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する中、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 の広がりと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。

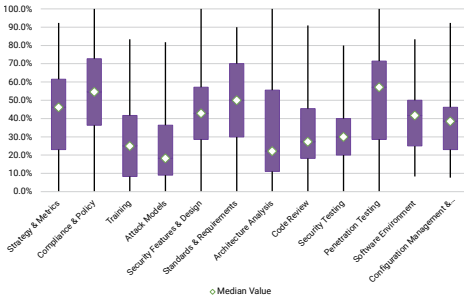
BSIMM には成熟度の高い組織が現在実施している実証済みアクティビティが掲載されており、SSI を構築および改善していく上で何が効果的なのかを知ることができます。自社の SSI の診断結果、BSIMM のアクティビティ、自社の目標に基づいて、真の改善に向けた戦略と優先順位を設定できます。

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。

カスタマイズした箱ひげ図。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。



GOVERNANCE			INTELLIGENCE			SSDL TOUCHPOINTS			DEPLOYMENT		
ACTIVITY	BSIMM9 FIRMS (OUT OF 121)	BSIMM9 FIRMS (PERCENTAGE)	ACTIVITY	BSIMM9 FIRMS (OUT OF 121)	BSIMM9 FIRMS (PERCENTAGE)	ACTIVITY	BSIMM9 FIRMS (OUT OF 121)	BSIMM9 FIRMS (PERCENTAGE)	ACTIVITY	BSIMM9 FIRMS (OUT OF 121)	BSIMM9 FIRMS (PERCENTAGE)
STRATEGY & METRICS			**ATTACK MODELS**			**ARCHITECTURE ANALYSIS**			**PENETRATION TESTING**		
[SM1.1]	90	74.38%	[AM1.2]	64	52.89%	[AA1.1]	99	81.82%	[PT1.1]	104	85.95%
[SM1.3]	72	59.50%	[AM1.3]	49	40.50%	[AA1.2]	56	46.28%	[PT1.2]	95	78.51%
[SM1.4]	109	90.08%	[AM1.5]	77	63.64%	[AA1.4]	55	45.45%	[PT1.3]	76	62.81%
[SM1.7]	72	59.50%	[AM2.1]	18	14.88%	[AA2.1]	37	30.58%	[PT2.2]	39	32.23%
[SM2.1]	65	53.72%	[AM2.6]	12	9.92%	[AA2.2]	38	31.40%	[PT2.3]	51	42.15%
[SM2.3]	67	55.37%	[AM2.7]	16	13.22%	[AA2.4]	40	33.06%	[PT3.1]	26	21.49%
[SM2.6]	69	57.02%	[AM2.8]	24	19.83%	[AA3.1]	20	16.53%	[PT3.2]	21	17.36%
[SM2.7]	52	42.98%	[AM2.9]	18	14.88%	[AA3.2]	8	6.61%			
[SM3.1]	30	24.79%	[AM3.2]	8	6.61%	[AA3.3]	18	14.88%			
[SM3.2]	23	19.01%	[AM3.4]	11	9.09%						
[SM3.3]	32	26.45%	[AM3.5]	10	8.26%						
[SM3.4]	11	9.09%									
[SM3.5]	1	0.83%									
COMPLIANCE & POLICY			**SECURITY FEATURES & DESIGN**			**CODE REVIEW**			**SOFTWARE ENVIRONMENT**		
[CP1.1]	98	80.99%	[SFD1.1]	93	76.86%	[CR1.2]	80	66.12%	[SE1.1]	76	62.81%
[CP1.2]	105	86.78%	[SFD1.2]	83	68.60%	[CR1.4]	106	87.60%	[SE1.2]	102	84.30%
[CP1.3]	94	77.69%	[SFD2.1]	42	34.71%	[CR1.5]	75	61.98%	[SE1.3]	87	71.90%
[CP2.1]	49	40.50%	[SFD2.2]	68	56.20%	[CR1.7]	51	42.15%	[SE1.4]	74	61.16%
[CP2.2]	58	47.93%	[SFD3.1]	18	14.88%	[CR2.6]	24	19.83%	[SE2.4]	51	42.15%
[CP2.3]	69	57.02%	[SFD3.2]	21	17.36%	[CR2.7]	19	15.70%	[SE2.5]	64	52.89%
[CP2.4]	60	49.59%	[SFD3.3]	12	9.92%	[CR2.8]	27	22.31%	[SE2.7]	42	34.71%
[CP2.5]	70	57.85%				[CR3.2]	16	13.22%	[SE3.2]	24	19.83%
[CP3.1]	36	29.75%				[CR3.3]	6	4.96%	[SE3.3]	17	14.05%
[CP3.2]	39	32.23%				[CR3.4]	3	2.48%	[SE3.6]	25	20.66%
[CP3.3]	13	10.74%				[CR3.5]	6	4.96%	[SE3.8]	3	2.48%
									[SE3.9]	3	2.48%
									[SE3.10]	0	0.00%
TRAINING			**STANDARDS & REQUIREMENTS**			**SECURITY TESTING**			**CONFIG. MGMT. & VULN. MGMT.**		
[T1.1]	62	51.24%	[SR1.1]	84	69.42%	[ST1.1]	102	84.30%	[CMVM1.1]	111	91.74%
[T1.7]	61	50.41%	[SR1.2]	96	79.34%	[ST1.3]	79	65.29%	[CMVM1.2]	85	70.25%
[T1.8]	50	41.32%	[SR1.3]	86	71.07%	[ST1.4]	54	44.63%	[CMVM1.3]	89	73.55%
[T2.5]	41	33.88%	[SR1.5]	96	79.34%	[ST2.4]	20	16.53%	[CMVM1.4]	88	72.73%
[T2.8]	25	20.66%	[SR2.2]	70	57.85%	[ST2.5]	34	28.10%	[CMVM2.3]	46	38.02%
[T2.9]	31	25.62%	[SR2.5]	62	51.24%	[ST2.6]	24	19.83%	[CMVM2.4]	41	33.88%
[T2.10]	25	20.66%	[SR2.7]	55	45.45%	[ST3.3]	16	13.22%	[CMVM3.1]	13	10.74%
[T2.11]	29	23.97%	[SR3.2]	19	15.70%	[ST3.4]	5	4.13%	[CMVM3.2]	24	19.83%
[T2.12]	38	31.40%	[SR3.3]	17	14.05%	[ST3.5]	6	4.96%	[CMVM3.3]	22	18.18%
[T3.1]	8	6.61%	[SR3.4]	20	16.53%	[ST3.6]	8	6.61%	[CMVM3.4]	31	25.62%
[T3.2]	14	11.57%	[SR3.5]	0	0.00%				[CMVM3.5]	17	14.05%
[T3.6]	9	7.44%							[CMVM3.6]	4	3.31%
									[CMVM3.8]	1	0.83%

FIGURE 18. BSIMM15 SCORECARD. This scorecard shows how often we observed each of the BSIMM15 activities in the data pool of 121 firms.

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。

ブラック・ダックについて

ブラック・ダックは、True Scale Application Security によって、モダン・ソフトウェアの経営レベルのリスクに対応し、規制された、AI を活用した世界におけるソフトウェアの信頼性を保証します。ブラック・ダックのソリューションは、セキュリティ、規制、ライセンスに関するリスクを排除しつつ、組織のスピード、精度、コンプライアンスのトレードオフから解放します。クラウドでもオンプレミスでも、コードが実行されるあらゆる場所でミッション・クリティカルなソフトウェアを保護するには、ブラック・ダックこそが選択肢となるのです。ブラック・ダックを活用することで、セキュリティ・リーダーはよりスマートな意思決定を行い、自信を持ってビジネス・イノベーションを推進することができます。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