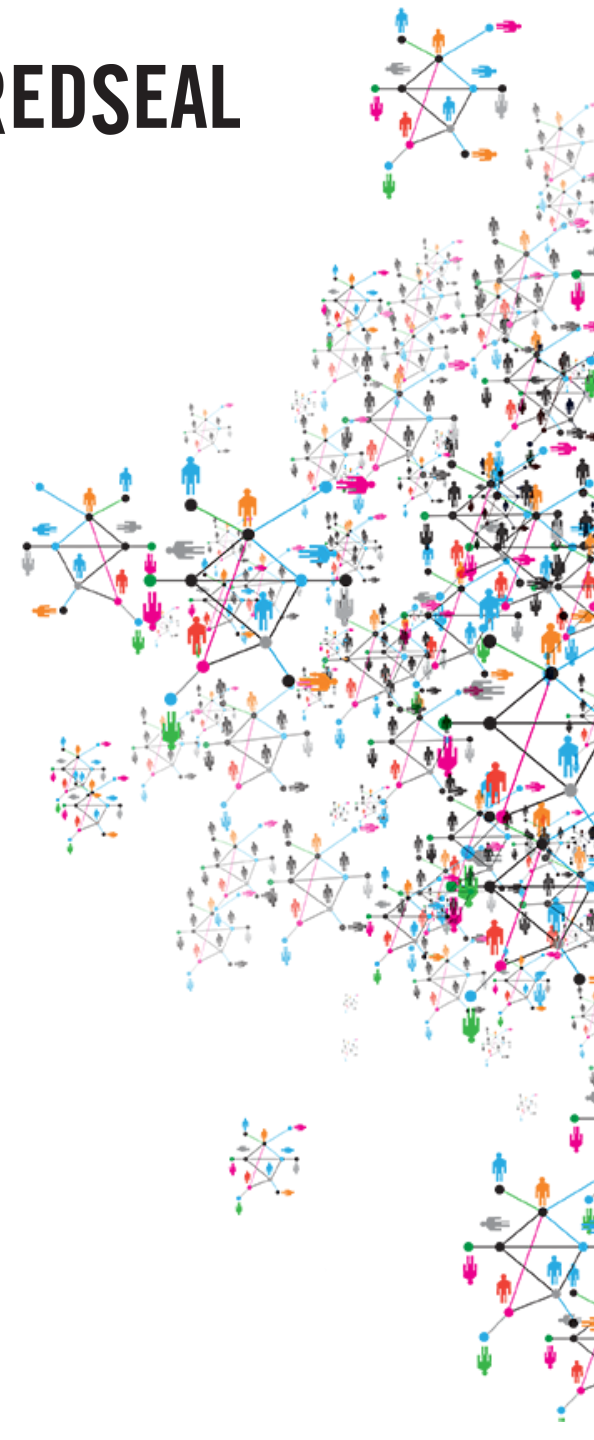


RedSeal Use Cases

May 2016



RedSeal System: 主要ユースケース集

1. 設定ファイルのハードニング
2. ネットワーク参照構成図
3. ネットワークセキュリティアーキテクチャーの照会
4. セグメンテーションの確認: RedSeal Policy
5. 脆弱性の優先付け
6. セキュリティ更新管理のアセスメント
7. エグゼクティブセキュリティ体制レポート
8. RedSeal マチュリティーモデル

設定ファイルのハードニング

- “ハードニング”とは“強化”の事を表す
 - “コンピューティングにおいて、ハードニングとは、脆弱性を減らす事でシステムのセキュリティ堅牢にすること。”(Wikipedia: <https://ja.wikipedia.org/wiki/ハードニング> 参照)
- デバイス(ルーター、ファイアウォール、ロードバランサー、無線コントローラー)の設定ファイルを自動的に確認する
 - チェック項目タイプは次の種類がある:
 - 100以上の“Standard”チェック
 - オプション仕様の“STIG Check”項目集
 - 米国防衛省のDISAで定義されている100以上のネットワーク関連チェック
 - カスタム設定チェック
 - 正規表現(Regular Expression)、又はJavaScriptで定義が可能なチェック

設定ファイルのハードニング

- ユーザープロフィール
 - デバイス設定の基準を定めるチーム
 - デバイス設定の管理に関わるチーム
- 達成目標
 - L3デバイス(ルーター、ファイアウォール、ロードバランサー、無線コントローラー)の設定ミス・矛盾を最低限に抑える
 - デバイス設定の基準に合っている事を自動的に確認する
 - 設定に何らかの問題が検知された際にSIEMに通知する

設定ファイルのハードニング

- 実装機能
 - RedSeal Best Practice Checks (ベストプラクティスチェック)
 - ネットワークデバイスメーカー、及び米国NIST機関の推奨に基づいたデバイス設定ハードニングチェック項目
 - オプションで次の機能、統合も実装
 - カスタムBPC
 - SIEMとの連携
 - 障害チケット管理システム(TTS)
 - RedSeal Rule Check
 - ファイアウォール、ルーターのACLを確認し、矛盾・重複・期限切れルールを見つけ出し指摘する
 - RedSeal Rule Usage
 - ACLのヒットカウンター情報を収集(対応機種に限る)

設定ファイルのハードニング

- 運営プロセスとインプリメンテーション
 - ベストプラクティスチェック項目の確認をし、必要ではないチェック項目を外す
 - カスタムBPCが必要かどうか確認し、必要なら追加する
 - レポート共有が必要なチーム別に作成する
 - 典型的な設定ファイルの収集頻度は毎日行われる
 - BPC警告はSIEM等にも送ることが可能
 - BPC“変動レポート”は通常週一回出力される
 - BPCレポートの使い方のトレーニングを実施する
 - 必要に応じてデバイスクリーンアップの機能を実行する

RedSeal “Best Practice Checks” (BPCs)

RedSeal Networks, Inc. - uiadmin@127.1.2.3 [Version: 7.0.0]

File Edit View Tools Admin Help

Home Maps & Views Zones & Policy **Best Practices** Model Issues Risk Reports

Checks Suppressions

Show All Checks 121 rows

Check ID	Title	Severity	Passed Devices	Failed Devices	Violation Instances
RS-36	IP Source Routing Enabled	HIGH	12	40	40
RS-51	Service PAD Enabled	LOW	0	34	34
RS-52	Bootp Server Not Disabled	LOW	0	34	34
RS-57	TCP Keepalives In Disabled	LOW	0	34	34
RS-58	TCP Keepalives Out Disabled	LOW	0	34	34
RS-37	No Enable Secret	HIGH	2	32	32
RS-18	IP Redirects	MEDIUM	34	16	16
RS-24	IP Proxy ARP				
RS-61	IP Unreachables				
RS-80	Telnet Enabled on Interface				
RS-102	HTTP Management Enabled on Interface				
RS-62	Untrusted Remote Login Access to Network Device				
RS-66	Untrusted Remote Login Access				
RS-72	DNS Not Configured				
RS-108	Policy List with No Deny				
RS-19	Telnet Server				
RS-110	Time Synchronization not Configured				
RS-112	No Pre-Login Banner				

Telnet Enabled on Interface

View by Device View by Violation

Status	Name
Failed	Campus-FW1-screensos
Severity	Summary
LOW	The telnet protocol is enable
Failed	ios-novrf-screensos
Failed	Branch-Vienna-Corp-screenso
Failed	Campus-FW2-screensos
Failed	Branch-Corp-Texas-screensos
Failed	Branch-Corp-Vienna-screenso
Failed	DMZ-FW2-screensos
Failed	PA1
Failed	screensos-VRF-screensos
Failed	ios-VRF-screensos
Failed	DMZ-FW1-screensos

Analysis Current

Home Maps & Views Zones & Policy **Best Practices** Vulnerabilities Model Issues Risk Reports

Checks Suppressions

Show All Checks 130 rows

Check ID	Title
RS-19	Telnet Server

Violation ID: 6,399

Title: Telnet Server

Check: RS-19

Summary: The telnet server is enabled

Description: The *telnet* service is enabled on the device. Use *ssh*, a more secure protocol, instead.

Remediation: Add one of the following commands to the top of the configuration. To allow no access through the vty: `config t`
`line vty <line numbers>`
`transport input none`
...or, to allow only desired access... `config t`
`line vty <line number>`
`transport input ssh`

First Noticed: 10/6/14 2:42 PM

- 設定ファイル内にて問題があると思われる記述をハイライトし、修正の推奨も提示する

設定ファイルのハードニング:事例

- 顧客:大規模ネットワーク機器メーカー
 - 目標:設定ファイルの記述ミス・不備およびセキュリティリスクを排除
 - プロセス:プロビジョニングシステムと統合し、バッチング作業で分析
 - 導入効果:500,000 以上の設定ミス・不備の修正し、セキュリティリスクを排除
-
- 顧客:金融系
 - 目標:設定ミスによるセキュリティインシデントをなくす
 - プロセス:積極的なカスタムチェックの導入
 - 導入効果:自動化とカスタムチェックにより、設定ミスの最小化
-
- 有効性:RedSeal の自動コンフィグアセスメント機能を導入すると、ネットワークインフラの完全性・安全性が担保できる

RedSeal System: 主要ユースケース集

1. 設定ファイルのハードニング
2. ネットワーク参照構成図
3. ネットワークセキュリティアーキテクチャーの照会
4. セグメンテーションの確認: RedSeal Policy
5. 脆弱性の優先付け
6. セキュリティ更新管理のアセスメント
7. エグゼクティブセキュリティ体制レポート
8. RedSeal マチュリティーモデル

ネットワーク参照構成図

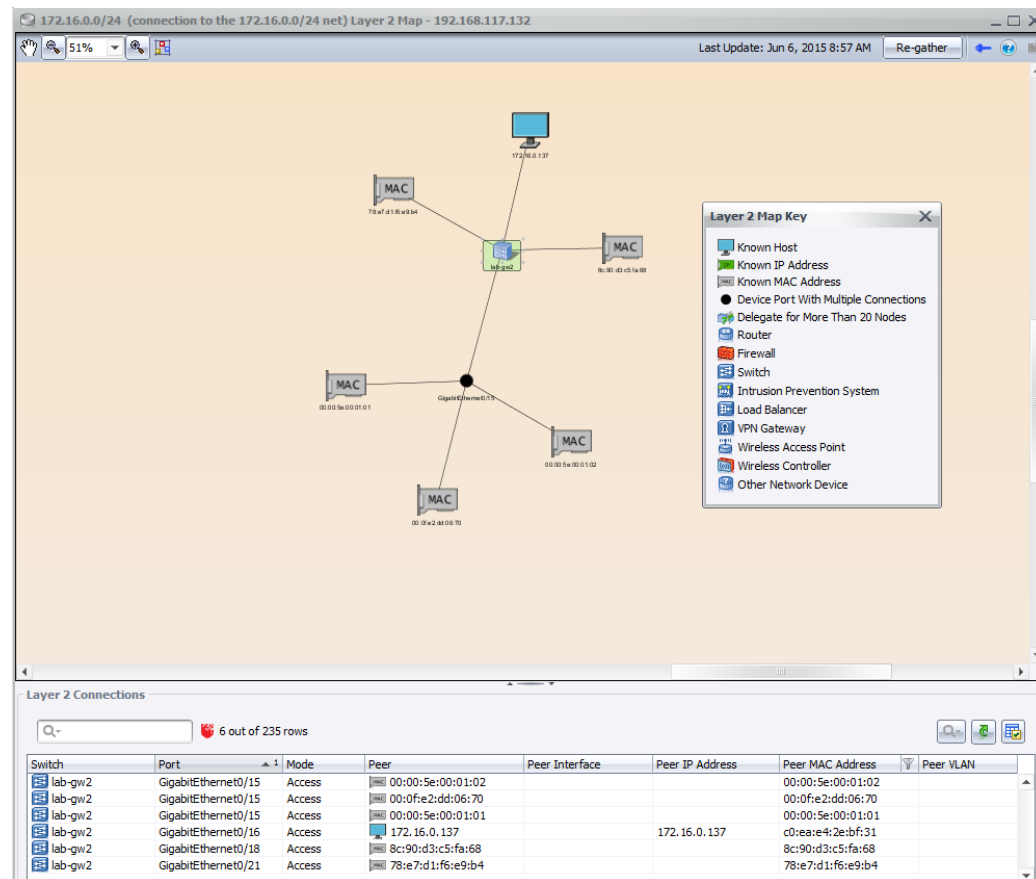
- ユーザープロフィール
 - セキュリティアーキテクチャーを考案するチーム
 - セキュリティの運営に関わるチーム
 - ネットワークの運営に関わるチーム
- 達成目標
 - 最新のネットワーク構成図を把握する
 - 最新ではないネットワーク図(例えばVisio等)を使用しない

ネットワーク参照構成図

- 実装機能
 - “Maps & Views”画面が自動的に収集されたコンフィグファイルを基に更新される
 - ドリルダウンでコンフィグの中身を参照
 - ネットワークの構成図を複数の形式で出力する(PDF、Visio、等)
- 運営プロセスとインプリメンテーション
 - コンフィグファイルの収集をスケジュール機能で自動的に動かす
 - RedSeal 管理者がトポロジーマップを随時更新する
 - 新しいトポロジーマップオブジェクトを適切なグループに振り分ける
 - RedSeal を使う人材のトレーニングを実施する

オプション: Layer 2 可視化機能

- オプションで Layer 2 ライセンスを組織内全てのスイッチ分購入する必要がある
- L2 トポロジーはサブネットからドリルダウンをした際に表示される
- L2 トポロジーのレイアウトは自動的に配置され、カスタマイズは出来ない



自動的に更新されるL3トポロジー

The screenshot displays the RedSeal Inc. network management interface. The main window is titled "RedSeal Inc. - uiadmin@localhost [Version: 7.1.3]". The interface is divided into several panes:

- View Selector:** A dropdown menu showing "View Topology".
- Inventory List:** A tree view on the left side listing various network components such as Border, Branch, Campus, Core, and Data Servers.
- Topology Pane:** A large central area displaying a complex network topology map with nodes and connections.
- Details Pane:** A pane at the bottom right showing details for the selected "Campus" view, including a table of devices.

The "Details Pane" table shows the following data:

Name	Capability	Last Imported	Modified	Routing Observed
Campus-lab-FW-MFE	Firewall	Oct 6, 2014 2:42:27 ...	Oct 6, 2014 2:42:27 ...	
Campus-Dev-ios	Router	Oct 6, 2014 2:42:40 ...	Oct 6, 2014 2:42:40 ...	

At the bottom of the interface, there is a status bar showing "Analysis Current" and resource usage: "Client 134 M of 989 M" and "Server 3,473 M of 13,510 M".

ネットワーク参照構成図：事例

- 顧客：流通系
 - 目標：新社員・新規スタッフの教育
 - 導入効果：RedSeal “Maps & Views” 機能を使い実際のネットワークを参照しながらトレーニングを実施
-
- 顧客：(多数)
 - 目標：最新のネットワークを把握する
 - 導入効果：コンフィグファイルの収集を自動化、そしてネットワーク構成図を常に最新のネットワークを反映させる
-
- 有効性：RedSeal を使い常に最新のネットワーク図を維持する事で、最新でない図に頼らずあらゆる作業の効率化に貢献する。古いネットワークマップを使用したことによるミスも防ぐ

RedSeal System: 主要ユースケース集

1. 設定ファイルのハードニング
2. ネットワーク参照構成図
3. ネットワークセキュリティアーキテクチャーの照会
4. セグメンテーションの確認: RedSeal Policy
5. 脆弱性の優先付け
6. セキュリティ更新管理のアセスメント
7. エグゼクティブセキュリティ体制レポート
8. RedSeal マチュリティーモデル

ネットワークセキュリティアーキテクチャーの照会

- ユーザープロフィール
 - セキュリティアーキテクチャーの定期精査
 - セキュリティの運営に関わるチーム
 - アドホックのクエリー操作をするスタッフ
 - インシデントレスポンスチーム
 - セキュリティコンプライアンスチーム
 - 脆弱性対策に関わるチーム
- 達成目標
 - セキュリティアーキテクチャーが促すポイントAからポイントBまでのアクセスの把握
 - セキュリティアーキテクチャーが*どの様に*ポイントAからポイントBへのアクセスが許可、もしくはブロックされているのかの把握

ネットワークセキュリティアーキテクチャーの照会

- 実装機能
 - Access Query
 - Explorer
 - Advanced Explorer
 - Security Information Center
 - Detailed Path Queries
 - Security Intelligence Center
 - Security Query Manager
 - 手動クエリー結果
 - ドリルダウン機能
- 運営プロセスとインプリメンテーション
 - Maps & Views のユーザートレーニング

ネットワークセキュリティアーキテクチャーの照会

The screenshot displays a network security tool interface with several panels:

- Access Results:** Shows a search for source IP 80.1.1.0/24. The results table has one row.
- Detailed Path - localhost:** Shows a "Fully Open Path" with a "Detailed Path Summary" and a "Paths Found" table.
 - Detailed Path Summary:**
 - Query Name: Fully Open Path
 - Query Date: Mar 6, 2015 11:49:57 AM
 - Query Status: Successful
 - Protocol: TCP
 - Source Node: 80.1.1.0/24 (connected to inter...)
 - Source IP: 0.0.0.0 - 9.255.255.255
 - Source Port: any
 - Destination Node: 10.101.3.0/24 (connected to 10...)
 - Destination IP: 10.101.3.206
 - Destination Port: 22
 - Route Consideration: Off
 - Paths Found:**
 - Path Discovered: Path 1 (5 hops)
 - Table with columns: Hop, Flow, Device
 - Hop 1: START, Flow 0.0.0.0 - 9.255.255.255
 - Hop 2: Edge-internet-2-ios
 - Hop 3: DMZ-FW1-screensos
 - Hop 4: DMZ-dist-1-ios
 - Hop 5: Core-1-ios
- Access Through Device: DMZ-FW1-screensos:** A table showing permitted input and output traffic.

Access	Device	Interface	VRF Table	Protocol	Source IP
Permitted Input	DMZ-FW1-screensos	172.16.106.1 (ethernet6)	trust-vr	TCP	0.0.0.0 - 9.255.255.25
Permitted Output	DMZ-FW1-screensos	172.16.101.1 (ethernet1)	trust-vr	TCP	0.0.0.0 - 9.255.255.25
- Filter/NAT Rules For Device: DMZ-FW1-screensos:** A table showing 3 rows of rules.

Device	Type	First Line/Description
DMZ-FW1-scre...	Filter Rule	(NetScreen Configuration:130) set policy id 7 from "Untrust" to "Trust" "Any"
DMZ-FW1-scre...	Filter Rule	(implicit) deny all
DMZ-FW1-scre...	NAT	(NetScreen Configuration:130) set policy id 7 from "Untrust" to "Trust" "Any"
- DMZ-FW1-screensos Juniper ScreenOS - localhost:** A configuration window showing a specific rule configuration.

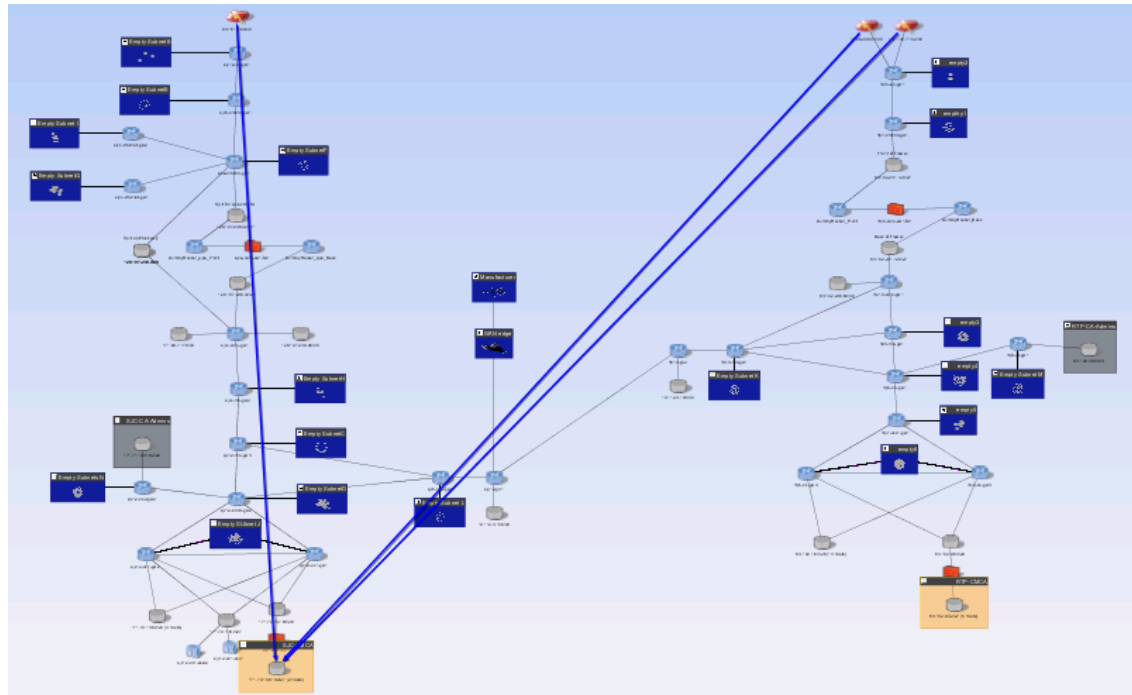
```
129 exit
130 set policy id 7 from "Untrust" to "Trust" "Any" "Any" "SSH" nat dst ip
10.101.3.206 port 22 permit
131 exit
132 set service "HTTP"
133 set service "HTTPS"
134 set service "PING"
```

- 概要画面からアクセスパスを選び、Detailed Pathで詳細を確認、そしてコンフィグの詳細もチェック

ネットワークセキュリティアーキテクチャーの照会

- 顧客:テクノロジー製造業
- 目標:クリITICALなネットワークへのアクセスを確認
- プロセス:RedSeal Access Queries

- 導入効果:(右画像参照)
想定外のアクセスパスを検出し、
攻略される前に対処した



RedSeal System: 主要ユースケース集

1. 設定ファイルのハードニング
2. ネットワーク参照構成図
3. ネットワークセキュリティアーキテクチャーの照会
4. セグメンテーションの確認: RedSeal Policy
5. 脆弱性の優先付け
6. セキュリティ更新管理のアセスメント
7. エグゼクティブセキュリティ体制レポート
8. RedSeal マチュリティーモデル

セグメンテーションの確認: RedSeal Policy

- ユーザープロフィール
 - アクセスコンプライアンスに関わるチーム
 - アクセス監査に関わるチーム
 - アクセスを監修するチーム

- 達成目標
 - コンプライアンスの順守を確認
 - PCI-DSS
 - NERC-CIP (米国電力規制)
 - 組織特有のセグメントポリシーの順守を確認
 - 継続的にモニタリング
 - アクセスの認証

- 実装機能
 - Zones & Policy

セグメンテーションの確認: RedSeal Policy

- 運営プロセスとインプリメンテーション
 - コンプライアンスの範囲を明確にする
 - セキュリティのセグメント割を明確にする
 - セグメントのアクセス必要性を確認する
 - セグメントのアクセスの認証をする
 - コンプライアンス検証結果を確認し、判断を下す
 - セキュリティ更新管理の一環として導入する
 - アクセスポリシーのレポート出力
 - Zones & Policy と Access Query のトレーニングを実施する

セグメンテーションの確認: RedSeal Policy

- “Zone”: セキュリティセグメント
- “Rule”: ゾーン間のルール
- RedSeal が全てのアクセスを解析
- RedSeal が全てのアクセスを “Business Decisions” に比べて解析
 - (approvals)
- “PCI Template” は PCI-DSS Section 1.1の検証を解析
- カスタマイズで組織特有のポリシーが構築可能

The screenshot displays the RedSeal Networks Inc. ZONES & POLICY interface. The main window shows a network diagram with zones: Cardholder, DMZ, General, Out of Scope, Untrusted, and Wireless. A legend indicates the status of connections: Pass (green arrow), Warning (yellow arrow), Fail (red arrow), and Zone Overlap (dashed red line).

Below the diagram, a table titled "Access From Cardholder to Untrusted" shows 40 rows of data. The table columns are Zone Pair, Protocols, Ports, Status, and Trouble Ticket.

Zone Pair	Protocols	Ports	Status	Trouble Ticket
From Cardholder to ...	any	any	Fail	
Destination IP	Protocols	Ports	Status	Trouble Ticket
0.0.0.0 - 10.100.102.0	any	any	Fail	
10.150.104.2 - 101.2.1.0	any	any	Fail	
10.100.104.2 - 101...	any	any	Fail	
0.0.0.0 - 10.141.10...	any	any	Fail	
0.0.0.0 - 10.150.10...	any	any	Fail	
192.168.101.3 - 255.25...	any	any	Fail	
0.0.0.0 - 10.150.10...	any	any	Fail	
10.100.101.2 - 101...	any	any	Fail	

セグメンテーションの確認：事例

- 顧客: 政府、金融、医療
- 目標: セキュリティセグメンテーションの確認
- プロセス: RedSeal カスタマイズポリシー
- 導入効果: 内部監査の実現

- 顧客: E-Commerce
- 目標: PCI-DSS コンプライアンス追従の確認
- プロセス: RedSeal PCI Policy テンプレートと更新管理プロセスとの統合
- 導入効果: PCI-DSS Section 1.1 のコンプライアンスを自動的に厳守

- 有効性:
 - 監査に向けての準備がより効率よく、無駄なく行える
 - 監査が行われた際に、監査に合格するだけでなく、安全性を高める効果もある
 - 監査期間が終了した後も継続的にコンプライアンスを厳守出来る

RedSeal System: 主要ユースケース集

1. 設定ファイルのハードニング
2. ネットワーク参照構成図
3. ネットワークセキュリティアーキテクチャーの照会
4. セグメンテーションの確認: RedSeal Policy
5. 脆弱性の優先付け
6. セキュリティ更新管理のアセスメント
7. エグゼクティブセキュリティ体制レポート
8. RedSeal マチュリティーモデル

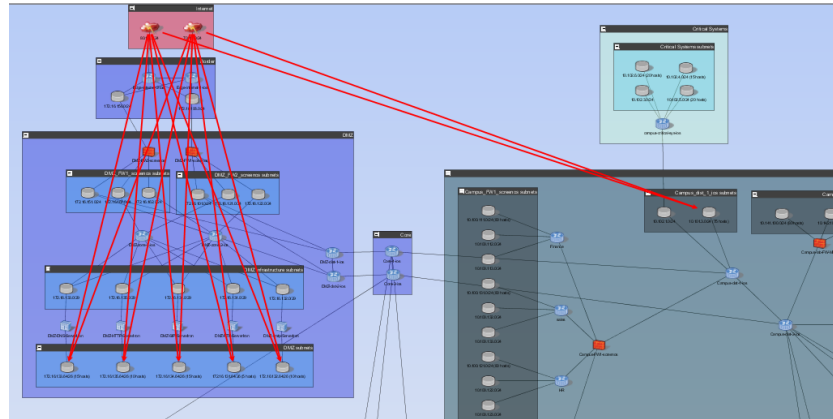
脆弱性の優先付け

- ユーザープロフィール
 - クエリーモード
 - 脆弱性に対応するチーム
 - レポートモード
 - スキャナー運営に関わるチーム
 - ホストのパッチングに関わるチーム
 - セキュリティの総合管理に関わるチーム
- 達成目標
 - 直接的・間接的に脅威に晒されている攻撃対象ターゲット
 - 直接的・間接的に脅威が攻略可能なアクセスパス
 - 脅威の露出度の把握

脆弱性の優先付け

- 実装機能
 - RedSeal Threat Query
 - 可視化機能
 - 照会結果の詳細
 - RedSeal Risk Map
 - 脆弱性関連のレポート出力
- 運営プロセスとインプリメンテーション
 - 脆弱性スキャンデータの取り込み
 - レポートの選別と構築
 - アクセスクエリー、Threats クエリー、リスクメトリクス、リスクマップ、カスタマイズレポートのエンデュースートレーニング

脆弱性の優先付け



- 外部から直接攻撃可能な脆弱性が依存するアクセスパスを自動的に検出
 - Leapfrog(踏み台攻撃)の有無も確認し、結果に含む
- 各ホスト、各脆弱性についてのスコアリング:
 - **[Business] Value (価値)**: 0~100の数値でビジネスに於ける資産価値を表す
 - デフォルト数値はエンドユーザー次第でカスタマイズ可能
 - **Exposure (露出度)**: 0~1(例:0.77)の率で脆弱性が攻撃される可能性を表す
 - **RedSeal Risk**: [Business] Value X Exposure
 - 例: $65 \times 0.77 = 50$

脆弱性の優先付け: 事例

- 顧客: (多数)
- 目標: 効率的な脆弱性対策の向上
- プロセス: RedSeal 定期レポート
 - 各コンピューターシステム部門に合わせて優先付けレポートを出力
- 導入効果: パッチング、そして脆弱性対応をピンポイントで最もインパクトの高いエリアで実施し、脆弱性対策の向上に貢献

RedSeal System: 主要ユースケース集

1. 設定ファイルのハードニング
2. ネットワーク参照構成図
3. ネットワークセキュリティアーキテクチャーの照会
4. セグメンテーションの確認: RedSeal Policy
5. 脆弱性の優先付け
6. セキュリティ更新管理のアセスメント
7. エグゼクティブセキュリティ体制レポート
8. RedSeal マチュリティーモデル

セキュリティ更新管理のアセスメント

- ユーザープロフィール:
 - 更新管理に関わるチーム
- 達成目標:
 - 更新要請を効率的、かつ正確に評価し、判断を下す
- 実装機能:
 - RedSeal Security Impact Query
 - 更新要請と現状: アクセスが既にあるか否か
 - アクセスがない場合、何故アクセスがブロックされているか
 - アクセスを開けたと仮定した場合に露出される脅威
 - アクセスを開けたと仮定した場合に影響が及ばせられるポリシー
- 運営プロセスとインプリメンテーション:
 - 更新管理プロセスの一環として導入
 - 更新管理プロセスとRedSeal UI のトレーニング
 - (オプション) Zones & Policy のプロセス導入化

セキュリティ更新管理のアセスメント: 事例

- 顧客: オンライン流通
- 目標: 更新管理のセキュリティ向上と正確な状況把握
- プロセス: RedSeal Security Impact Queries を更新管理プロセスの一環として導入
- 導入効果: 40%以上の変更リクエストは既に通信可能であった

セキュリティ更新管理のアセスメント

- RedSeal “Security Intelligence Center” は様々なクエリー機能を搭載
- Security Impact Analysis 機能を使うと次の情報が得られる:
 - 現状のネットワークがクエリーされたアクセスが可能か
 - クエリーされているアクセスが既存のポリシーに影響するか
 - クエリーされているアクセスが想定外のアクセスを可能にするか

The image shows two screenshots of the RedSeal Security Intelligence Center (SIC) interface. The top screenshot is the main SIC window, titled "Security Intelligence Center - localhost". It features a "Source" field with the IP address "70.1.1.0/24 (connected to internet1)" and a "Destination" field with "10.102.5.0/24 (connected to critSys-nfs)". Below these fields are "IPs" and "Ports" sections, each with an "Optional" dropdown menu and a "Select" button. The bottom screenshot is the "Security Impact Analysis - localhost" window. It displays the source and destination IP addresses at the top. The "Path Status" section indicates "This path is currently **BLOCKED**" and includes a "Detailed Path" button. The "Exposure" section shows a red box for "Source" (Untrusted) and a yellow box for "Destination" (Indirectly Attackable). The "Vulnerabilities on the Destination" section states: "Permitting this access exposes 96 vulnerabilities. 20 hosts are exposed in the destination. 20 of the exposed hosts have leapfrog vulnerabilities." It also lists: "Oldest scan date: Jan 8, 2014", "Number of unique vulnerabilities: 26", "Collective impact: **ACIS**", and "Max CVSS base score: 10.0". The "Downstream Impact" section shows "Source: crit-sys-nfs-srv-101, crit-sys-..." and "Destination: All Trusted Subnets", with a note that "816 hosts would be reachable via leapfrog vulnerabilities." It includes buttons for "Downstream Access" and "Downstream Threats". The "Policy Impact" section shows two red circles representing policy impacts for "NERC Example Policy" and "PCI Audit", each with "Details" and "New Decision" links. At the bottom of the window are "Export", "Close", and "Help" buttons.

RedSeal System: 主要ユースケース集

1. 設定ファイルのハードニング
2. ネットワーク参照構成図
3. ネットワークセキュリティアーキテクチャーの照会
4. セグメンテーションの確認: RedSeal Policy
5. 脆弱性の優先付け
6. セキュリティ更新管理のアセスメント
7. エグゼクティブセキュリティ体制レポート
8. RedSeal マチュリティーモデル

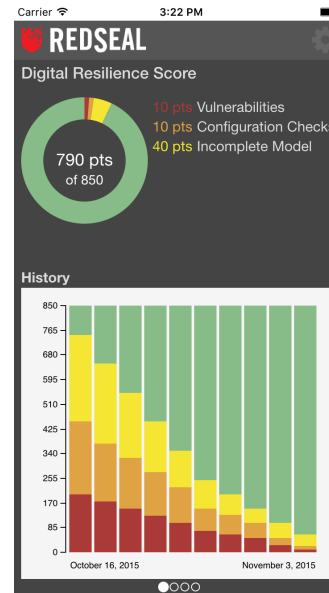
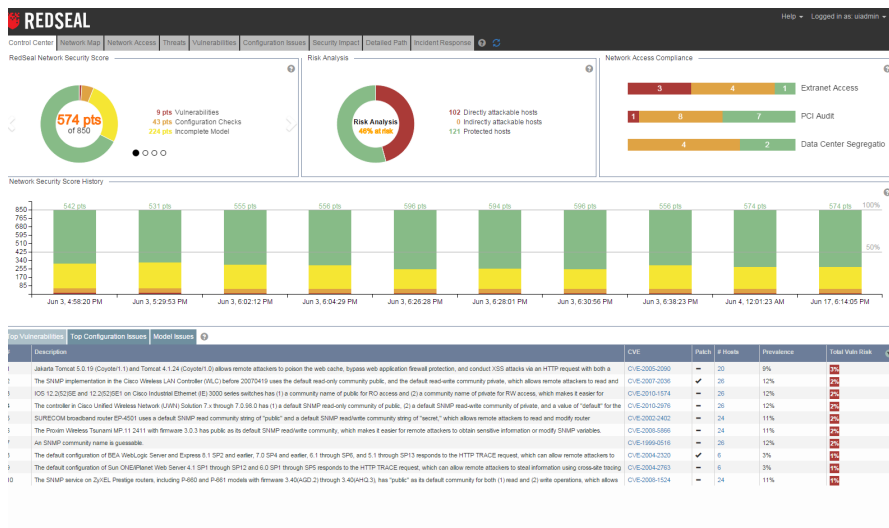
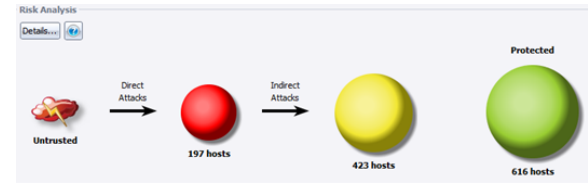
エグゼクティブセキュリティ体制レポート

- **ユーザープロフィール:**
 - セキュリティ管理に関わるチーム
 - IT 総括チーム
- **達成目標:**
 - セキュリティ体制の状況と進化の確認
- **実装機能:**
 - RedSeal ホーム画面
 - RedSeal Executive Summary ダッシュボード
 - カスタマイズレポート
- **運営プロセスとインプリメンテーション:**
 - 本番ネットワークと連動したRedSeal システムの運営
 - 包括的な脆弱性スキャナーの運営と RedSeal との連携
 - レポート構築と出力
 - レポートのユーザートレーニング

エグゼクティブセキュリティ体制レポート

- セキュリティ体制を統計的に解析、アセスメントを実施
 - 複数の RedSeal メトリクスを統計して解析をする

- ポイント: エグゼクティブ向けのKPI



エグゼクティブセキュリティ体制レポート: 事例

- 顧客: 医療系
- 目標: エグゼクティブに報告する為のセキュリティステータス
- プロセス:
 - RedSeal モデルの維持
 - 脆弱性スキャナーデータの取り込み
 - RedSeal API を使った他製品との統合
- 導入効果: 組織のセキュリティビジビリティを向上させ、体制・対策の向上を見守る

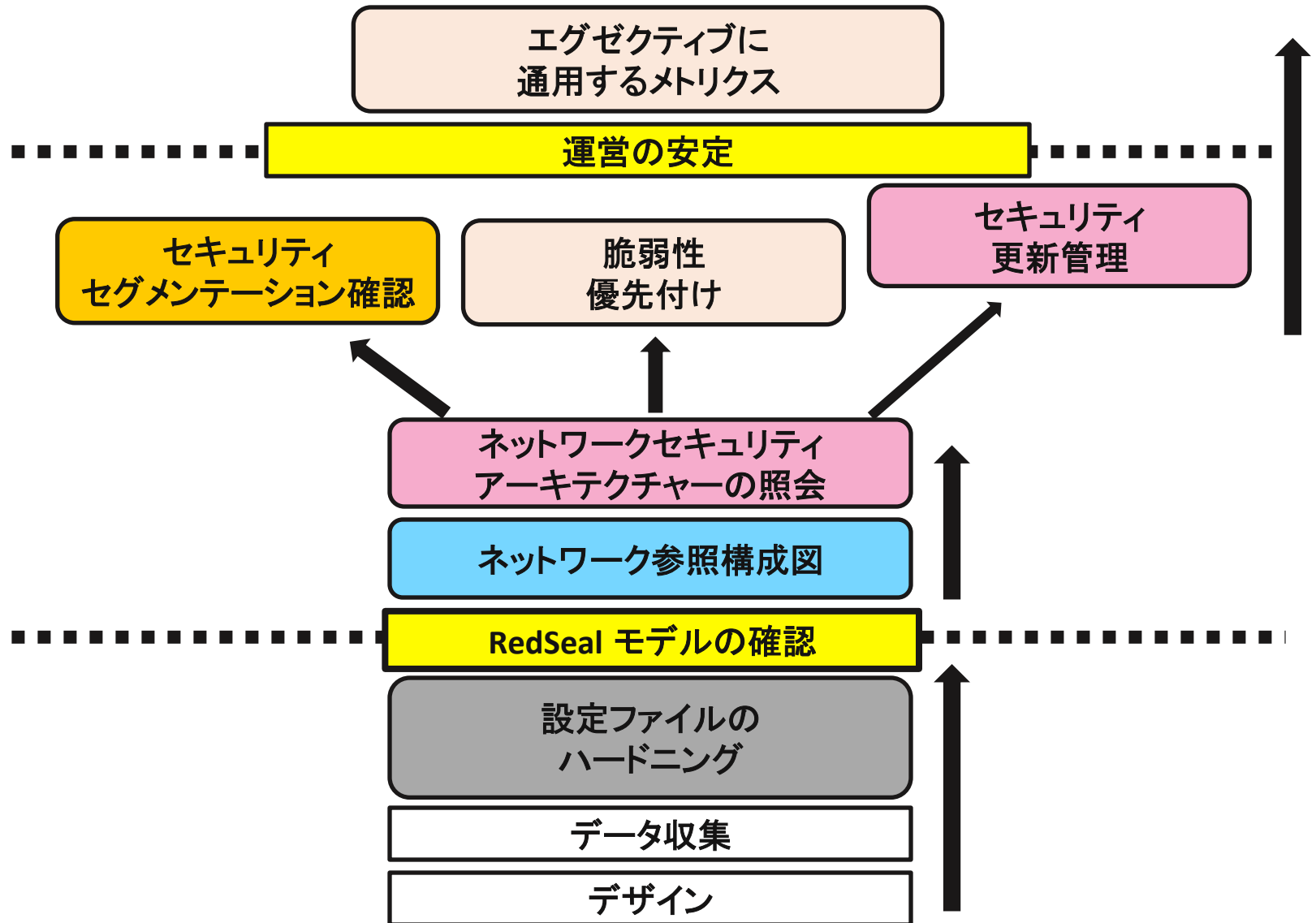
RedSeal System: 主要ユースケース集

1. 設定ファイルのハードニング
2. ネットワーク参照構成図
3. ネットワークセキュリティアーキテクチャーの照会
4. セグメンテーションの確認: RedSeal Policy
5. 脆弱性の優先付け
6. セキュリティ更新管理のアセスメント
7. エグゼクティブセキュリティ体制レポート
8. RedSeal マチュリティーモデル

RedSeal マチュリティーモデル

顧客の達成目標は何か？
現状は如何か？

RedSeal の価値を築く



RedSeal は機能が豊富...

Vuln Prioritization Rpt

Risk Map

Explorer:Threat

Risk and DSR Metrics

Compliance Custom Policy

PCI Policy Template

“What Is” Policy

SIC / SIM / Tracked Query

Detailed Path

Explorer:Access

Custom Groups

Topo Layout

Model Issues

Config Management

Device Cleanup

Custom BPCs

Best Practice Checks

... 機能の内には類義系の物がある

Vuln Prioritization Rpt

Risk Map

Explorer:Threat

Risk and DSR Metrics

Compliance Custom Policy

PCI Policy Template

“What Is” Policy

SIC / SIM / Tracked Query

Detailed Path

Explorer:Access

Custom Groups

Topo Layout

Model Issues

Config Management

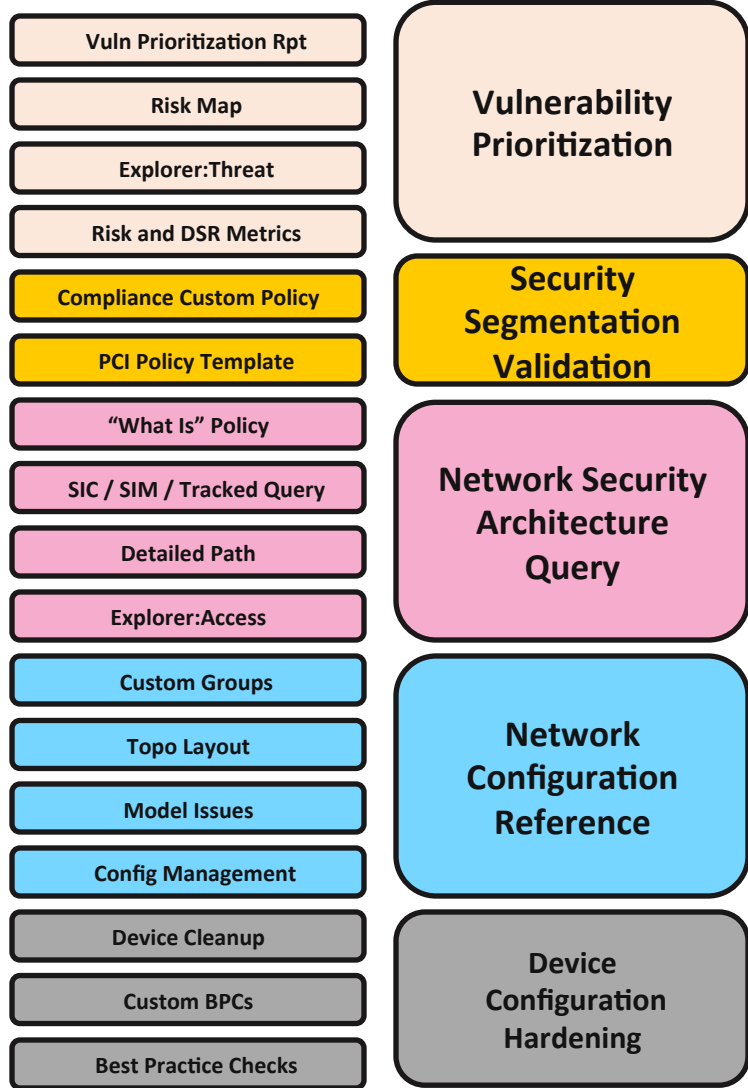
Device Cleanup

Custom BPCs

Best Practice Checks

RedSeal 機能

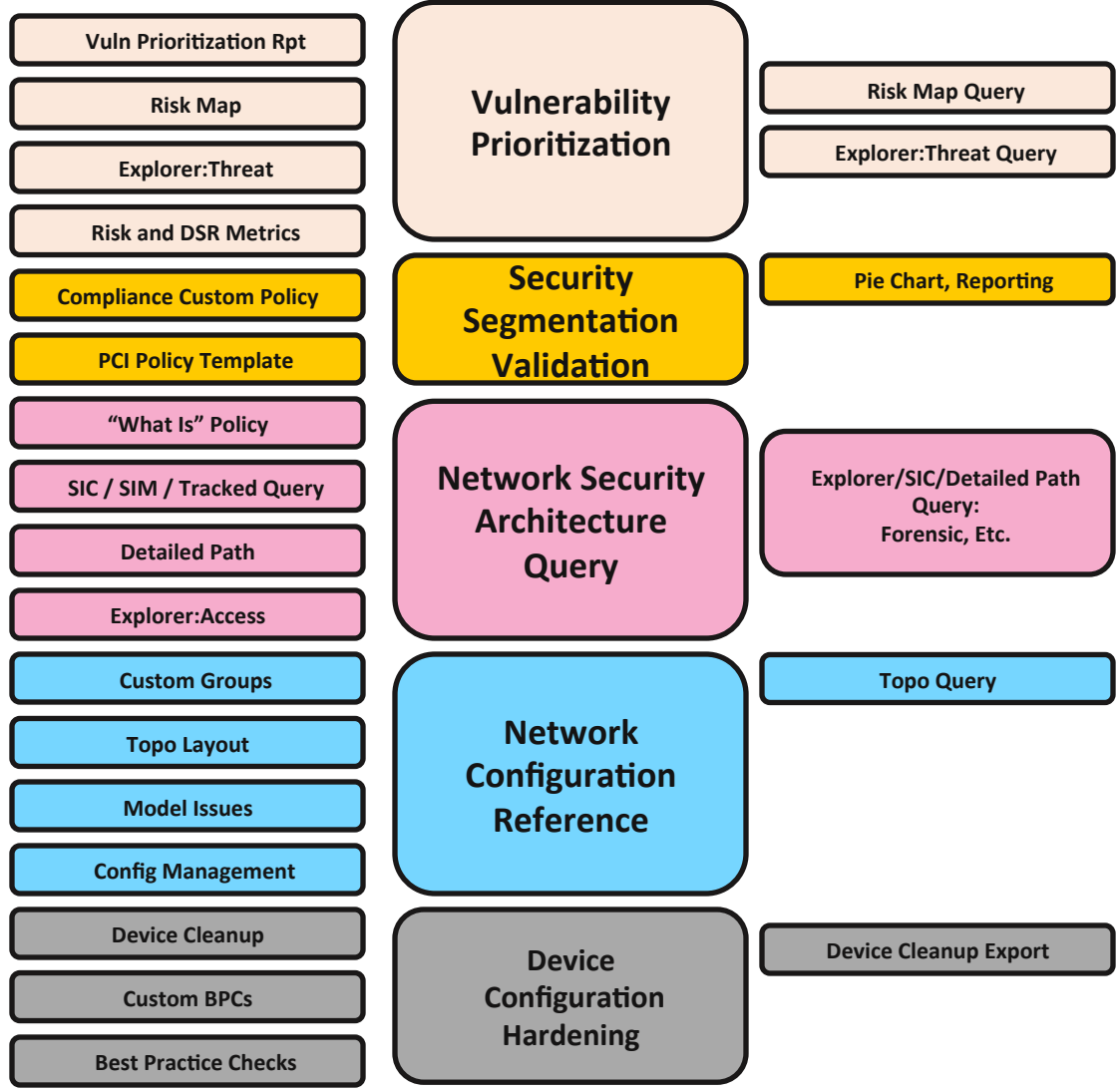
“機能群”



RedSeal 機能

“機能群”

アドホックな ユースケース

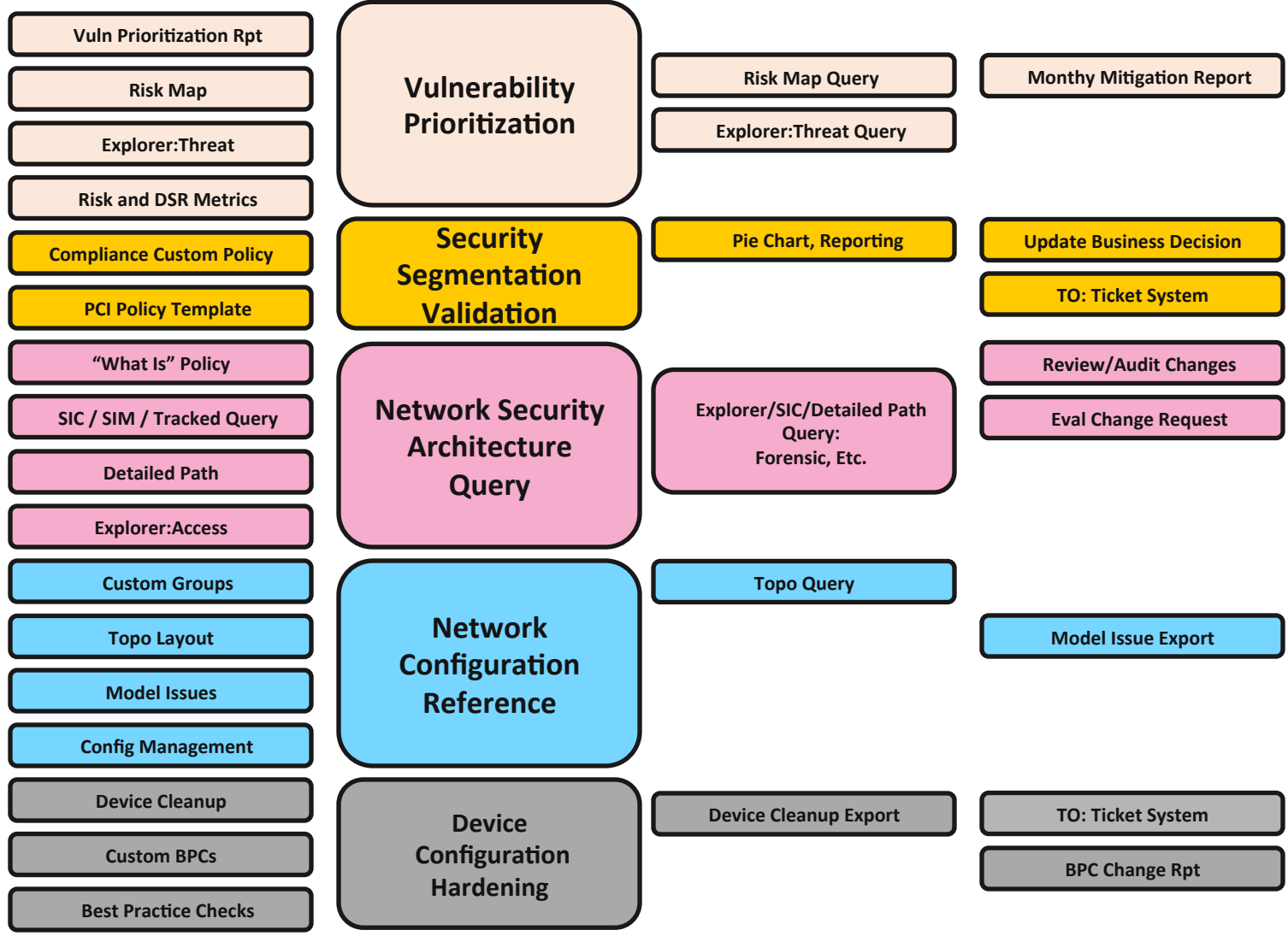


RedSeal 機能

“機能群”

アドホックな ユースケース

プロセス 統合



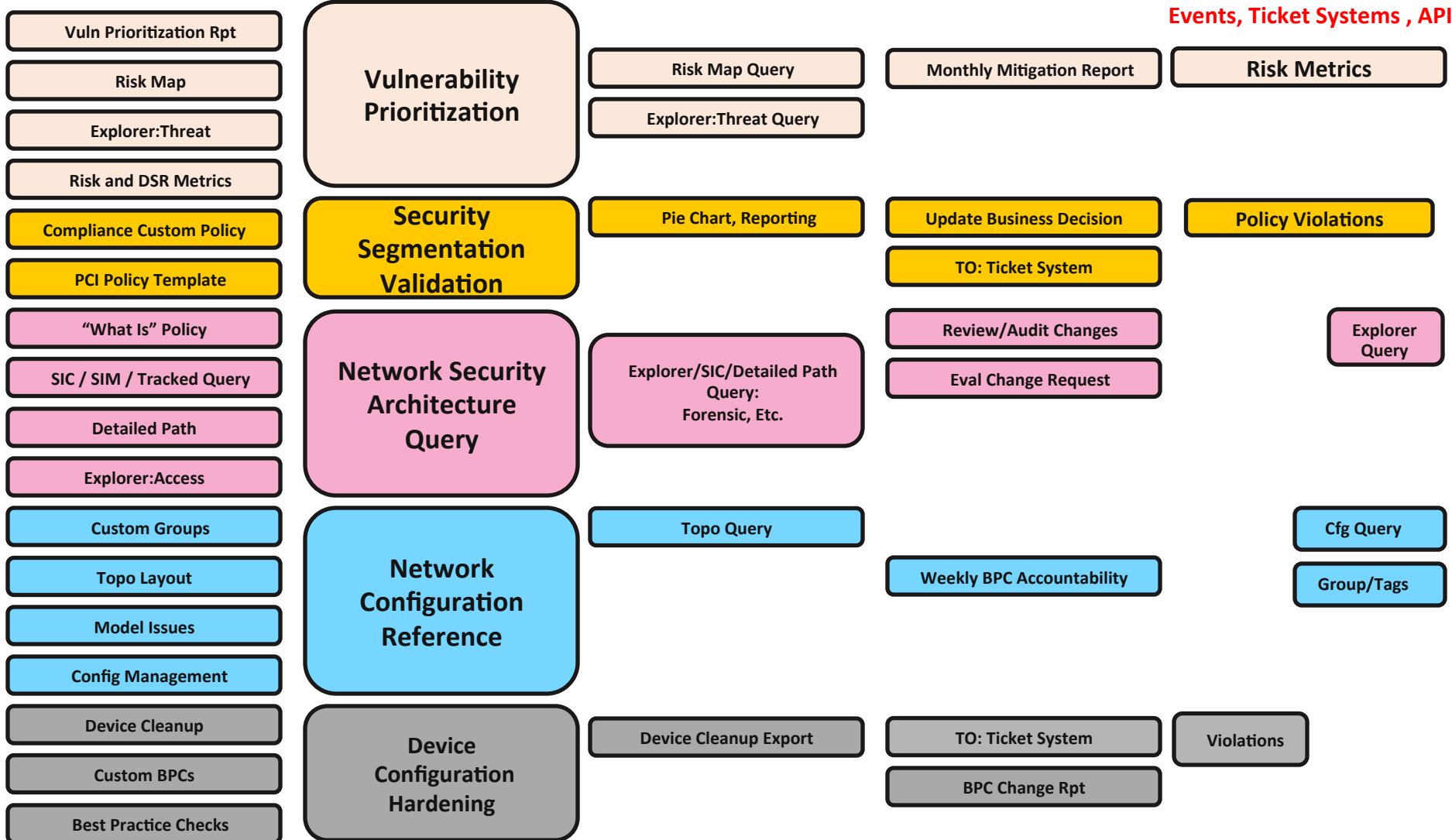
RedSeal 機能

“機能群”

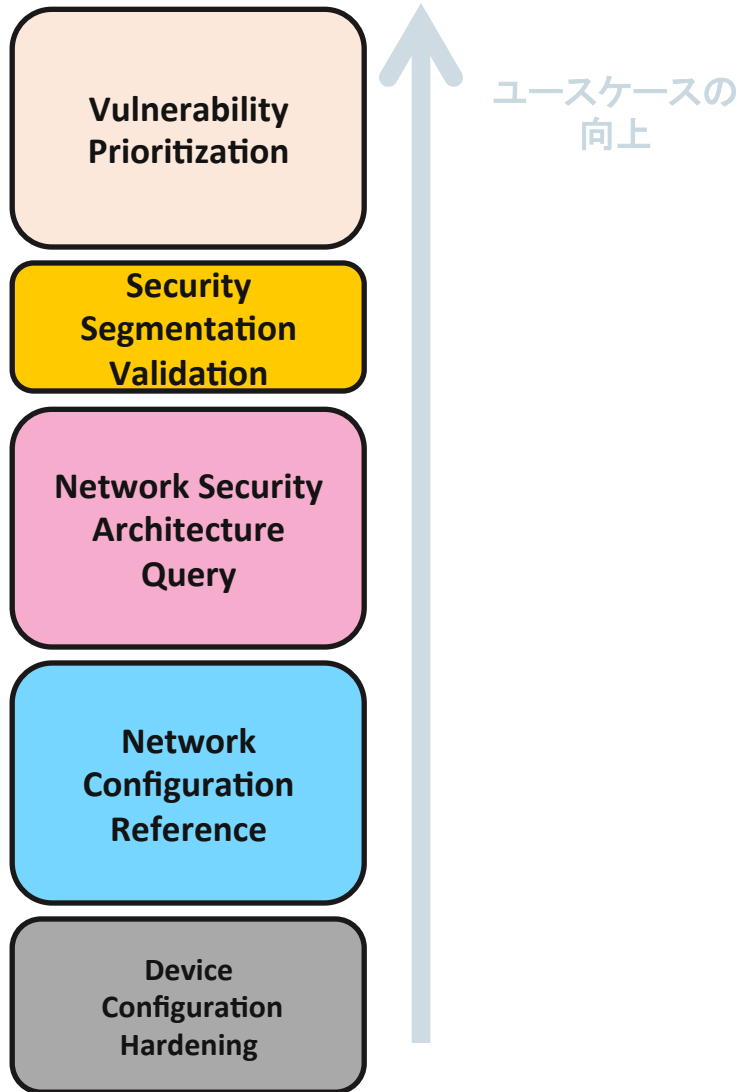
アドホックな ユースケース

プロセス 統合

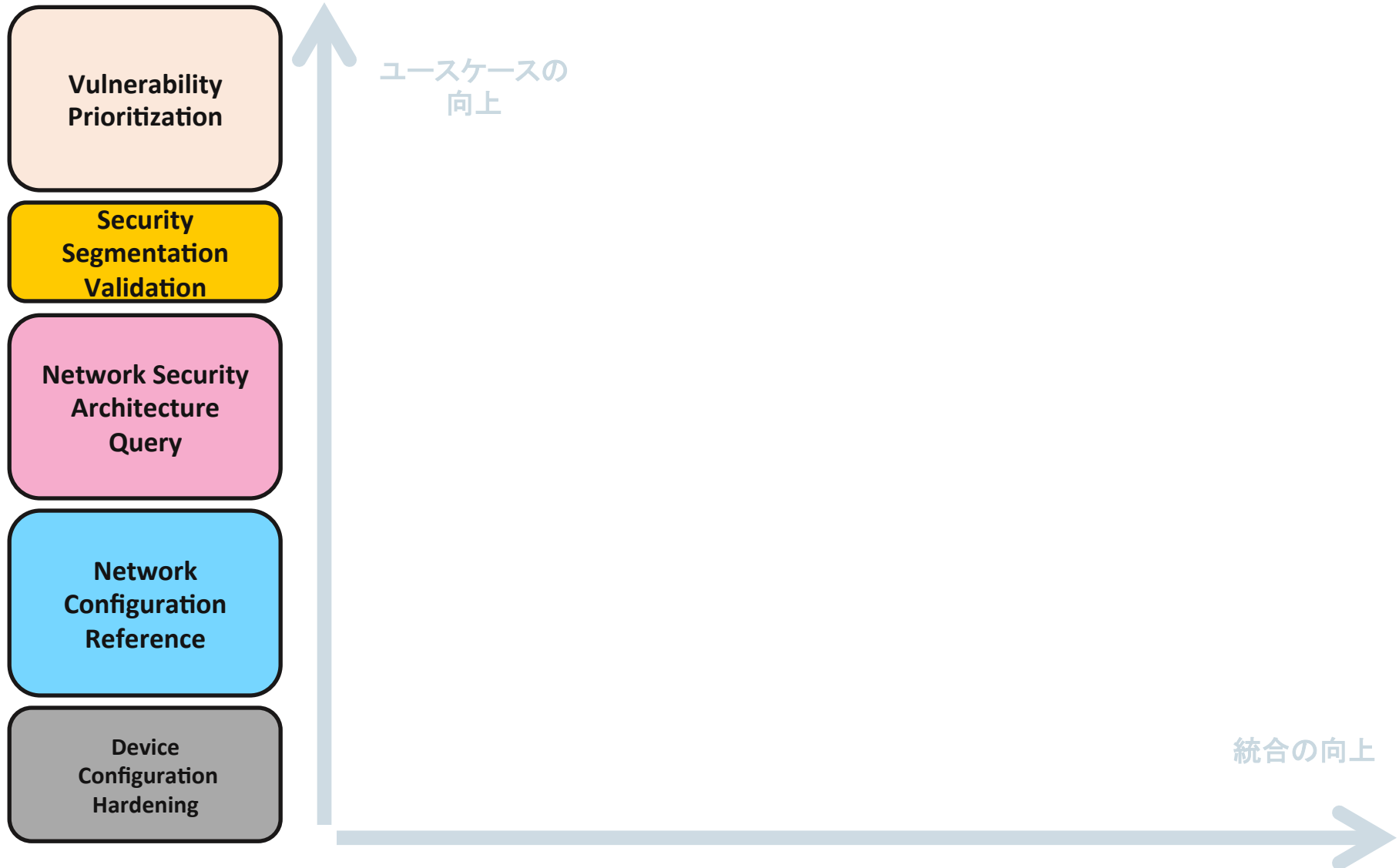
プログラム 統合



RedSeal マチュリティーモデル



RedSeal マチュリティーモデル



顧客マチュリティーモデル: 要望



顧客マチュリティーモデル: 要望

