NSS 侵害検出テストで シスコが首位を継続

シスコは 2016 年 NSS Labs 侵害検出システム（BDS）テストで 3 年連続で首位を獲得しました。シスコのソリューションは、マルウェア、エクスプロイト、回避を 100 % 検出し、検出所要時間は最短でした。

シスコのみが、脅威を見つけ次第すべての場所でブロックできる統合セキュリティ インフラストラクチャを提供できる多様なテクノロジーを保有しています。卓越したネットワーク プレゼンス、定評ある Talos のグローバル脅威インテリジェンス、および業界で最も多彩で優れたセキュリティ ポートフォリオを利用します。シスコのアーキテクチャ上のアプローチは、シンプルかつオープンで、自動化されたソリューションを実現します。各ソリューションはシームレスに連携し、リアルタイムに機能します。お客様は優れた可視性と応答性を得られるので、より多くの脅威を検出して迅速に修復できます。

また、他のどのベンダーよりも**多くのプラットフォーム**で優れた侵害検出を提供します。これには、次世代ファイアウォール、次世代 IPS、Unified Threat Management（UTM）、スイッチおよびルーティング インフラストラクチャ、電子メール、Web アプライアンスが含まれます。さらに、ネットワーク、データセンター、エンドポイント、モバイル デバイス、仮想マシン、電子メール、Web といった、**より多くの攻撃ベクトル**から保護します。この統合セキュリティ アーキテクチャによって、ネットワークは侵入に対して強固になり、自動応答によってセキュリティがシンプルになります。

最新のレポートをご覧になり、シスコが多様な脅威を迅速に阻止する方法をご確認ください。

攻撃者の活動時間と空間の削減

現在の防御側は、高度化と専門化が進むハッカーから自身を保護する必要があります。攻撃者は、拡大を続ける脅威の状況を理解し、あらゆる脆弱性を探してそれを悪用します。その手が緩むことはありません。攻撃者の影響力を削ぐためには、防御側は攻撃者が活動する時間と空間を削減しなければなりません。最新の中間サイバーセキュリティ レポート [英語] によると、シスコの検出時間（TTD）は **13 時間**でした。業界標準はおよそ **100 時間以上**です。

シスコには、他社よりも問題を迅速かつ明確に検出しているという利点があります。この可視性をインテリジェンスに変換し、より多くの脅威を迅速に阻止できるようにします。シスコの業界をリードする脅威インテリジェンス チーム、Talos は、1 日に 197 億件もの脅威をブロックしています。これは世界中で 1 日に 1 人あたり 2.5 件以上の脅威をブロックしている計算になります。また、他のどの組織よりも多くのデータを多くの方法で分析しています。この脅威インテリジェンスから 360 度ビューを作成し、すべてのシスコのセキュリティ製品で活用し、迅速で効果的なセキュリティを実現しています。

図 1. シスコの NSS 侵害検出テストの結果

製品				侵害検出率		NSS テスト スループット	
NGIPS v6.0 および Advanced Malware Protection 搭載の Cisco Firepower 8120				100.0%		1,000 Mbps	
100 万件に 1 件以下	ドライブバイ エクスプロイト	ソーシャル エクスプロイト	HTTP マルウェア	SMTP マルウェア	オフライン 感染	回避	安定性と 信頼性
0.33%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	合格

NSS 侵害検出システム（BDS）テストでシスコが首位を継続

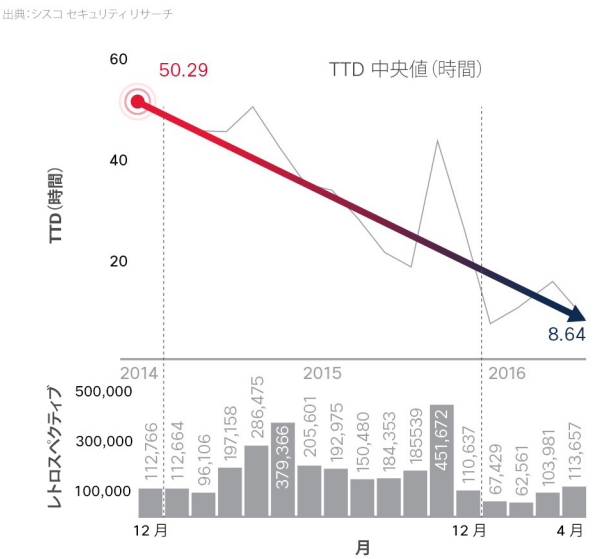
図 2. NSS 検出時間テストの結果

検出時間のスコア									
検出時間	製品 A	シスコ	製品 B	製品 C	製品 D	製品 E	製品 F	製品 G	製品 H
1 分未満	44.40%	67.00%	0.60%	48.90%	46.20%	5.50%	7.30%	6.50%	3.60%
3 分未満	75.90%	91.80%	2.90%	88.70%	84.20%	31.30%	17.90%	17.10%	26.70%
5 分未満	86.60%	96.30%	6.50%	91.00%	88.40%	47.80%	27.60%	27.00%	66.20%
10 分未満	97.40%	96.60%	15.20%	95.60%	91.30%	85.00%	43.10%	42.50%	90.10%
30 分未満	97.90%	97.10%	85.80%	98.50%	93.10%	96.90%	76.40%	75.40%	94.00%
60 分未満	98.20%	97.90%	90.80%	98.70%	93.10%	98.20%	97.90%	89.20%	96.30%
120 分未満	98.50%	98.50%	90.80%	98.90%	94.30%	98.40%	98.50%	89.70%	96.60%
240 分未満	98.90%	99.20%	91.60%	99.00%	97.60%	98.90%	98.50%	89.70%	96.80%
480 分未満	99.00%	99.40%	95.80%	99.00%	98.70%	99.40%	98.90%	90.00%	99.70%
720 分未満	99.20%	99.70%	96.40%	99.40%	98.70%	99.50%	98.90%	90.10%	99.80%
1080 分未満	99.40%	99.80%	96.80%	99.40%	98.70%	99.80%	98.90%	90.10%	99.80%
1440 分未満	99.40%	100.00%	96.80%	99.40%	99.00%	100.00%	98.90%	90.10%	99.80%
総合検出スコア	**99.40%**	**100.00%**	**96.80%**	**99.40%**	**99.00%**	**100.00%**	**98.90%**	**90.10%**	**99.80%**

	= > 90%
	= 80 - 89%
	= 60 - 79%
	= 40 - 59%
	= < 40%

この図は、検出時間に基づく効果の違いを示します。複数の製品について、最終行に同じ総合検出スコアが記載されています。この場合、検出速度が速い製品（上から下に向かって、先に数字が緑になる）の方が、攻撃者に与える活動時間と空間が減少するため、効果が高いと判断されます。

図 3. シスコ中間サイバーセキュリティ レポートでの検出時間



シスコのブログ [英語] では、検出時間が検出率 100 % よりも効果の測定基準として有効である理由を説明しています。