	PO.1.2, PO.3.2, PO.5.1, PO.5.2, PS.3.1, PS.3.2, PW.4.1, PW.4.4, RV.1.1, RV.1.2
4e(vii)	PS.3.2
4e(viii)	RV.1.1, RV.1.2, RV.1.3, RV.2.1, RV.2.2, RV.3.3
4e(ix)	All practices and tasks consistent with a risk-based approach
4e(x)	PS.2.1, PS.3.1, PS.3.2, PW.4.1, PW.4.4

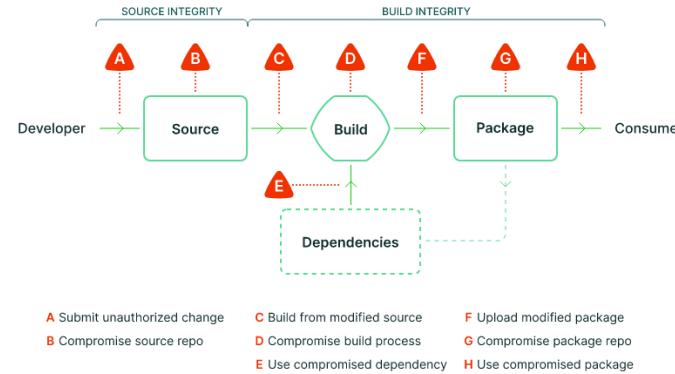
SLSA

Google - Supply chain Levels for Software Artifacts

三級供應鏈級別(Integrity)End-to-end

3級Trust Boundaries

Boundary Name	Requirements
Source Integrity	4
Build Integrity	8
Dependencies	5
(Common)	3



Summary table

Requirement	SLSA 1	SLSA 2	SLSA 3	SLSA 4
Source - Version controlled	✓	✓	✓	
Source - Verified history		✓	✓	
Source - Retained indefinitely			18 mo.	✓
Source - Two-person reviewed				✓
Build - Scripted build	✓	✓	✓	✓
Build - Build service	✓	✓	✓	
Build - Build as code		✓	✓	
Build - Ephemeral environment		✓	✓	

CNCF - Software Supply Chain Best Practices



- **Securing the Source Code**
- **Securing the Materials**
- **Securing the Build Pipelines**
- **Securing the Artefacts**
- **Securing Deployments**

Securing the Source Code

The foundational construct of any software supply chain is the source code. The initial step in securing a supply chain is establishing and ensuring the integrity of the source code. "Integrity" in this context means that the source code and tags found in the repository have not changed or altered from the code created by the developer. This includes potential malicious changes introduced by a local compromise on the developers machine. To maintain integrity, organizations must take steps to verify the source of the code added to their first party products and libraries.

It is fundamental to the supply chain that the development activity employs software development best practices. Agile methodologies of "continuous improvement" have been embraced in the industry and enabled through CI/CD pipelines and automated testing. These pipelines must be properly configured to access source code on-demand in order to build, deploy, and release artefacts at the cadence the organization needs.

Identity and Access management (IAM) is the biggest attack vector, regardless of platform or vendor, and it is critical to carefully manage IAM policies to provide both developers and agents secure access to source code. Pipeline agents and human developers must have their access and privileges calibrated to their roles within the organization and be given secure means to authenticate to those roles.

Verification:

Require signed commits

Assurance categories: Moderate to high and risk categories: Moderate to high

Signing source code¹⁸ (commits and tags) ensures integrity and non-repudiation of source code by enabling out-of-band verification of the code. An attack on the source code management

 Microsoft contributes S2C2F to OpenSSF to improve supply chain security

CNCF

CNCF - Software Supply Chain Best Practices

49 Software Supply Chain Best Practices

Comparing SLSA to the CNCF Software Supply Chain Best Practices Recommendations

Target	Practices
Source Code	Commitizen, CI/CD, Tests, AST, Code Owner
Materials	Checksum, SBOM
Pipelines	CI/CD, SPIFEE
Artefacts	OCI Registry, ocicrypto
Deployments	TUF (The Update Framework)

S2C2F

OSSF - Secure Supply Chain Consumption Framework

OSS Consumer → XXXXXXXX → OSS →
XXXXXX → 8 XXXXXXXX → 4 → XXXXXXXX

- **Ingest It:** OSS → XXXXXXXX
- **Scan It:** XXXXXXXX
- **Inventory It:** XXXXXXXX
- **Update It:** OSS → XXXXXXXX
- **Enforce It:** OSS → XXXXXXXX
- **Rebuild It:** XXXXXXXX
- **Fix It:** XXXXXXXX



Level 1	Level 2	Level 3	Level 4
<p> Minimum OSS Governance Program</p> <ul style="list-style-type: none">• Use package managers• Local copy of artifact• Scan with known vulns• Scan for software licenses• Inventory OSS• Manual OSS updates	<p> Secure Consumption and Improved MTTR</p> <ul style="list-style-type: none">• Scan for end life• Have an incident response plan• Auto OSS updates• Alert on vulns at PR time• Audit that consumption is through the approved ingestion method• Validate integrity of OSS• Secure package source file configuration	<p> Malware Defense and Zero-Day Detection</p> <ul style="list-style-type: none">• Deny list capability• Clone OSS source• Scan for malware• Proactive security reviews• Enforce OSS provenance• Enforce consumption from curated feed	<p> Advanced Threat Defense</p> <ul style="list-style-type: none">• Validate the SBOMs of OSS consumed• Rebuild OSS on trusted infrastructure• Digitally sign rebuilt OSS• Generate SBOM for rebuilt OSS• Digitally sign protected SBOMs• Implement fixes

XX: Microsoft contributes S2C2F to OpenSSF to improve supply chain security

Summary

- 容器化最佳实践
 - **SSDF**: 容器化最佳实践
 - **SLSA**: 容器化最佳实践
 - **CNCF**: 容器化最佳实践
 - **S2C2F**: 容器化最佳实践
- 容器化最佳实践**SLSA**和**CNCF**都提出了自己的最佳实践
- 容器化最佳实践**SSDF**尚未提出