Solution Brief

Tenable and Google

Secure Your Assets in the Google Cloud

The Challenge

As organizations look to improve business agility, lower costs and boost innovation, many are tapping the benefits of cloud computing. With these benefits, the rapid transition of moving key infrastructure and applications into the cloud also poses new challenges for security. Complexity is a big culprit, for as the attack surface grows with cloud, security managers need to extend their watch over this new vector:

- How many virtual machines are running in the cloud and when are new hosts created?
- Are logs being collected for all assets, including those in the cloud?
- What cloud assets have had brute force login attempts or unauthorized web app scans?

How you achieve this visibility will determine success in putting it to practical use. That's because adoption of the cloud typically produces a hybrid environment that includes traditional on-premises infrastructure. New zones in the hybrid environment may include infrastructure-as-a-service (IaaS) for compute resources, and/or platform-as-a-service (PaaS) for application middleware services.

Adding new tools to monitor the security of IaaS and PaaS can magnify the overhead on security professionals because they're also still watching existing infrastructure. As a result, using siloed tools for hybrid security requirements can slow discovery of urgent vulnerabilities, delay getting the right data to the appropriate team and hinder remediation. It's a recipe for potential breaches and expensive fallout.

The Solution

Tenable™ has partnered with Google to integrate Tenable SecurityCenter Continuous View® with Google Cloud Platform. This integrated solution supports both on-premises environments and cloud deployments in Google Cloud Platform. As a result, organizations using Tenable and Google can employ a single technology for monitoring hybrid environments, thereby eliminating the need to buy, deploy and manage multiple tools.

The Google Cloud Platform enables this integration via Google Stackdriver, its integrated cloud monitoring, logging and diagnostics service for applications on the platform. The integration mechanism is the Google Cloud Storage JSON API, which is a simple, JSON-backed interface for programmatically accessing and manipulating Google Cloud Storage projects. It shares many features with the Google Cloud Storage XML API and is compatible with Google APIs Client Libraries. With the JSON API, log data generated by hosts and applications in the Google Cloud Platform are presented for external use by Tenable.

SecurityCenter Continuous View provides the interface to security and configuration data from Google Cloud Platform. Logs from the platform provide the following types of information:

- New Host Discovery: the when and who of new hosts being provisioned
- Unauthorized Web Application Scanning: detects and alerts when public-facing infrastructure is being scanned
- Intrusion Reporting: detects brute force attacks on applications running on Google Cloud Platform

Components:

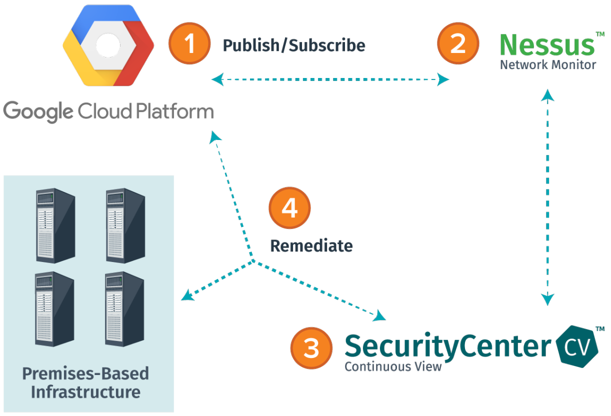
- SecurityCenter Continuous View 5.x or higher
- Tenable uses the Log Correlation Engine® 4.8+ via the Web Query Client
- Google Cloud Platform
- Google Cloud Platform Publish and Subscription Service

Benefits:

- **Unifies a single view** of your on-premises and Google Cloud Platform environments
- **Provides quicker time-to-resolution** and a better assurance of your security posture
- **Achieves compliance goals more easily** by automatically discovering new virtual systems
- **Saves time and money** purchasing, deploying and maintaining multiple solutions
- **Discovers malicious or unauthorized activity anywhere** in a hybrid environment

To acquire this data, the Tenable solution is provided with a service account in the Cloud Platform and permission to automatically receive cloud data subscribed to by SecurityCenter Continuous View. It uses the Log Correlation Engine via the Web Query Client and JSON API to grab Google log and event. Log retrievals occur every 10 seconds by default and are configurable by the Google Cloud Platform customer.

How It Works

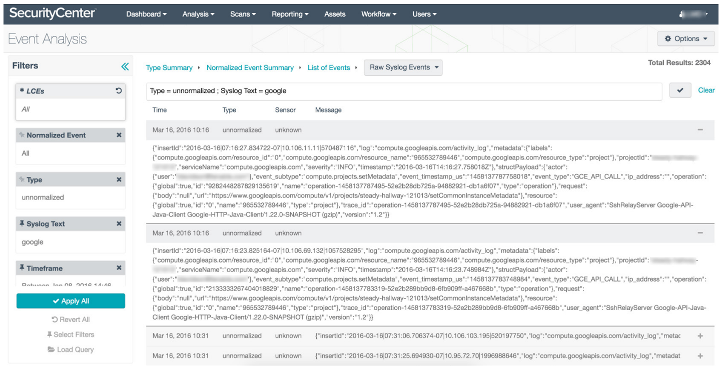


1. Google Cloud Platform host and application logs are programmatically presented via the JSON API in Google Cloud Platform Publish and Subscription Service.

2. Tenable Log Correlation Engine grabs JSON logs with Web Query Client and Google Cloud Platform Publish and Subscription service.

3. Tenable SecurityCenter Continuous View uses JSON log data to find vulnerabilities on hosts and applications in the Google Cloud Platform.

4. Tenable solution guides remediation for vulnerabilities discovered on hosts and applications in the Google Cloud Platform and in premises-based infrastructure.



Total Results: 2304

Type = unnormalized ; Syslog Text = google

* LCEs: All
Normalized Event: All
Type: unnormalized
Syslog Text: google
Timeframe: Between Jan 08, 2016 14:46

```
Time                Type           Sensor     Message
Mar 16, 2016 10:16  unnormalized   unknown
{"insertId":"2016-03-16|07:16:27.834722-07|10.106.11.11|570487116","log":"compute.googleapis.com/activity_log","metadata":{"labels":
{"compute.googleapis.com/resource_id":"0","compute.googleapis.com/resource_name":"965532789446","compute.googleapis.com/resource_type":"project"},"projectId":"[redacted]","serviceName":"compute.googleapis.com","severity":"INFO","timestamp":"2016-03-16T14:16:27.758018Z"},"structPayload":{"actor":
{"user":'[redacted]},"event_subtype":"compute.projects.setMetadata","event_timestamp_us":"1458137787758018","event_type":"GCE_API_CALL","ip_address":"","operation":
{"global":true,"id":"9282448287829135619","name":"operation-1458137787495-52e2b28db725a-94882921-db1a6f07","type":"operation"},"request":
{"body":"null","url":"https://www.googleapis.com/compute/v1/projects/steady-hallway-121013/setCommonInstanceMetadata"},"resource":
{"global":true,"id":"0","name":"965532789446","type":"project"},"trace_id":"operation-1458137787495-52e2b28db725a-94882921-db1a6f07","user_agent":"SshRelayServer Google-API-Java-Client Google-HTTP-Java-Client/1.22.0-SNAPSHOT (gzip)","version":"1.2"}}
Mar 16, 2016 10:16  unnormalized   unknown
{"insertId":"2016-03-16|07:16:23.825164-07|10.106.69.132|1057528295","log":"compute.googleapis.com/activity_log","metadata":{"labels":
{"compute.googleapis.com/resource_id":"0","compute.googleapis.com/resource_name":"965532789446","compute.googleapis.com/resource_type":"project"},"projectId":[redacted]","serviceName":"compute.googleapis.com","severity":"INFO","timestamp":"2016-03-16T14:16:23.748984Z"},"structPayload":{"actor":
{"user":"[redacted]"},"event_subtype":"compute.projects.setMetadata","event_timestamp_us":"1458137783748984","event_type":"GCE_API_CALL","ip_address":"","operation":
{"global":true,"id":"2133333267404018829","name":"operation-1458137783319-52e2b289bb9d8-6fb909ff-a467668b","type":"operation"},"request":
{"body":"null","url":"https://www.googleapis.com/compute/v1/projects/steady-hallway-121013/setCommonInstanceMetadata"},"resource":
{"global":true,"id":"0","name":"965532789446","type":"project"},"trace_id":"operation-1458137783319-52e2b289bb9d8-6fb909ff-a467668b","user_agent":"SshRelayServer Google-API-Java-Client Google-HTTP-Java-Client/1.22.0-SNAPSHOT (gzip)","version":"1.2"}}
Mar 16, 2016 10:31  unnormalized   unknown    {"insertId":"2016-03-16|07:31:06.706374-07|10.106.103.195|520197750","log":"compute.googleapis.com/activity_log","metac
Mar 16, 2016 10:31  unnormalized   unknown    {"insertId":"2016-03-16|07:31:25.694930-07|10.95.72.70|1996988646","log":"compute.googleapis.com/activity_log","metadat
```

Tenable SecurityCenter Continuous View automatically displays log data generated by hosts and applications in the Google Cloud Platform, thus integrating vulnerability scanning, analytics and remediation for a hybrid platform of virtual assets in the cloud and traditional premises-based infrastructure.

The Tenable and Google integrated solution gives your security team a single, unified view of security in a hybrid environment including traditional, premises-based infrastructure and hosts and applications located in the Google Cloud Platform, eliminating the need to buy, deploy and manage multiple siloed tools.

About Google

Google is an internet-related services and products company, including online advertising technologies, search, cloud computing and software. Google was founded by Larry Page and Sergey Brin in 1998 and went public in 2004. In 2015, Google announced plans to reorganize its various interests as a holding company, Alphabet, Inc., with Google as its leading subsidiary. Google is the umbrella company for Alphabet's internet interests – including Google Cloud Platform. To learn more about Google, visit google.com.

About Tenable

Tenable™ transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats and reduces exposure and loss. With more than one million users and more than 21,000 customers worldwide, organizations trust Tenable for proven security innovation. Tenable customers range from Fortune Global 500 companies, to the global public sector, to mid-sized enterprises in all sectors, including finance, government, healthcare, higher education, retail and energy. Transform security with Tenable, the creators of Nessus® and leaders in continuous monitoring, by visiting tenable.com.

tenable™

For More Information: Please visit tenable.com
Contact Us: Please email us at sales@tenable.com or visit tenable.com/contact