RedSeal Incident Response 機能

はじめに

バージョン 8.2 により新たにセキュリティ・インシデントが発生した際に、迅速にインシデント対応を行っていただくための情報を提供する機能が加わりました。
これにより、いち早く問題のあるホスト(マルウェアに感染していると思われるホスト)を特定し、切り離し、隔離を行うための情報を提供するとともに、感染したホストからアクセス可能なホストを特定し、被害を最低限に抑える上での必要な情報を提供します。

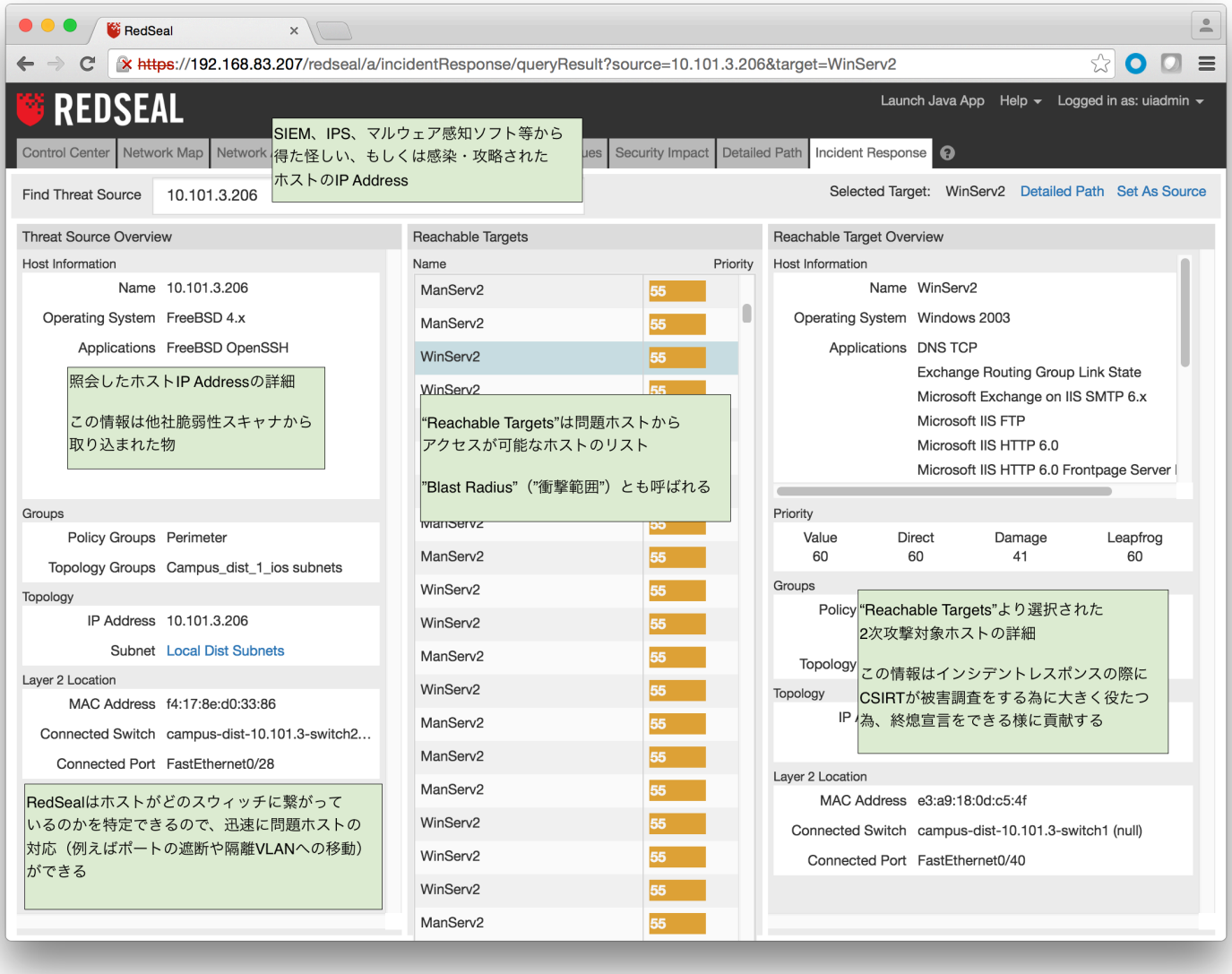

図 1：RedSeal Incident Response（解説を含む）

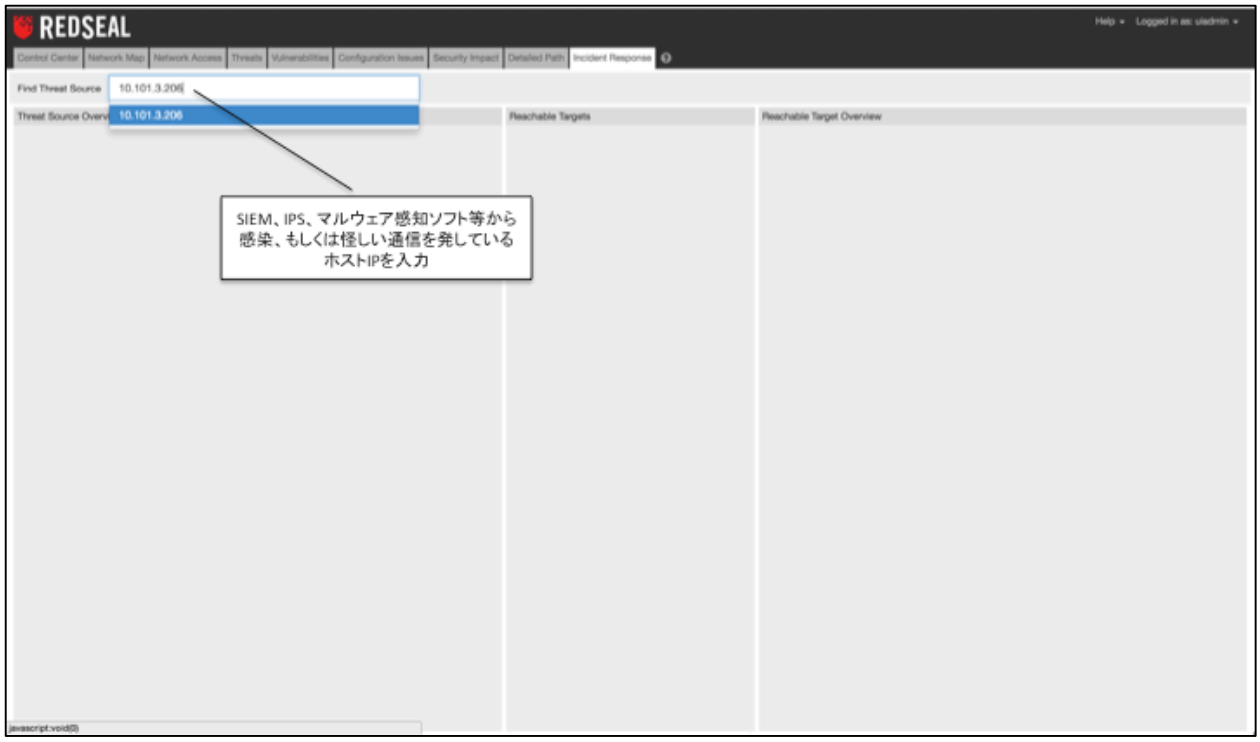

図 2：問題があると思われる IP Address をインプット

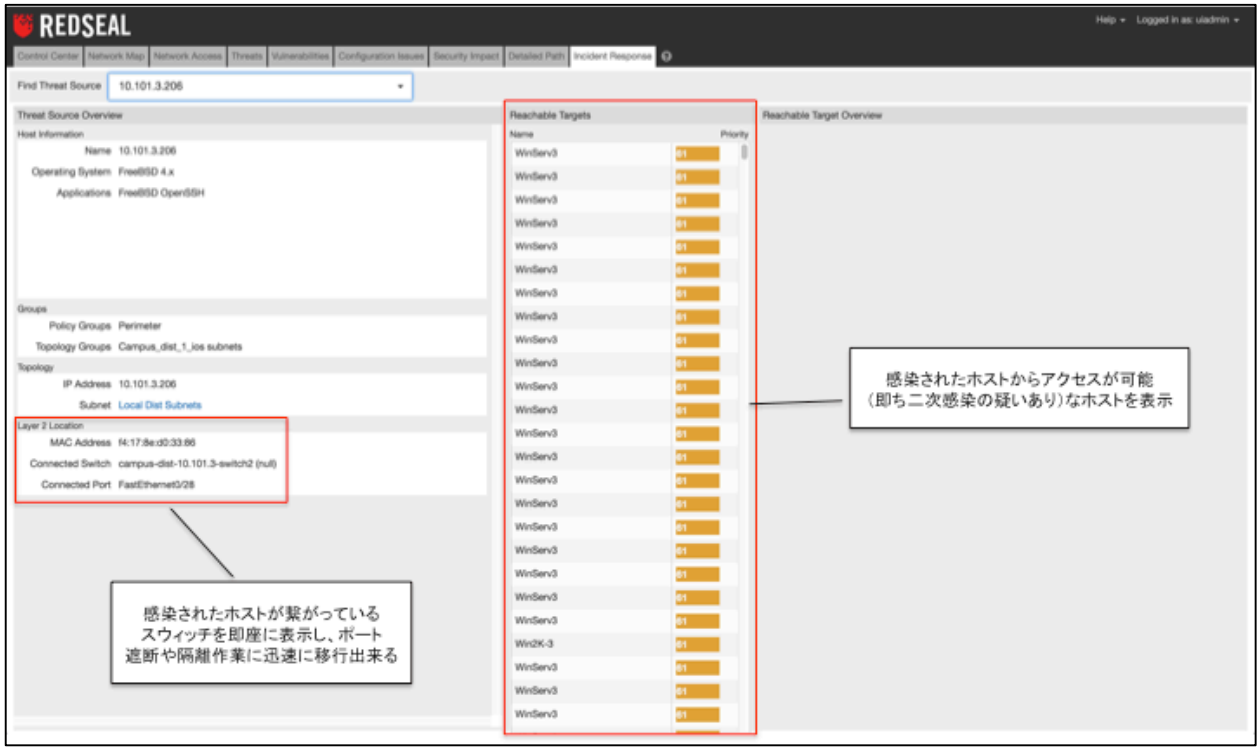

図 3：インプットされた IP Address とそのホストからアクセスが可能なホストのリスト

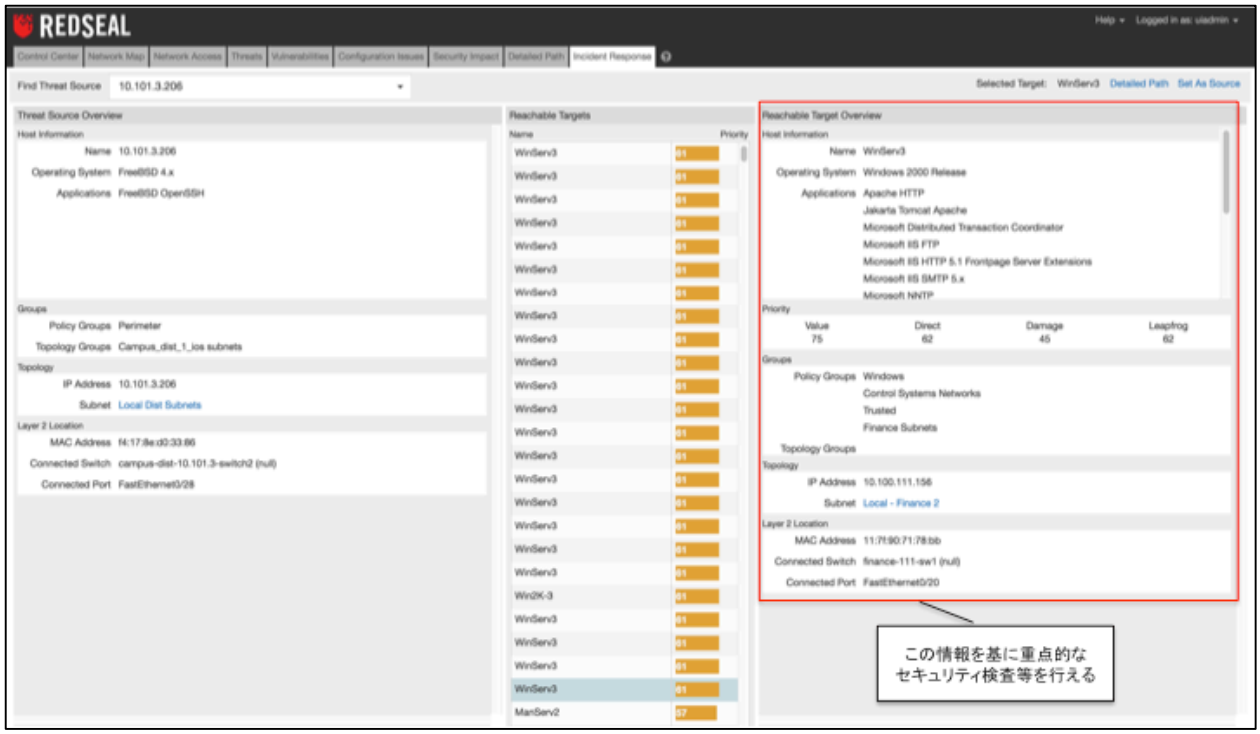

図 4：アクセス可能リストからセレクトされた 2 次被害の対象となるホストの詳細

RedSeal Incident Response 機能を活かすための条件：

RedSeal Incident Response 機能を利用するためには以下の条件があります：

- RedSeal Layer 2 ライセンス
- RedSeal からネットワーク機器への実機アクセス（SSH 等）
- 他社製脆弱性スキャナから収集された脆弱性データ
    - 対応している脆弱性スキャナ製品は次の通りです：
        - Alert Logic (Critical Watch) FusionVM
        - Digital Defense Frontline
        - BeyondTrust Retina CS
          BeyondTrust (eEye) Retina Network Security Scanner
        - McAfee Vulnerability Manager
        - Outpost24 OUTSCAN, HIAB
        - nMap
        - Qualys QualysGuard
        - Rapid7 NeXpose
        - Symantec Vulnerability Manager
        - Tenable Nessus
        - Tripwire (nCircle) IP360

RedSeal Incident Response を活用したユースケース：

Incident Response（インシデントレスポンス）とは即ち何かのセキュリティ障害が起こった際に行われる作業の事を言います。通常 Computer Security Incident Response Team（通称“CSIRT”）と言うチームが編成され、チームの中には企業のあらゆる部門の責任者が選ばれます。CSIRT は障害時のシミュレーション等を定期的に実施し、実際の障害に備えて組織のセキュリティ体制を保っています。

CSIRT が発動した際の通知は企業によっては様々ですが、殆どの場合は SIEM 、IPS およびマルウェア感知ツール等から問題があると思われる IP Address がその通知に含まれます。昨今の攻撃者は容易に攻撃できるホストをまず感染し、攻略した後にそこから手当たり次第 2 次攻撃を仕掛ける、と言うパターンが典型的な手口です。この為、感染されたホストが分かり次第迅速に対応（レスポンス）を実施する事が最重要事項です。

従来のやり方ですと一度 IP Address が判明するとネットワークの管理者が総出でそのホストの所在を確認する作業に取り組みます。この作業は時間がかかり、最悪のケースでは攻撃が進行していてもどのスウィッチにホストが繋がっているかが判明するまで手詰まり状態で被害が拡がる、ということも多くのケース・企業で見受けられます。即ち、インシデントレスポンスは時間との戦いです。
RedSeal のインシデントレスポンス機能を使うと瞬時にどのスウィッチに問題のあるホストが繋がっているかが分かります。その情報をもとにネットワーク管理者はそのポートを遮断したり、隔離 VLAN へ移動したり、といった対応を迅速に行えます。

特定された問題のあるホストの対応だけでは CSIRT の対応は終わりません。次の作業はどれだけ障害が拡がったのかを把握する事です。この作業は組織が大きければ大きいほど困難であり、大きな課題となります。典型的なやり方は問題ホストが属するサブネットに存在する全てのホストを脆弱性スキャナでスキャンをしたり、マルウェア感知ソフトを重点的にかけたり、アンチウィルスの更新等の作業が行われます。

一旦特定された問題のあるホストが属するサブネット確認を終えても作業は続きます。次の課題は特定された問題のあるホストが属するサブネットからどれだけの範囲で他のサブネットに影響があり得るのか、と言う課題です。「どこからどこまで確認作業をしなくてはならないのか？」、と言う問いかけに対して答えは決して容易に出せません。しかし、RedSeal の Incident Response 機能を使う事によって特定された問題のあるホストからアクセスが可能なホストのリストを割り出すことができます。このリストを使って確認作業を行うと最も脅威に晒されていたホストを優先的に確認できるので、インシデントの終息宣言に至るまでに的確にレスポンス作業を実施できます。

最後に：

RedSeal Incident Response はセキュリティ・インシデントが起こった際に貢献します。CSIRT にとってこの機能が提供する情報はタイムリー、かつ最も状況 に必要な物とも言えます。この様な機能がない場合のインシデント対応は無駄な努力と実際に被害の影響と範囲が分からないままに恐る恐る終息宣言を すると言う嵌めになりかねます。RedSeal Incident Response を活用すると的確にセキュリティ・インシデントに対応でき、自信を持って終息宣言を出すことができます。