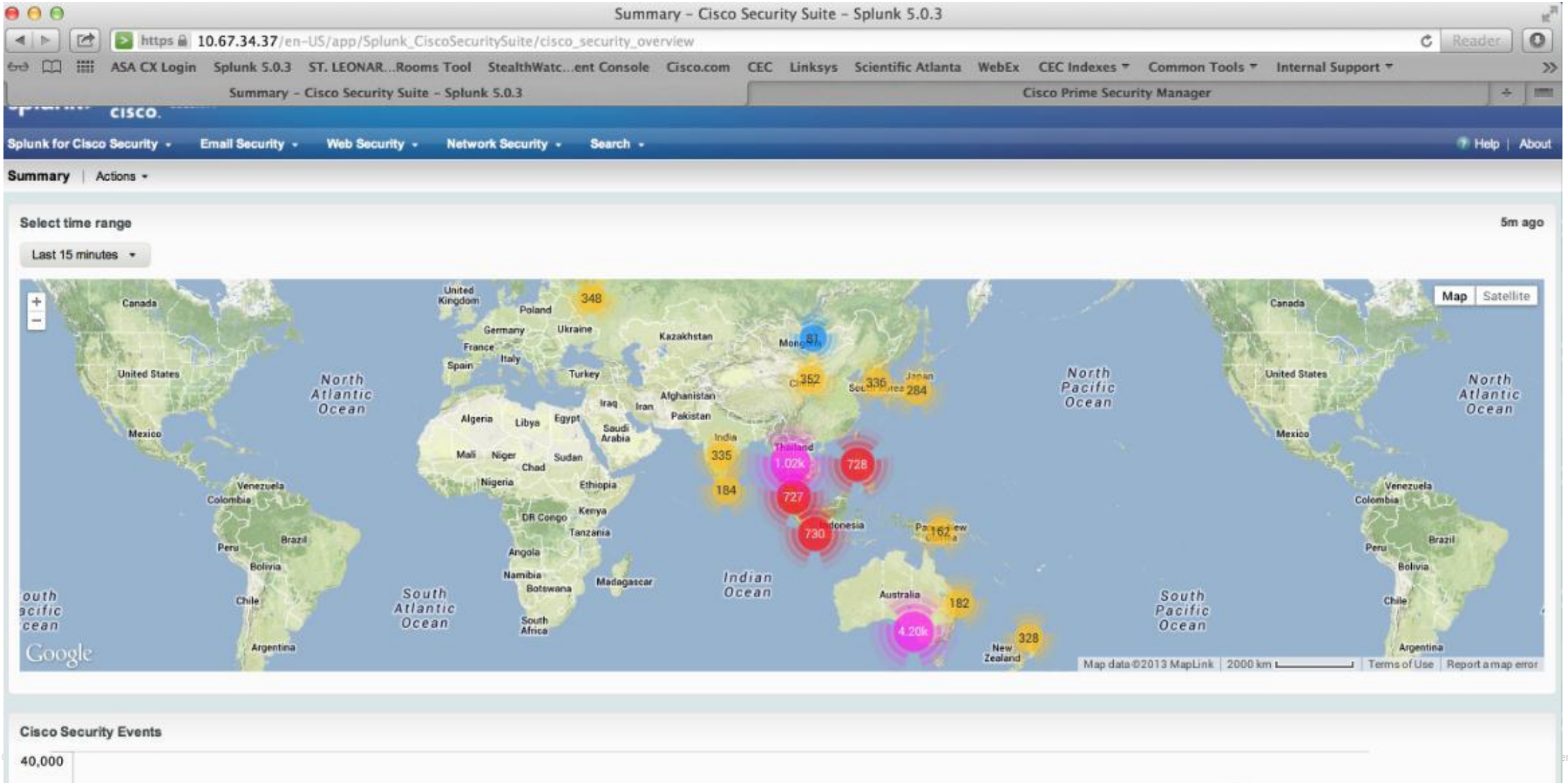
シスコ サイバーレンジサービス

シスコシステムズ合同会社

Cyber Rangeとは

- Cyber WAR ゲーム演習を中心としたCyber Securityサービスのパッケージ



サイバーレンジサービス概要

- 弊社CSIRTのネットワークセキュリティおよび監視モデルをベースに、サイバー空間で展開される最新のマルウェアをシミュレートし、検知の方法や防御の方法を体験する実践的なワークショッププログラムです
- ワークショップの中で以下のようなチーム編成によりそれぞれの役割を体験します。

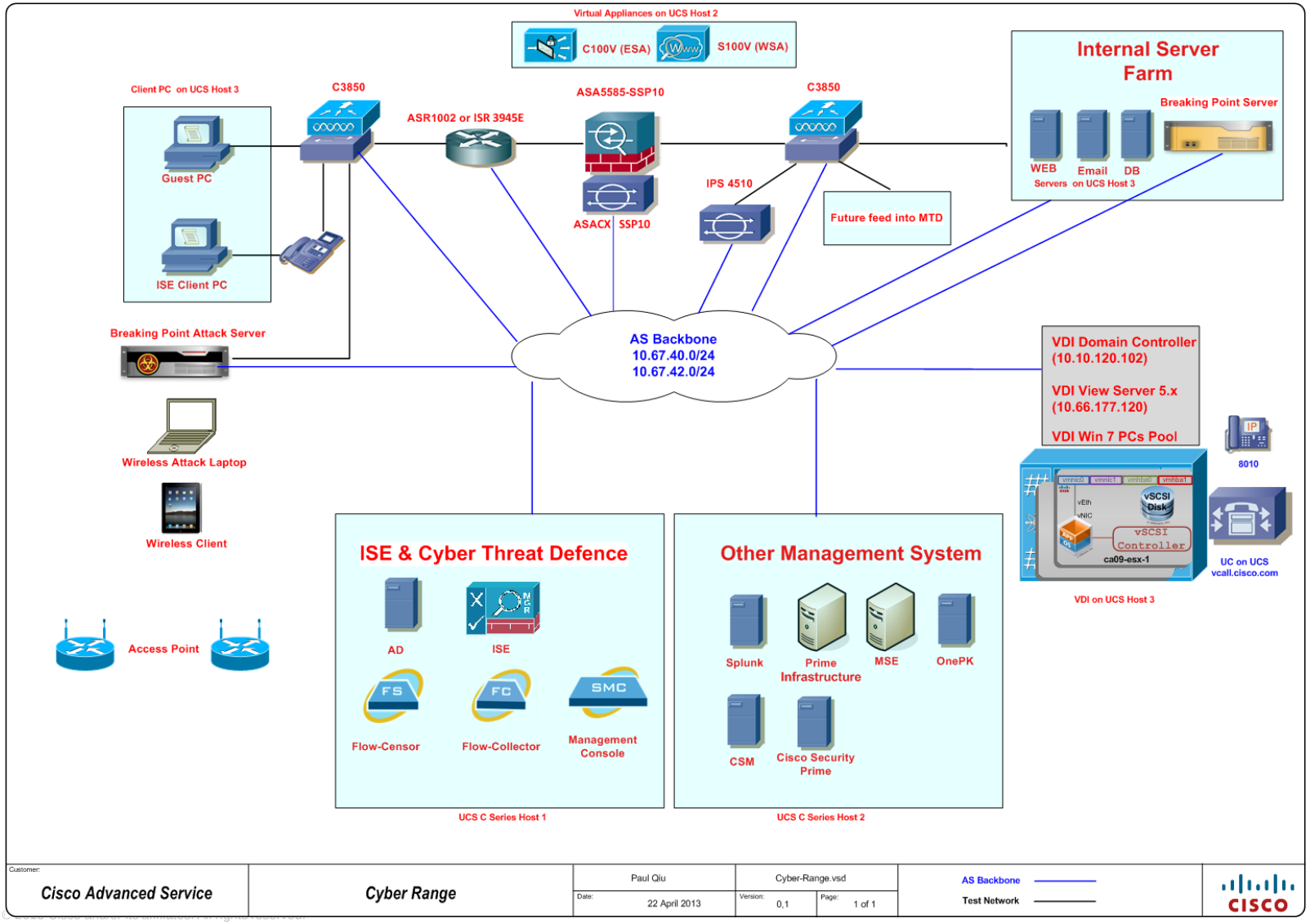
  GREEN TEAM：シミュレータを操作し、180以上のアプリケーションを使用した正規のユーザ通信をシミュレートします

  RED TEAM：シミュレータを操作し、5000種以上のネットワーク攻撃、28000種以上のマルウェア通信をシミュレートします

  BLUE TEAM：次世代ファイアウォール、ファイアウォール、アプリケーション認識、IPS、CSIRTの使用する各種検知システムを利用し、攻撃を検知、防御を実施します
- これらを総合的に体験することで、セキュリティイベント発生時のアラートやパターンを学習し、攻撃発生時にも正規の通信を保護しつつ不正な通信への正しい対応ができることができます

  * シミュレータとしてはPacific Endeavor でも採用されているIxia BreakingPoint を採用

サイバーレンジ・ラボ構成イメージ



Production構成
- Internetルータ
- NetFlow スイッチ
- NG Firewall
- IPS
- IDS
- Email Security Appliance
- Web Security Appliance

Management構成
- 認証サーバ
- ログ分析サーバ
- NetFlow分析サーバ
- FW/IPS管理サーバ
- 統合ネットワーク管理サーバ

Cyber Rangeサービス

- 以下の環境と攻撃、および対処方法を取得します

インフラストラクチャ	攻撃	防御
• 有線、無線、リモート アクセス • ネットワークおよびルーティング • クライアント シミュレータ • サーバ シミュレータ • アプリケーション シミュレータ • トラフィック生成	• DdoS （分散型 DoS 攻撃） • ゼロデイ攻撃 • ネットワーク偵察 • アプリケーション攻撃 • データ損失 • コンピュータ マルウェア • モバイル デバイス マルウェア • 不正行為の技術 • ボットネット シミュレーション • オープンソース攻撃ツール • 仮想ネットワーク攻撃	• グローバルな脅威に関するインテリジェンス • クライアント エンドポイント セキュリティ • ファイアウォール、IDS/IPS • シグニチャ ベースおよびふるまいにもとづいた検出 • Web および E メール プロキシ • ワイヤレス セキュリティ • アプリケーションの可視性と制御 • テレメトリ解析 • アイデンティティとアクセス管理 • セキュリティとイベント管理 • 調査ツール • オープンソース防御ツール • Cisco TrustSec® • SDN （Software Defined Network）

サイバーレンジワークショップ（実施例）

日程		トピック
第1日目	AM	・オープニング ・シスコセキュリティフレームワークについて ・CSIRTモデルについて
	PM	・ラボ構成と利用方法 ・攻撃ツールによる攻撃と防御例
第2日目	AM	・Cisco Cyber Threat DefenseおよびISE
	PM	・ISE、ASA-CX、パケットキャプチャリング、AVC（Application Visibility Control）による攻撃の視覚化
第3日目	AM	・WSA/ESAとSplunkの組み合わせによるMalwareの検知と防御
	PM	・ASA、IPSとゼロデイ攻撃
第4日目	AM	・DDoS攻撃と隔離
	PM	・Wireless攻撃
第5日目	AM	・総合演習
	PM	・演習レビューおよびおさらい

Package 1	Package 2
実施期間：5日間 実施場所：シスコラボ 参加者：6-10名	実施期間：5日間 実施場所：お客様環境 参加者：6-10名

VISIBILITY

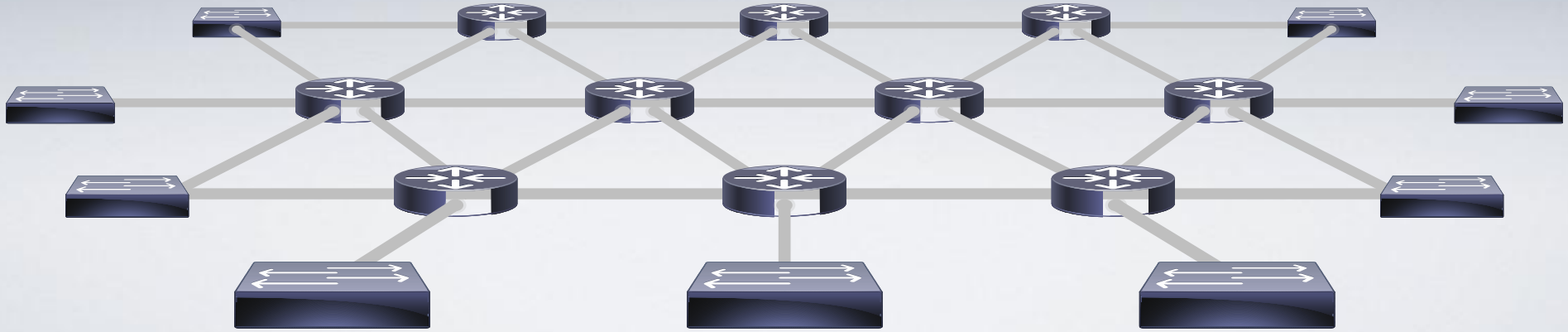
高度なアタックを検出するより細かい検知能力

INTELLIGENCE

ピンポイント攻撃に対する様々な情報による認識能力の向上

CONTROL

脅威を管理するネットワークワイドの防御



Thank you.