# Cisco Threat Response v1 – インスタント デモ

最終更新日:2018 年 11 月 13 日

## このデモンストレーションについて

この事前設定済みデモンストレーションのガイドには、次の内容が含まれています。



### カスタマイズ オプション

シナリオ 1 では、Threat Response のインターフェイスの概要をプレゼンテーションし、このインターフェイスで実行できる主なタスクをいくつか説明します。これらのタスクでは、API を使って他の製品の値を変更します。以下の「はじめに」セクションでは、デモンストレーションを進めながら反映された変更を確認するために、同じデモンストレーション環境でこれらの他のアプリケーションにログインする方法を説明します。

## 要件

次の表に、このデモンストレーションの要件の概要を示します。

**表 1.** 要件

| 必須 | オプション |
|---|---|
| ● ラップトップ<br>● Google Chrome | ● Cisco AnyConnect® |

## このソリューションについて

Cisco Threat Response では、特定のシスコ セキュリティ製品を自動的に統合し、検出、調査、修復という重要なセキュリティ運用機能を高速化します。Cisco Threat Response はシスコの統合型セキュリティ アーキテクチャの重要な柱です。Cisco Threat Response によって、サイバーセキュリティ インシデントの調査と修復に必要な時間と手作業を大幅に削減できます。Cisco Threat Response は、時間が最重要事項である場合、迅速で信頼性の高い、一貫性のある回答を提供して、Umbrella®、AMP for Endpoints®、Threat Grid® など、シスコの既存のセキュリティ製品の価値を高めます。シスコとサード パーティのセキュリティ製品は、Threat Response にモジュールとして追加されます。詳細については、www.cisco.com/go/threatresponseを参照してください。

# はじめに

**プレゼンテーションの前に**

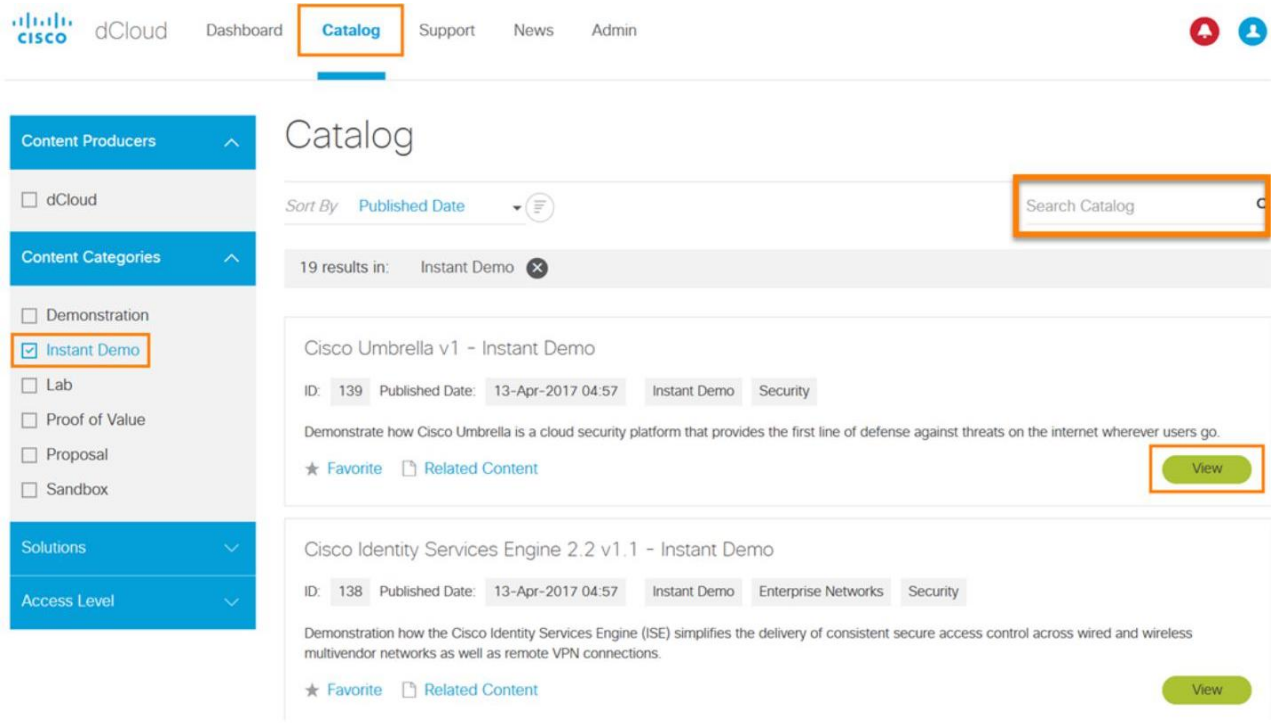
Cisco dCloud では、実際の対象者の前でプレゼンテーションを行う前に、アクティブなセッションを使用して、このドキュメントのタスクを実施しておくことを強く推奨します。そうすることで、ドキュメントとコンテンツの構成に慣れることができます。

場合によっては、環境を元の構成にリセットするため、このガイドに従った後に新しいセッションをスケジュールする必要があります。Threat Response は継続的に更新されます。このガイドでは、Threat Response バージョン 1.12 を対象にしています。

**プレゼンテーションを成功させるには入念な準備が不可欠です。**

次の手順に従ってコンテンツのセッションをスケジュールし、プレゼンテーション環境を設定します。

1. [カタログ（Catalog）] をクリックして、サイド バーから [インスタント デモ（Instant Demo）] を選択します。
2. Threat Response を検索します。




3. 以下の 4 つのデモがあります。

Cisco Threat Response v1 – インスタント デモ

Cisco Threat Response – AMP for Endpoints – インスタント デモ

Cisco Threat Response – Umbrella – インスタント デモ

Cisco Threat Response – Threat Grid – インスタント デモ

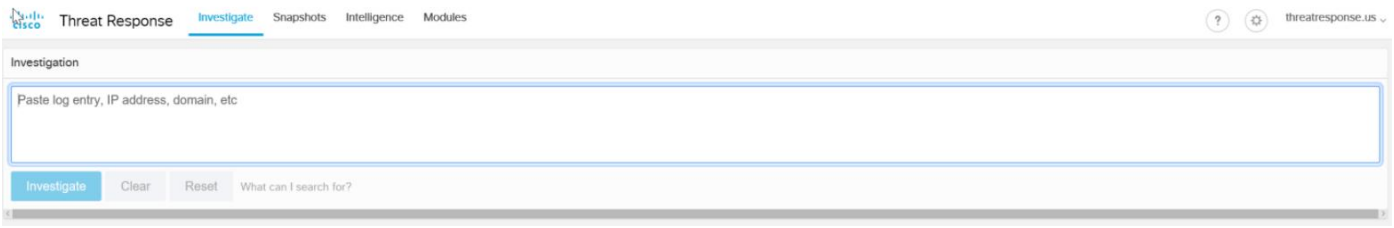
4. 各デモンストレーションの [表示（View）] ボタンをクリックします。
5. 「Cisco Threat Response」というラベルのタブでシナリオ 1 を開始します。

# シナリオ 1:　Cisco Threat Response ウォークスルー

## 手順

### セットアップ

1. セットアップで [表示（View）] をクリックした後、このタブにログイン画面が表示されますが、その後メインのインターフェイスに移動します。




2. 上の図の青で強調表示されているテキスト ボックスに以下のテキストをコピーします。これによって、生成されたトラフィックで検索する内容がデモンストレーションに伝えられます。実際には、この種の情報は Talos またはその他のソースから取得します。

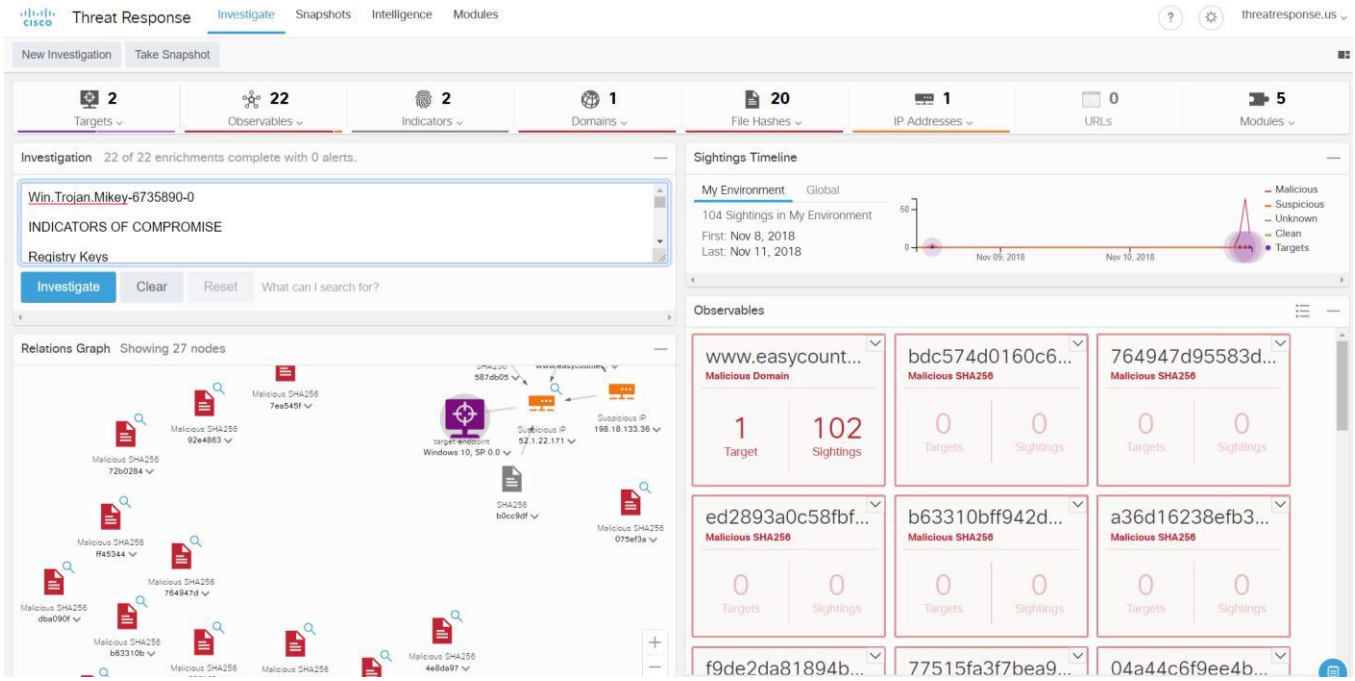
```
Win.Trojan.Mikey-6735890-0

INDICATORS OF COMPROMISE

Registry Keys
N/A
Mutexes
qazwsxedc
IP Addresses contacted by malware. Does not indicate maliciousness
52[.]1[.]22[.]171
Domain Names contacted by malware. Does not indicate maliciousness
www[.]easycounter[.]com
Files and or directories created
%WinDir%\cer61A0.tmp
%TEMP%\adminpak.msi
%SystemDrive%\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\C5MZMU22\adminpak[1].exe
%WinDir%\cluster\clcfgsrv.inf
%WinDir%\cluster\cluadmin.exe
File Hashes
04a44c6f9ee4b5f944038452d2669a9915e493f3d4aedd8603af6bcbf9fb157d
075ef3a40de2c10d52140c02fc604654e60eb1231659122640d93884a8f639d8
1ed41ccdce4f7c67dbeb57873ed69a0b53bd8c509a66f391fb4838cd26d32f88
4e8da970321ee8e38f2fe918ce8755ce504d0c54ad579c7a2d388ed65aceca3f
63562fa34ca55cbbc1f007ed6a199b625f277f02487d18c6a9a8e24354af6ea3
72b02849c7cde8ba42dfe04edf18b0ede900c66187a9e38f5d16eaf84ddfbfbe
764947d95583d3a134fc96d6ce06ce4175261d3b9b48d224238367054e187d93
77515fa3f7bea9043e954ac8cb13917edd930d0e5d87f2cbc9fa4d44bd281161
7ea545f0dd17684011d7bbdde7c004faccacd8edb6d011c4e023f2780279ae1f
92e4863e96df84117c1288ceb692823a6d86c0b3a09f29a5cbc4af6a83a03415
9d267ed7cc3efe21afd96a3717cf920376048528e7094c54defb915afbe96a80
a36d16238efb3b5f2ba5e9c23dd1db26a6b08fce8fa1d824e3006bc05f12a75f
b63310bff942d0fe4f131fbb777737b110ab630876e784ac843e0c4dcdebde44
bdc574d0160c6566738b039122d702a47aa10080b096cc3ca2729a2a5ca5f6f6
```

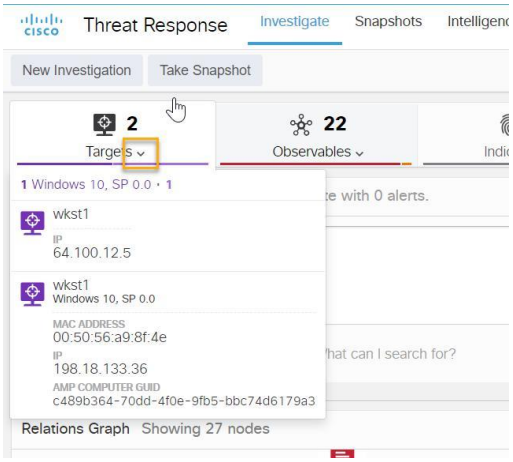
cf7236e1d8783d00cd54d9d821a1067a2c08cd7cb67b0c091f5826784403f67a
d7096f8904ebef796193afca1737f99e65c07ac7cf3c999aa46b5e60428ca006
dba090f098676f7f4d5bd9e71a5b24cb1dfc71edb6b8a0dc06082a60730a81d0
ed2893a0c58fbfaf73acdd4d7a7c9d8626e8609573739e8f0bf11c88d4b07303
f9de2da81894bbde4f6baf5909c3f3f6a5d5fc61a8df97836fb8db14fbdb6006

3. しばらくすると、以下の図のように監視対象が完全に示された状態でアプリケーションが戻ります。ウィンドウの幅が足りない場合は、[目撃タイムライン（Sightings Timeline）] と [監視対象（Observables）] ペインが [関係グラフ（Relations Graph）] の下に表示される場合があります。情報の最も重要な部分はレイアウトに関係なく、画面の上部に表示されます。

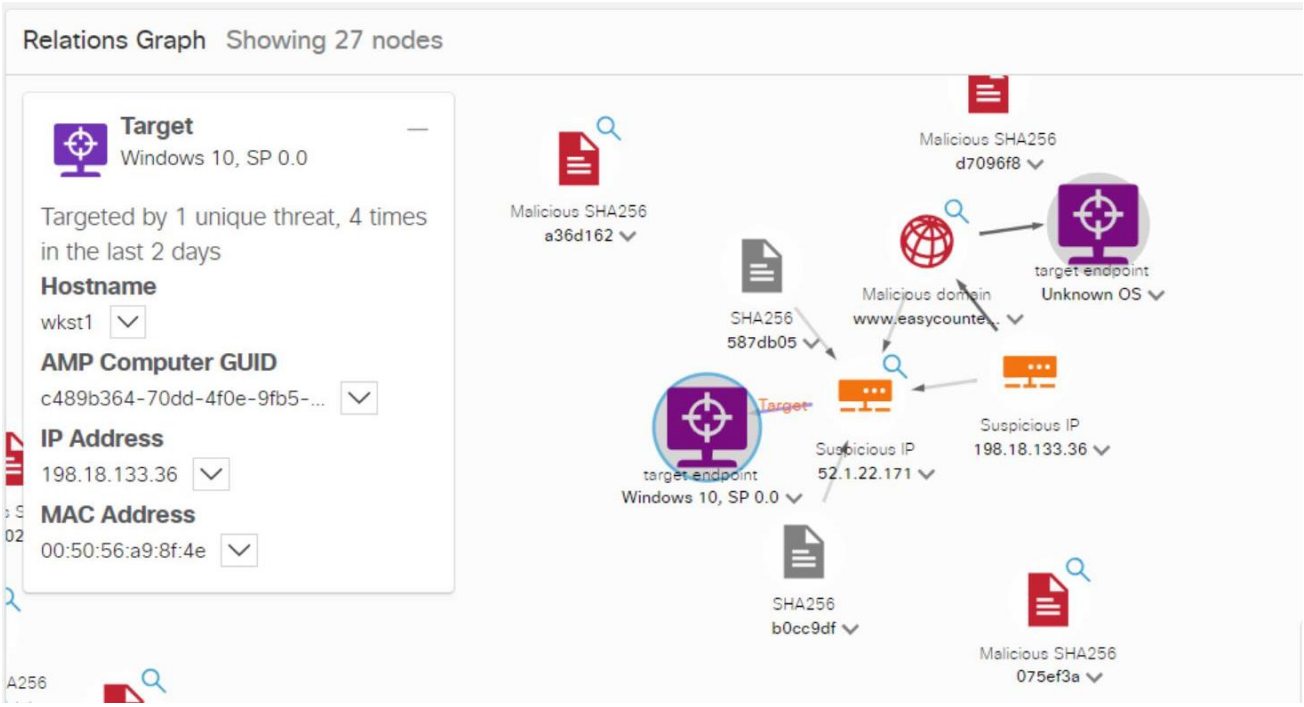



## 調査

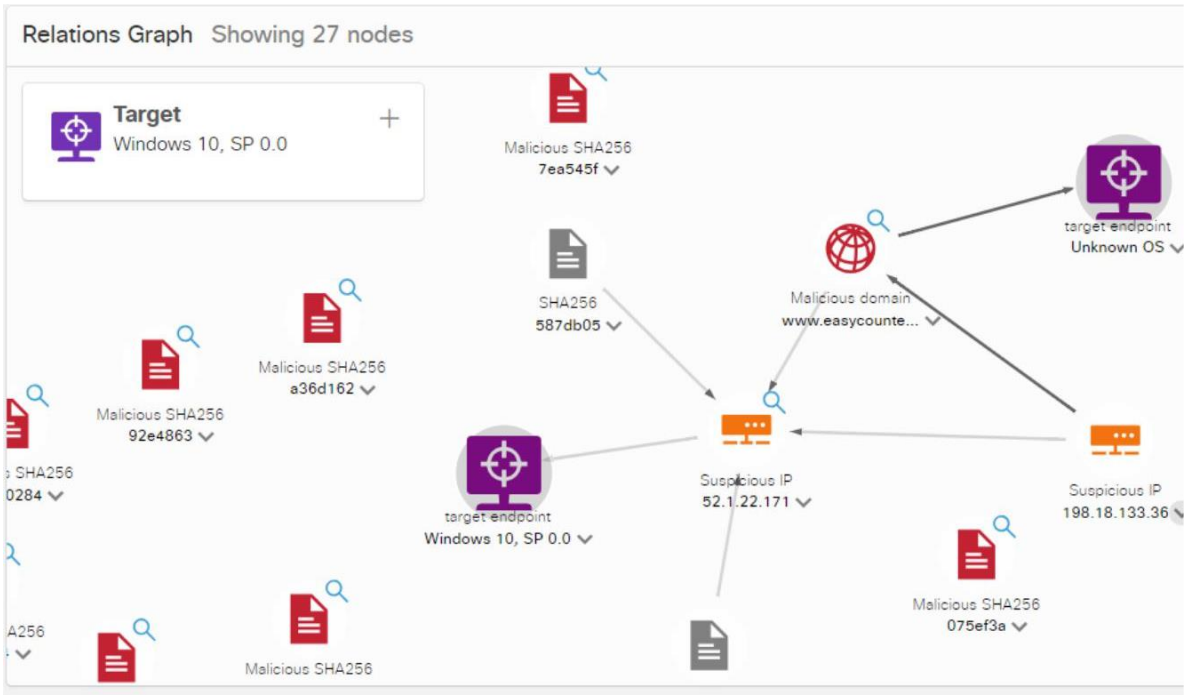
1. [ターゲット（Targets）] の横にある矢印をクリックすると、ターゲットのワークステーションの詳細を確認できます。この情報により、調査担当者は、監視対象についてモジュールからの目撃が報告されているためターゲットが影響を受けていることをすぐに把握できます。



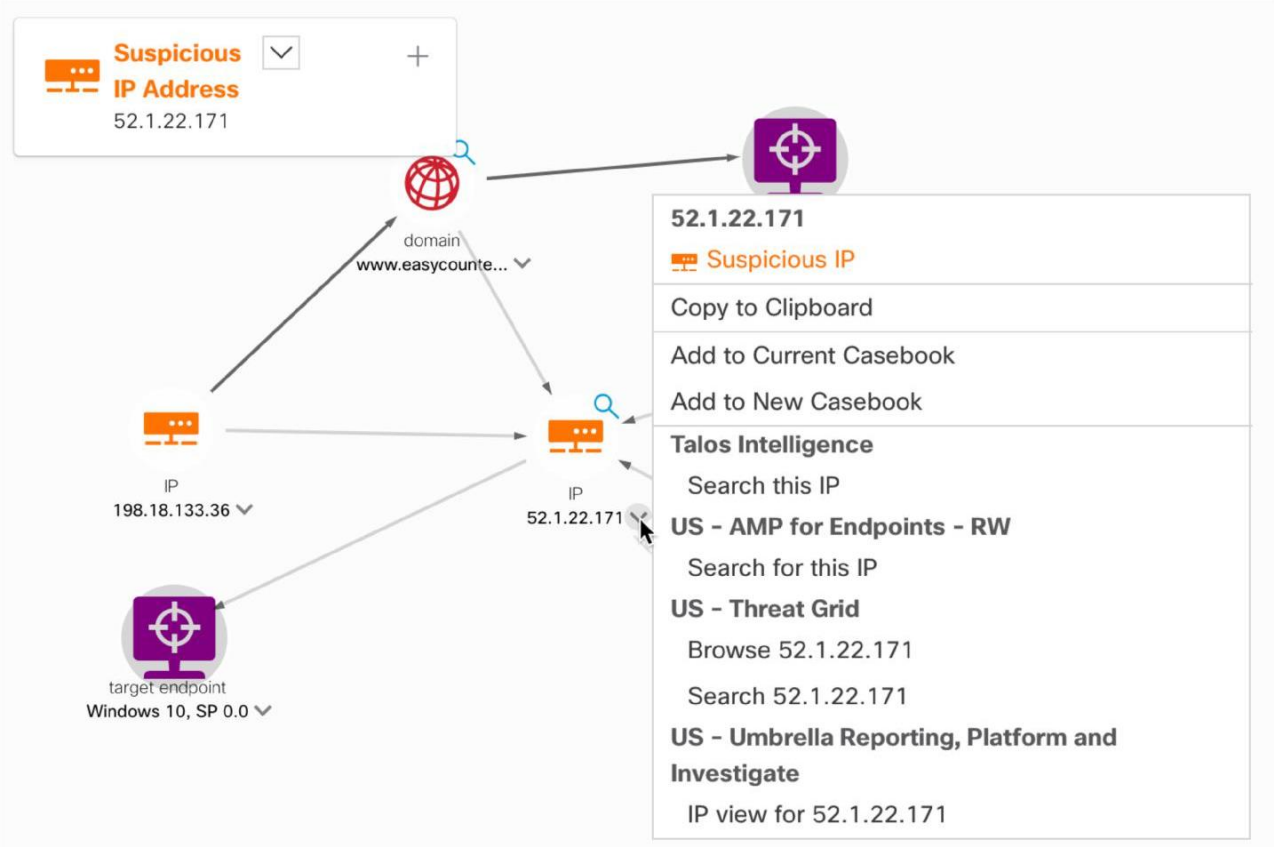
2. 結果のいずれかをクリックすると、その下にある [関係グラフ（Relations Graph）] の該当システムに移動します。




3. [関係グラフ（Relations Graph）] のいずれかのアイコンをクリックしてドラッグすると、それらの関係が明確に示されます。



4. アイコンの横にある三角形をクリックすると、グラフの各項目の詳細情報が表示されます。




5. 青い虫眼鏡アイコンの付いた各項目が監視対象で、画面の上部または [監視対象（Observables）] ペインに示されます。

6. 色にも注意する必要があります。

赤は悪意のある項目です。

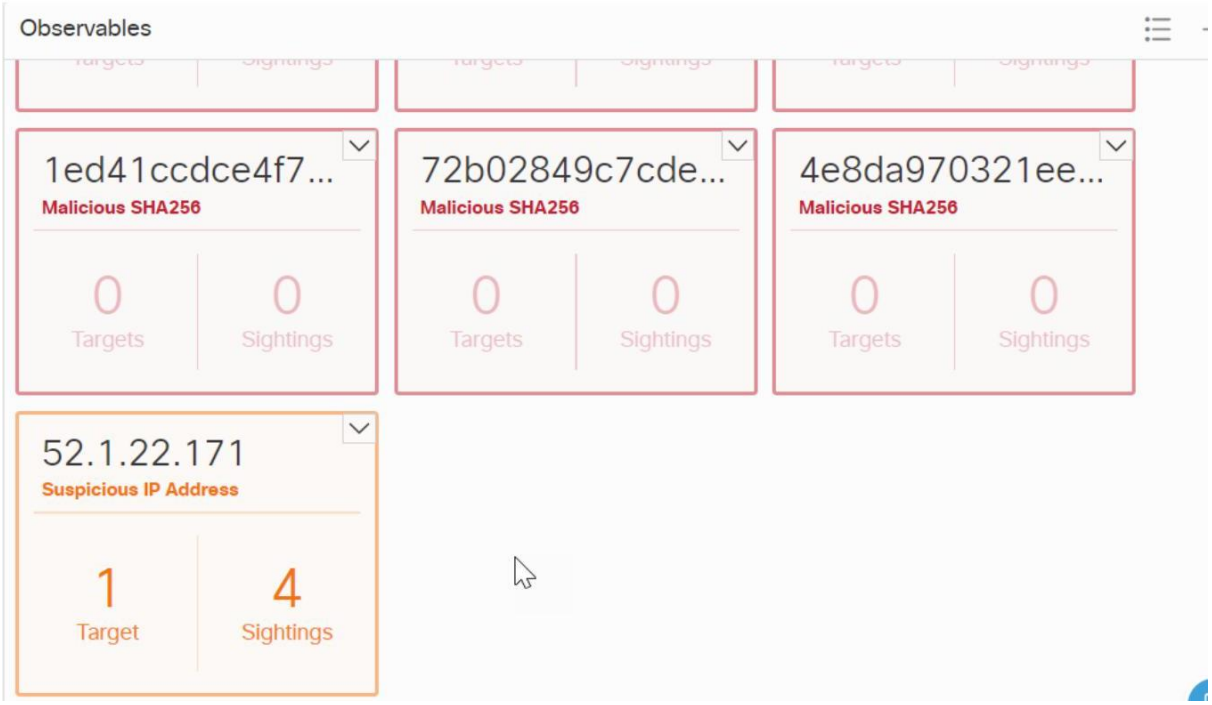
オレンジ色は疑わしい項目で、

紫の項目はターゲットを表します。

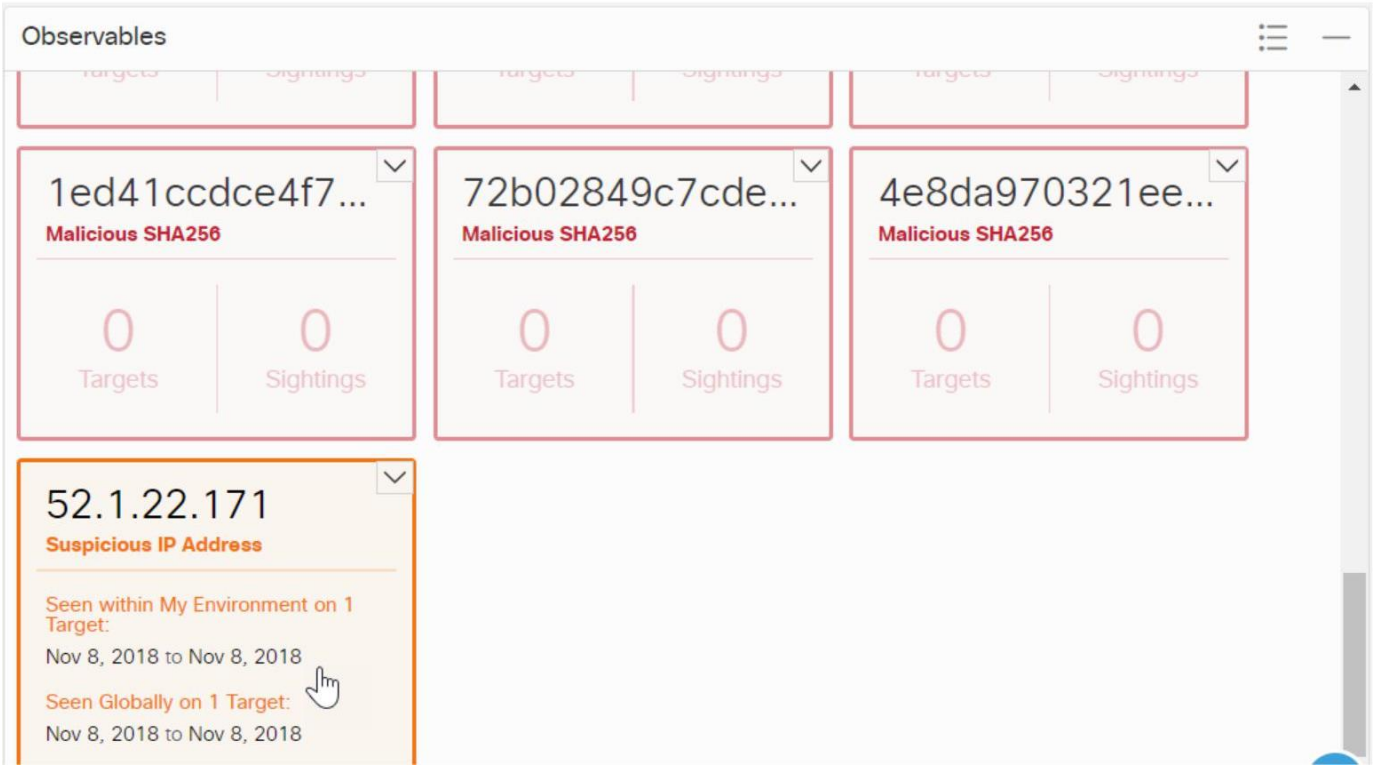
グレーは、この時点では不明です。

IP アドレスを囲むグレーの円は、RFC1918 アドレスを示しています。

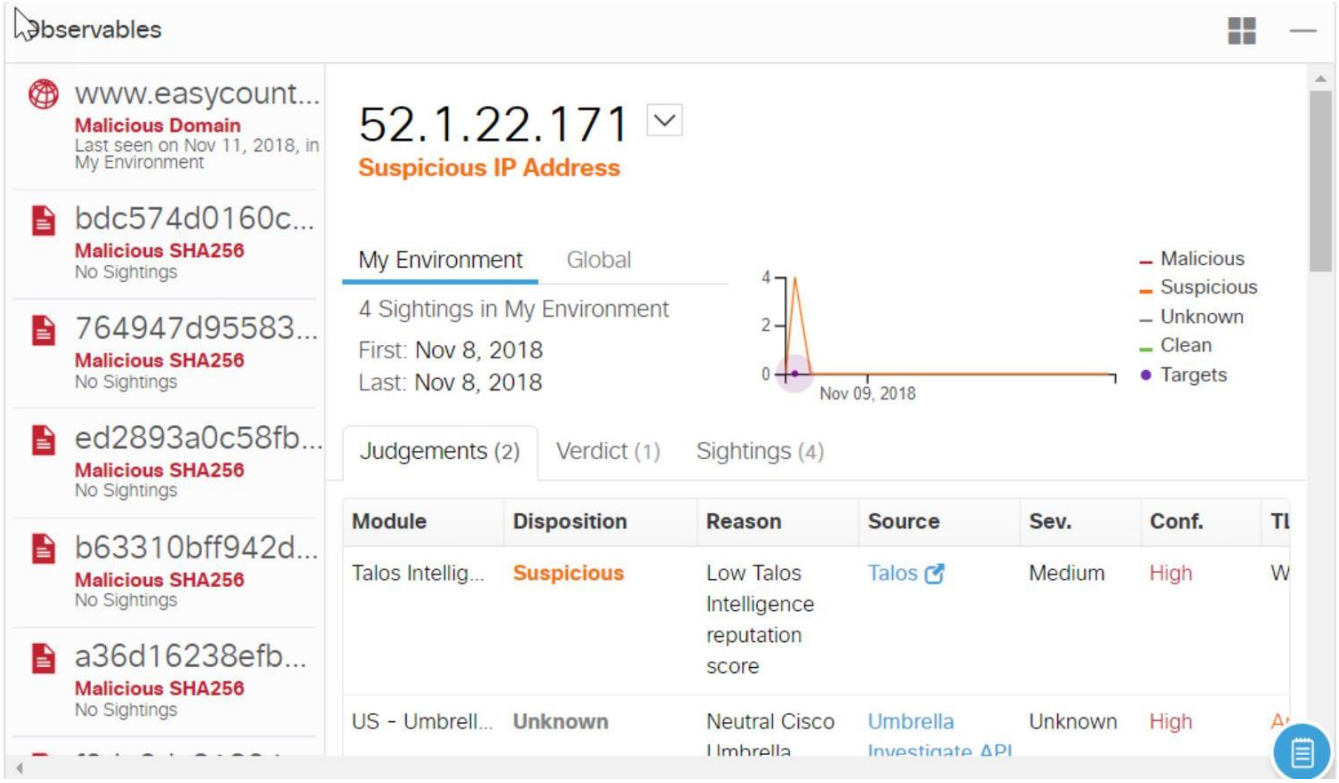
7. [監視対象（Observables）] ペインを見ると、最近のターゲットまたは目撃があった監視対象項目を見つけることができます。



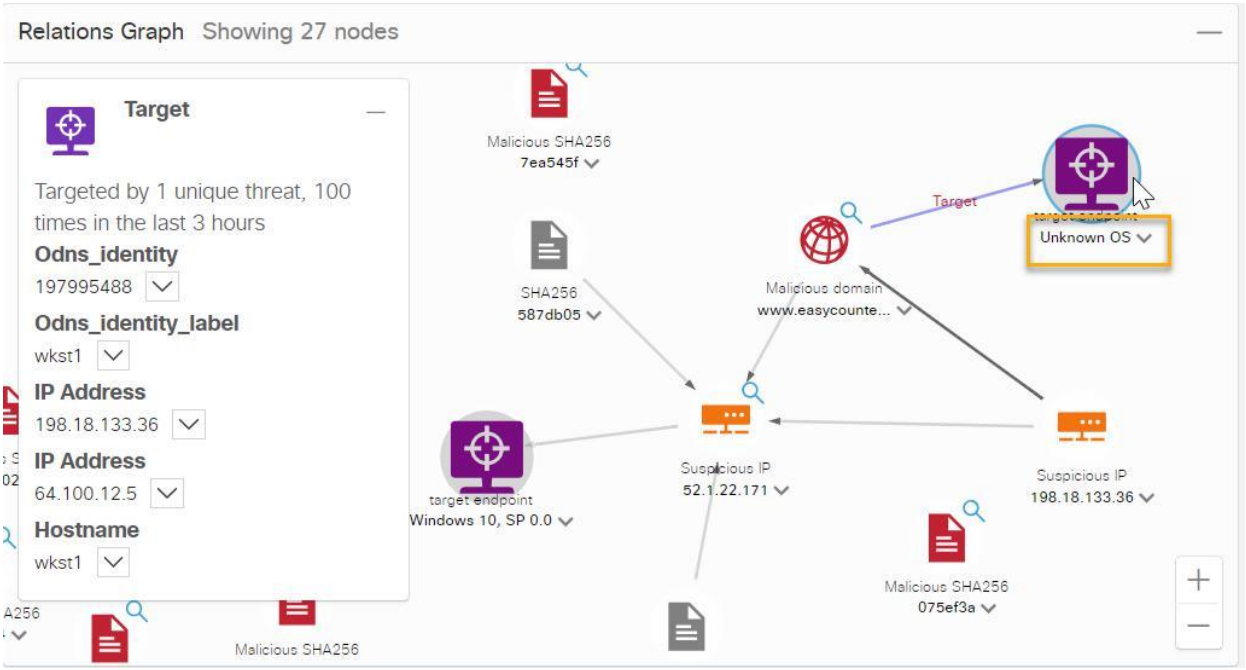

8. ボックスにマウスを合わせると、その項目の詳細が表示されます。



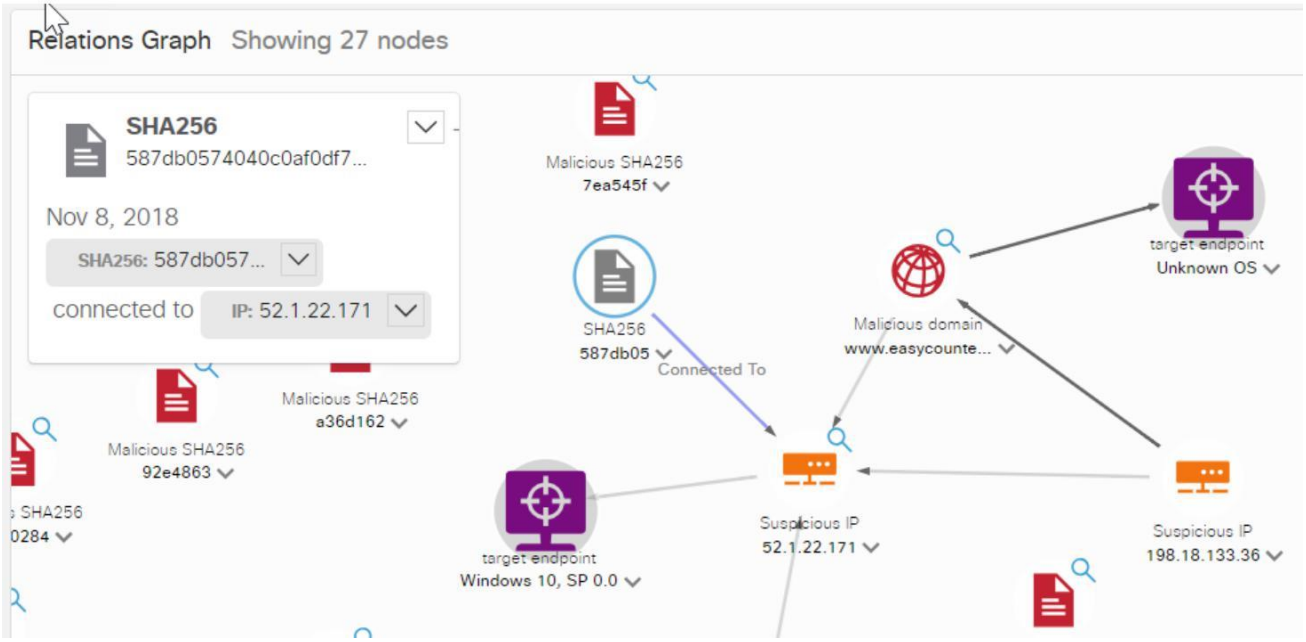
9. 最後に、ボックスをクリックすると、監視対象項目に関するすべての詳細情報が表示されます。



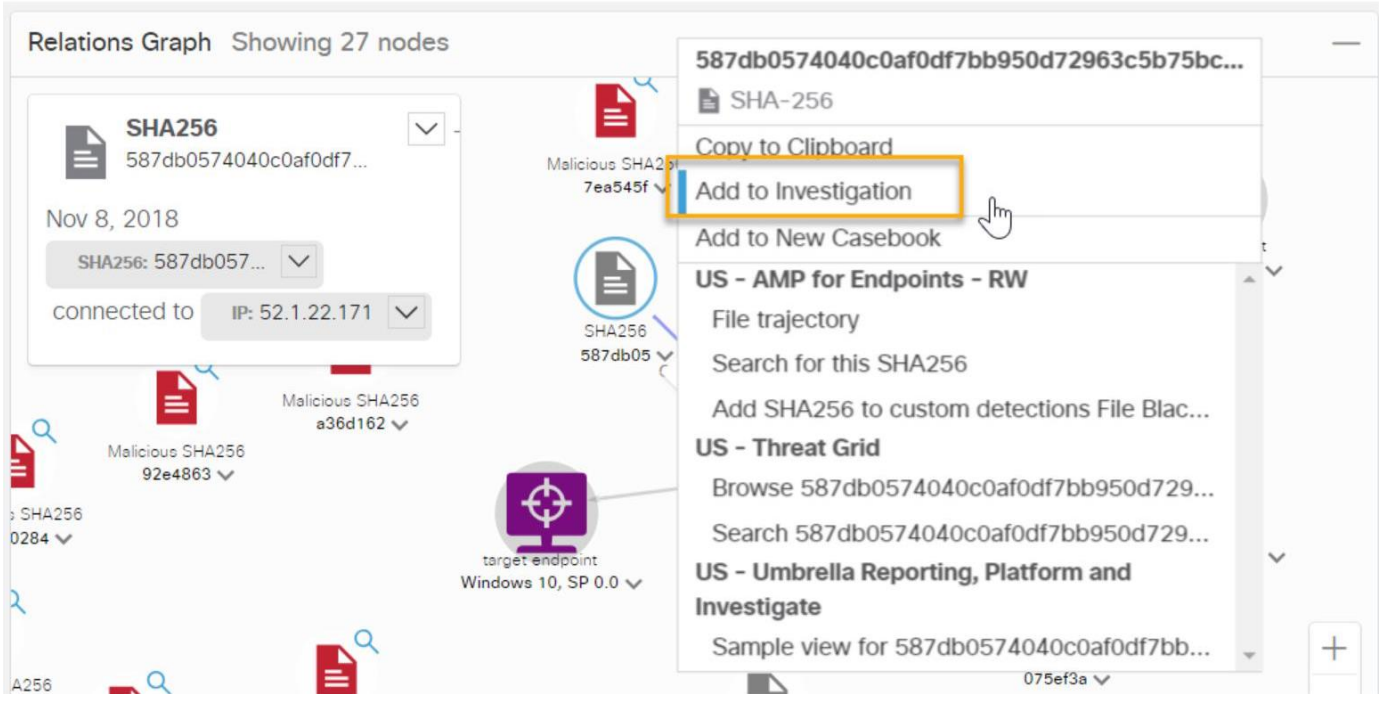

10. [関係グラフ（Relations Graph）]（または [ターゲット（Targets）] リスト）に戻ると、AMP for Endpoints の情報から、その項目が Windows 10 マシンであること、また Umbrella Reporting API の情報により、もう 1 つの項目が不明なオペレーティング システムを使用していることが簡単にわかります。不明なターゲットのアイコンをクリックすると、システムにすでにある情報を得ることができます。



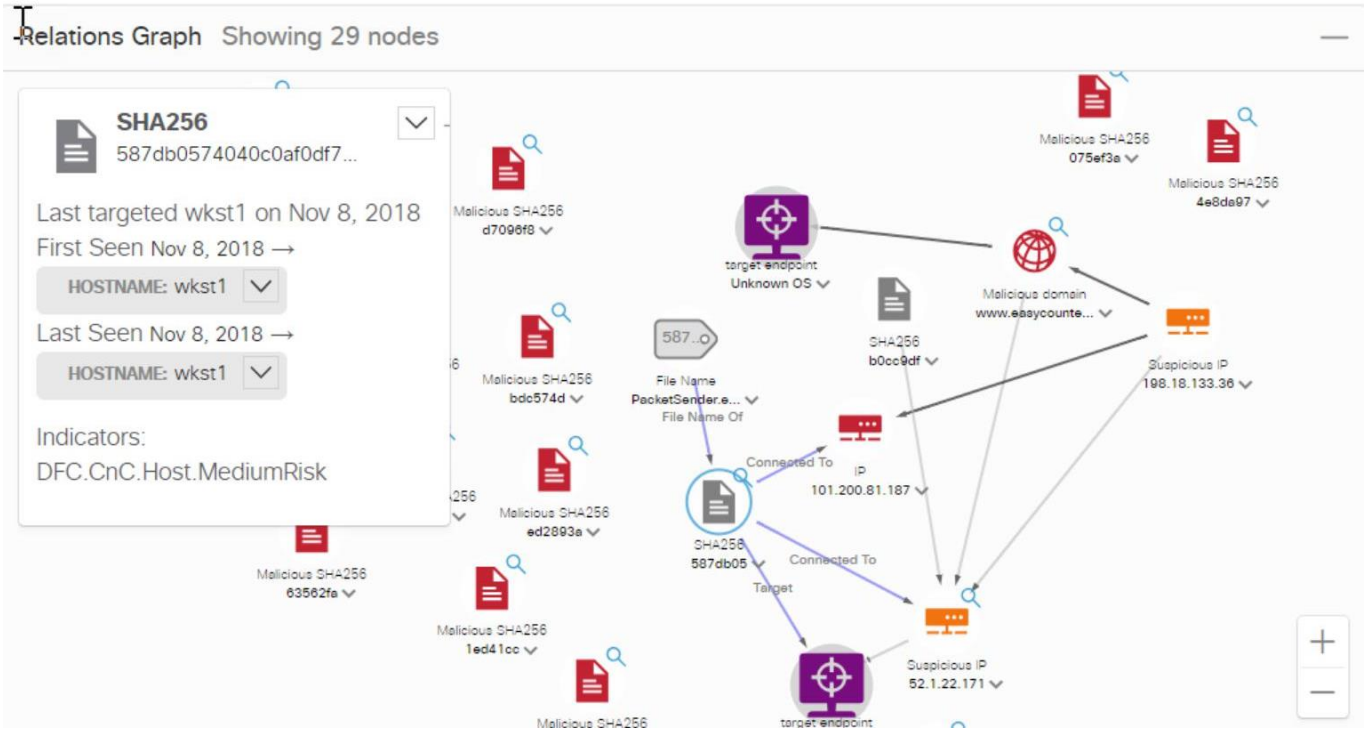
11. おそらくもっと重要なのは、ネットワークに接続されている不明な項目について詳細を把握することです。




12. その項目の詳細情報を得るには、その名前の横にある三角形をクリックし、メニューから [調査に追加（Add to Investigation）] を選択します。

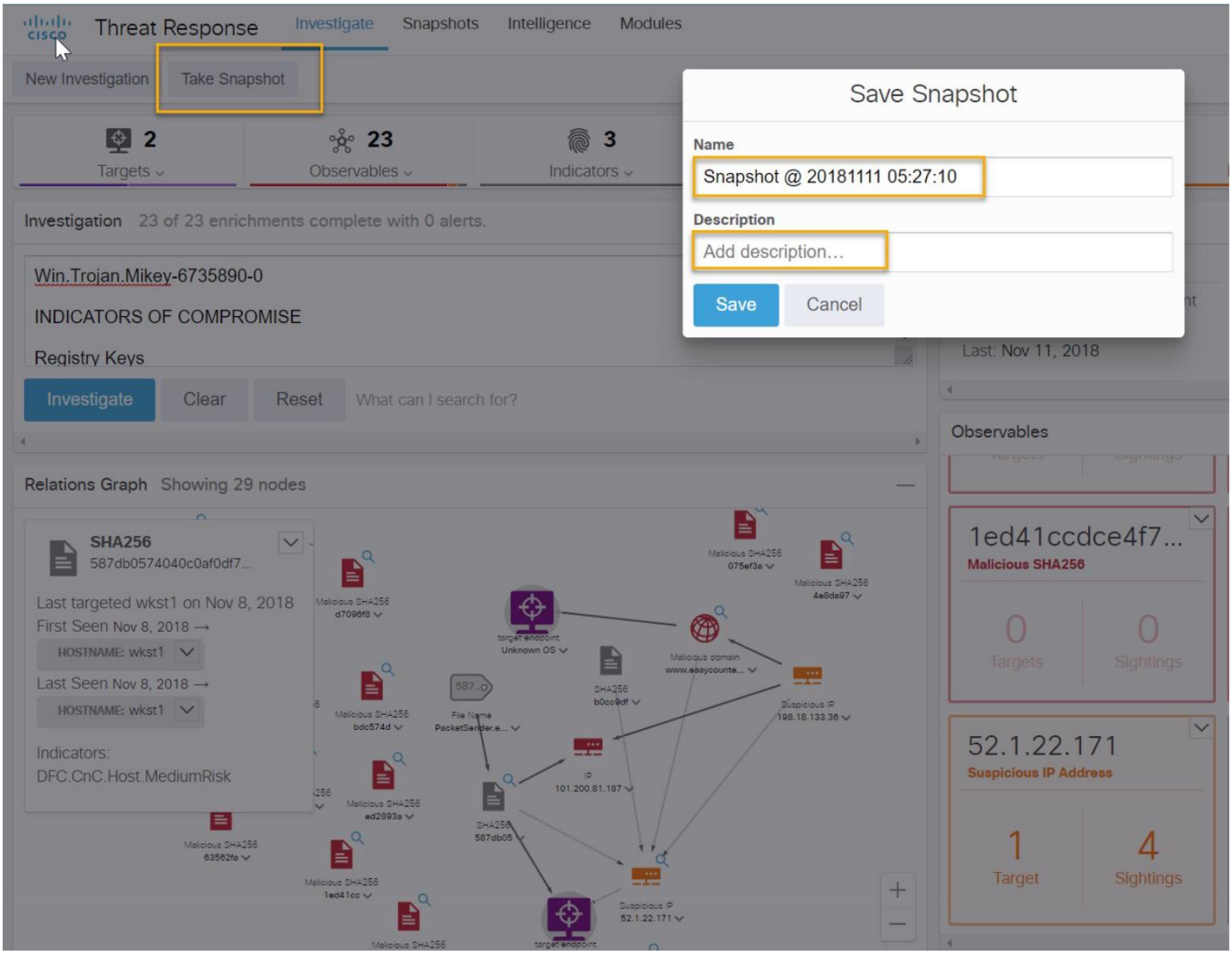


13. ファイルのハッシュ値と同様に、監視対象の数が 1 つずつ増えているのがわかります。また、[関係グラフ（Relations Graph）] も更新されていることに注意してください。

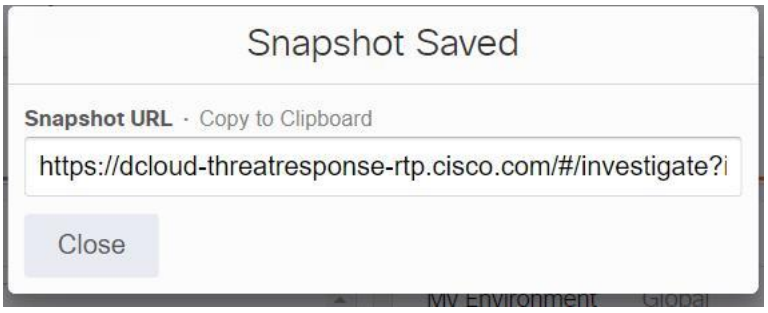


## 記録

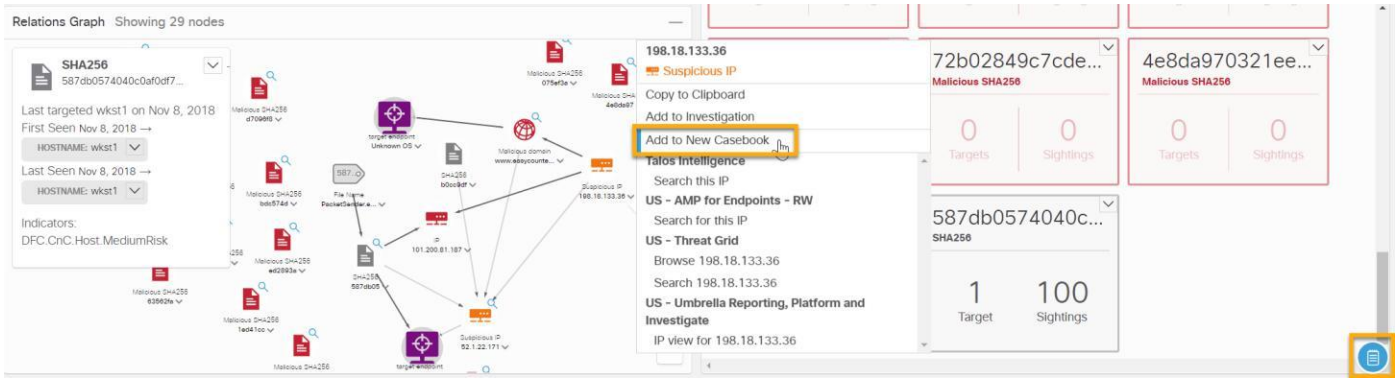
1. そのファイルに関する新しい情報を使って、検出した内容を文書化する場合があります。そのためには、最初に、画面の上部の [スナップショットの作成（Take Snapshot）] ボタンをクリックします。これで、ファイルを説明付きでローカルに保存できます。



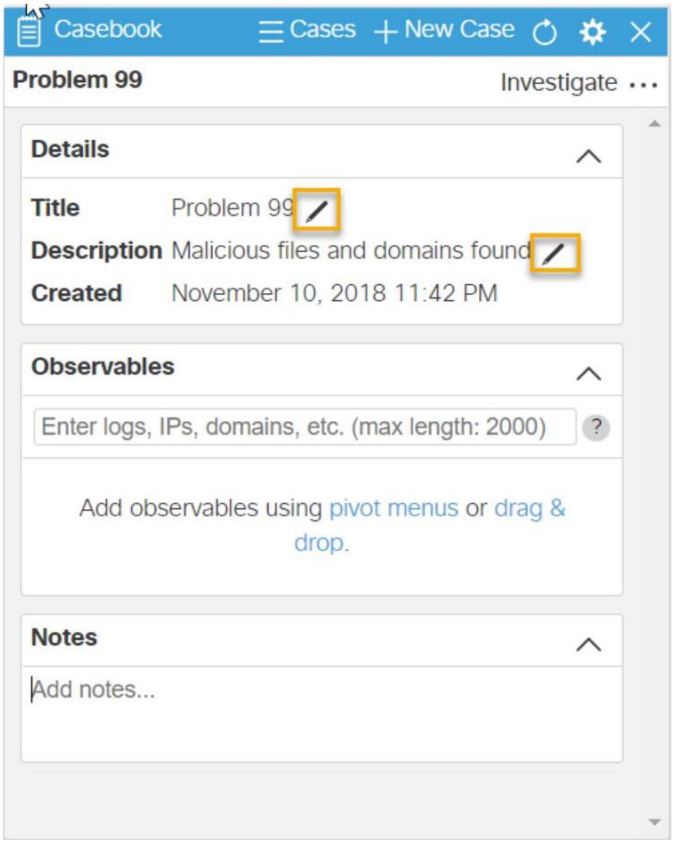

[保存（Save）] をクリックすると、情報を確認できる URL が示されます。



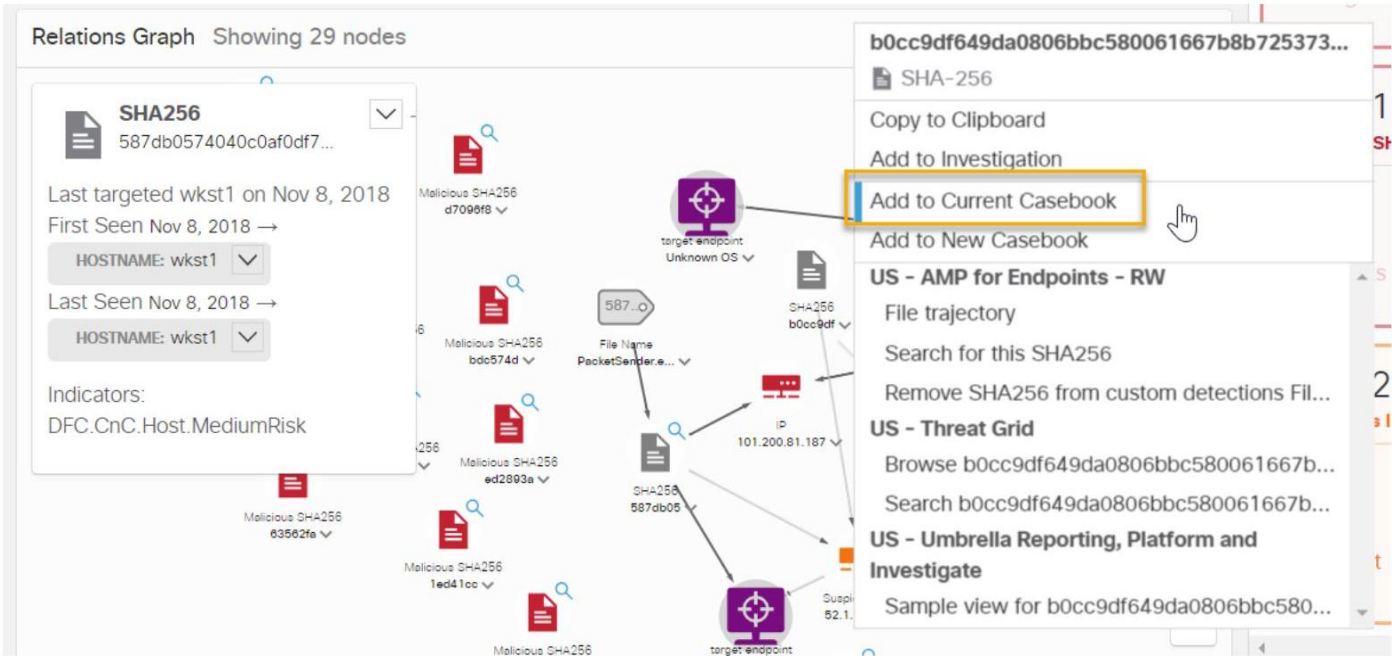
2. または、特定のインシデントを含むすべての証拠を示すケースファイルを作成することができます。この操作は、ウィンドウの右下隅の青い [ケースファイルの作成（Create Casefile）] ボタンまたは [関係グラフ（Relations Graph）] のいずれかの項目から実行できます。




3. ケースファイルを最初に開くときに、[詳細（Details）] セクションでカスタムのタイトルと説明を作成できます。

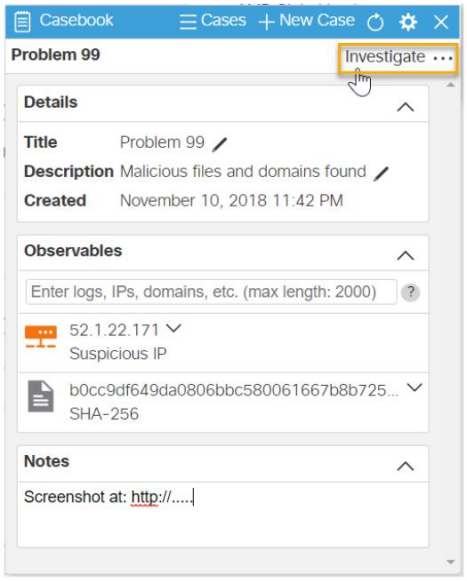


4. [関係グラフ(Relations Graph)] または [監視対象(Observables)] ペインにある項目のいずれかのドロップダウン メニューから [監視対象(Observables)] セクションに項目を追加します。




5. 以前使用したスナップショットの URL を含む他のメモをケースブックの下部にある [メモ(Notes)] ペインに追加できます。

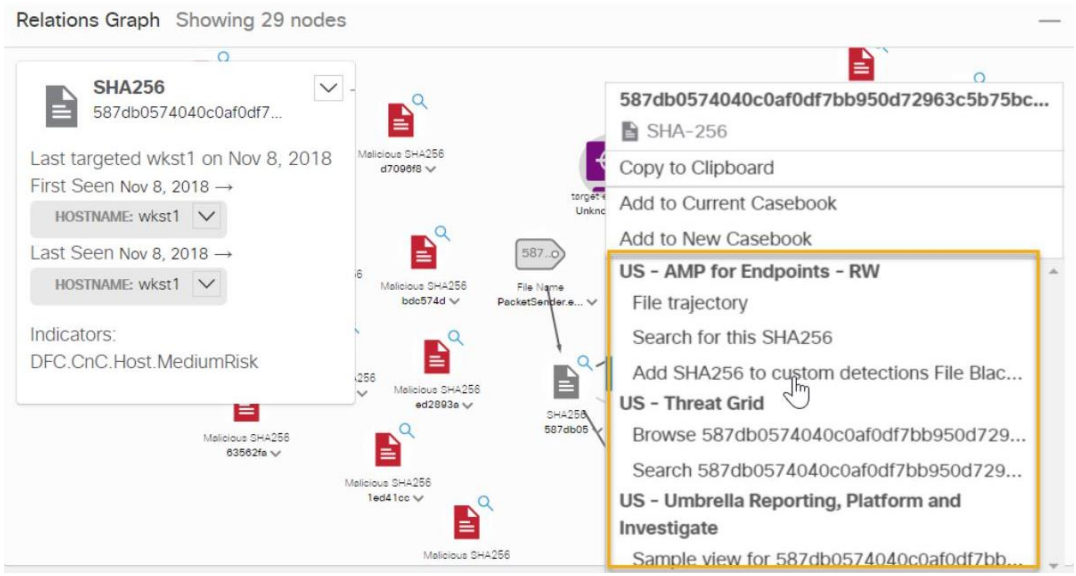
6. その後、そのケースブックを開き、ケースブックの上部にある [調査...(Investigate...)] をクリックして、Threat Response で含まれているすべての監視対象を新たに検索できます。



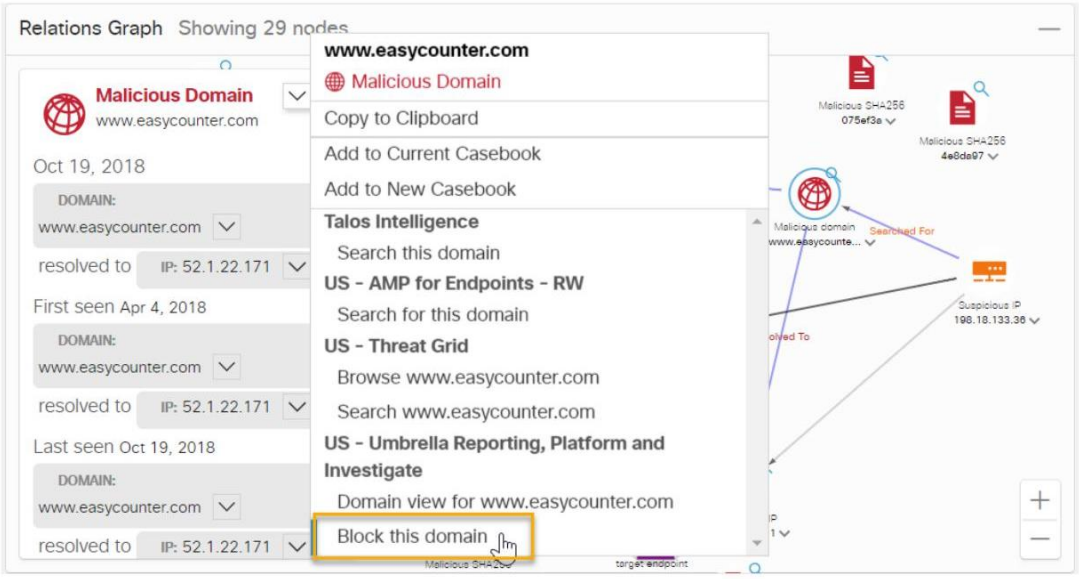

**注:**リンクをクリックすると、デモンストレーション環境から外れてライブの製品アドレスに移動するため、このデモンストレーションで機能しなくなります。

## 脅威のブロック

1. 状況を把握し、文書化したので、次は問題の解決を行います。[関係グラフ(Relations Graph)] または [監視対象(Observables)] ペインで、項目の横にある矢印をクリックしてそのオプション リストをもう一度取得します。




2. 強調表示されているエリアには、使用している他のソフトウェアで API を使って実行できる内容が示されています。上記の例では、エンドポイントを AMP for Endpoints のブロック リストに追加できます。以下は、Umbrella でドメインをブロックする方法を示す例です。




**注:** 他のユーザが同時にこのデモにログインしている可能性があります。他のユーザがすでに項目をブロックしている場合、そのオプションは表示されませんが、ブロック リストからその項目を削除するオプションは示されます。項目の削除や追加は自由に実行できます。

## まとめ

シナリオ 1 に用意されているデモンストレーションは、潜在的な脅威をブロックする Threat Response インターフェイスのシンプルなウォールスルーです。さらに詳しく学習する場合、各ドロップダウン メニューの他のオプションもデモンストレーションで利用できます。いくつかのオプションでは、製品を実行したまま他のブラウザ タブに移動します。これらすべての製品で利用できるすべての機能の完全なウォークスルーはこのドキュメントに含まれていませんが、これらの各製品の詳細は、それぞれの dCloud デモンストレーションで確認できます。



お問い合せ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp