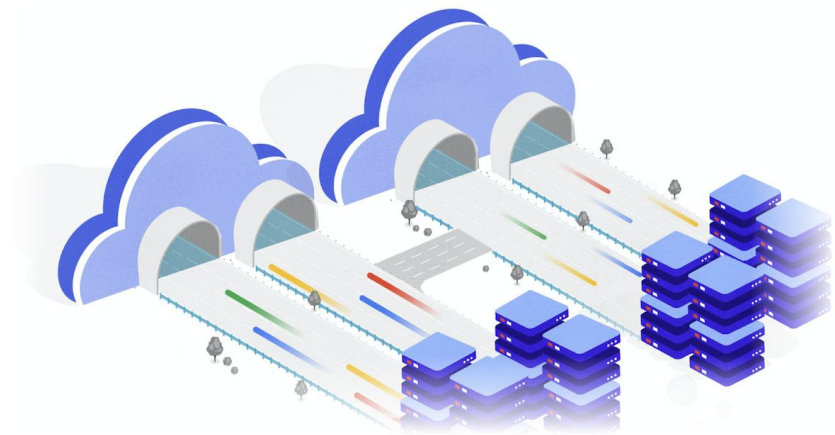


Security Command Center 紹介

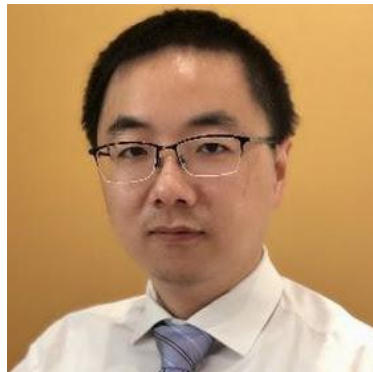
Google Cloud
カスタマー エンジニア
Mao Ye



自己紹介

叶 茂 (Mao Ye) Customer Engineer

- 職種: Google Cloud Pre-Sales Engineer
- 担当領域: Security, Networking, AI/ML
- 担当業種: 通信
- 経歴: 日系 Software Vendor の ERP 製品開発部門
外資大手金融企業の IT Architecture 部門
外資大手 Network 企業の Technical Consulting 部門
その後 Google Cloud に Join

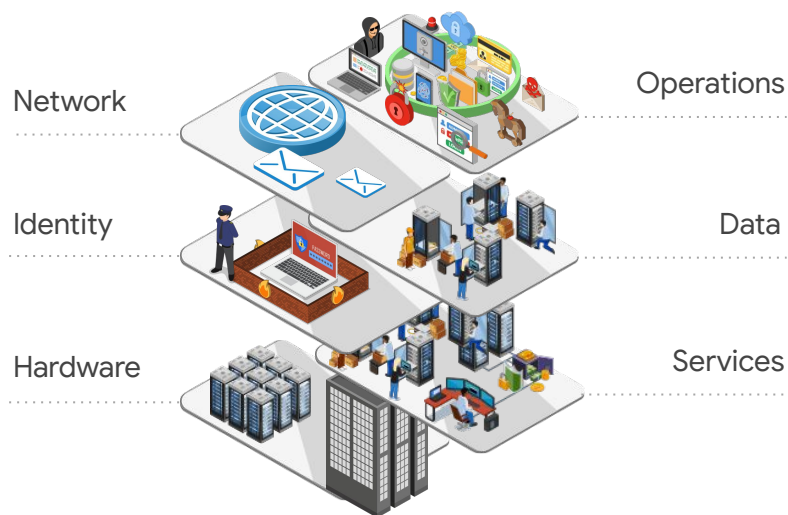


セキュアな基盤



多層防御によるセキュアなシステム

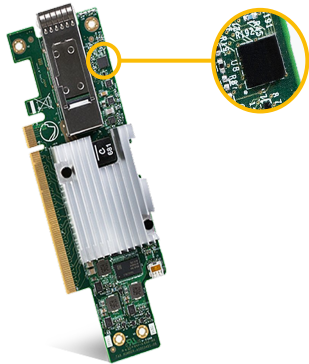
Layered Defense in Depth (多層防御)



レイヤ	主なセキュリティ対策の例
オペレーション	侵入検知システム、インサイダーリスク低減技術、従業員によるU2F 使用、ソフトウェア開発プラクティス
ネットワーク	Google Front End 、DoS 攻撃防御の組み込み
データ	保存データの暗号化
アイデンティティ	U2F サポートを含む一元的な識別サービス
サービス	サービス間通信の暗号化
ハードウェア	ハードウェアの設計と供給、ブートスタックのセキュリティ、構内セキュリティ

セキュアな基礎を用いた構成

Titan



専用の
チップ



専用の
サーバー



専用の
ストレージ



専用の
ネットワーク



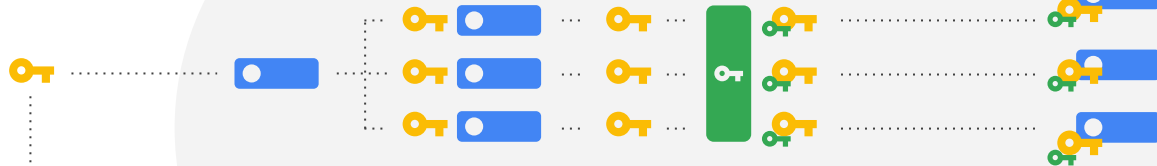
専用の
データセンター

周辺の HW、ブートは電子証明書で確認
悪意ファームウェア (UEFI、ドライバーなど) があれば検知し、起動不可能
Google の専用 TPM チップ

各層の信頼性を確認

全てデフォルトで暗号化

通信暗号
TLS



データが細分化され、細分化された個々が独自のデータ暗号鍵で暗号化される

データ暗号鍵 (DEK) が鍵暗号鍵 (KEK) でラップされる

暗号化された個々のデータとラップされた暗号鍵は、Google のストレージで配布

Google のセキュリティ基盤

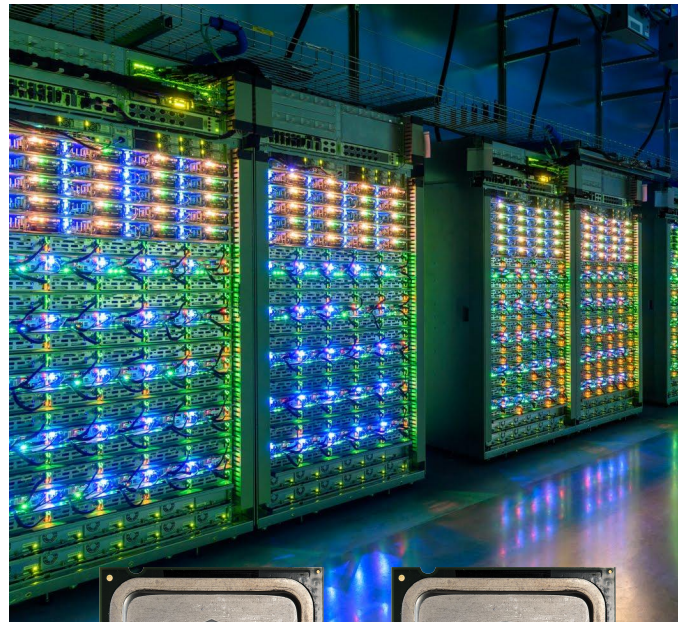
豊富なセキュリティ知識とデータ

900 人以上 セキュリティ エンジニア
アプリ設計からインフラ運用まで深く関与

Project Zero 脆弱性・攻撃コード研究
自社だけではなく、世界へも貢献

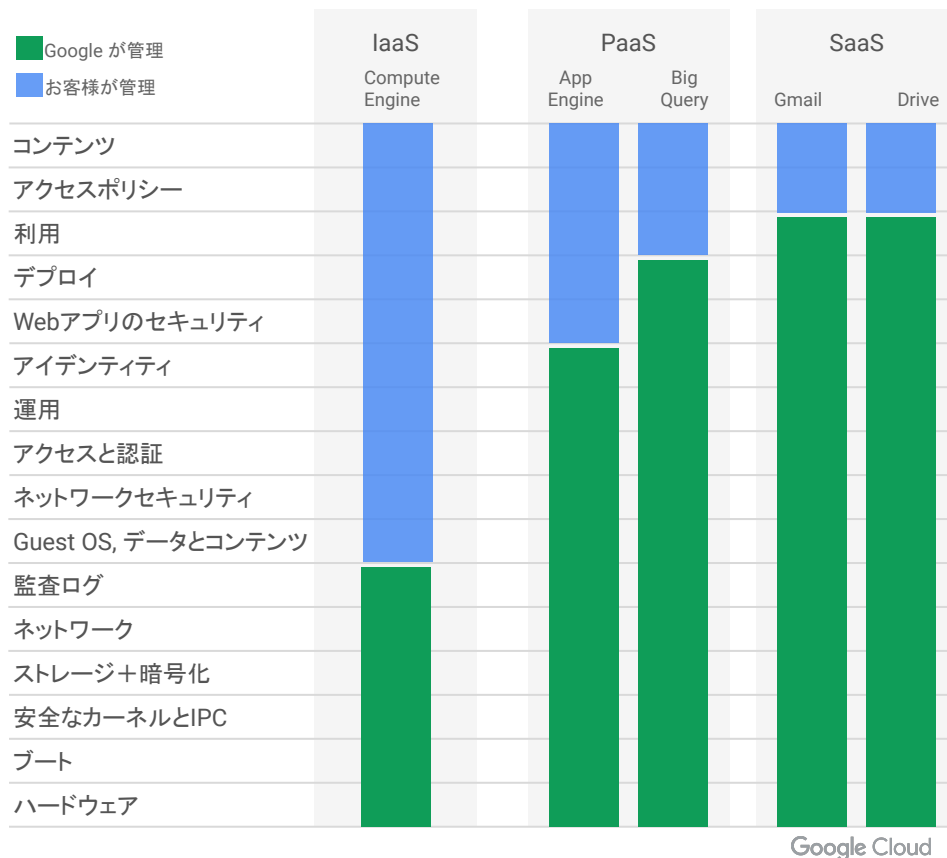
VirusTotal 豊富なマルウェア データベース

Safe browsing 悪意のあるドメイン データベース



Google の責任共有モデル

どのサービスをご利用いただくかにより
責任共有範囲が変わります



Google Cloud のセキュリティ関連サービス



ガバナンス、リスク管理 コンプライアンス

Third-party audits
International Certifications
Access Transparency
Access Approvals
Key Access Justifications
Google Vault for G Suite
Cloud Storage Retention Policy
Cloud Audit Logging

ID とアクセス管理

Cloud Identity IAM IAP Conditions Recommender Troubleshooter Validator

アプリケーションセキュリティ

ReCaptcha Web Risk BeyondCorp Cloud Security Scanner Binary Authorization

データセキュリティ

Encryption by Default CMK CSK HSM External Key Manager DLP API G Suite ACLs

インフラセキュリティ

Titan Shielded VM・GKE Binary Auth Confidential Computing Container Threat Detection

ネットワークセキュリティ

Shared VPC VPC Firewalls ALTS Cloud Armor VPC Service Controls Packet Capture

端末セキュリティ

ChromeOS Chrome Browser SafeBrowsing Device Management ChromeBook Pixel

セキュリティの 監視と業務

Stackdriver Logging,
Security Command Center
Incident Response Management
Security Health Analytics
Event Threat Detection
Cloud Anomaly Detection
VirusTotal
Chronicle

Cloud 利用者における Security リスクと挑戦



利用している Cloud Resource に対しての Visibility と Control の不足



Resource が正しく設定されているかが不明



Cloud の利用状況が Compliance 要件に順守していることを継続的にチェックしていない



攻撃を検知する能力が持ってない、足りない

Security
Command
Center (SCC) の
機能紹介



SCC : リスク管理の目標

ダッシュボードに限らず、全体的な Google Cloud リスク管理

1) 把握

- どんなアセットがあるか

2) 保護

- どんなリスクがあるか

3) 検出

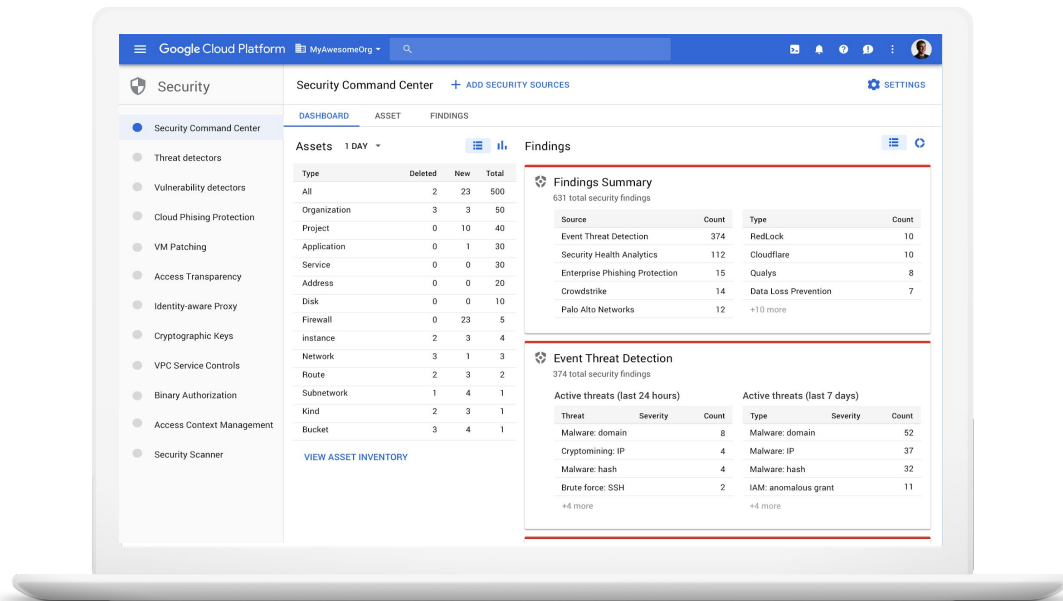
- そのリスクが実際に発生したか

4) 報告

- 報告ができるか

5) 対応

- 対応ができるか



SCC : アセット

どんなアセットがあるか明確に

- どのアセットがあるか把握可能
- 継続的に Google Cloud にあるアセットを確認
- アセットの変更履歴を含めて状況をほぼリアルタイムに把握可能
- 数分以内に新しいアセット、またはアセット変更が検出でき、通知を受け取り、アクションを実行可能

DASHBOARD

ASSET

FINDINGS

Assets

1 DAY

Type	Deleted	New	Total
All	2	23	500
Organization	3	3	50
Project	0	10	40
Application	0	1	30
Service	0	0	30
Address	0	0	20
Disk	0	0	10
Firewall	0	23	5
instance	2	3	4
Network	3	1	3
Route	2	3	2
Subnetwork	1	4	1
Kind	2	3	1
Bucket	3	4	1

VIEW ASSET INVENTORY

SCC : 脆弱性

どんなリスクがあるかを明確に

ストレージ



- 公開されているバケット
- レガシーバケット ACL の使用

ネットワーク



- オープンなファイアウォールルール
- デフォルト・レガシーネットワークの使用
- Google API へのプライベートアクセスを使用しないサブネットワーク

ログ・モニタリング



- 無効になっているモニタリング
- ロギングが無効のストレージバケット
- Kubernetes クラスタの Cloud モニタリングが有効になっていない
- VPC フローログが無効

VM



- IP フォワーディングが有効
- SSH やアクセス制御の設定ミス

GKE クラスタ



- プライベートクラスタが無効
- Network policy が無効
- マスター承認済ネットワークが無効
- IP alias が無効
- レガシーな認証が有効化されている

コンプライアンス



- CIS Benchmarks 1.0 に適合
- PCI-DSS, ISO 27001, NIST 800-53, OWASP Top 10 などにマッピング

SCC : ウェブ脆弱性

どんなリスクがあるかを明確に



自動的にアプリを発見し、スキャン実施

- GKE、GCE、GAE にあるウェブアプリを自動的に発見し、脆弱性スキャンを行う
- 定期的なスキャンをスケジュール可能、脆弱性が検出された場合は SCC で表示



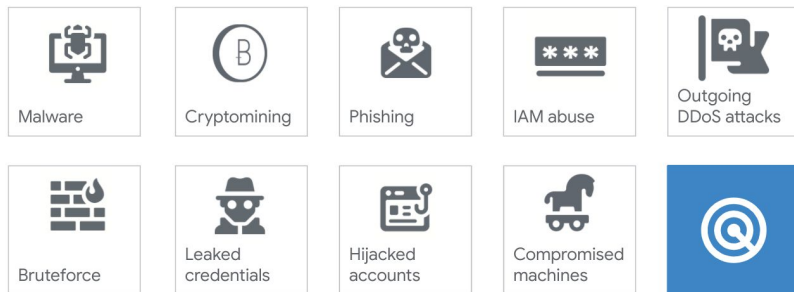
OWASP 脆弱性を検出可能

- OWASP トップ 10 を含めて、11 以上の脆弱性カテゴリを検出可能
- SCC ダッシュボードでセキュリティ状況を確認でき、脆弱性に対応する

SCC : 脅威ダッシュボード

どんな脅威が実際にあるかを明確に

- Google と同様な対策で脅威を発見
- 業界最高レベルの脅威情報 (IOC)
- ほぼリアルタイムで複数種類のログを検索し、検出結果は SCC に表示



Event Threat Detection

374 total security findings

Active threats (last 24 hours)

Threat	Severity	Count
Malware: domain		8
Cryptomining: IP		4
Malware: hash		4
Brute force: SSH		2

+4 more

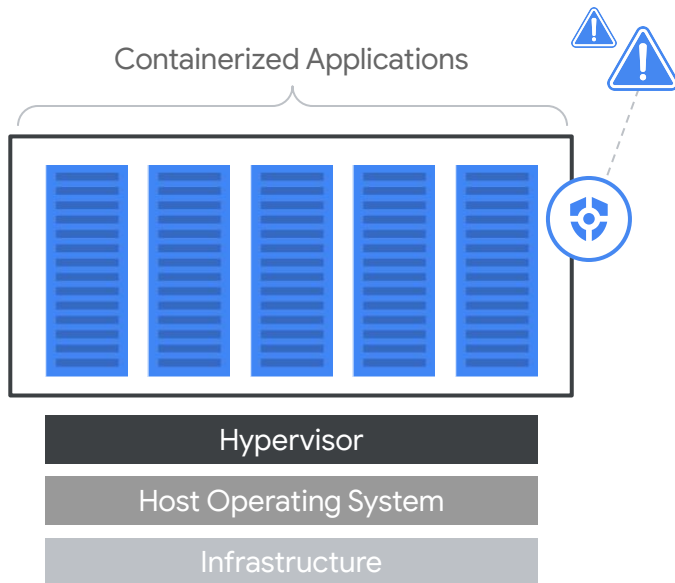
Active threats (last 7 days)

Type	Severity	Count
Malware: domain		52
Malware: IP		37
Malware: hash		32
IAM: anomalous grant		11

+4 more

SCC : コンテナ脅威も検出可能

どんな脅威が実際にあるかを明確に



不審な行動を検出

- バイナリが追加された
- ライブラリーが追加された
- リバースシェルが実行された

以下の機能と統合

- SCC ダッシュボード
- GKE でワンクリックでデプロイ
- Cloud Audit Log
- COS イメージを使えば検出はカーネルレベルで行う

SCC : 他サービスと統合

Google Cloud サービスとパートナーソフトが統合され、独自の検出内容も追加可能

Google Cloud



Binary
Authorization



Cloud
DLP API



Cloud
Security
Scanner



Forseti



Google
Anomaly
Detection



Event Threat
Detection



Security
Health
Analytics



Cloud
Armor

Partners

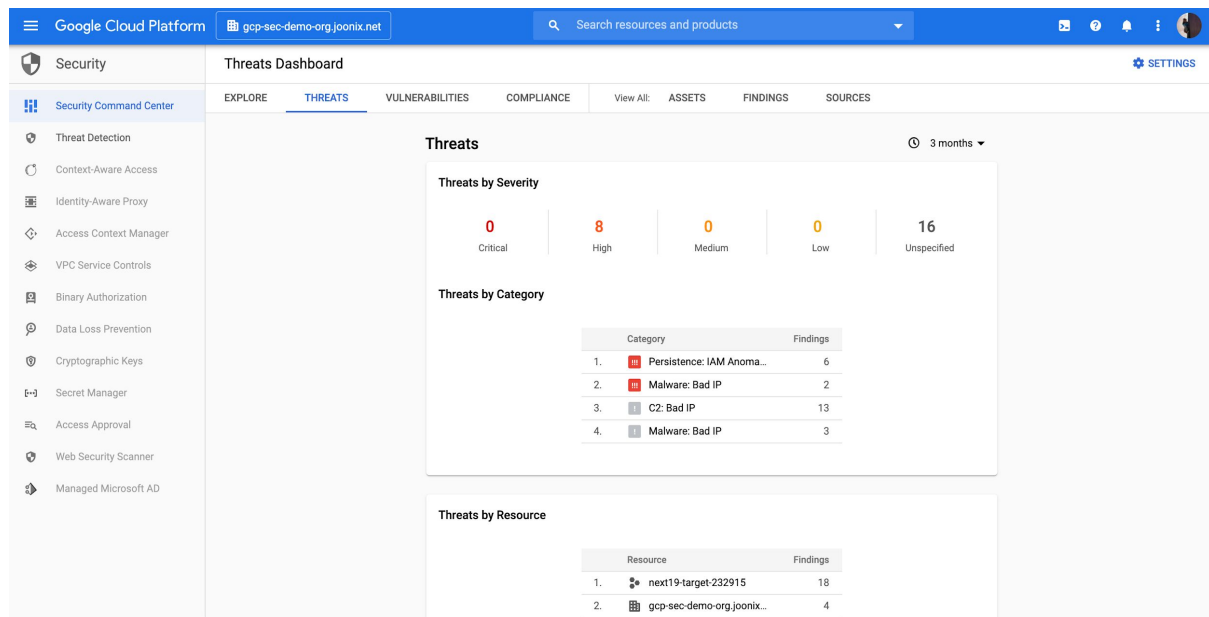


SCC : 報告

ダッシュボードで様々な情報を可視化

ダッシュボード

- 脅威
- 脆弱性
- コンプライアンス
- ソース
- アセット
- 検出結果



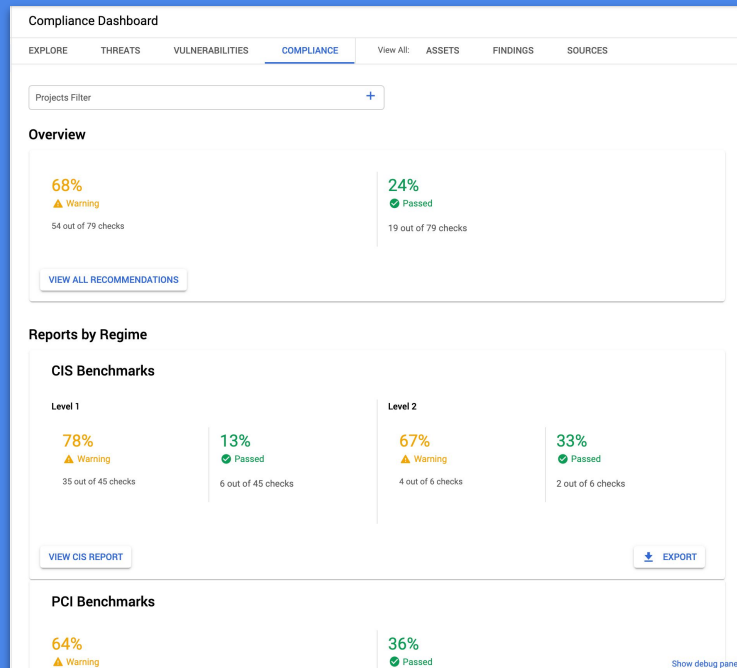
SCC : 報告

各コンプライアンス ベンチマークとの差異を報告

グローバル標準の項目を追加。その他も今後追加予定

- Center for Internet Security (CIS) 1.0 Benchmark & version 1.1 coming soon
- Payment Card Industry Data Security Standard (PCI)
- International Organization for Standardization (ISO 27001)
- National Institute of Standards and Technology (NIST 800-53)

報告



🛡️

Security Health Analytics Dashboard

⚙️ SETTINGS

EXPLORE

THREATS

VULNERABILITIES

COMPLIANCE

View All: ASSETS

FINDINGS

SOURCES

🏠

🛡️

🔄

📊

🔍

🔒

🔗

🛡️

🔧

Recommendations

Projects Filter

☰

Benchmarks : PCI

OR

Benchmarks : CIS

OR

Benchmarks : OWASP

Filter table

✕ ⓘ

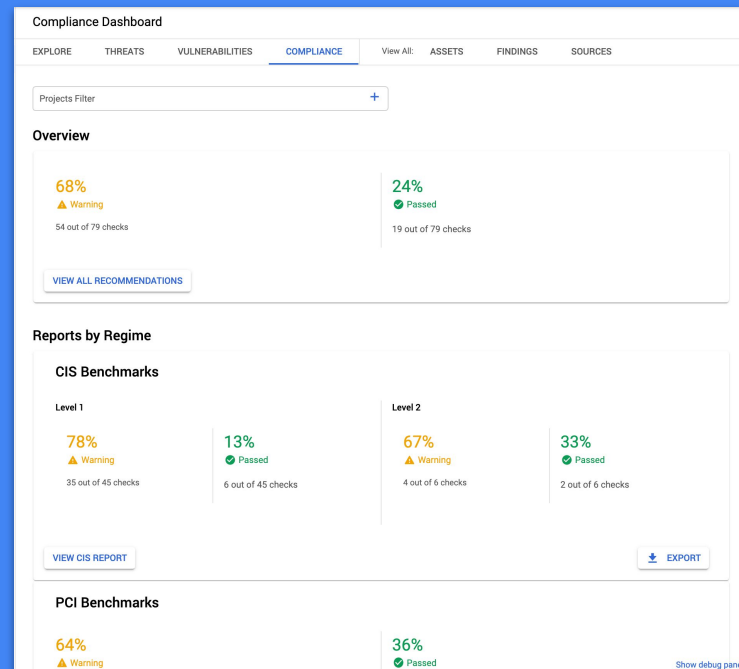
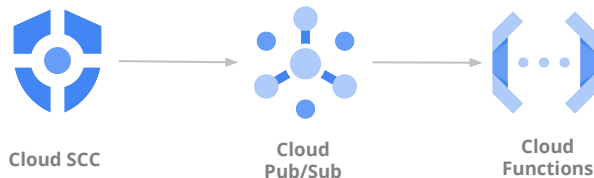
Status	Category	Recommendation	Active	Severity	↑	Benchmarks
⚠️	NON_ORG_IAM_MEMBER	Corporate login credentials should be used instead of Gmail accounts	8	🔴		CIS : 1.1 PCI : 7.1.2
⚠️	OPEN_FIREWALL	Firewall rules should not allow connections from all IP addresses	14	🔴		PCI : 1.2.1
⚠️	OPEN_RDP_PORT	Firewall rules should not allow connections from all IP addresses on TCP or UDP port 3389	48	🔴		CIS : 3.7 PCI : 1.2.1
⚠️	OPEN_SSH_PORT	Firewall rules should not allow connections from all IP addresses on TCP or SCTP port 22	74	🔴		CIS : 3.6 PCI : 1.2.1
⚠️	PUBLIC_BUCKET_ACL	Cloud Storage buckets should not be anonymously or publicly accessible	8	🔴		CIS : 5.1 PCI : 7.1
⚠️	PUBLIC_IP_ADDRESS	VMs should not be assigned public IP addresses	45	🔴		PCI : 1.2.1 PCI : 1.3.5
⚠️	PUBLIC_LOG_BUCKET	Storage buckets used as log sinks should not be publicly accessible	N/A	🔴		PCI : 10.5
⚠️	PUBLIC_SQL_INSTANCE	Cloud SQL database instances should not be publicly accessible by anyone on the internet	1	🔴		CIS : 6.2 PCI : 1.2.1
⚠️	SQL_NO_ROOT_PASSWORD	MySQL database instance should not allow anyone to connect with administrative privileges.	4	🔴		CIS : 6.3
⚠️	SSL_NOT_ENFORCED	Cloud SQL database instance should require all incoming connections to use SSL	4	🔴		CIS : 6.1 PCI : 2.3
⚠️	WEB_UI_ENABLED	Kubernetes web UI / Dashboard should be Disabled	6	🔴		CIS : 7.6 PCI : 6.5.8 PCI : 6.6
⚠️	XSS	Validate and escape untrusted user-supplied data	887	🔴		OWASP : A7
⚠️	XSS_ANGULAR_CALLBACK	Validate and escape untrusted user-supplied data handled by Angular framework	15	🔴		OWASP : A7
✅	XSS_ERROR	Validate and escape untrusted user-supplied data	0	🔴		OWASP : A7

脆弱性ダッシュボード: リスクと脆弱性の検出結果だけではなく、コンプライアンスのマッピングも明確に

SCC : 対応

自動的にリスクや脅威に対応可能

- 新しい脅威は調査し、理解することが重要
- よく理解したら、防止方法を検討
- 防止策がなく、対応がいつも同じになるのであれば、その対応を自動化
- 何かを検出したら PubSub 経由で Cloud Function を実行し、API で望ましい処理を定義可能



対応