CyberSiege™

スケーラブルで包括的なセキュリティテスティングプラットフォーム

Spirent TestCloud™でのテストには制約がありません

CyberSiege は、最新のセキュリティ攻撃、マルウェア、ファジングアルゴリズム、インターネットアプリケーション、モバイルアプリケーション、エンタープライズプロトコルから成るきわめて豊富なオンラインライブラリを活用します。必要な要素だけを選択することもできますし、全部を選択することもできます。CyberSiege および TestCloud は、更新を自動あるいは手動に設定して実行でき、ラボ環境をセキュアな状態に保ちます。

重要なインフラストラクチャコンポーネントの評価、導入、運用を行う場合に、すべてではないにせよほとんどの技術要件に優先するのがセキュリティです。セキュリティがなければ信頼性は得られません。信頼性がなければ安心は得られません。

真のセキュリティとは、脆弱性を見つけてそこにパッチを当てること、コンプライアンスを徹底すること、パスワードを掛けること、統制手段を講じることです。

セキュリティテストとは、アプリケーション、デバイス、オペレーション、プロセスに潜んでいる障害ポイントを見つけ出すことです。セキュリティをテストするときには、テクノロジ、テスト&測定、プロセス、トレーニング、データ分析を活用しながら、信頼性の高い現実的なトラフィックを使います。その際、スケーラブルで包括的なソリューションとなるのが Spirent のセキュリティテストプラットフォームです。

きわめて現実的なシミュレーション

CyberSiege で生成されるアプリケーショントラフィックおよびセキュリティトラフィックは、ファイアウォールエンジニア、IPS エンジニア、セキュリティアナリスト、ネットワークエンジニアが、アプリケーションレベルファイアウォール、IPS、ウイルス対策アプリケーション、DDoS アプライアンス、ルータ、スイッチ、その他ネットワーキングデバイスを使うことによって、検出、特定、隔離することができます。

CyberSiege は、セキュリティテスト用として多種多様な実トラフィックを生成します。以下に例を示します。

- **SNS &インターネットアプリケーション:** SNS（Twitter や Facebook）、検索エンジントラフィック（Google、Yahoo、Bing）、Web メール/チャットサービス（Gmail、Yahoo!メール、Hotmail、Yahoo!メッセンジャー）などの一般的なプロパティも含め、実際のビデオとオーディオをストリーミングします。
- **モバイルアプリケーション:** 今やインターネットトラフィックのかなりの部分を占めるようになりました。Android クライアント、iOS クライアントで特に人気のモバイルデバイスから、複数のユーザエージェントおよびアプリケーション ID に対応したサーバトランザクションに至るまで、無数のモバイルアプリケーションをシミュレートします。
- **エンタープライズサービス:** IT 企業がそのユーザ基盤に提供するサービスです。IMAP、POP、SMTP といったプロトコルをベースにした電子メールサービスから、MySQL、Oracle といったデータベースサービスに至るまで、多岐にわたります。Spirent の各種ソリューションは、サイバーレンジトラフィックジェネレータの基本要件の 1 つである SIP プロトコルをベースとしたテストサービスを提供します。

テストの統合

CyberSiege とセキュリティデバイスとの統合は容易です。また、セキュリティデバイスの評価/ベイクオフとオペレーショントレーニングに対応したサイバーレンジ環境との統合も容易です。CyberSiege は、ファイアウォール、IPS、ロードバランサ、サーバ、ルータ、スイッチに物理的に接続できます。

CyberSiege™

スケーラブルで包括的なセキュリティテスティングプラットフォーム

CyberSiege

CyberSiege は、民間および行政機関のオペレータ、サービスプロバイダ、一般企業に対してセキュリティの堅牢性を保証する、Next Generation Security Platform（次世代セキュリティプラットフォーム、NGSP）の 1 つです。

NGSP の条件:

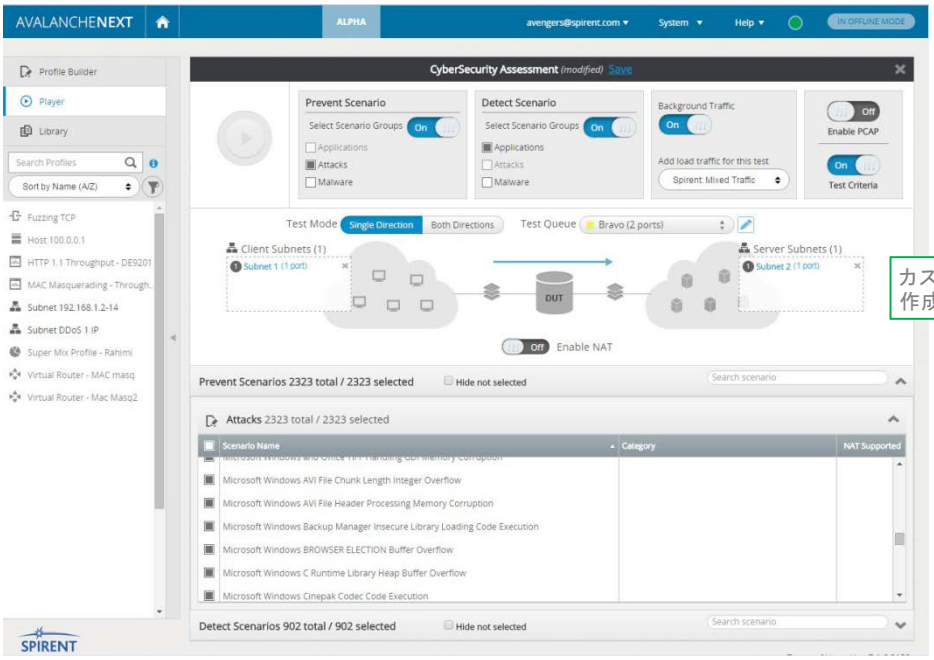
- 包括的であること、スケーラブルであること、フレキシブルであること。
- 重要なインフラストラクチャ、エンタープライズ、アプリケーション、エンクレーブのセキュリティ体制が改善できること。
- アセスメント、テスト&測定、シミュレーション、オペレーション、トレーニングに対応していること。
- 新規インフラストラクチャおよびサービスの導入を促す効果があること。

スケーラブルな NGSP の条件:

- サブスクリプションサービスを備えていること。ゼロデイセキュリティ攻撃および関連攻撃、マルウェア、インターネットアプリケーション、アプリケーションプロトコル、エンタープライズプロトコル、高度なファジングアルゴリズムの継続的アップデートに対応していること。
- NGSP のデータベースおよびソフトウェアアプリケーションのスキーマ、サイズ、フォーマットが拡張できること。

フレキシブルな NGSP の条件:

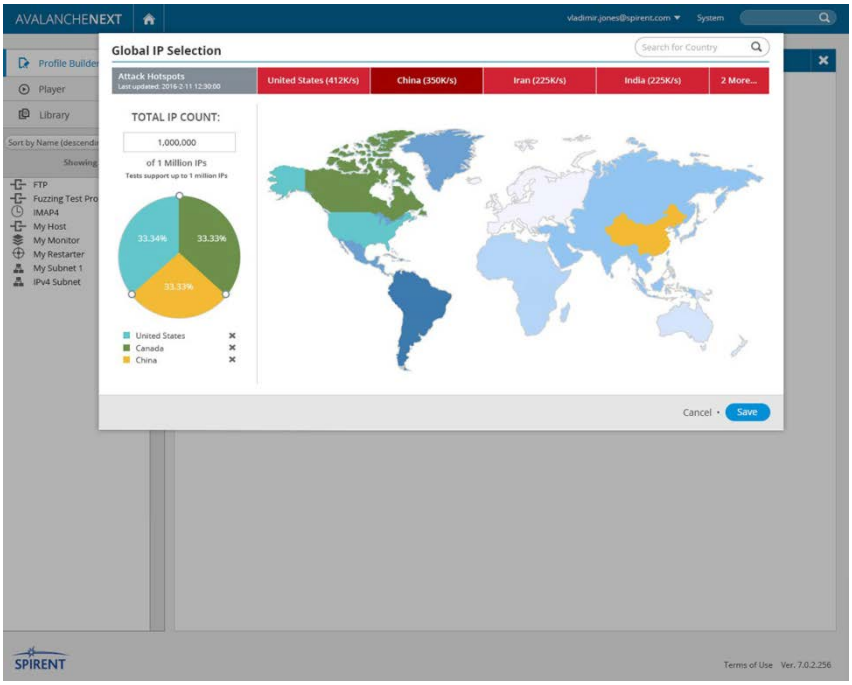
- 実稼働ネットワーク、ステージングネットワーク、テストネットワークにおけるロールを持っていること。
- サイバーレンジの OPS とトレーニングとをサポートしていること。
- インシデントレスポンスチーム（IRT）、ファイアウォールエンジニア、IPS エンジニア、セキュリティアナリスト、ネットワークエンジニアのオペレーショントレーニングが円滑化できること。
- 企業、データセンタ、ネットワークオペレーションセンタ（NOC）、セキュリティオペレーションセンタ（SOC/NOSC）を行き交う現実的なトラフィックをシミュレートすること。



NGSP によって、重要なインフラストラクチャコンポーネントのアセスメントと評価とを行うための現実的なトラフィックが生成されます。重要なインフラストラクチャには、クライアント/サーバコンピューティングデバイス、モバイルデバイス、セキュリティデバイス、ネットワークデバイスなどさまざまなネットワーク要素があります。

特徴

シンプルでユーザフレンドリ: Spirent のユーザインターフェイス（UI）のわかりやすさは業界随一です。CyberSiege を使う人が、数学者、科学者である必要はありません。



IANA トラフィックセレクタ（国ごとにサブネット IP アドレスを選択）: 世界地図上で地域を選び、1 か国あたり複数の IANA ネットワークアドレスを使うことにより、テストの現実味を高めるとともに問題解決の難易度を上げたトレーニングを行います。

ヘイスタックトラフィック（規模の大きい現実的なトラフィック）の生成: アプリケーション認識型デバイスをテストするときに重要なことは、L2 から L7 をミックスした現実世界の条件が反映されていることです。実際のユーザが実際のデバイスで実際のアプリケーションを使うときの相互作用を利用したテストの作成により、並外れた現実感が得られます。

見つけ出すべきニードル（攻撃とマルウェア）の生成: CVE（Common Vulnerabilities and Exposures）にマッピングされるセキュリティ攻撃（マルウェア、シグニチャ攻撃、プロトコルファジングなど）がすばやく生成されます。スクリプトを作成しなくても、独自のプロトコルおよびアプリケーションのためのカスタムテストが生成されます。さらに、高性能の修復ツールが活用できますので、脆弱性の解消にかかる時間が短くて済みます。

DDoS 攻撃（ボリューム型～アプリケーションレイヤ型）の生成: 本物のトラフィック量を持ったラインレートの DDoS 攻撃を仕掛け、現実世界の条件下でセキュリティデバイスをテストします。L2～L7 を組み合わせた攻撃を発展させて、テストサイクルに次世代型 DDoS 攻撃を適用します。

ポートごとに複数のネットワーク（エンクレーブ）をサポート: 複数のネットワークからエミュレートしたトラフィックを作成して、最善のリスク軽減テストアーキテクチャを実現します。多層保護、多層防御を設定してシングルポイント障害を回避できます。

仮想ルータのサポート（複数のソースからの着信トラフィックをエミュレート）: クラウドからのトラフィックを作成します。OpenStack、VMware vCloud、Cloudstack、Amazon Web Services などのクラウドサービスのパフォーマンス、可用性、セキュリティ、スケールをテストします。

REST API（自動化用）: スクリプティング言語、プログラミング言語、オペレーティングシステムのいずれにも縛られない自動化環境を作ります。他のデバイスとのオーケストレーションが可能です。1 つのテストケースの中で多くのさまざまなテクノロジを自動化します。

CyberSiege™

スケーラブルで包括的なセキュリティテスティングプラットフォーム

Spirent の各種サービス

Spirent Global Services では、さまざまな専門的サービス、サポートサービス、教育サービスを提供します。いずれのサービスも、お客様の複雑なテストおよびサービス保証要件への対応サポートに重点を置いています。

詳しくは、Global Services の Web サイト（www.spirent.com）をご覧になるか弊社までお問い合わせください。

サイバーレンジのオペレーション&トレーニングを効果的に行う CyberSiege

サイバーレンジとは、ネットワーク、セキュリティ、データセンタでのオペレーションをサポートする OPS 担当者のトレーニングに用いるトレーニング環境です。その主な機能は、重要なインフラストラクチャ資産を守るためのトレーニングを課すこと、および重要なインフラストラクチャをシミュレートした模擬ターゲットにサイバースペース領域で攻撃を仕掛けることにあります。米軍の分類によれば、「サイバースペース」は現在以下のように定義されています。

「情報技術、インフラストラクチャ（インターネットを含む）、遠隔通信ネットワーク、コンピュータシステム、埋め込みプロセッサ、埋め込みコントローラのそれぞれが相互に依存したネットワークから成る、情報環境内のグローバル領域のこと」

この領域には、TCP/IP プロトコルを使用しないネットワークと要素（産業用制御システム（ICS）や全地球航法衛星システム（GNSS）など）も含まれます。現在使われている GNSS は、GPS、Galileo（EU 版 GPS）、GLONASS（ロシア版 GPS）、北斗（中国版 GPS）など複数あります。

次世代サイバーレンジの強化ポイント:

シミュレーション

- Internet Assigned Number Authority（IANA）から割り当てられるホストアドレス、ネットワークアドレスを使って現実の IP アドレスをエミュレートするなど、地域ごと、国ごとのトラフィックを含めてインターネットを包括的にシミュレートして、現実感を高める必要があります。

重要なインフラストラクチャターゲット

- 重要なインフラストラクチャターゲットに負荷を掛けること、およびそうしたターゲットにセキュリティ攻撃を仕掛けることができるようにします。ターゲットトラフィックプロファイルの設定が短時間で済むよう、トラフィックジェネレータでデータがインポートできるようにします。

マルチメディアの現実感（Skype、Voice over IP（VoIP）、Voice over LTE（VoLTE）など）

- 音声サービス、ビデオサービス、オーディオサービスのエミュレートを行います。それには、Web ブラウザなどのインターネットクライアントアプリケーションで視聴可能な実際の音声/映像を生成できるトラフィックジェネレータが含まれます。

株式会社 東陽テクニカ 情報通信システムソリューション部
〒103-8284 東京都中央区八重洲 1-1-6
TEL.03-3245-1250（直通） FAX.03-3246-0645 E-Mail : ict_contact@toyo.co.jp
www.toyo.co.jp/ict/

大 阪 支 店	〒532-0003	大阪府大阪市淀川区宮原 1-6-1（新大阪ブリックビル）	TEL.06-6399-9771	FAX.06-6399-9781
名古屋営業所	〒465-0095	愛知県名古屋市名東区高社 1-263（一社中央ビル）	TEL.052-772-2971	FAX.052-776-2559
宇都宮営業所	〒321-0953	栃木県宇都宮市東宿郷 2-4-3（宇都宮大塚ビル）	TEL.028-678-9117	FAX.028-638-5380
電子技術センター	〒103-8284	東京都中央区八重洲 1-1-6	TEL.03-3279-0771	FAX.03-3246-0645
テクノロジーインターフェースセンター	〒103-0021	東京都中央区日本橋本石町 1-1-2	TEL.03-3279-0771	FAX.03-3246-0645

JQA-EM4908 JQA-QM8795 電子技術センター