CISCO
SECURE

cisco The bridge to possible

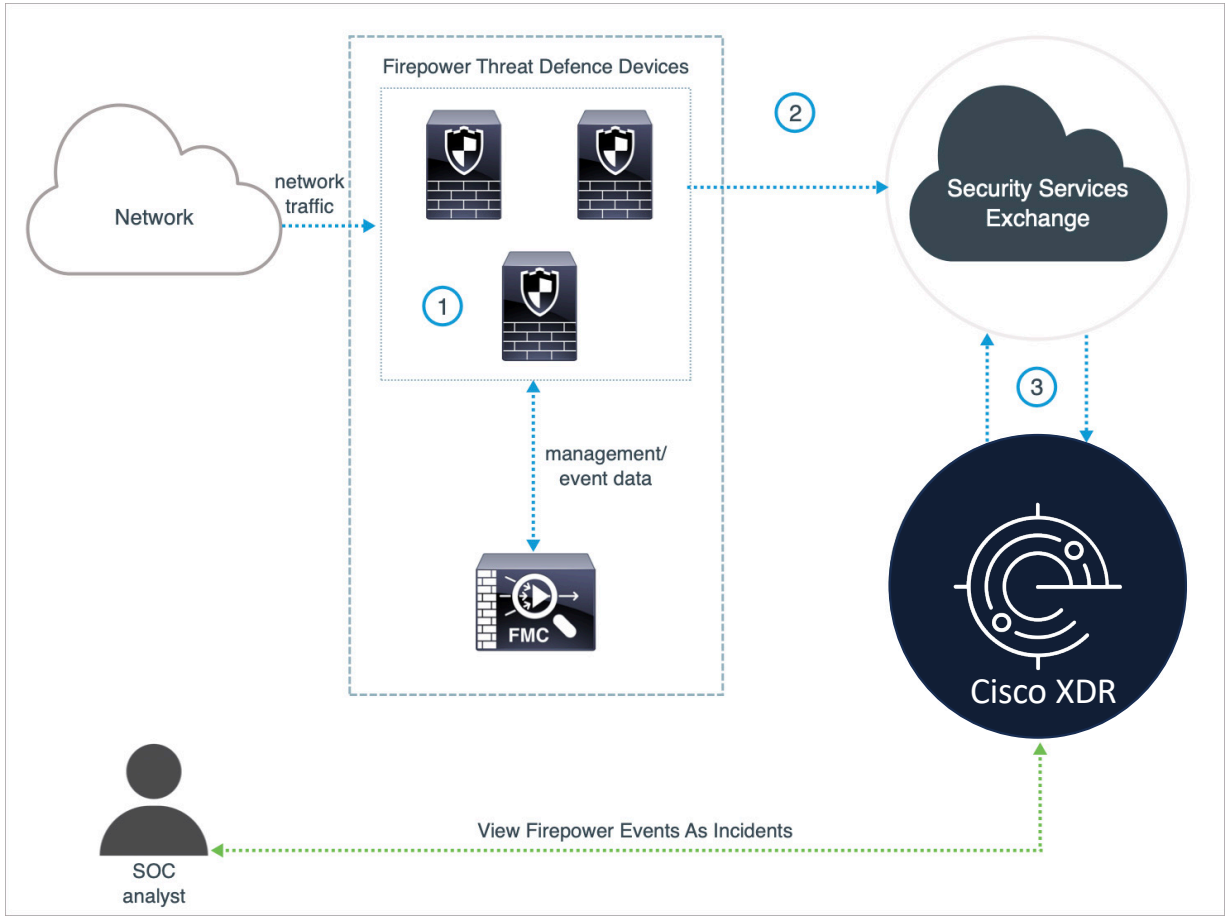
PSU VoD

Cisco XDR
製品統合ガイド
Firewall Threat Defense 編

2024年3月

シスコシステムズ合同会社　セキュリティ事業

XDR – Firewall Threat Defense
構成と動作の仕組み



動作概要

1) FMC で管理している FTD デバイスがイベントを生成
2) FTD デバイスが、サポートされているイベントを Security Service Exchange (SSX) に送信
3) XDR が検出情報を SSX に照会し、XDR にイベントやインシデントとして表示

XDR – Firewall Threat Defense
本ガイドでの条件

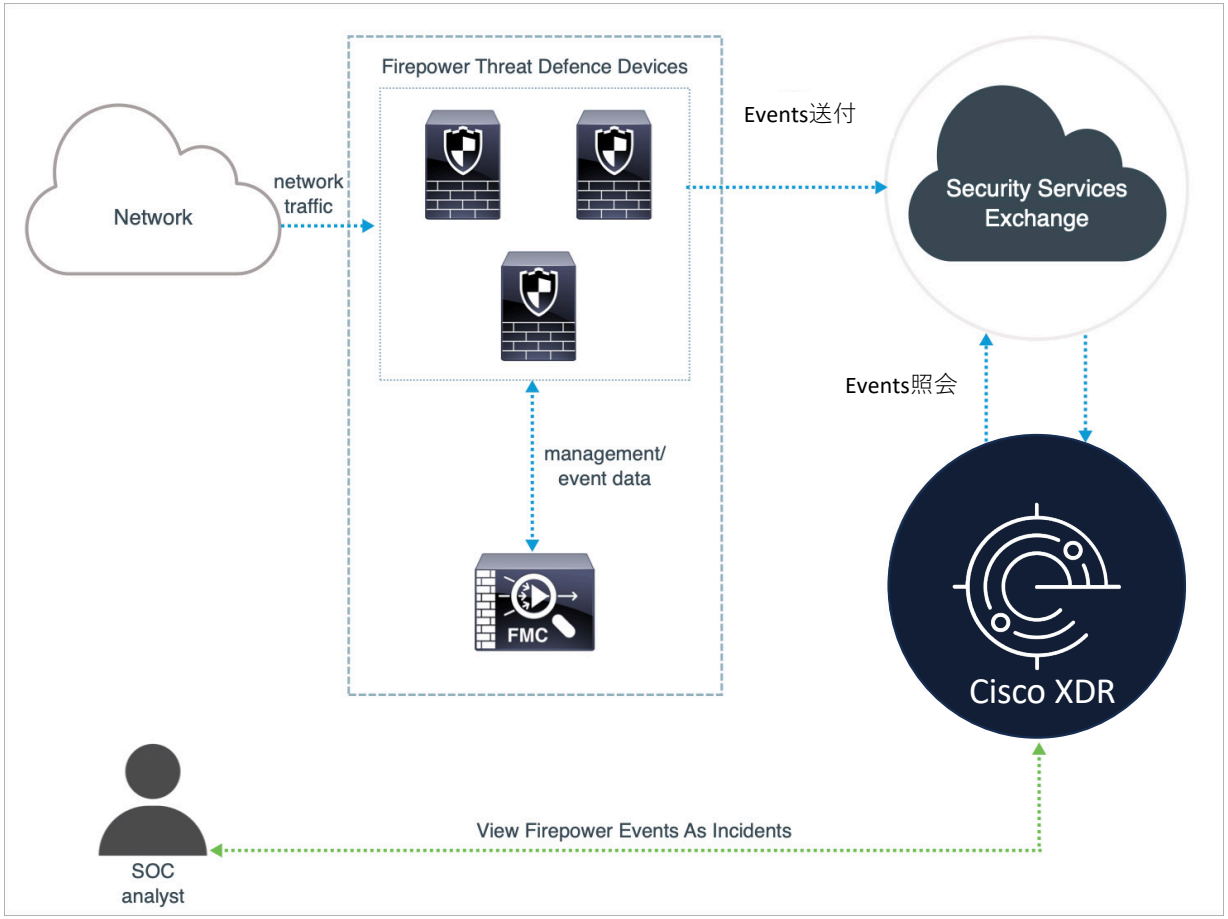
- FMC 管理の FTD と XDR の連携方法を解説
  FDM 管理でも XDR との連携は可能だが本ガイドでは割愛

- FMC / FTD バージョン 7.2 以降で、FTD と XDR が直接連携する方法を解説
  Syslog 経由であればバージョン 6.3 から、直接連携であればバージョン 6.4 から FTD と XDR との連携は可能だが、バージョン 7.2 以降の直接連携が最もシンプルでわかりやすいので、本ガイドはその方法の解説に注力

- FMC でレジストしている Smart Account の Virtual Account に管理者権限が必要
  評価期間中の FMC / FTD (Smart License 未登録) では連携設定不可

- XDR と CDO のテナントが必要

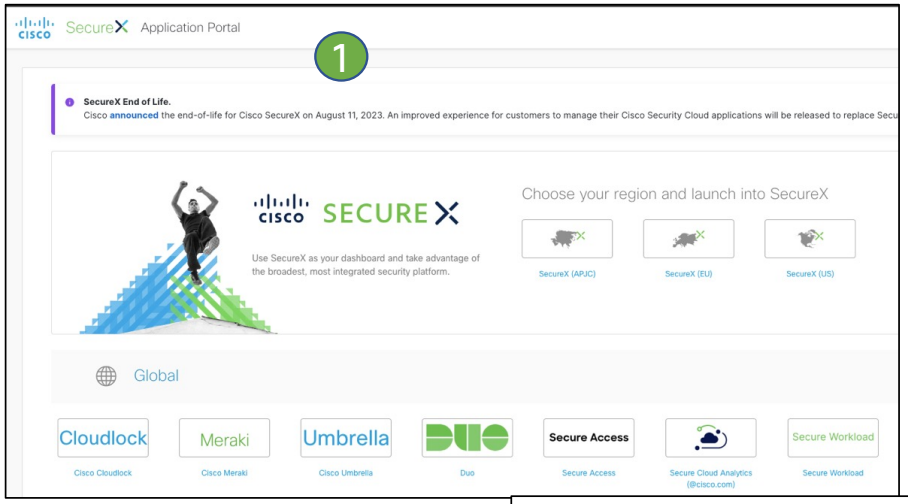
XDR – Firewall Threat Defense
設定手順の流れ



設定手順

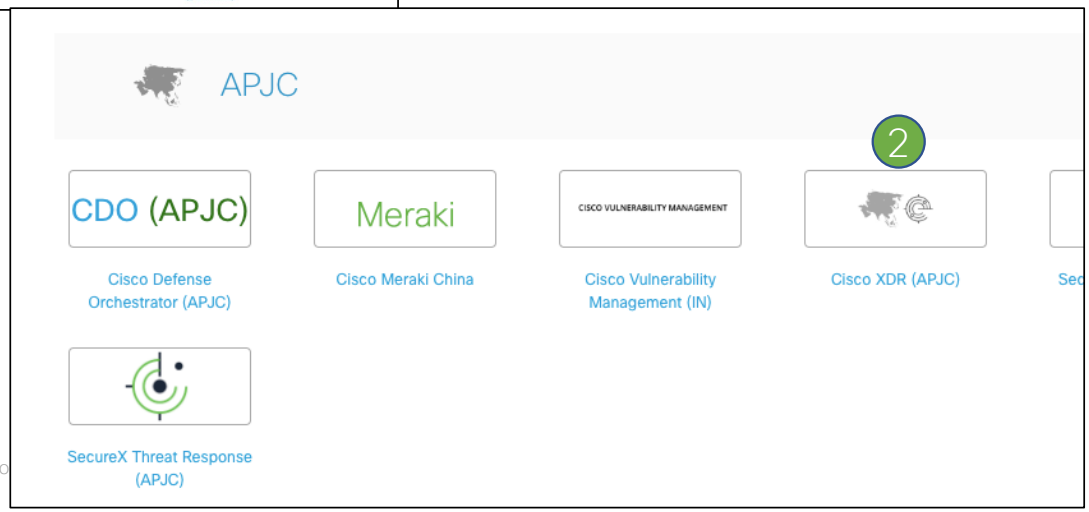
1) Security Services Exchange (SSX) **にて** Smart Account **を紐付け**
2) Firewall Management Center (FMC) **にて** XDR **との連携設定**
3) XDR **管理コンソールにて** Secure Firewall (FTD) **インテグレーションの確認**
4) **動作確認**

設定1) SSX で Smart Account の紐付け

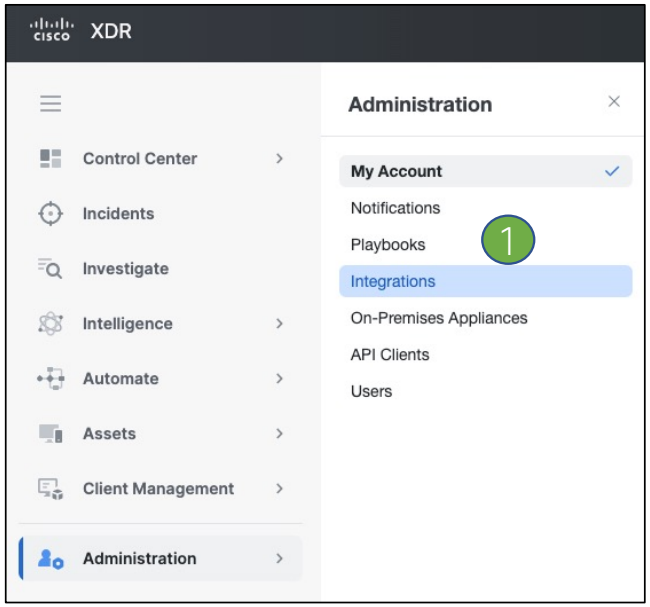


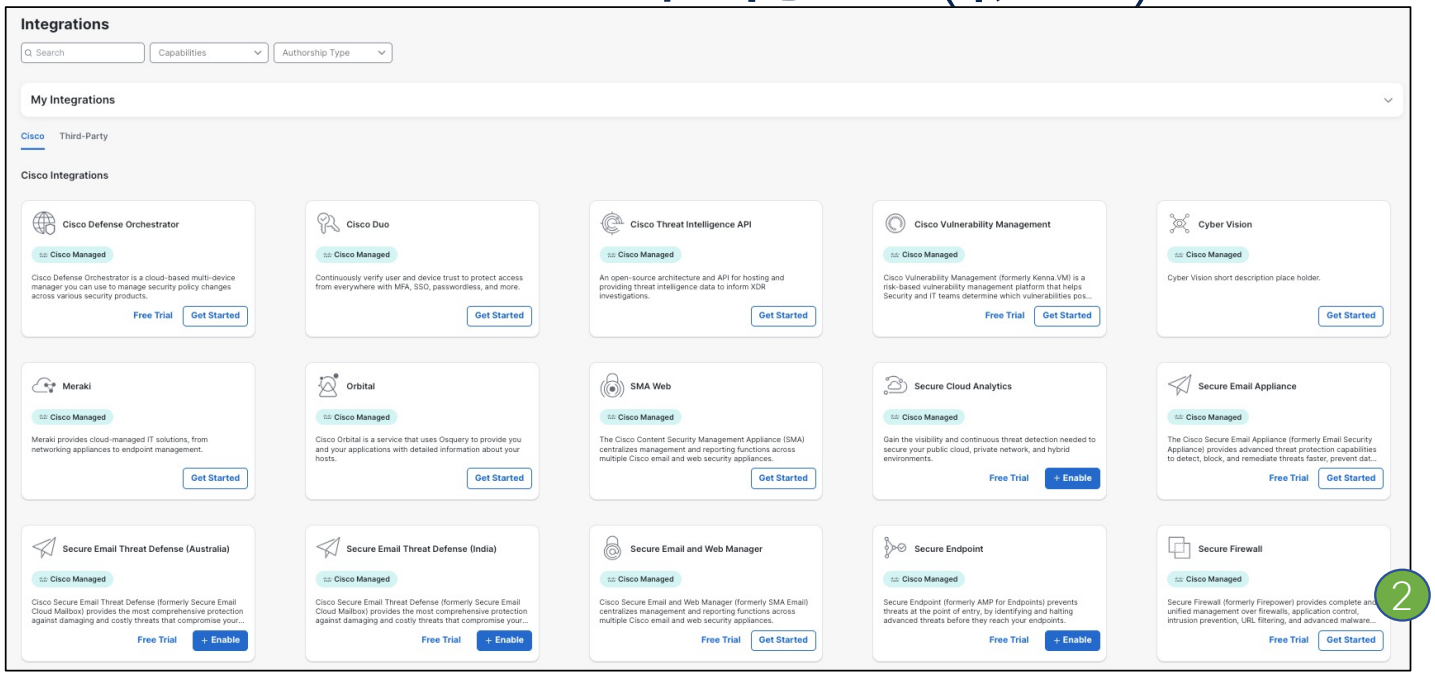
1 Cisco Security Cloud にログイン
https://sign-on.security.cisco.com

2 使っているデータセンターの XDR をクリックして XDR 管理画面にログイン (本ガイドでは APJC)



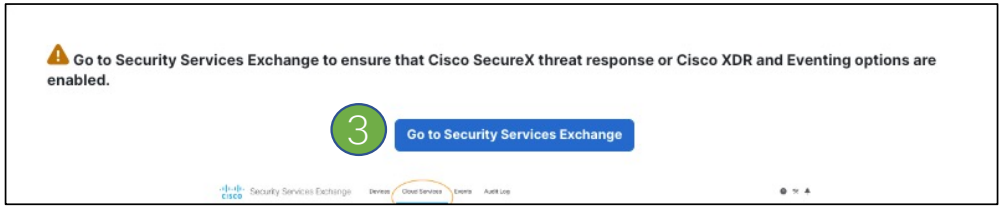
設定1) SSX で Smart Account の紐付け (続き)





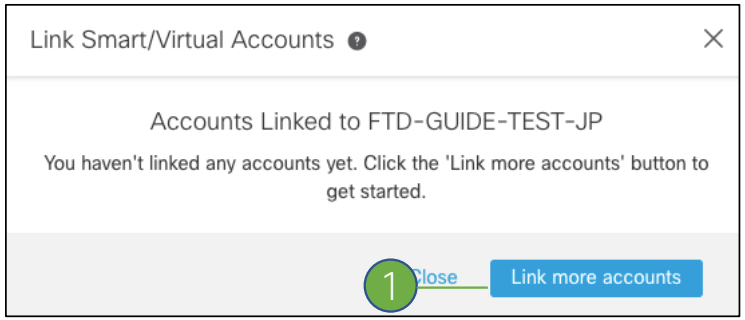
1 XDR 画面左メニューより Administration → Integration をクリック

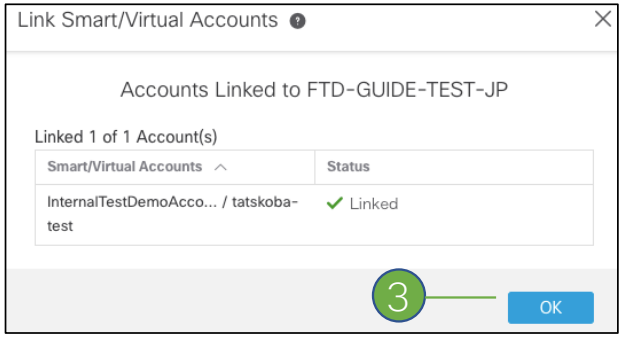
2 Cisco Integrations から Secure Firewall の Get Started をクリック

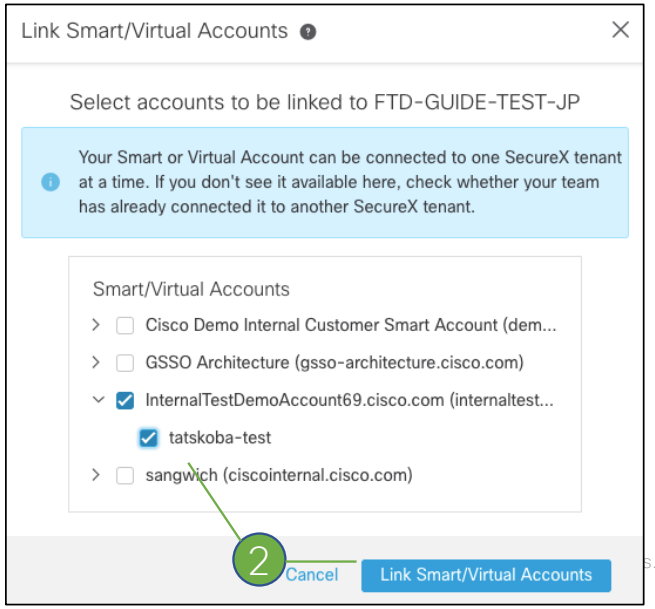


3 Go to Security Service Exchange をクリック

設定1) SSX で Smart Account の紐付け (続き)

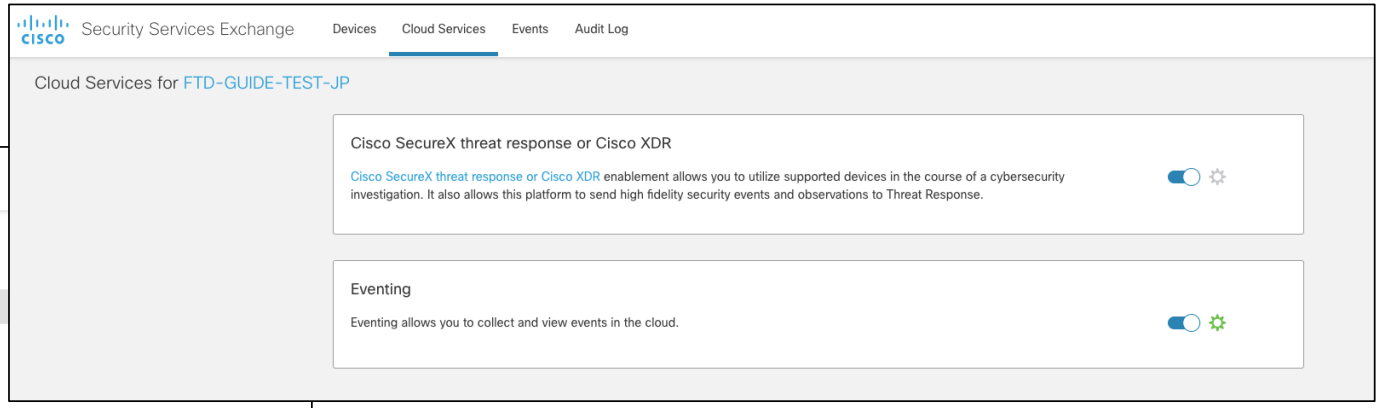


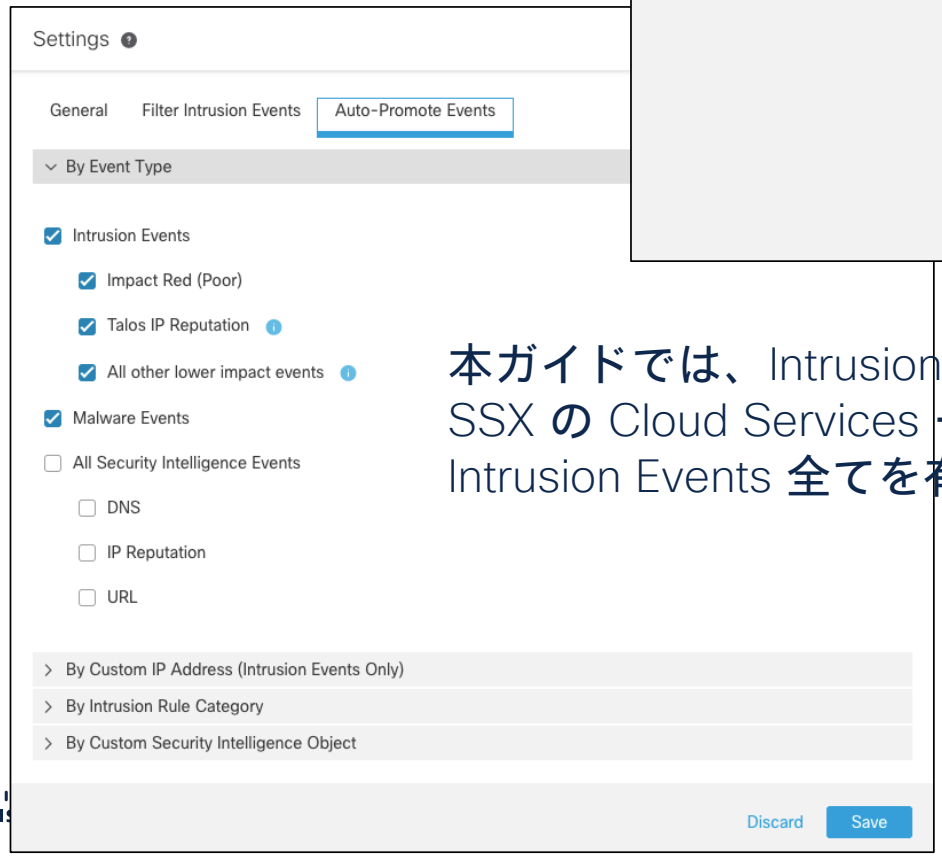




1. Link More accounts をクリック
2. FMC にてレジストしている Virtual Account (要管理者権限) を選択して Link Smart/Virtual Accounts をクリック
3. Smart/Virtual Account が SSX に紐付いたことを確認して OK をクリック

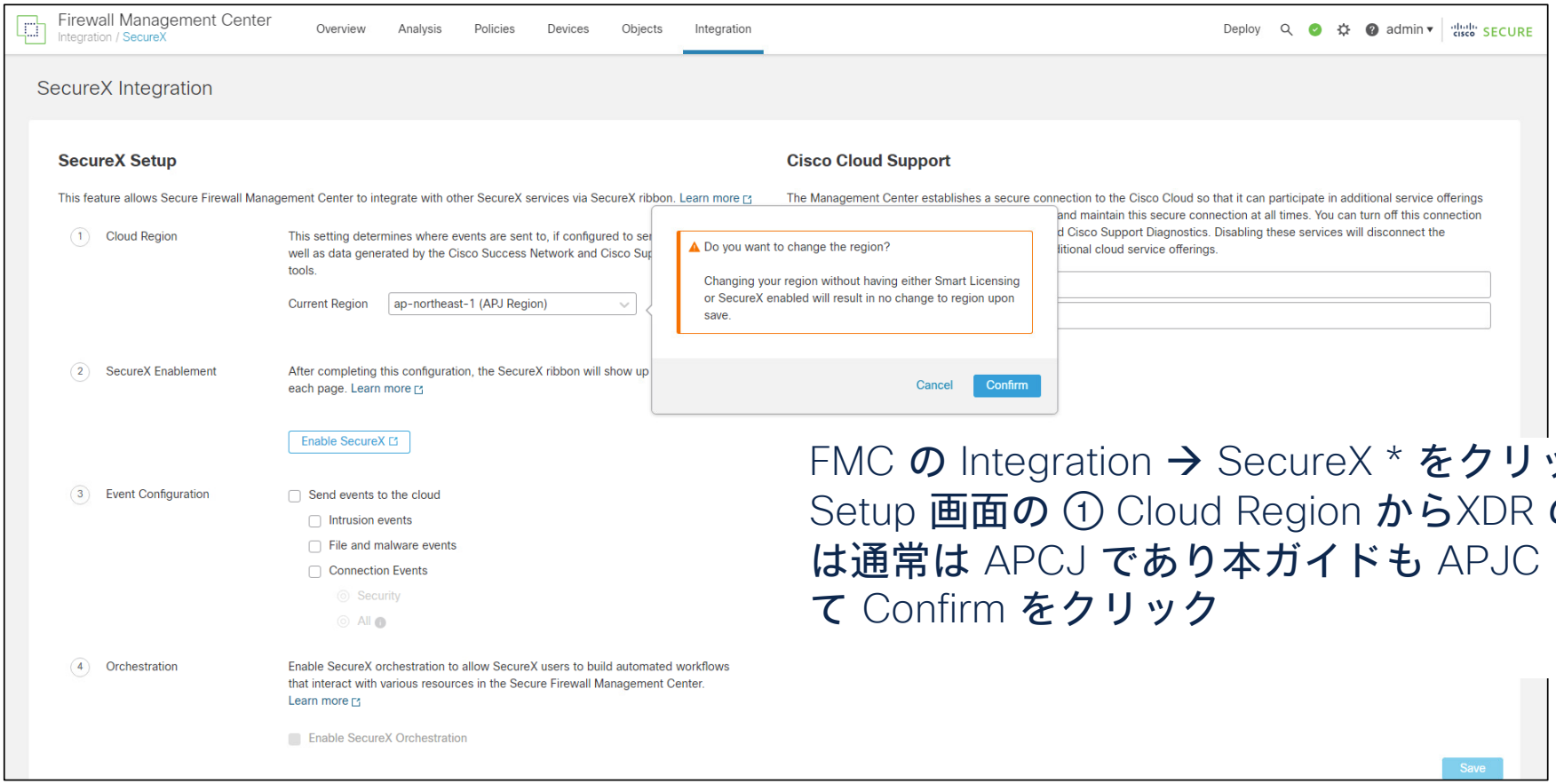
補足) SSX でのイベントプロモート





本ガイドでは、Intrusion Event を全て SSX 経由で XDR で解析するため、SSX の Cloud Services → Eventing を有効にして Auto-Promote Events で Intrusion Events 全てを有効にしておくこと

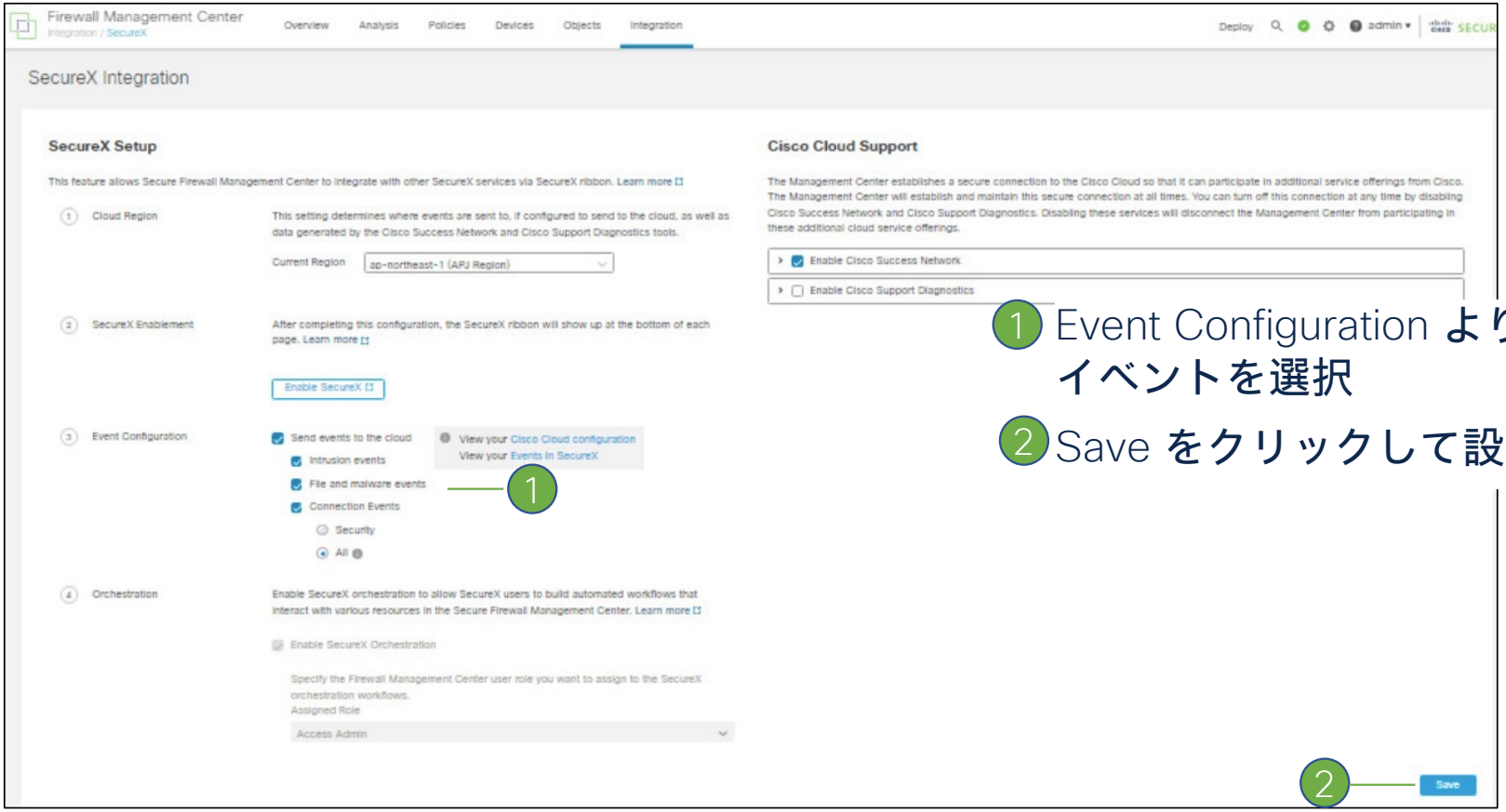
設定2) FMC にて XDR 連携を設定



FMC の Integration → SecureX * をクリック、SecureX Setup 画面の ① Cloud Region からXDR の Region (日本では通常は APCJ であり本ガイドも APJC を利用) を選択して Confirm をクリック

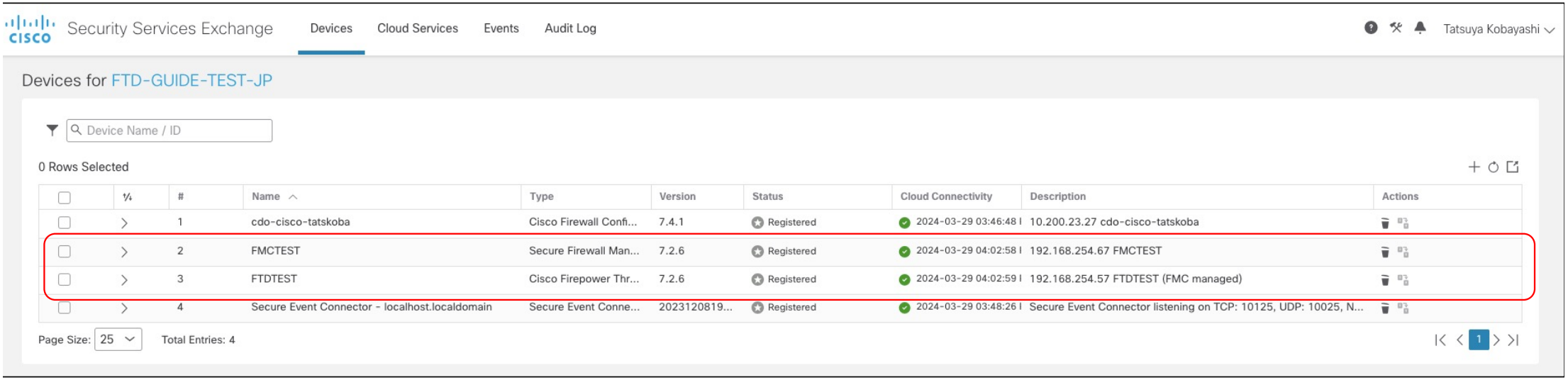
SE*注) FMC での XDR 連携設定のメニューは、まだ SecureX という表記になっている

設定2) FMC にて XDR 連携を設定 (続き)



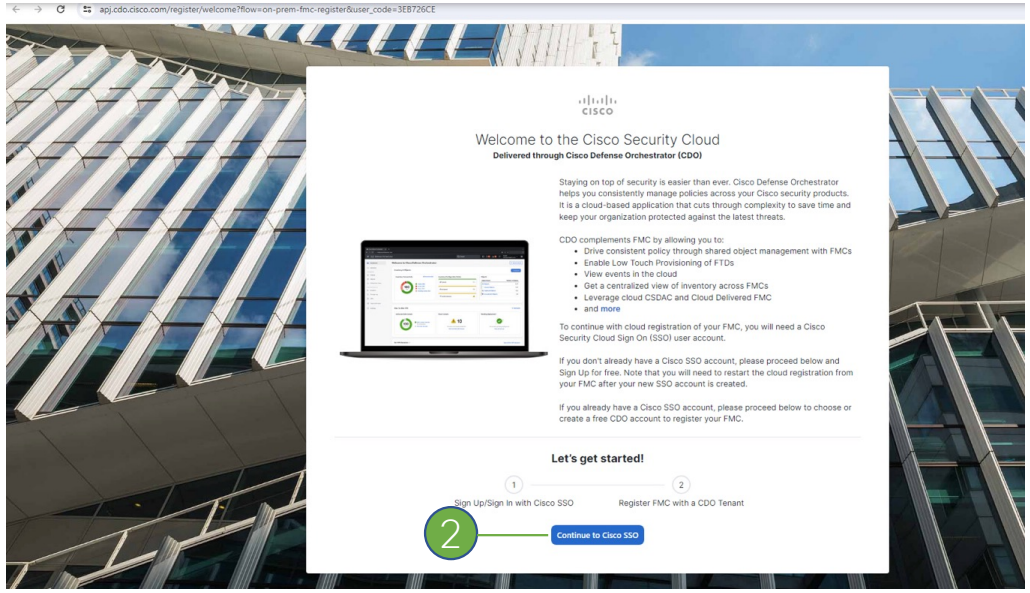
1. Event Configuration より XDR (SSX) に送りたいイベントを選択
2. Save をクリックして設定を反映させる

設定2) FMC にて XDR 連携を設定 (続き)



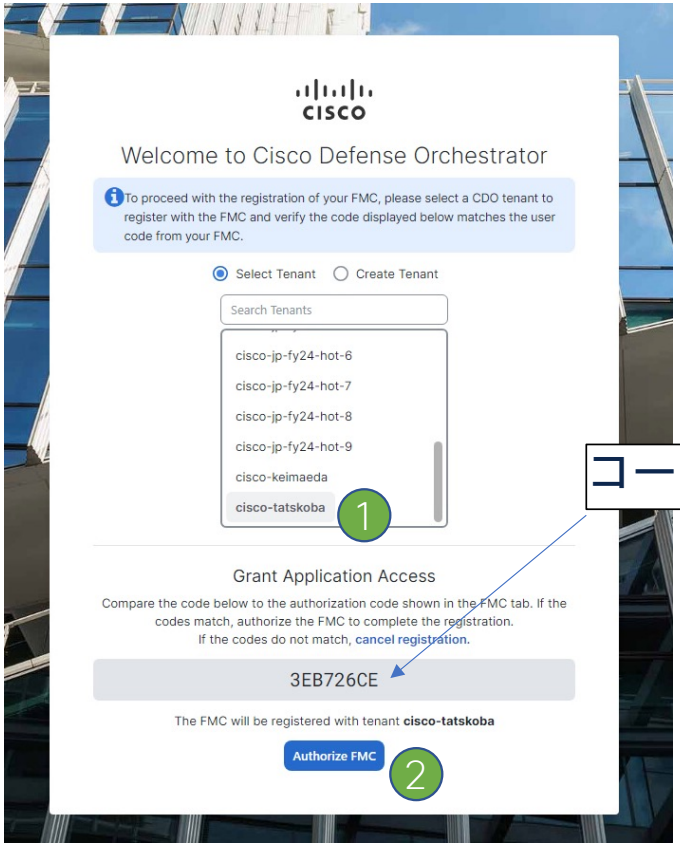
FMC 側での Cloud Region 指定が終わると、SSX の Devices の画面に、FMC と FTD デバイスの一覧が表示される

設定2) FMC にて XDR 連携を設定 (続き)

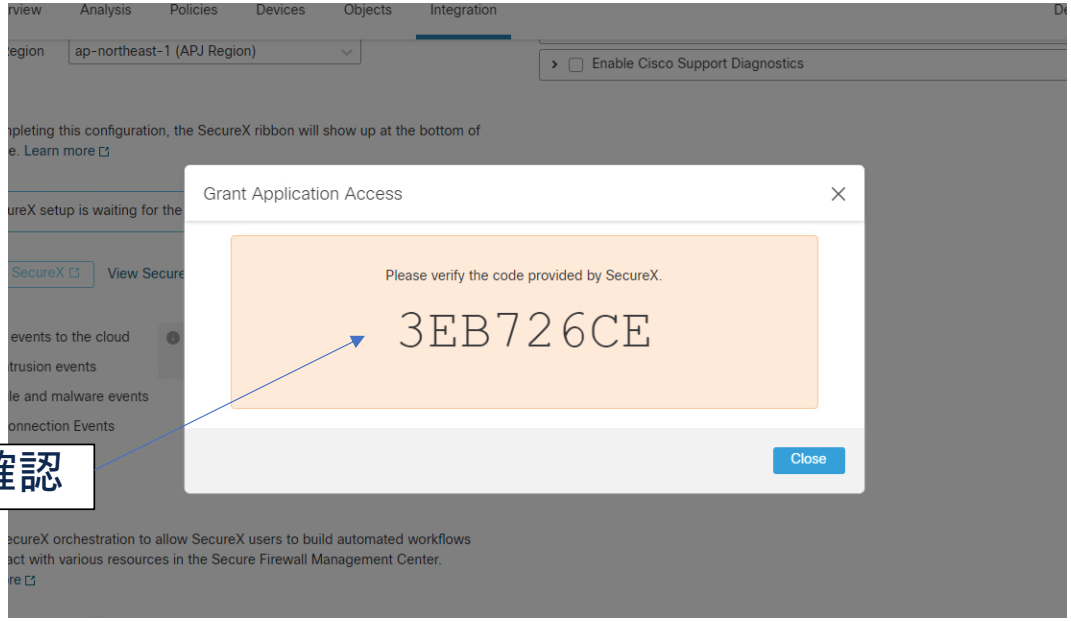


1. FMC に戻って ② SecureX Enablement にある Enable SecureX というボタンをクリック
2. ブラウザ内で新たなタブが起動、Continue to Cisco SSO をクリック、Cisco Security Cloud へのログインを行う

設定2) FMC にて XDR 連携を設定 (続き)

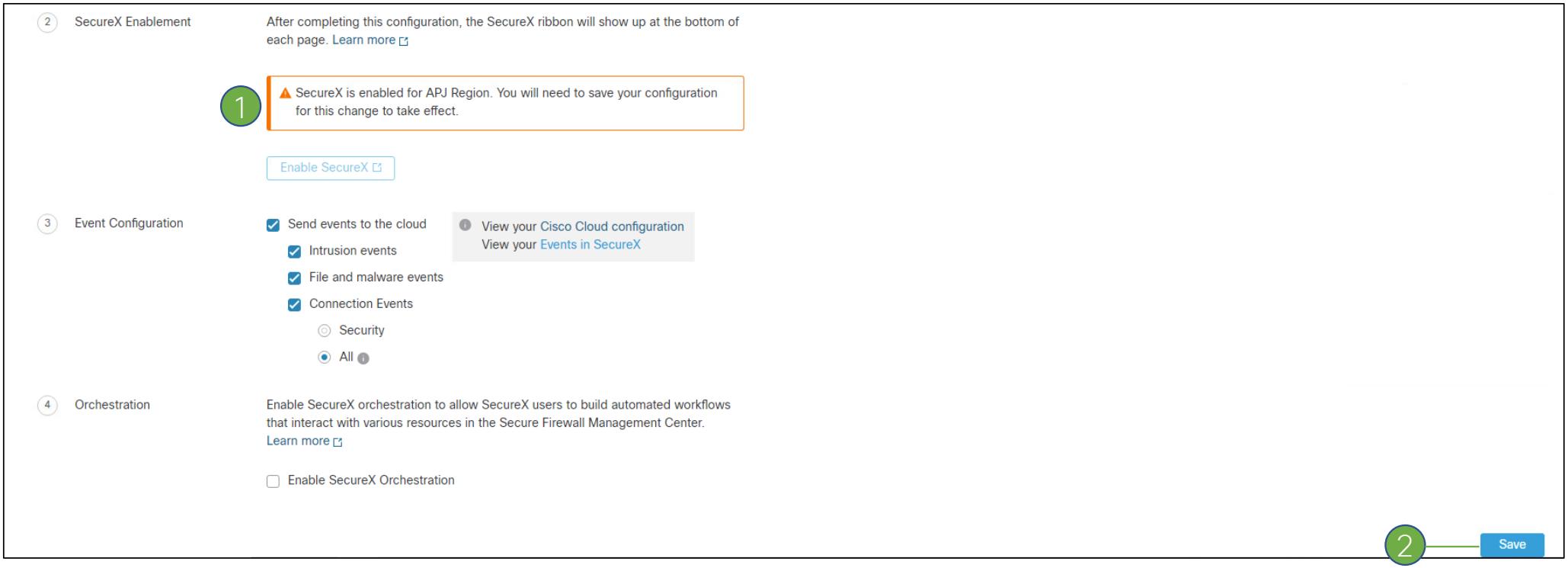


コードの合致を確認



1. Cisco Security Cloud にログイン後、利用する　CDO のテナントが表示される (複数のテナントがあれば複数が表示されるので利用するテナントを選択)
2. 画面下部に表示されたコードと、FMC の画面に表示されているコードが合っていることを確認して Authorize FMC をクリック

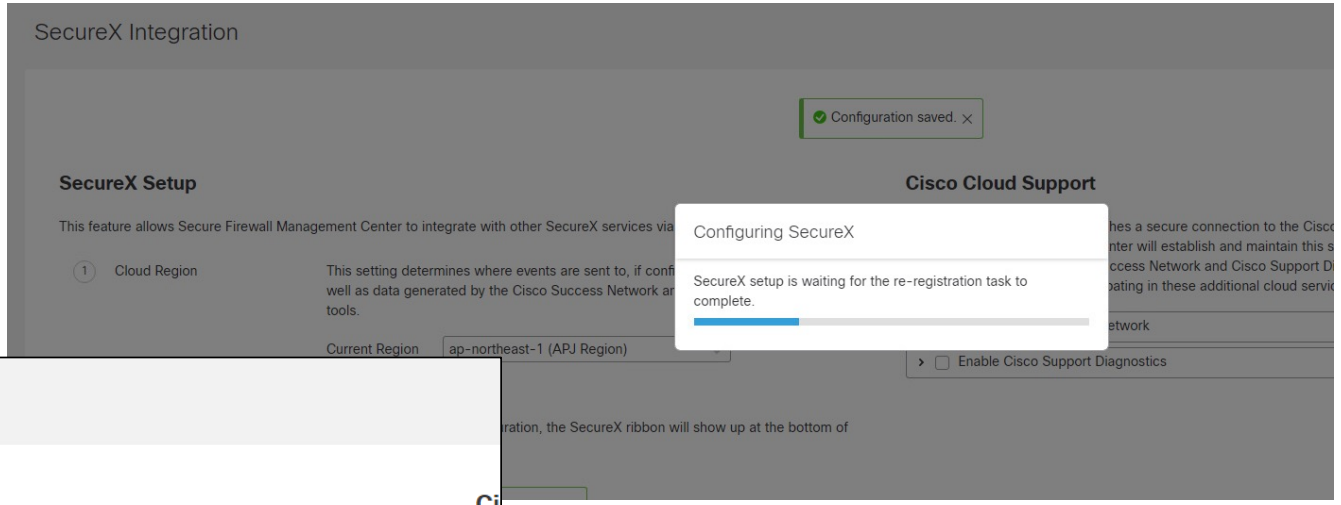
設定2) FMC にて XDR 連携を設定 (続き)

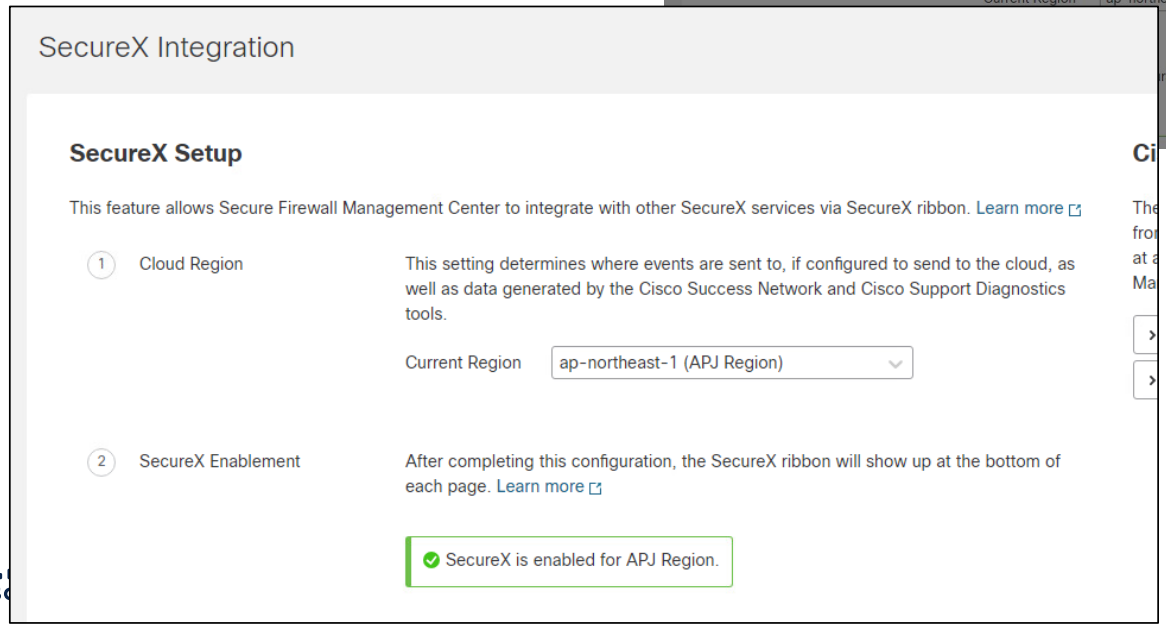


1. Authorized FMC が終わると Region で XDR (表示は SecureX) が Enable になった旨のメッセージが表示される
2. Save をクリックして設定を保存

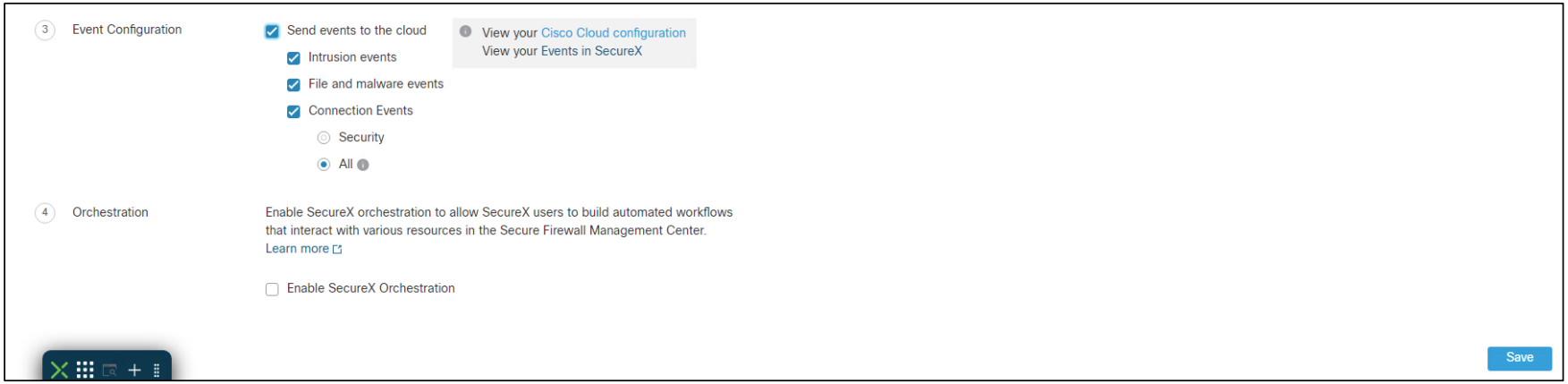
設定2) FMC にて XDR 連携を設定 (続き)

XDR へのレジストが終わり、XDR が有効になった旨のメッセージ (表示は SecureX) が表示される

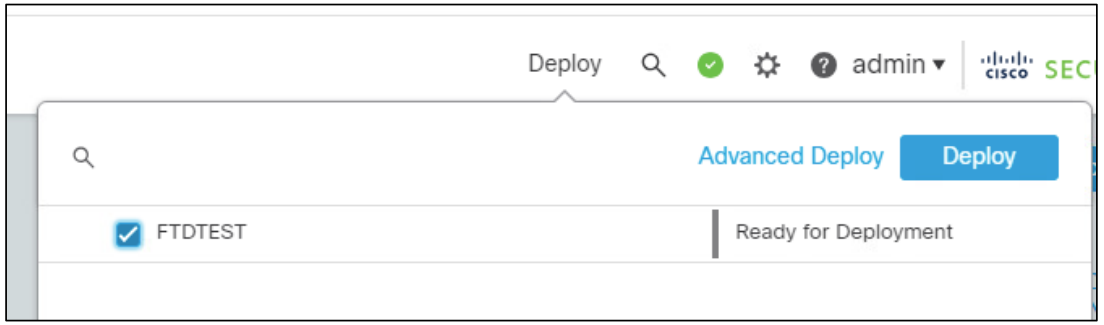




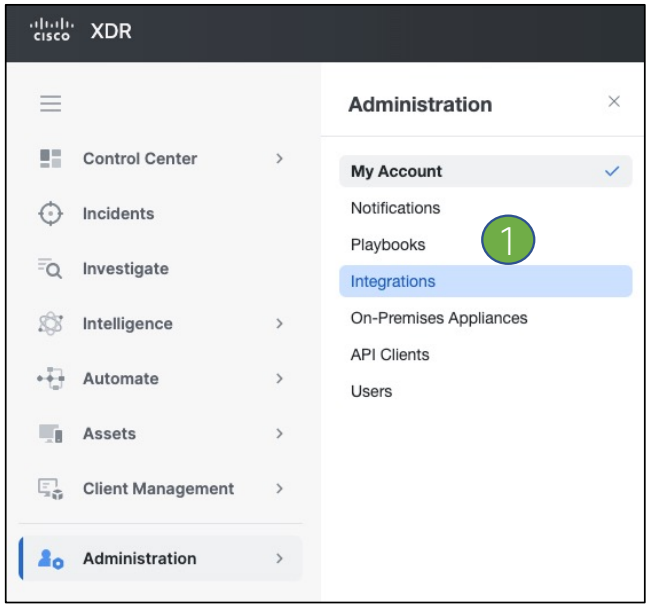
設定2) FMC にて XDR 連携を設定 (続き)



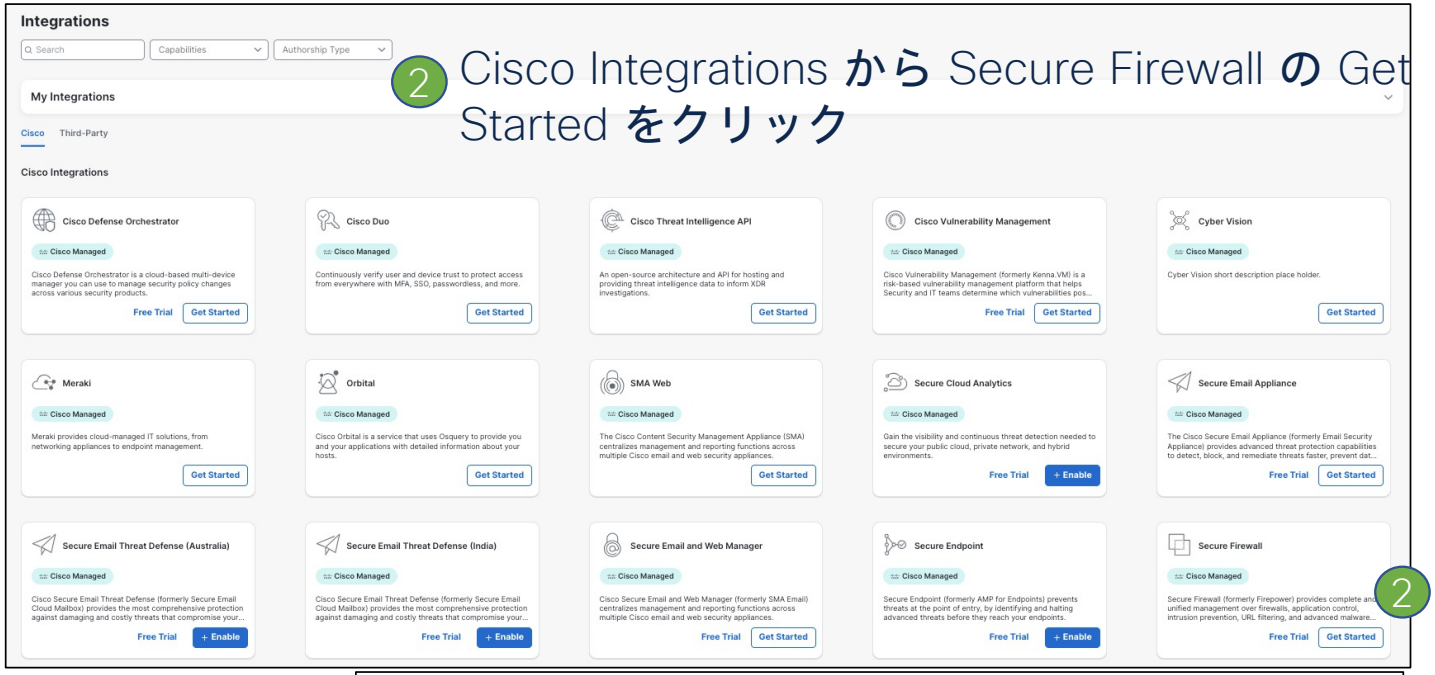
Security Events を Cloud に送る設定になっていることを確認 (なっていなければ再度設定して Save) し、Deploy を実施



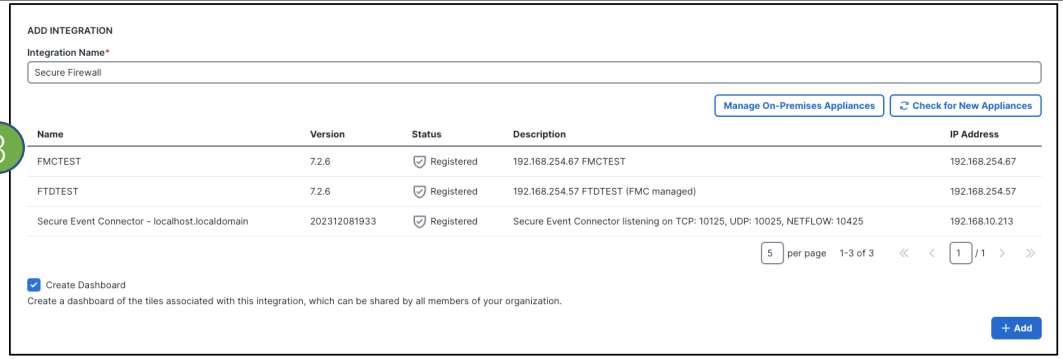
設定3) XDR にて FMC & FTD の登録を確認



1 XDR 画面左メニューより Administration → Integration をクリック

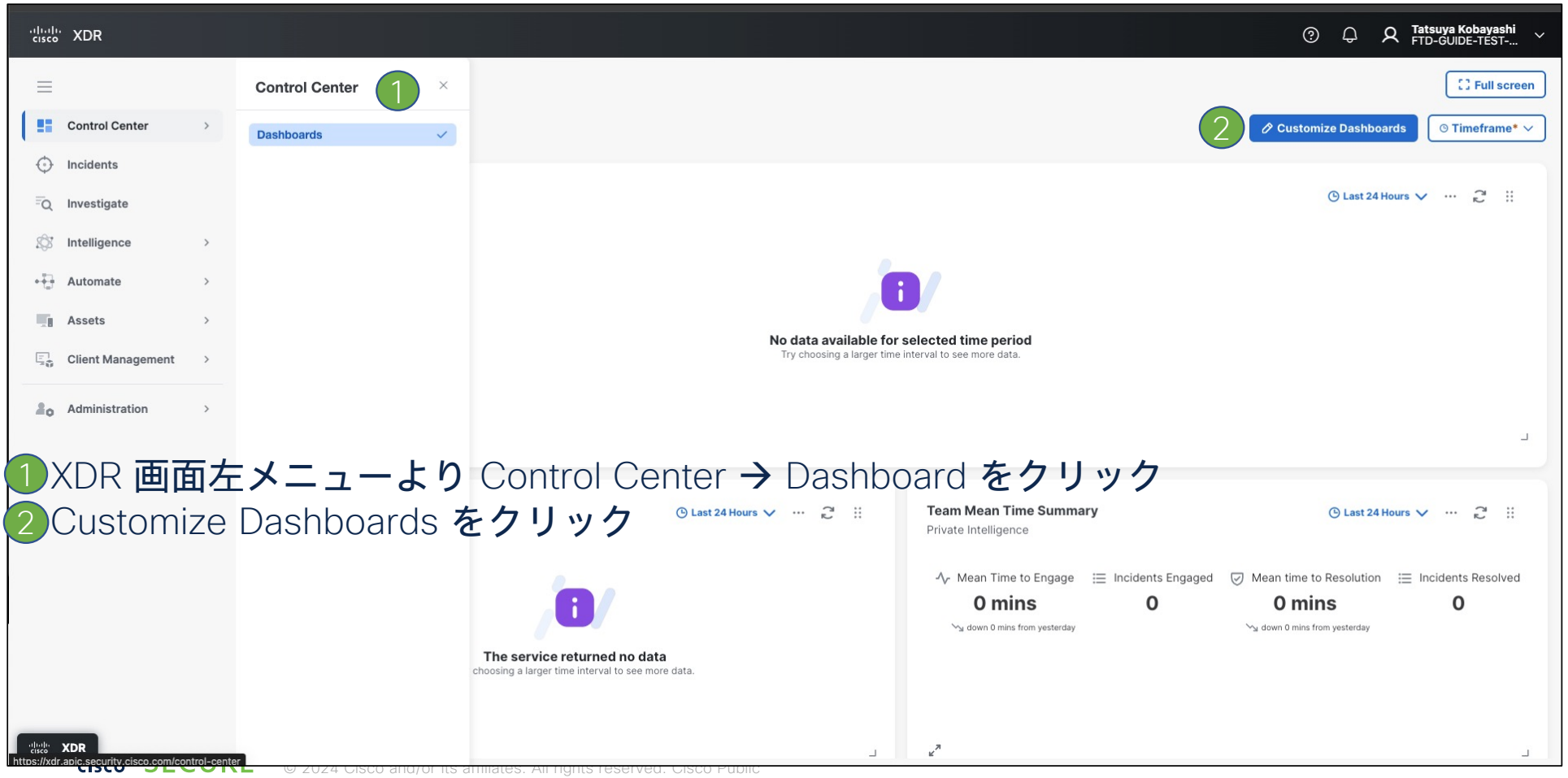


2 Cisco Integrations から Secure Firewall の Get Started をクリック



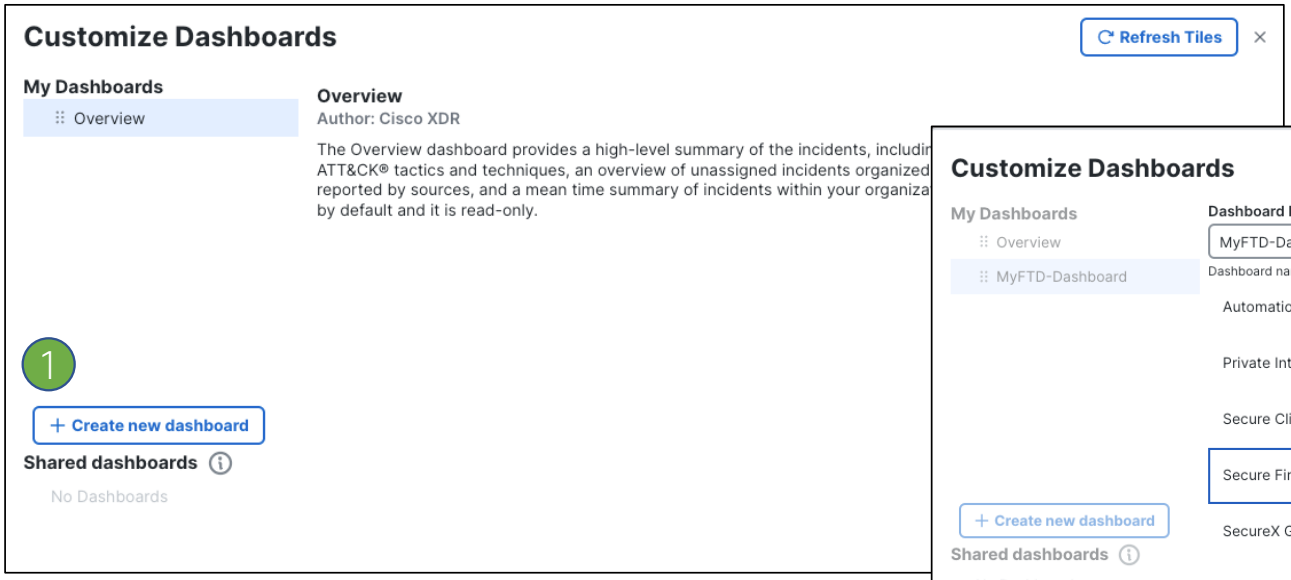
3 FMC と FTD が登録されていることを確認

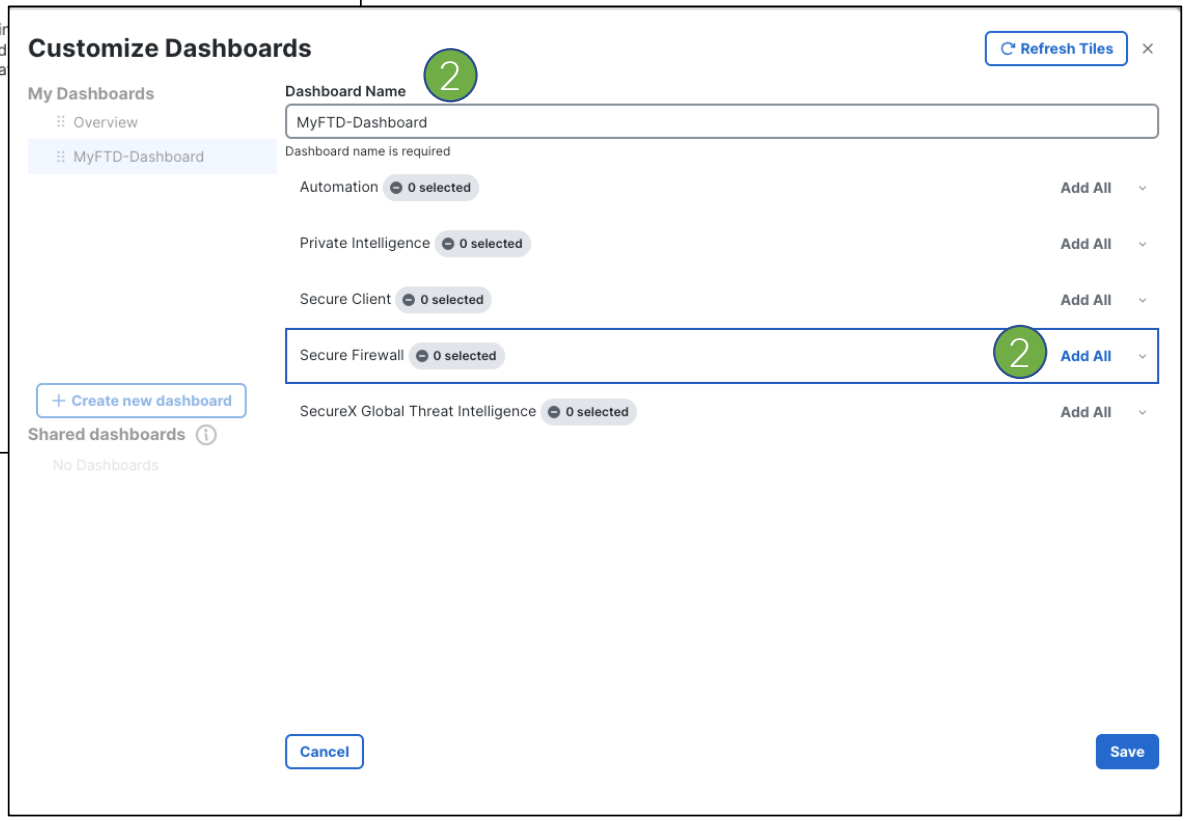
設定4) XDR にて FTD Dashboard を作成



1 XDR 画面左メニューより Control Center → Dashboard をクリック
2 Customize Dashboards をクリック

設定4) XDR にて FTD Dashboard を作成 (続き)





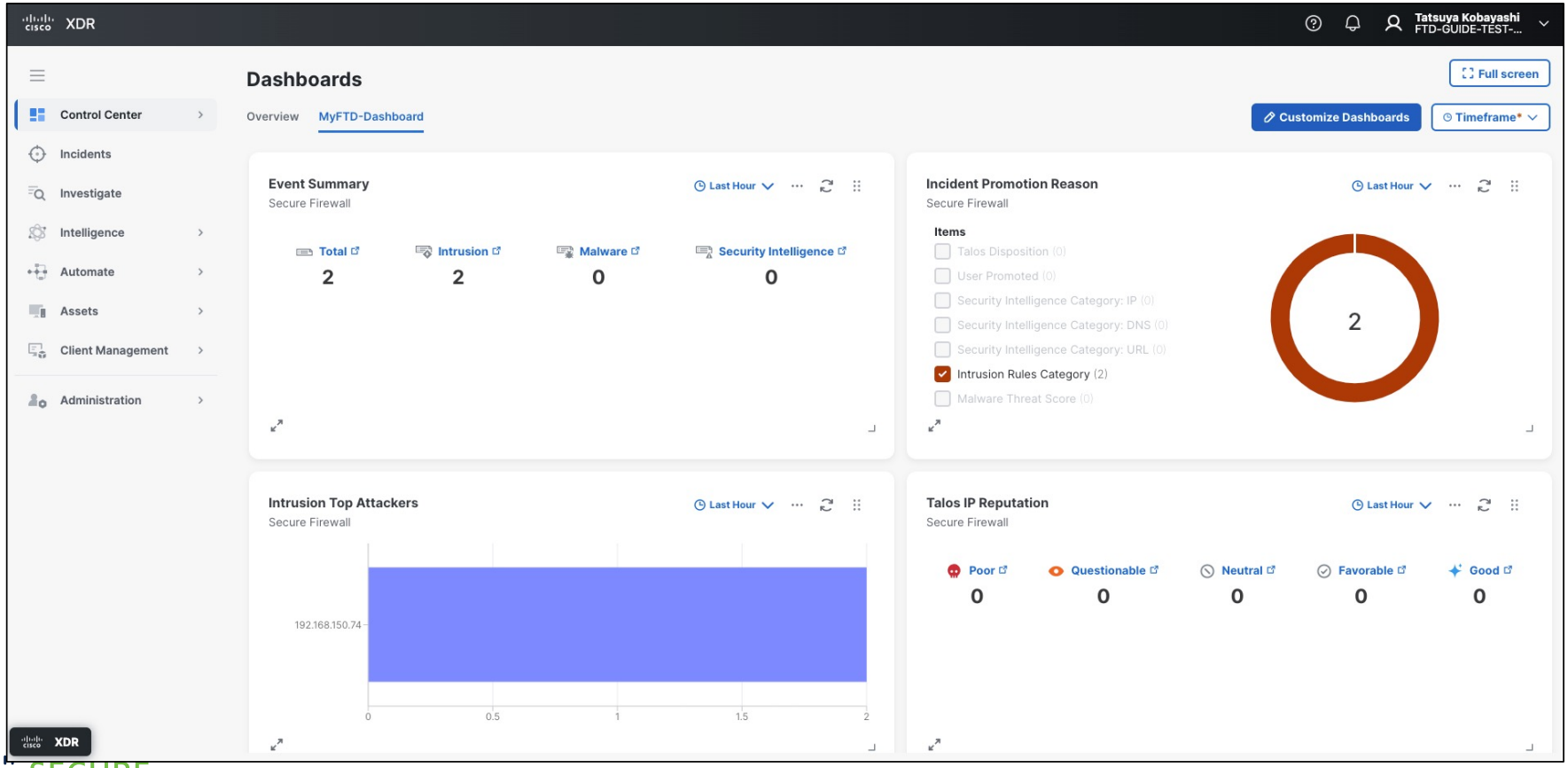
1. + Create new dashboard をクリック
2. 任意の Dashboard 名を追記し、
   Secure Firewall の Add All をクリック

設定4) XDR にて FTD Dashboard を作成 (続き)

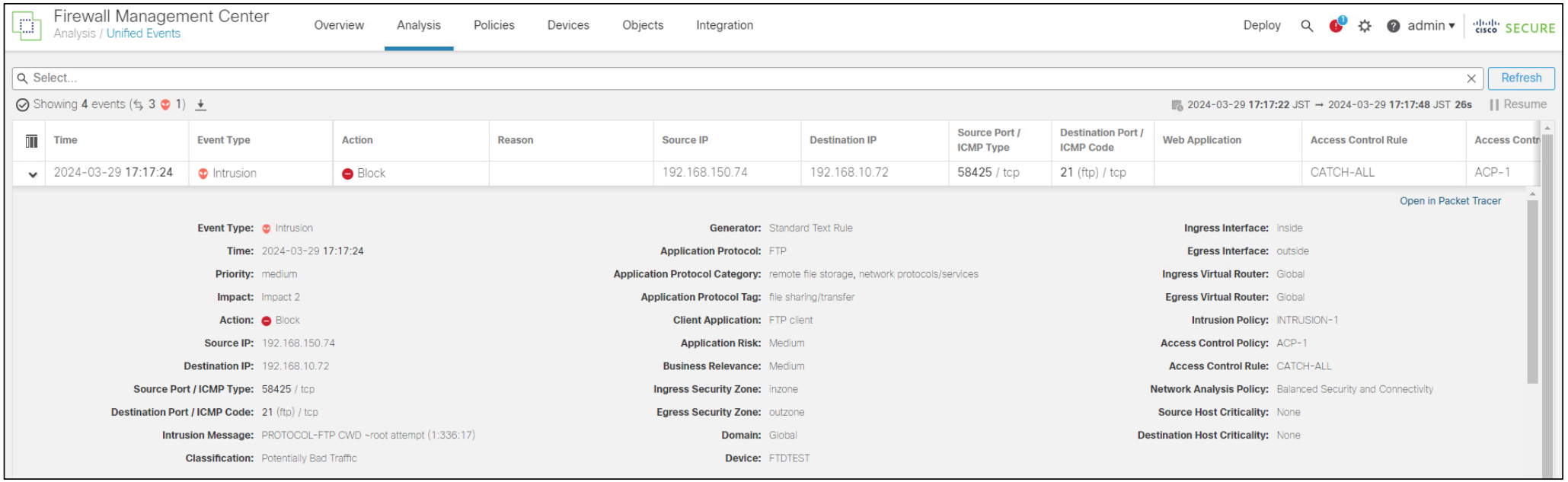
Secure Firewall で 9 selected (今後の Version によって数は変更有り) となったことを確認して Save をクリック

設定4) XDR にて FTD Dashboard を作成 (続き)

FTD の Dashboard が作成されたことを確認

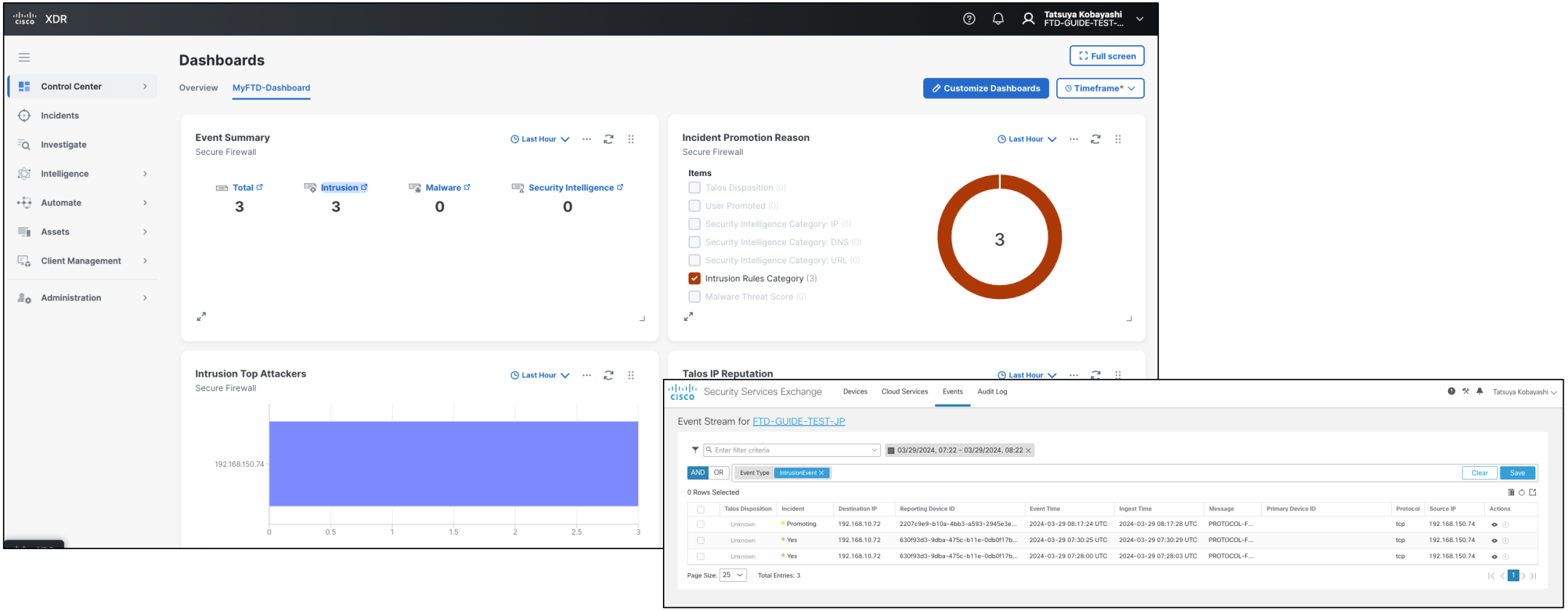


設定5) 動作確認



テスト用のイベントを発生させる。この例では、SID 336 の Intrusion Rule を Block に変更 (FTP サーバにログインして cd ~root を実施したら通信ブロック) し、実際にこの Rule にヒットするテスト通信を発生させている

設定5) 動作確認 (続き)



数分後、XDR の Dashboard にて Intrusion Event がカウントアップしていることを確認

SSX のイベント画面でも同様に確認可能


CISCO
SECURE