

セキュア開発成熟度モデル

(BSIMM)

ソフトウェア・セキュリティに 科学的アプローチを適用

ソフトウェア環境が刻々と 変化中、SSI にも 変化が求められます。

- 開発スピードの上昇
- 自動化によって駆動されるアプリケーション・ライフサイクル管理プロセス
- エンジニアリング主導のソフトウェア・セキュリティ対策
- コンテナ、マイクロサービス、仮想環境へのシフト
- マルチクラウド・デプロイメント戦略の競合
- 「Everything as Code」(あらゆるものをコード化)
- 新しいアプリケーション・アーキテクチャ

概要

ソフトウェア・セキュリティの変化がアジャイル、CI/CD、DevOpsといったエンジニアリング・チームの新しい取り組みから生まれているにせよ、中央のソフトウェア・セキュリティ・グループ(SSG)からトップダウン式に発生しているにせよ、リスク管理を成功させるにはソフトウェア・セキュリティ・イニシアティブ(SSI)の成熟度を高めることが鍵となります。しかし自社のSSIの現状を可視化するデータがなければ、改善への戦略を立てることもSSIの改革に優先順位を付けることもできません。

こうした問題を解決するのが、セキュア開発成熟度モデル(BSIMM)です。BSIMMはこれまで10年以上にわたるSSIの調査結果を独自の業界モデルとしてまとめたもので、SSIを測定する基準として利用されています。BSIMMはさまざまな組織で実施されているアクティビティを定量化し、これら組織にどのような共通点と相違点があるのかを記述します。BSIMMスコアカードは、SSIの現状を診断し、目標とのギャップを見つけ、今後の改革の優先順位を付け、リソースをどの部分にどれだけ投入すれば即座の改善が見込めるかを判断する上での材料となります。

BSIMM を使ってできること

1. 現実のデータに即してソフトウェア・セキュリティ・イニシアティブ(SSI)を開始する。

まだSSIを実施していない場合、早急に開始する必要があります。SSIを開始したら、BSIMMを利用することで、企業の業種や規模、デプロイメント・モデル、コンプライアンス要件を問わず、成功を収めているSSIが共通して実施している中心的アクティビティを知ることができます。

2. 同業他社とSSIを比較する。

BSIMMは、自社のSSIを測定してさまざまな業界の企業との間で結果を比較できる現在唯一の評価ツールです。目標が明確になれば、現在地から目標地点までの距離を容易に把握できます。

3. 繰り返し測定してSSIの成長を追跡する。

BSIMMは、自社のSSIの広がりや深さを繰り返し測定できる唯一にして最高の方法です。SSIが確立されれば、BSIMMを利用することでSSIの改善を毎年継続的に測定できます。また、自社のセキュリティの取り組みがどれだけ効果を上げているかを経営陣や取締役会に示すための具体的な詳細情報もBSIMMによって得られます。

4. 成熟度の高い SSI から得られた教訓を自社の SSI 改善に活かす。

BSIMM には成熟度の高い組織が現在実施している実証済みアクティビティが掲載されており、SSI を構築および改善していく上で何が効果的なのかを知ることができます。自社の SSI の診断結果、BSIMM のアクティビティ、自社の目標に基づいて、真の改善に向けた戦略と優先順位を設定できます。

カスタマイズしたレポートをご提供

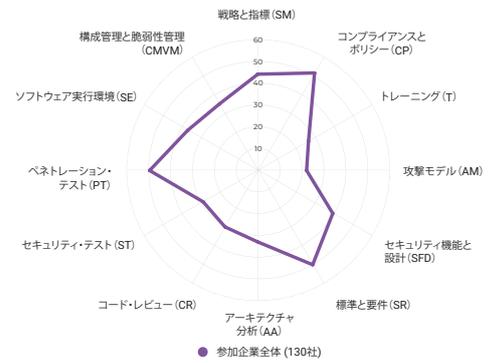
BSIMM の診断を受けると、自社の SSI の優れた部分と改善の余地がある部分を指摘した詳細なレポートを受け取ることができます。また、経営幹部や取締役会への報告資料として、以下のものも利用できます。

カスタマイズしたレーダーチャート。 他社と比較して進んでいる部分、遅れているかもしれない部分を一目で把握できます。BSIMM を測定ツールとして使用する段階から SSI 立案ツールとして使用する段階へ移行すると、これらの結果を客観的なフィードバックとして利用して進捗状況を追跡できます。

BSIMM スコアカード。 他社の SSI と比較して、自社の SSI の現状を捉えることができます。これを利用して、自社の SSI 全体の経年変化や、個々の事業部門、ビジネス・パートナー、および取引先ベンダーの状況を見ることができます。

価値を引き出す

Lenovo のインフラストラクチャー・ソリューション・グループ、プロダクト・セキュリティ・オフィスのエグゼクティブ・ディレクターである Bill Jaeger は、「2015 年に BSIMM コミュニティに参加し、毎年更新される観察結果から得られる洞察を活用して、自社のセキュリティ・プログラムの計画や測定を支援し、また顧客にとって最も重要である実践分野の把握に役立つ大きな価値を発見しました」と語っています。



カバレッジ		インテリジェンス		SSDL タッチポイント		デフォイメント		
スコア	割合	スコア	割合	スコア	割合	スコア	割合	
EMM1.1	98	75.4%	EMM1.2	85	41.5%	EMM1.3	112	66.5%
EMM1.2	82	63.1%	EMM1.3	42	32.2%	EMM1.4	55	40.8%
EMM1.3	117	90.8%	EMM1.4	76	58.5%	EMM1.5	69	53.1%
EMM2.1	79	56.2%	EMM2.2	16	12.3%	EMM2.3	21	23.9%
EMM2.2	62	48.5%	EMM2.3	11	8.9%	EMM2.4	32	24.6%
EMM2.3	69	53.1%	EMM2.4	16	12.3%	EMM2.5	38	29.2%
EMM2.4	71	54.6%	EMM2.5	16	12.3%	EMM3.1	20	15.4%
EMM3.1	64	49.2%	EMM3.2	14	10.8%	EMM3.3	4	3.1%
EMM3.2	27	20.8%	EMM3.3	9	6.9%	EMM3.4	15	11.5%
EMM3.3	18	13.9%	EMM3.4	5	3.9%			
EMM3.4	26	20.0%	EMM3.5	11	8.5%			
EMM3.5	5	3.9%						
EMM3.6	0	0.0%						

コンプライアンスとポリシー		セキュリティ機能と設計		コード・レビュー		ソフトウェア実行環境		
スコア	割合	スコア	割合	スコア	割合	スコア	割合	
EP1.1	103	77.7%	EP1.2	104	80.0%	EP1.3	83	63.9%
EP1.2	116	86.8%	EP1.3	92	69.2%	EP1.4	107	82.2%
EP1.3	98	75.4%	EP1.4	39	30.0%	EP1.5	62	47.7%
EP2.1	58	44.6%	EP2.2	64	49.2%	EP2.3	54	41.5%
EP2.2	59	45.4%	EP2.3	17	13.1%	EP2.4	28	21.5%
EP2.3	73	56.2%	EP2.4	18	13.9%	EP2.5	20	15.4%
EP2.4	62	47.7%	EP2.5	7	5.4%	EP3.1	34	26.2%
EP3.1	62	47.7%			EP3.2	14	10.8%	
EP3.2	30	23.1%			EP3.3	8	6.2%	
EP3.3	28	21.5%			EP3.4	2	1.5%	
EP3.4	11	8.5%			EP3.5	3	2.3%	

トレーニング		標準と要件		セキュリティテスト		構成管理と脆弱性管理		
スコア	割合	スコア	割合	スコア	割合	スコア	割合	
TT1.1	71	54.6%	TT1.2	96	73.9%	TT1.3	106	81.5%
TT1.2	58	44.6%	TT1.3	103	77.7%	TT1.4	87	66.6%
TT1.3	53	40.8%	TT1.4	80	61.5%	TT1.5	56	43.1%
TT1.4	38	29.2%	TT1.5	62	47.7%	TT2.1	25	19.2%
TT2.1	28	21.5%	TT2.2	62	47.7%	TT2.3	31	23.9%
TT2.2	33	25.4%	TT2.3	63	48.5%	TT2.4	21	16.2%
TT2.3	28	21.5%	TT2.4	53	40.8%	TT2.5	12	9.2%
TT2.4	27	20.8%	TT2.5	19	14.6%	TT3.1	4	3.1%
TT3.1	9	6.9%	TT3.2	17	13.1%	TT3.3	4	3.1%
TT3.2	16	12.3%	TT3.3	19	14.6%	TT3.4	3	2.3%
TT3.3	22	16.9%			TT3.5	3	2.3%	
TT3.4	7	5.4%			EMM4.1	114	87.2%	
					EMM4.2	100	76.9%	
					EMM4.3	95	73.1%	
					EMM4.4	98	75.4%	
					EMM4.5	62	47.7%	
					EMM4.6	11	8.5%	
					EMM4.7	19	14.6%	
					EMM4.8	26	20.0%	
					EMM4.9	13	10.0%	
					EMM4.10	20	15.4%	
					EMM4.11	9	6.9%	

ブラック・ダックについて

ブラック・ダックは、業界で最も包括的かつ強力な信頼できるアプリケーション・セキュリティ・ソリューション・ポートフォリオを提供します。ブラック・ダックには、世界中の組織がソフトウェアを迅速に保護し、開発環境にセキュリティを効率的に統合し、新しいテクノロジーで安全に革新できるよう支援してきた比類なき実績があります。ソフトウェア・セキュリティのリーダー、専門家、イノベーターとして認められているブラック・ダックは、ソフトウェアの信頼を築くために必要な要素をすべて備えています。詳しくは www.blackduck.com/jp をご覧ください。

ブラック・ダック・ソフトウェア合同会社

www.blackduck.com/jp

©2024 Black Duck Software, Inc. All rights reserved. Black Duck® は Black Duck Software, Inc. の米国およびその他の国における登録商標です。その他の会社名および商品名は各社の商標または登録商標です。2024年9月