



Visibility, prevention and detection on Google Cloud

Andy Chang
Senior Product Manager, Google Cloud Security
andychang@

Google Cloud

Agenda

- Overview Google Cloud Security
- Cloud Operations Suite (formerly Stackdriver)
- Cloud Security Command Center - Threat prevention, detection, response
- Q&A



Enterprise CISO objectives

Protect your business and your customers - connect only the right people to the right data, for the right purpose each and every time.

Meet your audit and regulatory obligations

Evolve and innovate, be proactive to stay ahead of threats

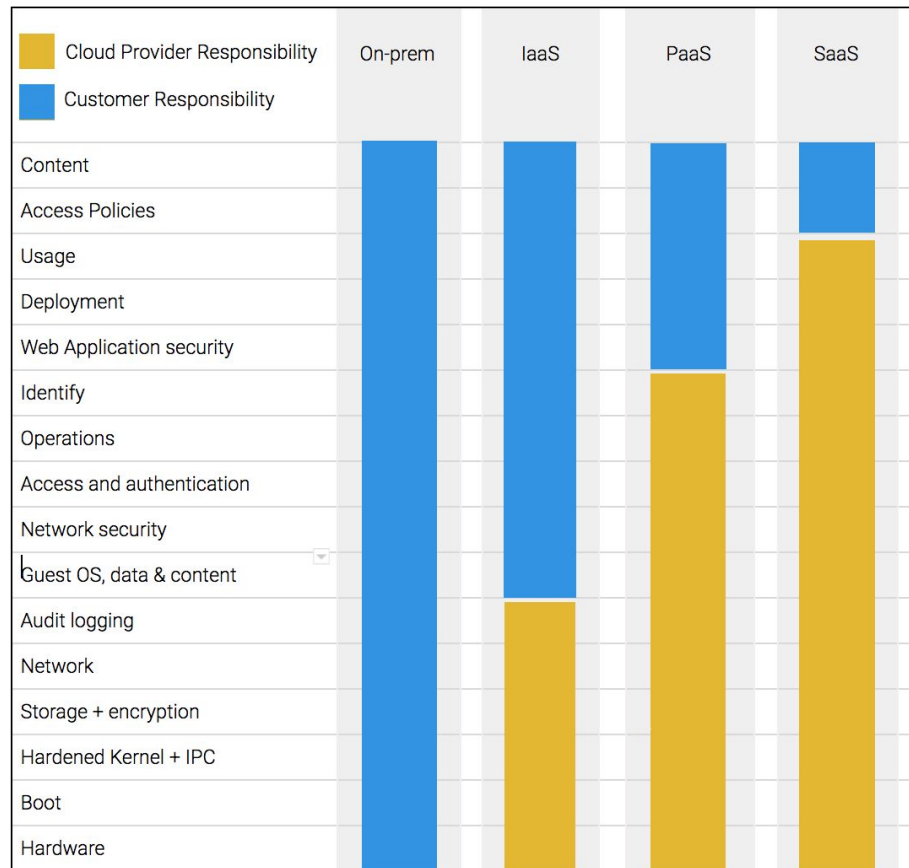
Provide sufficient visibility and control to meet the requirements of your business

Understand and be empowered to execute your part of shared responsibility model

Understanding Shared Responsibility

The **boundaries change** based on the services selected by the customer

Customers can use multiple classes of services **simultaneously**



Cloud security challenges



**Lack of visibility
and control**



**Inability to detect
and respond to
threats**



**Increase in
complexity**



Google security principles



You determine and control what happens to your data

Defense *in depth, at scale, by default*

Identity as the perimeter supported by hardware attestation and provenance

Move security policy, controls, enforcement and detection *up the stack*

Transparency - reduce the unverifiable trust surface including

Customers have the **control** and **visibility** they need to help build secure apps and businesses in the cloud in an easy and effective way

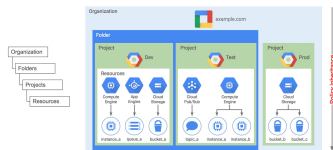
Control & Visibility



Leverage native built-in security



Resource Hierarchy



Organization Policies



Curated IAM Roles Policy Intelligence



Encryption: Default/CMEK/EKM



VPC Service Controls



Shared VPC's



Binary Authorization



Access Approvals



BeyondCorp Remote Access





Control: top-down, logically central, globally distributed

Leverage native built-in security



Cloud Security Command Center Cloud Operations Suite and Logging

Access Transparency/
Access Justifications
Key Access Justifications



Cloud DLP API



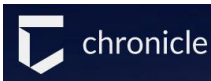
Config Validator



Container
Vuln Scanning



Chronicle



Third party review,
validation & certifications



Visibility: Cloud Operations Suite

Cloud Operations Suite provides **comprehensive observability** of Cloud Operations at scale for all **GCP customers**. It helps Developers and Operators efficiently run their workloads and keep their systems and applications fast and available

The best solution for GCP. Works on **every** GCP-managed environment

Observability of workloads running in Google Cloud, on prem and in other clouds through **Anthos**

Set SREs up for success! Made for **scaling data analytics and greater automation** - this is what we at Google do best!

1

Value Proposition

2

Differentiation Statement

3

How our customers succeed

Visibility: Security Command Center - Premium & Std

Google Cloud Platform | gcp-sec-demo-org.joomla.net

Security Command Center + ADD SECURITY SOURCES

DASHBOARD ASSETS FINDINGS

Assets 14y ▼

3008 total assets

Asset	New	Deleted	Total
Route	21	0	999
Subnetwork	20	0	923
Firewall	6	0	224
containerImage	1	0	169
ServiceAccount	5	0	125
Bucket	2	0	94
Disk	6	12	80
computeInstance	6	6	69
resourceManagerProject	3	0	55
Version	0	0	50
Network	1	0	49
computeProject	1	0	44
Service	0	0	17
InstanceTemplate	2	4	17
Application	1	0	13
HttpHealthCheck	0	0	12
InstanceGroup	0	2	12
BackendService	0	0	9
Cluster	0	0	8
Snapshot	0	0	7
Address	1	0	5
sqlInstance	1	0	4
Phone	0	0	4

Findings

Security Health Analytics

1,045 current findings

Finding	Count
OPEN_FIREWALL	165
PUBLIC_BUCKET_ACL	7
PUBLIC_IP_ADDRESS	67
SSL_NOT_ENFORCED	2
WEB_UI_ENABLED	5

+22 More

Event Threat Detection

8 current findings

Finding	Count
Persistence: iam Anomalous Grant	8

Findings Summary

7,857 total security findings for the organization

Source	Findings
Access Transparency	7

Cloud Anomaly Detection

7 current findings

Finding	Count
account_hak_khaled_credentials	1

Google Cloud Platform | gcp-sec-demo-org.joomla.net

Assets

View by: [Asset type] [Asset type] [Asset type]

Search source type

Asset type	Asset ID	Findings	Severity	Asset owner
computeInstance	gcp-sec-demo-vm-1	1	High	user@domain.com
computeInstance	gcp-sec-demo-vm-2	1	High	user@domain.com
computeInstance	gcp-sec-demo-vm-3	1	High	user@domain.com
computeInstance	gcp-sec-demo-vm-4	1	High	user@domain.com
computeInstance	gcp-sec-demo-vm-5	1	High	user@domain.com
computeInstance	gcp-sec-demo-vm-6	1	High	user@domain.com
computeInstance	gcp-sec-demo-vm-7	1	High	user@domain.com
computeInstance	gcp-sec-demo-vm-8	1	High	user@domain.com
computeInstance	gcp-sec-demo-vm-9	1	High	user@domain.com
computeInstance	gcp-sec-demo-vm-10	1	High	user@domain.com
computeInstance	gcp-sec-demo-vm-11	1	High	user@domain.com
computeInstance	gcp-sec-demo-vm-12	1	High	user@domain.com
computeInstance	gcp-sec-demo-vm-13	1	High	user@domain.com
computeInstance	gcp-sec-demo-vm-14	1	High	user@domain.com
computeInstance	gcp-sec-demo-vm-15	1	High	user@domain.com
computeInstance	gcp-sec-demo-vm-16	1	High	user@domain.com
computeInstance	gcp-sec-demo-vm-17	1	High	user@domain.com
computeInstance	gcp-sec-demo-vm-18	1	High	user@domain.com
computeInstance	gcp-sec-demo-vm-19	1	High	user@domain.com
computeInstance	gcp-sec-demo-vm-20	1	High	user@domain.com

Google Cloud Platform | gcp-sec-demo-org.joomla.net

Findings

View by: [Findings type] [Findings type] [Findings type]

Filter by attributes, properties and rules

Asset type	Category	ResourceName	Asset ID	Findings Count	Parent	Severity
computeInstance	Security Health Analytics	gcp-sec-demo-vm-1	gcp-sec-demo-vm-1	1	gcp-sec-demo-vm-1	High
computeInstance	Security Health Analytics	gcp-sec-demo-vm-2	gcp-sec-demo-vm-2	1	gcp-sec-demo-vm-2	High
computeInstance	Security Health Analytics	gcp-sec-demo-vm-3	gcp-sec-demo-vm-3	1	gcp-sec-demo-vm-3	High
computeInstance	Security Health Analytics	gcp-sec-demo-vm-4	gcp-sec-demo-vm-4	1	gcp-sec-demo-vm-4	High
computeInstance	Security Health Analytics	gcp-sec-demo-vm-5	gcp-sec-demo-vm-5	1	gcp-sec-demo-vm-5	High
computeInstance	Security Health Analytics	gcp-sec-demo-vm-6	gcp-sec-demo-vm-6	1	gcp-sec-demo-vm-6	High
computeInstance	Security Health Analytics	gcp-sec-demo-vm-7	gcp-sec-demo-vm-7	1	gcp-sec-demo-vm-7	High
computeInstance	Security Health Analytics	gcp-sec-demo-vm-8	gcp-sec-demo-vm-8	1	gcp-sec-demo-vm-8	High
computeInstance	Security Health Analytics	gcp-sec-demo-vm-9	gcp-sec-demo-vm-9	1	gcp-sec-demo-vm-9	High
computeInstance	Security Health Analytics	gcp-sec-demo-vm-10	gcp-sec-demo-vm-10	1	gcp-sec-demo-vm-10	High
computeInstance	Security Health Analytics	gcp-sec-demo-vm-11	gcp-sec-demo-vm-11	1	gcp-sec-demo-vm-11	High
computeInstance	Security Health Analytics	gcp-sec-demo-vm-12	gcp-sec-demo-vm-12	1	gcp-sec-demo-vm-12	High
computeInstance	Security Health Analytics	gcp-sec-demo-vm-13	gcp-sec-demo-vm-13	1	gcp-sec-demo-vm-13	High
computeInstance	Security Health Analytics	gcp-sec-demo-vm-14	gcp-sec-demo-vm-14	1	gcp-sec-demo-vm-14	High
computeInstance	Security Health Analytics	gcp-sec-demo-vm-15	gcp-sec-demo-vm-15	1	gcp-sec-demo-vm-15	High
computeInstance	Security Health Analytics	gcp-sec-demo-vm-16	gcp-sec-demo-vm-16	1	gcp-sec-demo-vm-16	High
computeInstance	Security Health Analytics	gcp-sec-demo-vm-17	gcp-sec-demo-vm-17	1	gcp-sec-demo-vm-17	High
computeInstance	Security Health Analytics	gcp-sec-demo-vm-18	gcp-sec-demo-vm-18	1	gcp-sec-demo-vm-18	High
computeInstance	Security Health Analytics	gcp-sec-demo-vm-19	gcp-sec-demo-vm-19	1	gcp-sec-demo-vm-19	High
computeInstance	Security Health Analytics	gcp-sec-demo-vm-20	gcp-sec-demo-vm-20	1	gcp-sec-demo-vm-20	High



Cloud Operations Suite:

Capture events in your system

With **Cloud Operations Suite** you are able to

- **Collect** signals across GCP internal/external apps, platforms and services
- **Analyze** and visualize those signals
- Set up appropriate performance and availability **indicators**
- Use built-in observability to **troubleshoot** and improve your applications.
- **Automate** Ops using programmatic interfaces and out-of-the-box practices

1

Value Proposition

2

Differentiation Statement

3

How our customers succeed

Customer use cases

- Can you help us **discover/map** our workloads?
- Can you **show us how** our cloud deployment is behaving?
- Can you tell us **when** we are broken?
- Can you help us **root cause, remediate, and resolve** issues?
- Can you help us **reduce** our cost?

Cloud Security Command Center: Visibility, prevention, detection and response



Manage and review your security posture from one place in Google Cloud

Security Command Center



Organizational level visibility, management, and control of your security posture



Prevent threats with vulnerability and misconfiguration detections



Detect and respond to active threats against your cloud assets

Google Cloud Platform | gcp-sec-demo-org.joonix.net | Search resources and products

Security

Threats Dashboard

EXPLORE | **THREATS** | VULNERABILITIES | COMPLIANCE | View All: ASSETS | FINDINGS | SOURCES

Threats

3 months

Threats by Severity

0	8	0	0	16
Critical	High	Medium	Low	Unspecified

Threats by Category

Category	Findings
1. Persistence: IAM Anoma...	6
2. Malware: Bad IP	2
3. C2: Bad IP	13
4. Malware: Bad IP	3

Threats by Resource

Resource	Findings
1. next19-target-232915	18
2. gcp-sec-demo-org.joonix...	4



Security Command Center

Premium

Advanced features for near-real-time prevention, detection, response and compliance

Paid Service

Standard

Security foundation - visibility w/ scans for key vulnerabilities and abuse

Free service

Security Command Center Premium



Prevent threats

Web Security Scanner with managed scans

Security Health Analytics
continuous compliance



Detect threats

Cloud Abuse Detection

Event Threat Detection

Container Threat Detection (Beta)

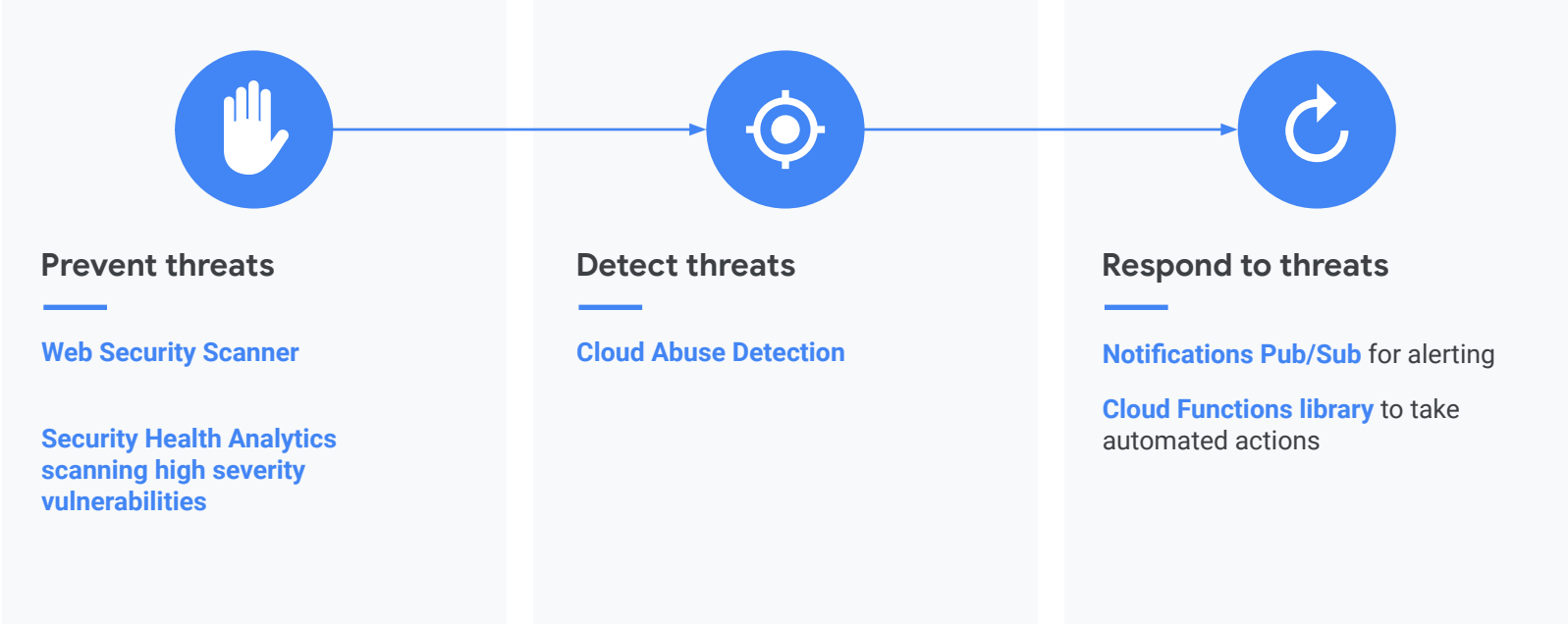


Respond to threats

Notifications Pub/Sub for alerting

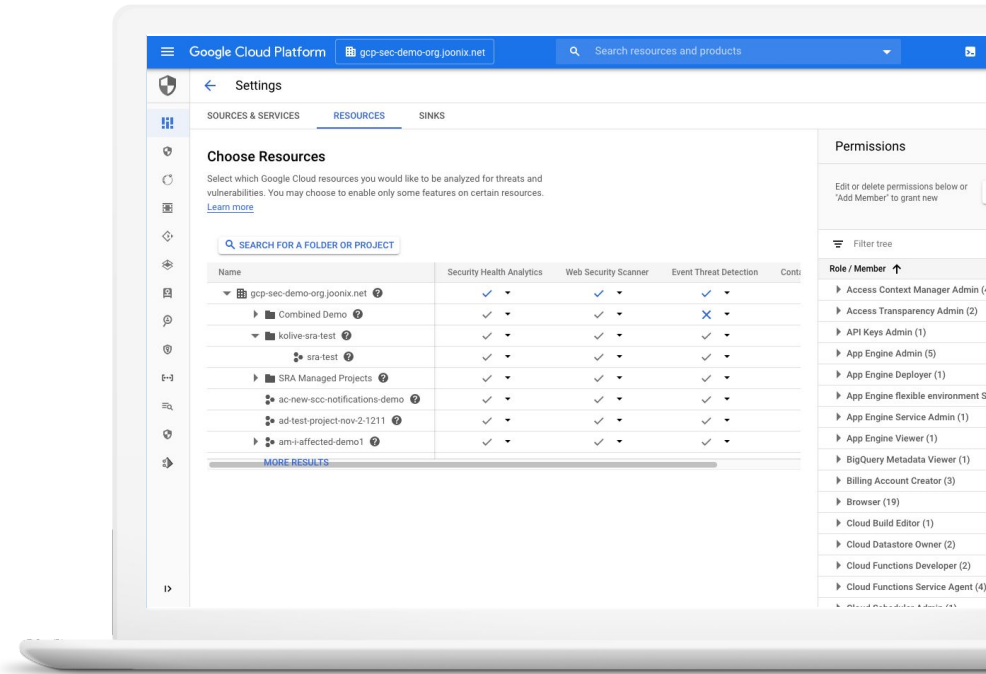
Cloud Functions library to take automated actions

Security Command Center Standard



Organization onboarding and configuration

- **Organization level configuration and onboarding:** Control threat and vulnerability detection from the top of your hierarchy for current and future projects. Protection for new resources happens immediately, without security team toil
- **Common IAM roles:** Curated IAM roles with necessary permissions to operate across findings providers
- **Common UI and API:** Consistent set of gcloud commands to manage all threat prevention and detection



Security Command Center Dashboards

Built in monitoring and visibility:

- Threat Dashboard
- Vulnerability Dashboard
- Compliance Dashboard
- View All: ASSETS FINDINGS SOURCES
- Source Dashboard
- Asset inventory
- Findings Inventory

Google Cloud Platform gcp-sec-demo-org.joonix.net Search resources and products

Security Threats Dashboard SETTINGS

EXPLORE THREATS VULNERABILITIES COMPLIANCE View All: ASSETS FINDINGS SOURCES

Threats 3 months

Threats by Severity

0	8	0	0	16
Critical	High	Medium	Low	Unspecified

Threats by Category

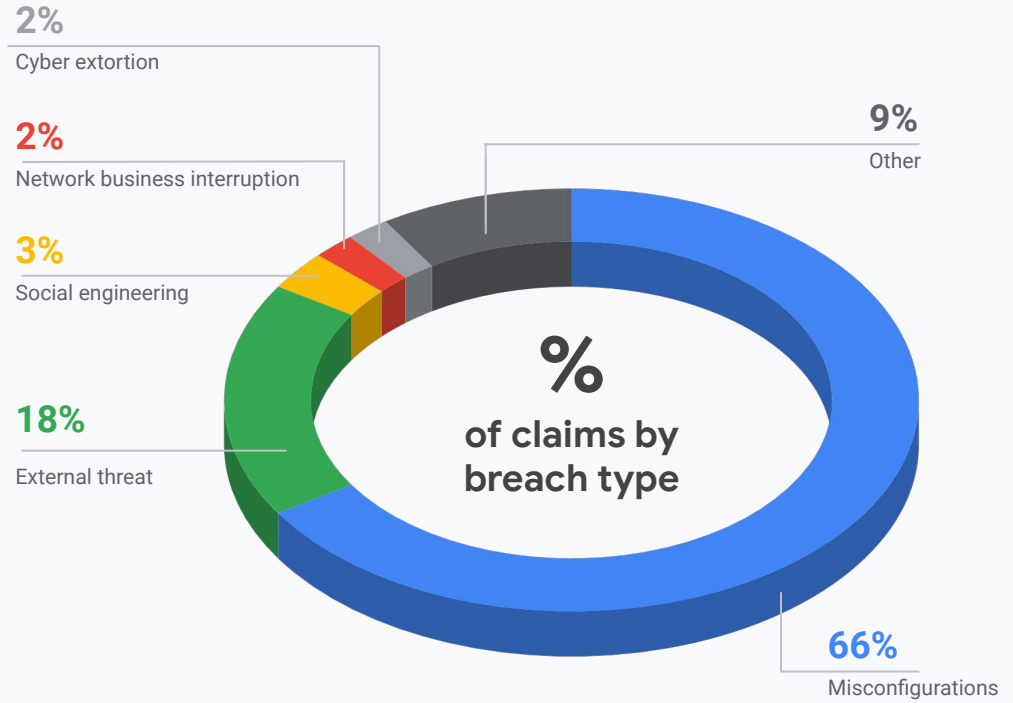
Category	Findings
1. Persistence: IAM Anoma...	6
2. Malware: Bad IP	2
3. C2: Bad IP	13
4. Malware: Bad IP	3

Threats by Resource

Resource	Findings
1. next19-target-232915	18
2. gcp-sec-demo-org.joonix...	4

Prevent threats

Misconfigurations are the largest cause of breaches!





Prevent threats and meet compliance requirements with visibility and control over GCP data and resources

- Take inventory of your cloud assets
- View Google Cloud Platform resources and partner solutions
- Identify misconfigurations, vulnerabilities and compliance violations and reduce your exposure to threats



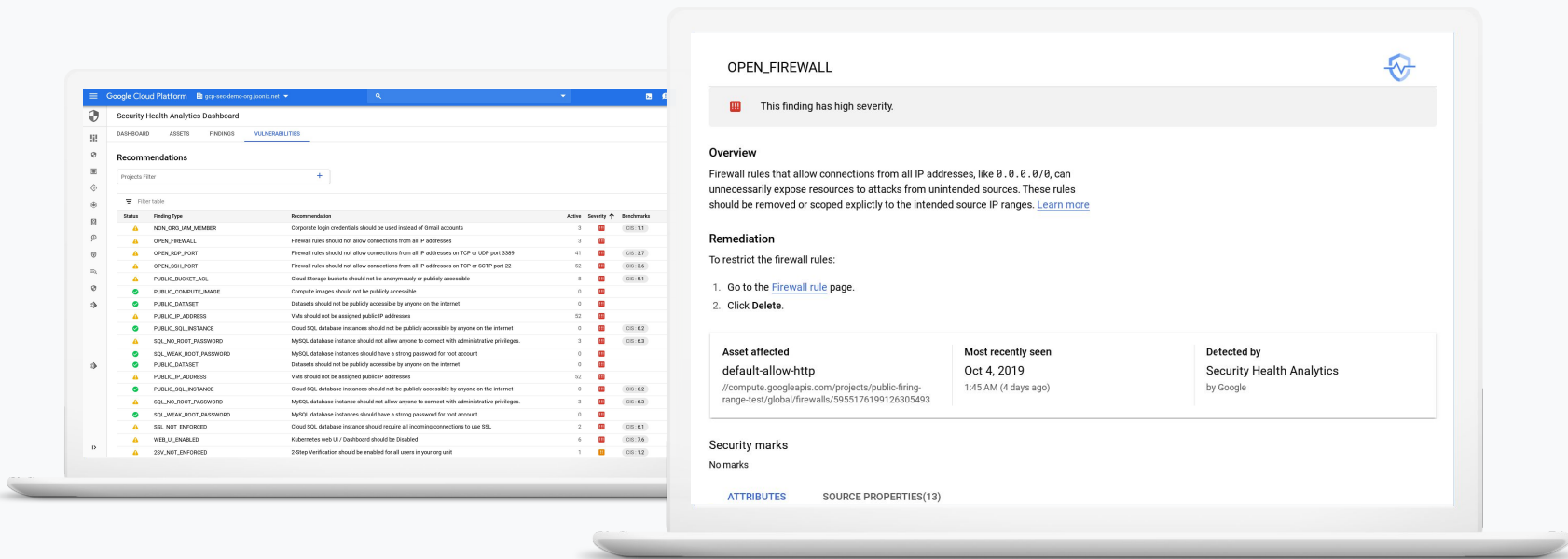
Type	Deleted	New	Total
All	2	23	500
Organization	3	3	50
Project	0	10	40
Application	0	1	30
Service	0	0	30
Address	0	0	20
Disk	0	0	10
Firewall instance	2	3	4
Network	3	1	3
Route	2	3	2
Subnetwork	1	4	1
Kind	2	3	1
Bucket	3	4	1

[VIEW ASSET INVENTORY](#)

Status	Category	Recommendation	Active	Severity	Benchmark
▲	NON_ORG_IAM_MEMBER	Corporate login credentials should be used instead of Gmail accounts	8	High	CIS 1.1 PCI 7.1.2
▲	OPEN_FIREWALL	Firewall rules should not allow connections from all IP addresses	14	High	PCI 1.2.1
▲	OPEN_RDP_PORT	Firewall rules should not allow connections from all IP addresses on TCP or UDP port 3389	48	High	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	High	CIS 3.6 PCI 1.2.1
▲	PUBLIC_BUCKET_ACL	Cloud Storage buckets should not be anonymously or publicly accessible	8	High	CIS 5.1 PCI 7.1
▲	PUBLIC_IP_ADDRESS	VMs should not be assigned public IP addresses	45	High	CIS 1.2.1 PCI 1.3.5
○	PUBLIC_LOG_BUCKET	Storage buckets used as log sinks should not be publicly accessible	N/A	High	PCI 10.5
▲	PUBLIC_SQL_INSTANCE	Cloud SQL database instances should not be publicly accessible by anyone on the internet	1	High	CIS 6.2 PCI 1.2.1
▲	SQL_NO_ROOT_PASSWORD	MySQL database instance should not allow anyone to connect with administrative privileges.	4	High	CIS 6.3
▲	SSL_NOT_ENFORCED	Cloud SQL database instance should require all incoming connections to use SSL.	4	High	CIS 6.1 PCI 2.3
▲	WEB_UI_ENABLED	Kubernetes web UI / Dashboard should be Disabled	6	High	CIS 7.4 PCI 6.5.8 PCI 6.6
▲	XSS	Validate and escape untrusted user supplied data	887	High	OWASP A7
▲	XSS_AJAX_CALLBACK	Validate and escape untrusted user supplied data handled by Angular framework	15	High	OWASP A7
●	XSS_ERROR	Validate and escape untrusted user supplied data	0	High	OWASP A7

Security Health Analytics

Analytics dashboard helps you to view security misconfigurations by severity, CIS Benchmark, or project -- and take action.



Security Health Analytics Compliance

Standards



- CIS GCP Foundation 1.0
- PCI
- ISO 27001
- NIST 800-53
- More to come...

Dashboard



- Standard specific
- Filterable by resource hierarchy

Reporting



- Standard specific
- Filterable by resource hierarchy
- Exportable to .csv

Security Health Analytics examples of misconfiguration and compliance violations detected

Storage



- Publicly exposed buckets
- Use of legacy bucket ACLs

Networking



- Overly permissive firewall rules
- Use of default and/or legacy networks
- Subnetworks that do not use private access to Google APIs

Logging/ Monitoring



- Monitoring disabled
- Storage buckets with logging disabled
- Stackdriver monitoring for Kubernetes clusters not enabled
- VPC Flow logs disabled

VM Instances



- IP forwarding enabled
- SSH and access misconfigurations

GKE Clusters



- Private cluster disabled
- Network policy disabled
- Master authorized network disabled
- IP alias disabled
- Legacy authorization enabled

CIS Benchmarks

- Monitoring against the CIS GCP Foundation benchmark
- Certified for CIS Benchmarks 1.0, with more certifications to come

How Security Health Analytics works in 3 steps



Leverages built-in
GCP configurations
checks for assets

Processes
configurations and
monitors for
violations

Misconfigurations
with actionable
recommendations
are surfaced in the
Vulnerabilities
dashboard

Web application vulnerabilities

Detected by Web Security Scanner for web apps built on Google Cloud Platform



Cross-site scripting

- XSS Callback
- XSS Angular Callback
- XSS Error



Vulnerable resources

- Accessible GIT repository
- Accessible SVN repository
- Insecure library
- Clear text password
- Rosetta flash



Misconfigurations

- Mixed content
- Invalid headers
- Invalid content type
- Misspelled Security Header Name
- Mismatching Security Header Values

How Web Security Scanner works in 3 steps



Create a scan configuration, telling the scanner where your web app is and where it's not allowed to go.

Scans run on the schedule you configure, navigate through your website and attempt to find real vulnerabilities.

Vulnerabilities are reported in Cloud Security Command Center for review.



Detect and respond to threats targeting your GCP assets

- Detect compromised machines and other anomalous activity
- Industry-leading threat intelligence surfaces suspicious activity within Stackdriver security logs
- Take action on security risks

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

Cloud Anomaly Detection

9 current findings

Finding	Count
Leaked Credentials	2
Data Exfiltration Risk	2
Intrusion Attempt	1
Resource Compromised	1

Event Threat Detection

- Inspired by how Google protects itself
- Powered by industry-leading threat intelligence
- Near real-time detection against platform, network, and compute logs

Event Threat Detection					
374 total security findings					
Active threats (last 24 hours)			Active threats (last 7 days)		
Threat	Severity	Count	Type	Severity	Count
Malware: domain		8	Malware: domain		52
Cryptomining: IP		4	Malware: IP		37
Malware: hash		4	Malware: hash		32
Brute force: SSH		2	IAM: anomalous grant		11
+4 more			+4 more		

Event Threat Detection **Current**



Malware



Cryptomining



Phishing



IAM abuse



Outgoing
DDoS attacks



Bruteforce



Leaked
credentials



Hijacked
accounts



Compromised
machines



How Event Threat Detection works in 3 steps



- Cloud Audit Logs
- VPC Flow logs
- Cloud DNS logs
- syslog via fluentd

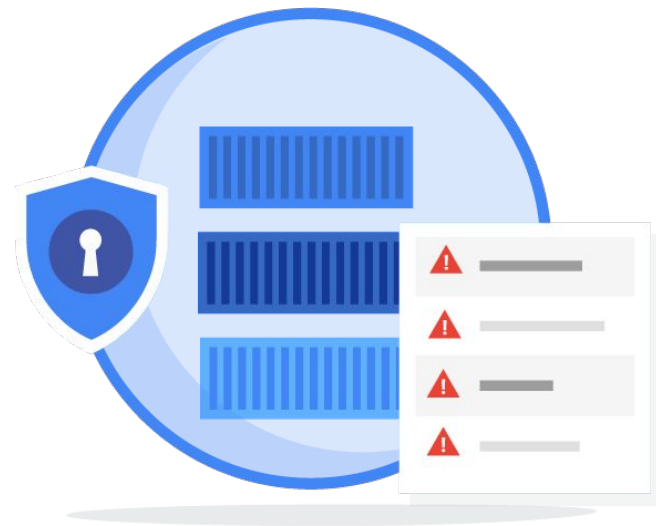
Processes logs using Detection Logic + Google Threat Intelligence

Remediate findings in **Security Command Center** using **Cloud Pub/Sub** and **Cloud Functions**



Container Threat Detection^{Beta} detects common threats against containers

- Kernel-level detection for top attacker techniques
 - Execution of added binaries
 - Execution of new library linking
 - Opening shells to the Internet
- Integrations with
 - Cloud Security Command Center
 - GKE for one-click deployment
- Kernel integrations available in COS
- Managed daemonset deployment





Alert and respond to threats targeting your Google Cloud Platform resources

- Define a query that generates a Cloud Pub/Sub event
- Build or leverage existing Cloud Functions on [GitHub](#) to take specific actions on Cloud Pub/Sub events

Name	Region	Trigger	Runtime	Memory allocated	Executed function	Last deployed
bucket-acl	us-central1	Topic: bucket-acl	Python 3.7	256 MB	remove_bucket_acls	4/5/19, 6:46 PM
firewall-repair	us-central1	Topic: firewall	Python 3.7	256 MB	disable_rules	4/5/19, 6:34 PM
logger	us-central1	Topic: logger	Node.js 6	256 MB	log	4/2/19, 10:38 AM
transformer	us-central1	Topic: endpoint	Node.js 6	256 MB	transform	4/3/19, 8:20 AM
vm-snapshot	us-central1	Topic: vm-snapshot	Python 3.7	256 MB	create_snapshot	4/5/19, 7:28 PM



Integrate with your heterogenous, multi-platform environment

- Leverage the Command Center REST API or console to access assets and findings and easily integrate with existing systems
- Export findings to your SIEM
- Take advantage of existing partner solutions you're using on-premises and use them in Google Cloud



Cloudflare

1,545 current security findings

Top threat origins	Finding count
United states	405
Thailand	376
Vietnam	206

Type of threats	%
IP address block	25%
Country block	75%

Firewall events	Last seen
Rule 1001 199.15.244 UX..	1 hour ago
Rule 3211 XSS ES Block	2 hours ago



Forseti Security

126 current findings

Finding	Count
IAM Policy Violation	65
Firewall Deny Violation	14
Bucket Violation	6
IAP Violation	2

+3 more



Palo Alto Networks

45 current findings

Finding type	Count
Wildfire-virus	12
virus	9
spyware	8
vulnerability	4



SCC supports findings from Google security products and partner security products

Google



Partners





Cloud Security Command Center is the cloud security posture management tool for Google Cloud Platform that helps you prevent, detect, and respond to threats.



Thank you

Google Cloud