SYNOPSYS®

セキュリティ構築の成熟度モデル
(BSIMM)

ソフトウェアセキュリティに科学的アプローチを導入

BSIMM の成果として、ソフトウェアセキュリティ対策の現状評価、不足箇所の特定、変更の優先順位付け、速やかな改善を実現するためにリソースを配分すべき場所と方法の決定が可能になります。

BSIMM の成果

1. 実際のデータを使用してソフトウェア・セキュリティ・イニシアティブ（SSI）をスタートできる

ソフトウェアセキュリティ対策をまだ講じていない場合は、対策を立てる必要があります。対策に着手する前に、BSIMM を適用することで、成功を導く対策の中で必ず取り組む核となるアクティビティを特定できるようになります。これは業種を問いません。

2. 自社の SSI を同業他社と比較できる

BSIMM は、自社の SSI が同業他社と比較・評価するうえで現在利用できる判断基準としては非常に優れたものです。ある目標を念頭に置いて、要求水準に対してどのレベルにあるかをすばやく見極めることができます。

3. SSI の進捗を評価して管理できる

BSIMM は、SSI の有効性を評価するうえで、唯一繰り返し利用可能な最も優れた方法です。SSI を確立したら、BSIMM を利用して対前年比での継続的改善具合を評価できます。また、セキュリティの取り組みがどの程度効果を出しているかを経営陣や取締役に示すための具体的な詳細情報も得られます。

4. 成熟した対策から学んだ教訓を活かして自社の対策を展開する

BSIMM は、ソフトウェアセキュリティ対策の立案と展開に関する実際の「成功事例」のレポートです。BSIMM は、成熟した組織が現在実践している実績のあるアクティビティから構成されます。自社の評価結果、BSIMM のアクティビティおよび目標を用いて真の改善のための戦略と優先度を設定できます。

5. 共通の問題に直面している専門家と交流できる

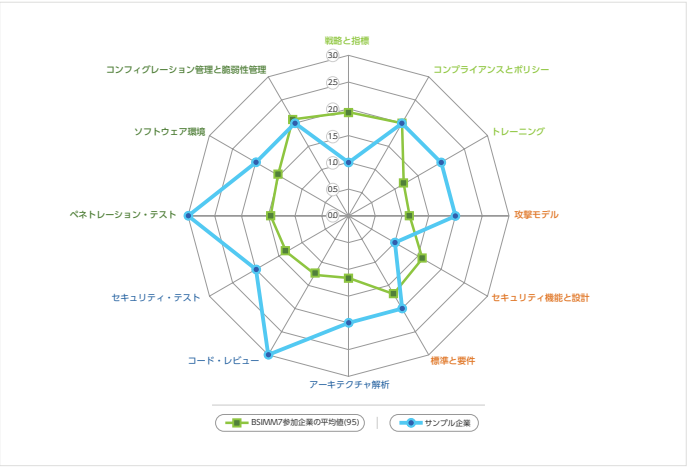
BSIMM に加えて、BSIMM 専用のコミュニティを利用すれば、月次ニュースレターを購読したり、四半期毎の専門 Web セミナー、アメリカとイギリスで開催される年次カンファレンス、RSA カンファレンス・ネットワーキング・イベント、活発なオンライン・コミュニティーなどに参加することもできます。

パーソナライズされたレポートを提供

BSIMM には必ず、強みのある領域と改善が必要なポイントを示した、次のような詳細なレポートが付属します。

- **カスタマイズされたレーダーチャート。**この図は、優位な点と劣っている点が一目で分かるようになっています。測定モードからソフトウェアセキュリティ対策計画モードに切り替えると、すぐに実行できる客観的な指標が結果に表示されます。
- **BSIMM 企業スコアカード。**この表から他社のすべての対策に対して自社の置かれている状況が分かります。これを使用して長期的な全体対策、個別の事業単位、ビジネスパートナー、協力ベンダーについて検討できます。

サンプル企業のレーダーチャート



BSIMM 参加者の言葉

消費者や専門家、さらに人類がデジタル体験を取り入れるようになるにつれて、ソフトウェアの日常生活への影響はますます大きくなっています。BSIMM を利用してソフトウェアセキュリティのレジリエンス対策を評価するトップ企業は、市場で大きな競争優位を確立できます。

～ジム・ルース、最高セキュリティ責任者、AETNA

2009 年以来、BSIMM の新バージョンが出るたびに、ソフトウェアセキュリティの主流化が進み、企業の採用数が常に増加していることが明らかになっています。BSIMM7 も例外ではなく、ソフトウェアセキュリティが次第に開発業務の一部となり、ソフトウェアエンジニアリングとの関連性が深まる転換点となる可能性があります。

～エリック・ベイズ、シニアディレクター、プロダクトセキュリティオフィス、DELL EMC

BSIMM7 は、世界中の企業の実際の取り組みについての生のデータとそのデータを分類し、理解する一貫した体系的手法に基づいて、ソフトウェアセキュリティ対策のしっかりした基礎や強化を求める企業にとっては重要なリソースです。

～イバン・アルセ、セキュリティディレクター、ICT プログラム、SADOSKY FOUNDATION

サンプル企業のBSIMM7スコアカード | 測定結果：37

ガバナンス			インテリジェンス			SSDLタッチポイント			展開		
アクティビティ	BSIMM7 参加企業(95)	サンプル企業	アクティビティ	BSIMM7 参加企業(95)	サンプル企業	アクティビティ	BSIMM7 参加企業(95)	サンプル企業	アクティビティ	BSIMM7 参加企業(95)	サンプル企業
戦略と指標			攻撃モデル			アーキテクチャ解析			ペネトレーション・テスト		
[SM1.1]	47	1	[AM1.2]	63		[AA1.1]	81	1	[PT1.1]	82	1
[SM1.2]	48		[AM1.3]	34		[AA1.2]	29	1	[PT1.2]	58	1
[SM1.3]	46	1	[AM1.5]	48	1	[AA1.3]	23	1	[PT1.3]	54	
[SM1.4]	81	1	[AM2.1]	8		[AA1.4]	47		[PT2.2]	21	1
[SM2.1]	41		[AM2.2]	8	1	[AA2.1]	15		[PT2.3]	16	
[SM2.2]	35		[AM2.5]	13	1	[AA2.2]	12	1	[PT3.1]	10	1
[SM2.3]	33		[AM2.6]	9	1	[AA2.3]	5		[PT3.2]	6	
[SM2.5]	19		[AM2.7]	9		[AA3.1]	4				
[SM2.6]	33		[AM3.1]	4		[AA3.2]	0				
[SM3.1]	14		[AM3.2]	2							
[SM3.2]	9										
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			ソフトウェア環境		
[CP1.1]	56	1	[SFD1.1]	74		[CR1.2]	58	1	[SE1.1]	46	
[CP1.2]	84		[SFD1.2]	65	1	[CR1.4]	63	1	[SE1.2]	78	1
[CP1.3]	50	1	[SFD2.1]	27		[CR1.5]	28		[SE2.2]	27	1
[CP2.1]	24		[SFD2.2]	40		[CR1.6]	34	1	[SE2.4]	24	
[CP2.2]	31		[SFD3.1]	6		[CR2.5]	22		[SE3.2]	12	
[CP2.3]	34		[SFD3.2]	10		[CR2.6]	15		[SE3.3]	3	
[CP2.4]	36		[SFD3.3]	1		[CR2.7]	19		[SE3.4]	0	
[CP2.5]	38	1				[CR3.2]	3	1			
[CP3.1]	19					[CR3.3]	2				
[CP3.2]	13					[CR3.4]	3				
[CP3.3]	5					[CR3.5]	5				
トレーニング			標準と要件			セキュリティ・テスト			コンフィグレーション管理と脆弱性管理		
[T1.1]	69	1	[SR1.1]	60	1	[ST1.1]	78	1	[CMVM1.1]	82	1
[T1.5]	27		[SR1.2]	66		[ST1.3]	72	1	[CMVM1.2]	84	
[T1.6]	17	1	[SR1.3]	64	1	[ST2.1]	22	1	[CMVM2.1]	69	1
[T1.7]	37		[SR2.2]	28	1	[ST2.4]	10		[CMVM2.2]	74	
[T2.5]	13		[SR2.3]	22		[ST2.5]	7		[CMVM2.3]	41	
[T2.6]	14	1	[SR2.4]	21		[ST2.6]	9		[CMVM3.1]	3	
[T2.7]	5		[SR2.5]	22		[ST3.3]	4		[CMVM3.2]	5	
[T3.1]	3		[SR2.6]	17	1	[ST3.4]	2		[CMVM3.3]	8	
[T3.2]	5		[SR3.1]	8		[ST3.5]	4		[CMVM3.4]	6	
[T3.3]	2		[SR3.2]	11							
[T3.4]	7										
[T3.5]	2										

シノプシスの特色

シノプシスは、お客様のセキュア開発ライフ・サイクル (SDLC) とサプライ・チェーンにインテグリティ（セキュリティと品質）を組み込むための極めて包括的なソリューションをご提案します。最先端のテスト技術、自動解析、エキスパートが一体となって、堅牢な製品およびサービスのポートフォリオを構成しています。このポートフォリオを利用してプログラムをカスタマイズすることで、開発プロセスの初期段階での不具合や脆弱性の検知および修正が可能になり、リスクを最小化しつつ生産性を最大化できます。 シノプシスは、アプリケーション・セキュリティ・テストのリーダーとして認められており、IoT、DevOps、CI/CD、クラウドといった新しいテクノロジーやトレンドにベスト・プラクティスを適用できる独自の地位を確立しています。テストが終了しても、終わりではありません。 オリエンテーションから展開の支援、的を絞った修正の手引き、さまざまなトレーニング・ソリューションまでを提供することで、お客様の投資を最大限に有効化します。まだ対策を始めたばかりか、あるいはすでに着実に進めつつあるかを問わず、シノプシスのプラットフォームを利用することで、ビジネスを推進するアプリケーションのインテグリティを確保できます。

詳しくは、www.synopsys.com/jp/software をご覧ください。

日本シノプシス合同会社 ソフトウェア インテグリティ グループ
〒 158-0094 東京都世田谷区玉川 2-21-1 二子玉川ライズオフィス
TEL: 03-6746-3600

Email: sig-japan-sales@synopsys.com
www.synopsys.com/jp/software

SYNOPSYS®
Silicon to Software™

©2017 Synopsys, Inc. All rights reserved. Synopsys は Synopsys, Inc. の米国およびその他の国における登録商標です。Synopsys の商標に関しては、こちらをご覧ください。http://www.synopsys.com/copyright.html 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。