Visibility, prevention and detection on Google Cloud

Andy Chang
Senior Product Manager, Google Cloud Security
andychang@
Agenda

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

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

Control: top-down, logically central, globally distributed
Leverage native built-in security
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!
Visibility: Security Command Center - Premium & Std
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
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
Security Command Center

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

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

Paid Service

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**

**Prevent threats**
- Web Security Scanner
- Security Health Analytics scanning high severity vulnerabilities

**Detect threats**
- Cloud Abuse Detection

**Respond to threats**
- Notifications Pub/Sub for alerting
- Cloud Functions library to take automated actions
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
- Source Dashboard
- Asset inventory
- Findings Inventory
Prevent threats

Misconfigurations are the largest cause of breaches!

- Misconfigurations: 66%
- External threat: 18%
- Social engineering: 3%
- Network business interruption: 2%
- Cyber extortion: 2%
- Other: 9%
- Other claims by breach type: 66%
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

Google Cloud
Security Health Analytics

Analytics dashboard helps you to view security misconfigurations by severity, CIS Benchmark, or project -- and take action.
<table>
<thead>
<tr>
<th>Standards</th>
<th>Dashboard</th>
<th>Reporting</th>
</tr>
</thead>
</table>
| • CIS GCP Foundation 1.0  
• PCI  
• ISO 27001  
• NIST 800-53  
• More to come... | • Standard specific  
• Filterable by resource hierarchy | • Standard specific  
• Filterable by resource hierarchy  
• Exportable to .csv |
## Security Health Analytics examples of misconfiguration and compliance violations detected

<table>
<thead>
<tr>
<th>Storage</th>
<th>Networking</th>
<th>Logging/ Monitoring</th>
<th>CIS Benchmarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Publicly exposed buckets</td>
<td>• Overly permissive firewall rules</td>
<td>• Monitoring disabled</td>
<td>• Monitoring against the CIS GCP Foundation benchmark</td>
</tr>
<tr>
<td>• Use of legacy bucket ACLs</td>
<td>• Use of default and/or legacy networks</td>
<td>• Storage buckets with logging disabled</td>
<td>• Certified for CIS Benchmarks 1.0, with more certifications to come</td>
</tr>
<tr>
<td></td>
<td>• Subnetworks that do not use private access to Google APIs</td>
<td>• Stackdriver monitoring for Kubernetes clusters not enabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• VPC Flow logs disabled</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VM Instances</th>
<th>GKE Clusters</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• IP forwarding enabled</td>
<td>• Private cluster disabled</td>
<td>• Master authorized network disabled</td>
<td></td>
</tr>
<tr>
<td>• SSH and access misconfigurations</td>
<td>• Network policy disabled</td>
<td>• IP alias disabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Master authorized network disabled</td>
<td>• Legacy authorization enabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Network policy disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Master authorized network disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IP alias disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Legacy authorization enabled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Google Cloud**
How Security Health Analytics works in 3 steps

**STEP 01**
Leverages built-in GCP configurations checks for assets

**STEP 02**
Processes configurations and monitors for violations

**STEP 03**
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

**STEP 01**
Create a scan configuration, telling the scanner where your web app is and where it’s not allowed to go.

**STEP 02**
Scans run on the schedule you configure, navigate through your website and attempt to find real vulnerabilities.

**STEP 03**
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

<table>
<thead>
<tr>
<th>Threat</th>
<th>Severity</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware: domain</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Cryptomining: IP</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Malware: hash</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Brute force: SSH</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

+4 more

<table>
<thead>
<tr>
<th>Type</th>
<th>Severity</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware: domain</td>
<td></td>
<td>52</td>
</tr>
<tr>
<td>Malware: IP</td>
<td></td>
<td>37</td>
</tr>
<tr>
<td>Malware: hash</td>
<td></td>
<td>32</td>
</tr>
<tr>
<td>IAM: anomalous grant</td>
<td></td>
<td>11</td>
</tr>
</tbody>
</table>

+4 more

### Cloud Anomaly Detection

9 current findings

<table>
<thead>
<tr>
<th>Finding</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leaked Credentials</td>
<td>2</td>
</tr>
<tr>
<td>Data Exfiltration Risk</td>
<td>2</td>
</tr>
<tr>
<td>Intrusion Attempt</td>
<td>1</td>
</tr>
<tr>
<td>Resource Compromised</td>
<td>1</td>
</tr>
</tbody>
</table>
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 **Current**

- Malware
- Cryptomining
- Phishing
- IAM abuse
- Outgoing DDoS attacks
- Bruteforce
- Leaked credentials
- Hijacked accounts
- Compromised machines
How Event Threat Detection works in 3 steps

1. Cloud Audit Logs
2. VPC Flow logs
3. Cloud DNS logs
4. syslog via fluentd

Logs are sent to Event Threat Detection

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
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
SCC supports findings from Google security products and partner security products
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