



Cloud Security Command Center

Manage your cloud security at scale with Google Cloud Security Command Center's AI Features

[Jason Callaway | jasoncallaway@google.com](mailto:jasoncallaway@google.com)

Google Cloud Platform

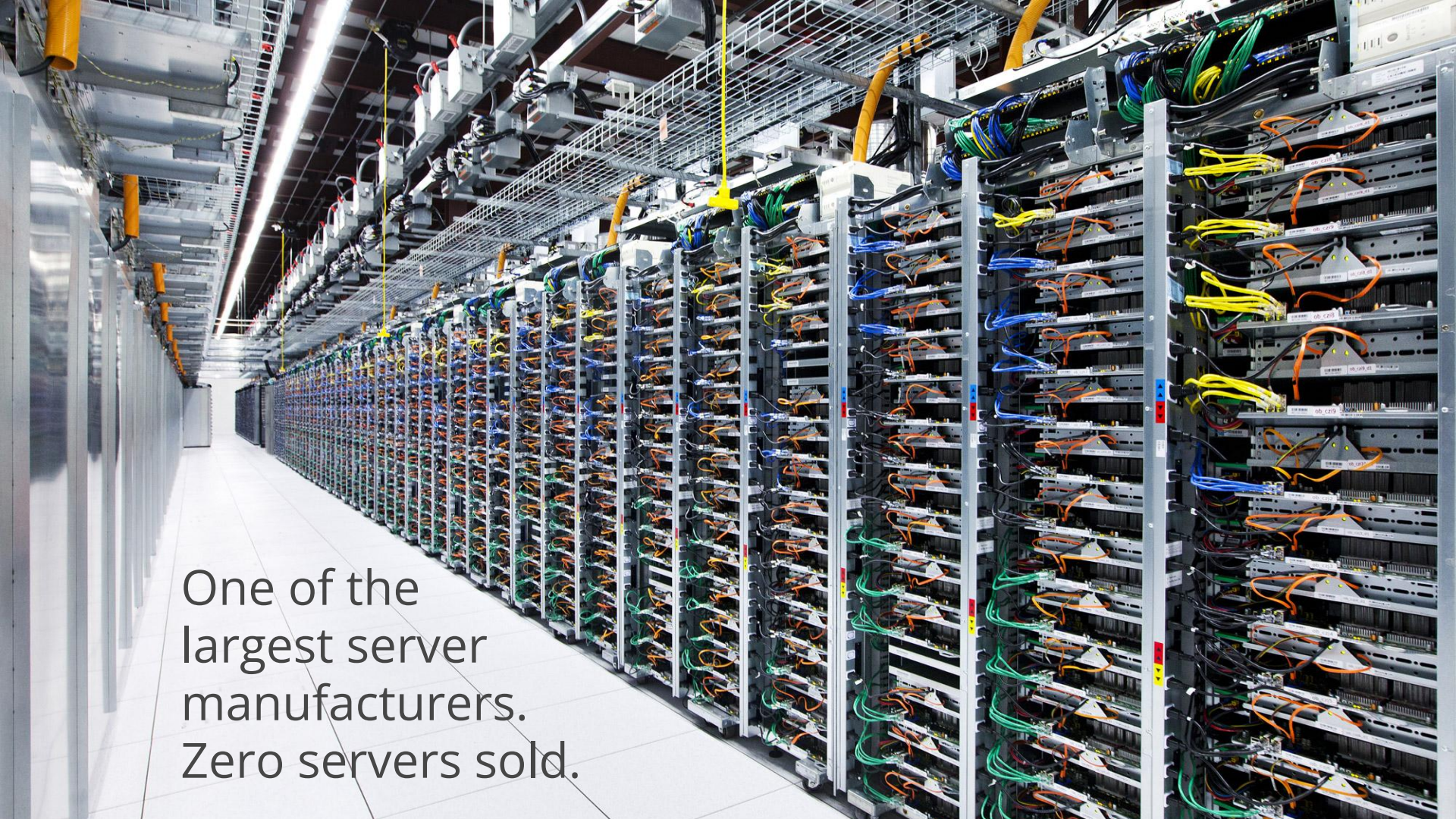


1
BILLION
users



An aerial photograph of a large data center complex at dusk. The facility consists of several large, white, rectangular buildings with flat roofs, some of which are illuminated from within. A prominent feature is a large, multi-story building with a glass facade that reflects the twilight sky. The complex is situated on a hillside overlooking a wide river. In the background, rolling hills and mountains are visible under a sky filled with dark, dramatic clouds. The overall scene is a mix of industrial infrastructure and natural landscape.

Google has built the world's
largest, most advanced,
computing infrastructure.

A perspective view of a server room aisle. On the right, multiple rows of server racks are filled with server units. Each unit is densely packed with various components and connected by a complex network of colorful cables (blue, orange, yellow, green, black). The racks are supported by metal frames. On the left, there are more server racks, but they are mostly obscured by a large, white, curved structure that appears to be part of a cooling or ventilation system. The floor is a light-colored, polished tile. The lighting is bright and even, highlighting the intricate details of the server hardware and the organized chaos of the cabling.

One of the
largest server
manufacturers.
Zero servers sold.

Compliance offerings

Americas



Global

ISO/IEC 27001
ISO/IEC 27017
ISO/IEC 27018
ISO/IEC 27701
SOC 1
SOC 2
SOC 3
PCI DSS
CSA STAR
MPAA
Independent Security Evaluators Audit
GxP



USA

HIPAA
HITRUST
FedRAMP
FIPS 140-2
COPPA
FERPA
NIST 800-53
NIST 800-171
NIST 800-34
Sarbanes- Oxley
SEC Rule 17a-4(f)
CFTC Rule 1.31(c)-(d)
FINRA Rule 4511(c)
HECVAT
DISA IL2
CCPA
CJIS



Canada

PIPEDA
Personal Health Information Protection Act



Argentina

Personal Data Protection Law

Europe, Middle East & Africa



Europe

GDPR
EU Model Contract Clauses
TISAX
EBA Guidelines



Germany

BSI C5



Switzerland

FINMA



France

HDS



Spain

Esquema Nacional de Seguridad



South Africa

POPI



UK

NCSC Cloud Security Principles
NHS IG Toolkit

Asia Pacific



Australia

Australian Privacy Principles
Australian Prudential Regulatory Authority Standards
IRAP



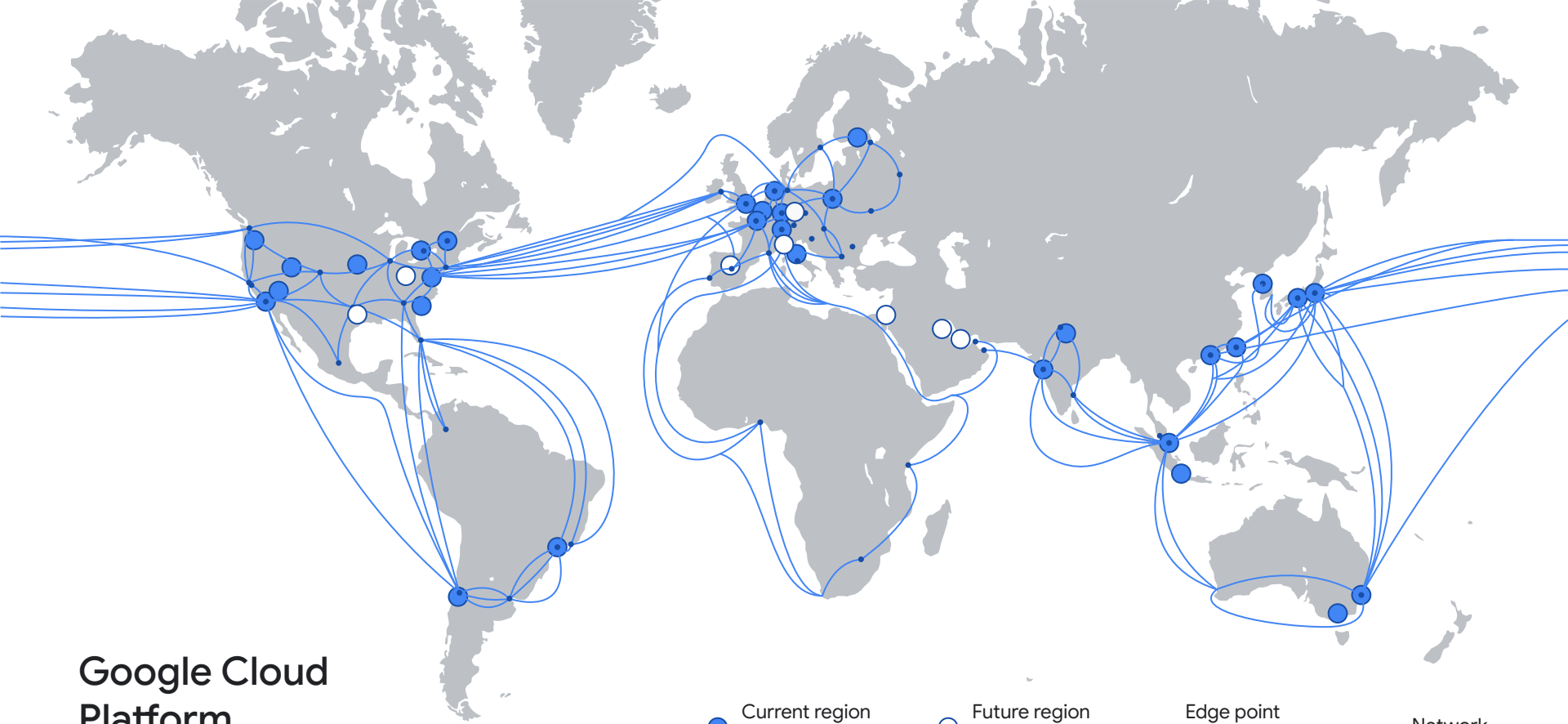
Japan

FISC
My Number Act
NISC
CSV Guidelines
3G3M



Singapore

MTCS Tier 3
OSPAR
MAS Guidelines
ABS Guide



Google Cloud Platform

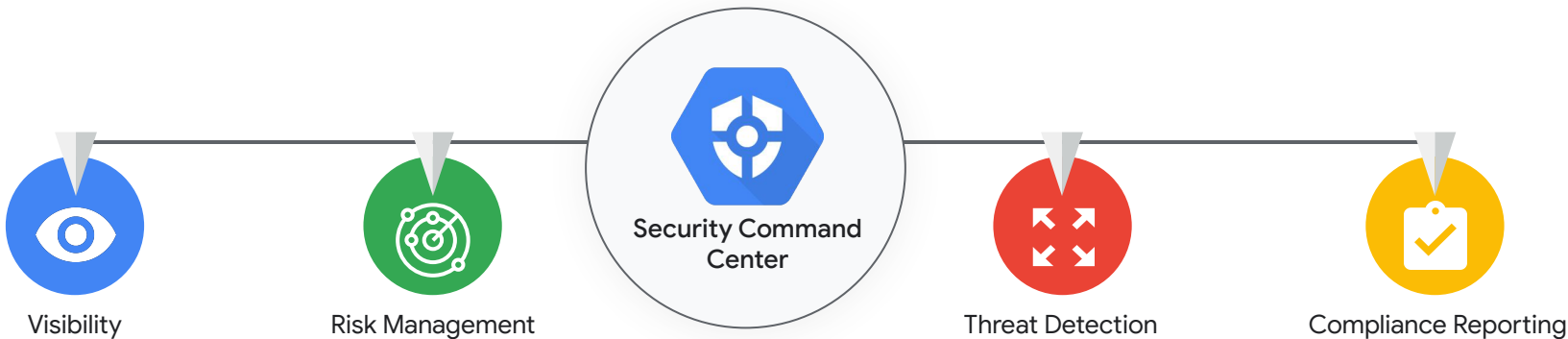
- Current region with 3 zones
- Future region with 3 zones
- Edge point of presence
- Network

Regions, PoPs, and network

Security Command Center

Cloud Native Protection

Security Command Center



- Asset Inventory
- Asset tracking

- Platform Misconfigurations
- OS and web app vulnerabilities

- Malicious activity in network and account
- Suspicious activity in containers and hosts

- NIST Best practices CIS 1.1, NIST 800-53
- PCI Industry Standards, PCI DSS v3.2.1, ISO 27001

Visibility

Cloud Asset Inventory



Gain centralized visibility and control over your Google Cloud data and resources

- Complete view into your Google Cloud resources and their policies
- Near real-time visibility into exactly what changed in your asset history and respond to the most pressing issues first
- Receive notifications about findings associated with your critical assets and and take action



CryptoKey



CryptoKeyVersion



Bucket



TargetVpnGateway



UriMap



Version



VpnTunnel



Network



Node



NodePool



Organization



Pod



Policy



Disk



Firewall



Folder



Application



Compute Instance



Find and fix vulnerabilities and risky misconfigurations

- Identify security misconfigurations in your Google Cloud assets and resolve them by following actionable recommendations
- Catch web app vulnerabilities before they hit production and reduce your exposure to risks
- Monitor compliance control violations that are associated with the vulnerability and misconfiguration findings.

Misconfigurations & Web App vulnerabilities



Compute Image



Compute Instance



API Keys



GKE (Container)



Firewall



IAM



KMS



Storage



Cross-site scripting (XSS)



Flash injection



Mixed-content



Clear text passwords



Usage of insecure JavaScript libraries

Risk Management

Security Health Analytics



Continuous assessment of GCP infrastructure for misconfigurations and vulnerabilities

Storage



- Publicly exposed buckets
- Storage resources missing CMEK
- 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

Identity



- Overprovisioned admin accounts
- Permission grants outside your org
- Insufficient separation of duties

VM Instances



- IP forwarding enabled
- Broad service account or API access enabled
- SSL & SSH misconfigurations

GKE Clusters



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

Risk Management

Web Security Scanner



Continuous assessment of web applications on Google Cloud



One-click coverage

- Turn on managed scans to automatically discover public web apps running on GKE/GCE/GAE
- Schedules weekly scans and detects changes and new apps



Detect Key Application Vulnerabilities

- Detect 11+ categories of vulnerabilities, from XSS to app misconfigurations, including vulnerabilities from the OWASP Top 10
- Assess and triage security posture in unified Security Command Center dashboards

Compliance Reporting

Demonstrate and maintain compliance



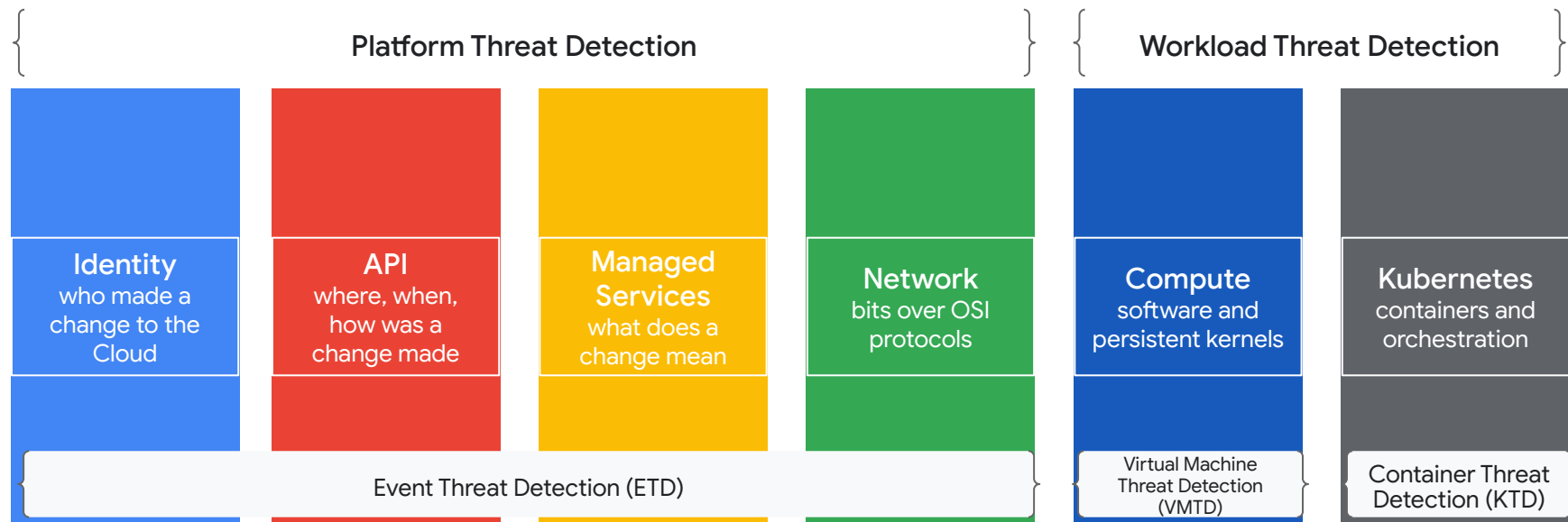
- Identify compliance violations in your Google Cloud assets and resolve them by following actionable suggestions
- Review and export compliance reports to ensure all your resources are meeting their compliance requirements
- Support for compliance standards such as
 - Center for Internet Security (CIS) 1.0, 1.1, 1.2 Benchmarks and OWASP Top 10
 - Payment Card Industry Data Security Standard (PCI DSS v3.2.1)
 - International Organization for Standardization (ISO 27001)
 - National Institute of Standards and Technology (NIST 800-53)





Threat Detection

Event Threat Detection, Virtual Machine Threat Detection,
Container Threat Detection

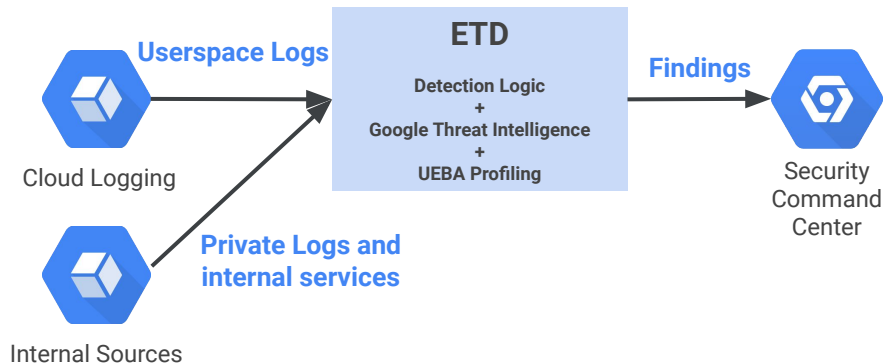


Diving deeper on Event Threat Detection

Threat Detection: Event Threat Detection

Streaming threat detection for Google Cloud as a Platform

- Event Threat Detection protects your use of Google Cloud Platform from the Identity layer up through Network layer detections
- Same protection as Google uses to protect its use of Google Cloud
- Integrated deeply with Google Cloud, including with Google Groups for privileged insights
- Managed detection for false positive control
- UEBA protection for IAM and Service Accounts
- Configurable Modules in private preview





Detect threats targeting your Google Cloud assets

- Identity, API, Network, and Compute layer threat detection for Google Cloud. Event Threat Detection (ETD) provides a variety of log-informed detections from indicator matching to User Entity Behavioral Analytics (UEBA) at cloud scale
- Container Threat Detection (KTD) shrinks the available attack surface for containerized workloads: with an org-wide enforceable configuration and kernel integration, KTD makes detection deployment seamless.
- ETD uses the same threat intelligence as Google uses to protect itself, and both products are used to secure Alphabet's use of Google Cloud.

Event Threat Detection



Malware



IAM abuse



Cryptomining



Leaked credentials



Phishing



Hijacked Accounts



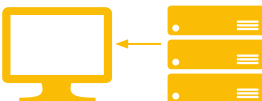
Bruteforce



Compromised machines



Outgoing DDoS attacks



Reverse Shell

Container Threat Detection



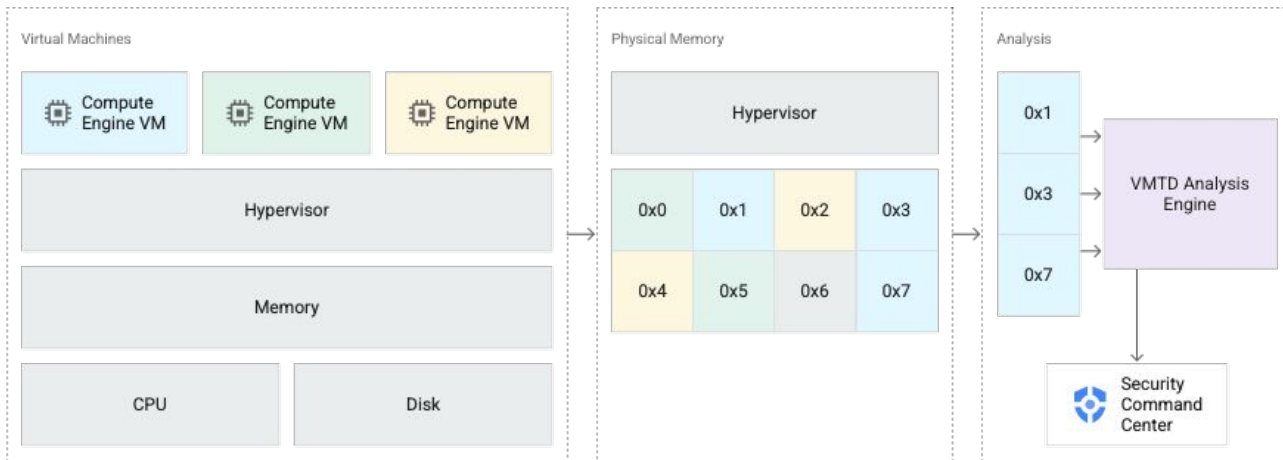
Suspicious binary



Suspicious Library

Threat Detection: Virtual Machine Threat Detection

Kernel visibility and cryptomining detection built into the fabric of Google Cloud

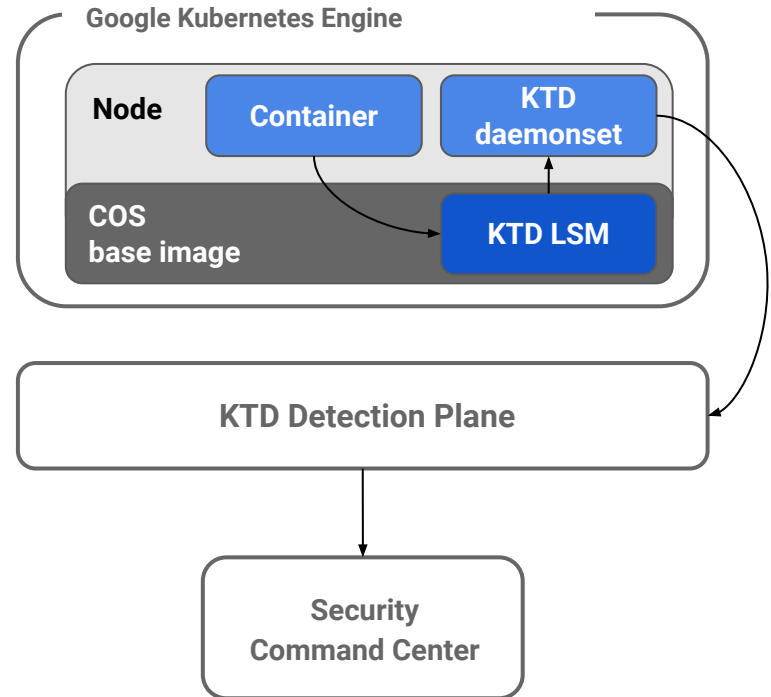


- First-to-market agentless detection capability baked into a public cloud provider
- Detects cryptomining threats today, more coming very soon!
- Complementary to Confidential Compute: choose your own threat model (Google insider vs. outsider threat)

Threat Detection: Container Threat Detection

Managed threat detection for Google Kubernetes Engine

- Three pillars of securing Kubernetes:
 - Secure to Deploy
 - Secure to Build
 - Secure to Run
- Container Threat Detection: **runtime detection** to cover outside-in compromise
- Google machine learning expertise:
 - Malicious bash script execution
 - Suppresses false positives
- Designed to minimize node performance impact with off-node detection plane
- Declarative, managed configuration



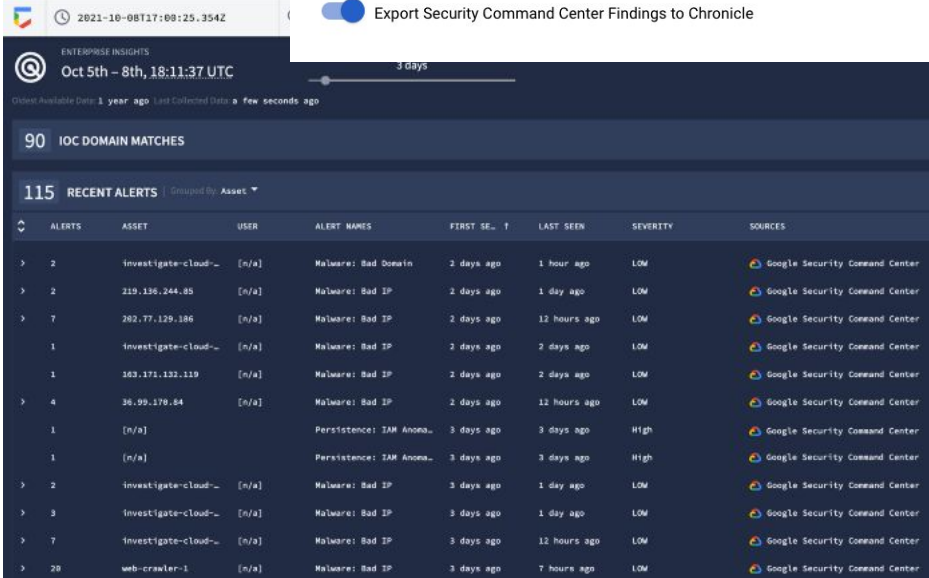
Threat Detection: Chronicle Integration

- Real-time threat detection at every layer for Google Cloud from SCC Premium
- Resilient real-time integration to import assets, logs, and SCC threat findings into Chronicle
- One-click pivot from SCC to deep investigation with cloud specific investigative journeys

Google Cloud Export Settings

Enable export to Chronicle for logs, asset metadata and Security Command Center findings. [Learn more about exporting to Chronicle](#)

- Export Cloud Logs to Chronicle
- Export Cloud Asset Metadata to Chronicle
- Export Security Command Center Findings to Chronicle



The screenshot shows the Google Chronicle Enterprise Insights interface. At the top, it displays the date range 'Oct 5th - 8th, 18:11:37 UTC' and a '3 days' time filter. Below this, there are sections for '90 IOC DOMAIN MATCHES' and '115 RECENT ALERTS'. The 'RECENT ALERTS' section is expanded to show a table of alerts. The table has columns for 'ALERTS', 'ASSET', 'USER', 'ALERT NAMES', 'FIRST SEEN', 'LAST SEEN', 'SEVERITY', and 'SOURCES'. The alerts listed are primarily 'Malware: Bad IP' and 'Persistence: IAM Anoma...'.

ALERTS	ASSET	USER	ALERT NAMES	FIRST SEEN	LAST SEEN	SEVERITY	SOURCES
> 2	investigate-cloud-	[n/a]	Malware: Bad Domain	2 days ago	1 hour ago	LOW	Google Security Command Center
> 2	219.136.244.85	[n/a]	Malware: Bad IP	2 days ago	1 day ago	LOW	Google Security Command Center
> 7	262.77.129.186	[n/a]	Malware: Bad IP	2 days ago	12 hours ago	LOW	Google Security Command Center
1	investigate-cloud-	[n/a]	Malware: Bad IP	2 days ago	2 days ago	LOW	Google Security Command Center
1	163.171.132.119	[n/a]	Malware: Bad IP	2 days ago	2 days ago	LOW	Google Security Command Center
> 4	36.99.179.64	[n/a]	Malware: Bad IP	2 days ago	12 hours ago	LOW	Google Security Command Center
1	[n/a]		Persistence: IAM Anoma...	3 days ago	3 days ago	High	Google Security Command Center
1	[n/a]		Persistence: IAM Anoma...	3 days ago	3 days ago	High	Google Security Command Center
> 2	investigate-cloud-	[n/a]	Malware: Bad IP	3 days ago	1 day ago	LOW	Google Security Command Center
> 3	investigate-cloud-	[n/a]	Malware: Bad IP	3 days ago	1 day ago	LOW	Google Security Command Center
> 7	investigate-cloud-	[n/a]	Malware: Bad IP	3 days ago	12 hours ago	LOW	Google Security Command Center
> 28	web-crawler-1	[n/a]	Malware: Bad IP	3 days ago	7 hours ago	LOW	Google Security Command Center

Cyber Big Data Analytics with BigQuery

BigQuery



Query GBs, TBs, even PBs at interactive speed

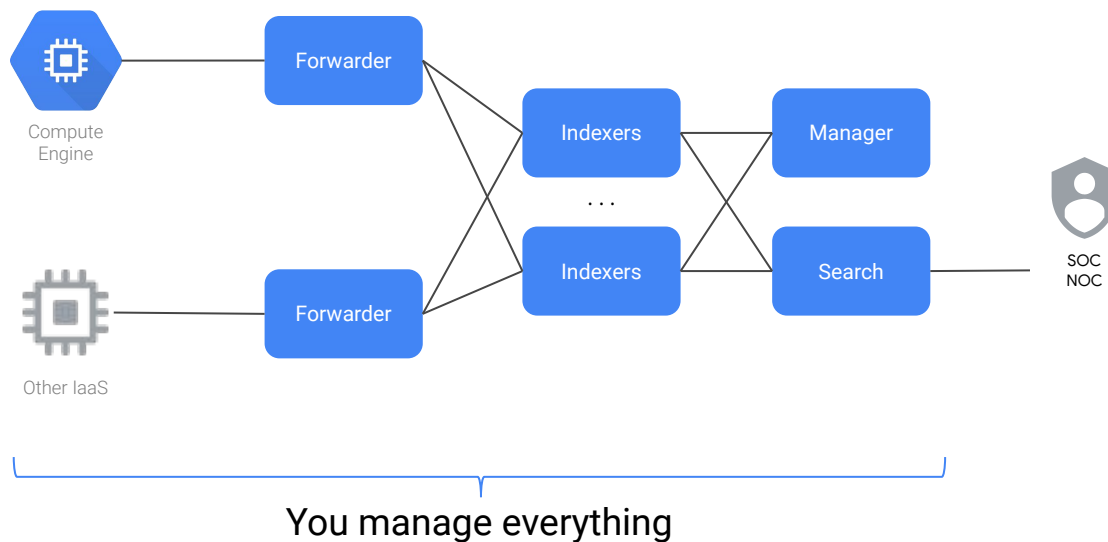
Familiar SQL syntax, powerful analytics functions

Query across any dataset

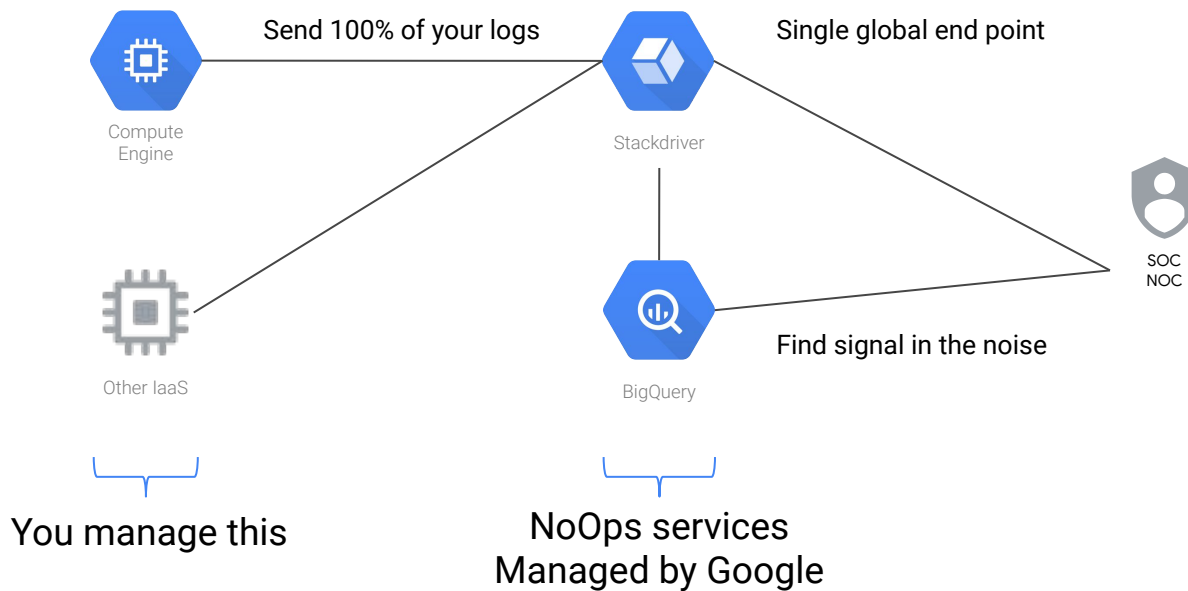
No setup, management, or maintenance

Highly available

Other cyber analytic platforms



Cyber analytics in GCP



Operations Suite Logging sink

Schema is automatically generated at sink creation

The screenshot displays the Google Cloud Platform BigQuery interface. On the left, the Explorer pane shows a project named 'jasoncallaway-202114' with a folder 'auth' containing 87 tables. The 'auth_20181221' table is selected. The main pane shows the schema for this table, which is a RECORD type. The schema includes the following fields:

Field name	Type	Mode	Collation	Policy Tags	Description
logName	STRING	NULLABLE			
resource	RECORD	NULLABLE			
type	STRING	NULLABLE			
labels	RECORD	NULLABLE			
textPayload	STRING	NULLABLE			
timestamp	TIMESTAMP	NULLABLE			
receiveTimestamp	TIMESTAMP	NULLABLE			
severity	STRING	NULLABLE			
insertId	STRING	NULLABLE			
httpRequest	RECORD	NULLABLE			
requestMethod	STRING	NULLABLE			
requestUri	STRING	NULLABLE			
requestSize	INTEGER	NULLABLE			
status	INTEGER	NULLABLE			
responseSize	INTEGER	NULLABLE			
userAgent	STRING	NULLABLE			
remoteIp	STRING	NULLABLE			
serverIp	STRING	NULLABLE			
referrer	STRING	NULLABLE			
cacheLookup	BOOLEAN	NULLABLE			
cacheHit	BOOLEAN	NULLABLE			
cacheValidatedWithOriginServer	BOOLEAN	NULLABLE			
cacheFillBytes	INTEGER	NULLABLE			
protocol	STRING	NULLABLE			
labels	RECORD	NULLABLE			
compute.googleapis.com.resource_name	STRING	NULLABLE			
operation	RECORD	NULLABLE			
id	STRING	NULLABLE			
producer	STRING	NULLABLE			

```
jasoncallaway@cloudshell:~ (jasoncallaway-202114)$ bq query --use_legacy_sql=false \  
> "SELECT textPayload FROM `jasoncallaway-202114.aafes2.auth*` LIMIT 10"
```

```
Waiting on bqjob_r68e70d74ba22746e_000001641941f419_1 ... (1s) Current status: DONE
```

```
+-----+  
|                               textPayload                               |  
+-----+  
| Jun 19 07:17:01 aafes-1 CRON[16933]: pam_unix(cron:session): session opened for user root by (uid=0) |  
| Jun 19 06:26:16 aafes-1 CRON[15489]: pam_unix(cron:session): session closed for user root           |  
| Jun 19 06:25:01 aafes-1 CRON[15563]: pam_unix(cron:session): session opened for user root by (uid=0) |  
| Jun 19 06:26:02 aafes-1 sshd[15668]: Received disconnect from 122.226.181.165 port 58174:11: [preauth] |  
| Jun 19 06:24:20 aafes-1 sshd[15559]: Received disconnect from 221.194.47.221 port 40797:11: [preauth] |  
| Jun 19 06:26:07 aafes-1 sshd[15666]: Received disconnect from 122.226.181.167 port 48108:11: [preauth] |  
| Jun 19 06:20:14 aafes-1 sshd[15521]: Connection closed by 221.194.47.236 port 35322 [preauth]       |  
| Jun 19 06:17:01 aafes-1 CRON[15489]: pam_unix(cron:session): session opened for user root by (uid=0) |  
| Jun 19 06:26:02 aafes-1 sshd[15668]: Disconnected from 122.226.181.165 port 58174 [preauth]       |  
| Jun 19 06:26:07 aafes-1 sshd[15666]: Disconnected from 122.226.181.167 port 48108 [preauth]       |  
+-----+
```

```
jasoncallaway@cloudshell:~ (jasoncallaway-202114)$
```

```
jasoncallaway@cloudshell:~ (jasoncallaway-202114)$ bq query --format=prettyjson --use_legacy_sql=false \  
> "SELECT textPayload FROM `jasoncallaway-202114.aafes2.auth*` \  
> WHERE textPayload LIKE '%cowboys%' LIMIT 5"  
Waiting on bqjob_r2caaeddeaa3151f2_00000164194555ee_1 ... (1s) Current status: DONE  
[  
  {  
    "textPayload": "Jun 18 13:44:27 aafes-1 sudo: jasoncallaway : TTY=pts/0 ; PWD=/home/jasoncallaway ; USER=root ;  
COMMAND=/bin/grep cowboys /var/log/messages"  
  },  
  {  
    "textPayload": "Jun 18 13:43:24 aafes-1 sshd[23949]: Invalid user cowboys from 76.106.10.79 port 50681"  
  },  
  {  
    "textPayload": "Jun 18 13:44:45 aafes-1 sudo: jasoncallaway : TTY=pts/0 ; PWD=/home/jasoncallaway ; USER=root ;  
COMMAND=/bin/grep cowboys /var/log/alternatives.log /var/log/alternatives.log.1 /var/log/apt /var/log/audit  
/var/log/auth.log /var/log/auth.log.1 /var/log/auth.log.2.gz /var/log/auth.log.3.gz /var/log/auth.log.4.gz  
/var/log/btmp /var/log/btmp.1 /var/log/daemon.log /var/log/daemon.log.1 /var/log/daemon.log.2.gz  
/var/log/daemon.log.3.gz /var/log/daemon.log.4.gz /var/log/debug /var/log/debug.1 /var/log/debug.2.gz  
/var/log/dpkg.log /var/log/dpkg.log.1 /var/log/faillog /var/log/google-fluentd /var/log/journal /var/log/kern.log  
/var/log/kern.log.1 /var/log/kern.log.2.gz /var/log/lastlog /var/log/messages /var/log/messages.1  
/var/log/messages.2.gz /var/log/messages.3.gz /var/log/messages.4.gz /var/log/ntpstats /var/log/puppetlabs  
/var/log/syslog /var/log/syslog.1 /var/log/syslog.2.gz /var/log/syslog.3.gz /var/log/syslog.4.gz /var/log/syslog.5.gz  
/var/log/syslog.6.gz /var/log/syslog.7.gz"  
  }  
]
```

```
jasoncallaway@cloudshell:~ (jasoncallaway-202114)$ bq query --format=prettyjson --use_legacy_sql=false \  
> "SELECT jsonPayload.host, jsonPayload.message FROM `jasoncallaway-202114.aafes2.sst_df_gce_linux_syslog*` \  
> WHERE jsonPayload.message LIKE '%BREAK-IN%' LIMIT 5"  
Waiting on bqjob_r69cc78a4c0135f15_000001641948d1d8_1 ... (1s) Current status: DONE  
[  
  {  
    "host": "aafes-3",  
    "message": "reverse mapping checking getaddrinfo for 65.218.214.190.static.anycast.cnt-grms.ec [190.214.218.65]  
failed - POSSIBLE BREAK-IN ATTEMPT!"  
  },  
  {  
    "host": "aafes-3",  
    "message": "reverse mapping checking getaddrinfo for 163.170.45.59.broad.fx.ln.dynamic.163data.com.cn  
[59.45.170.163] failed - POSSIBLE BREAK-IN ATTEMPT!"  
  },  
  {  
    "host": "aafes-3",  
    "message": "reverse mapping checking getaddrinfo for 163.170.45.59.broad.fx.ln.dynamic.163data.com.cn  
[59.45.170.163] failed - POSSIBLE BREAK-IN ATTEMPT!"  
  },  
  {  
    "host": "aafes-3",  
    "message": "reverse mapping checking getaddrinfo for 163.170.45.59.broad.fx.ln.dynamic.163data.com.cn  
[59.45.170.163] failed - POSSIBLE BREAK-IN ATTEMPT!"  
  },  
  {  
    "host": "aafes-3",  
    "message": "reverse mapping checking getaddrinfo for 163.170.45.59.broad.fx.ln.dynamic.163data.com.cn  
[59.45.170.163] failed - POSSIBLE BREAK-IN ATTEMPT!"  
  }  
]  
]
```

```
jasoncallaway@cloudshell:~ (jasoncallaway-202114)$ bq query --use_legacy_sql=false \  
> "SELECT DISTINCT jsonPayload.host FROM `jasoncallaway-202114.aafes2.sst_df_gce_linux_syslog*` \  
> WHERE jsonPayload.message LIKE '%BREAK-IN%'"  
Waiting on bqjob_r32ff39e277575c6c_00000164194d64dd_1 ... (1s) Current status: DONE  
+-----+  
| host |  
+-----+  
| aafes-3 |  
+-----+
```



Not limited to OS
logs...

NETRESEC | Products | Training | Resources | Blog | About Netresec

NETRESEC > Resources > PCAP Files > MACCDC

Capture files from Mid-Atlantic CCDC



The U.S. [National CyberWatch Mid-Atlantic Collegiate Cyber Defense Competition \(MACCDC\)](#) is a unique experience for college and university students to test their cybersecurity knowledge and skills in a competitive environment. The MACCDC takes great pride in being one of the premier events of this type in the United States.

While similar to other cyber defense competitions in many aspects, the MA CCDC, as part of the National CCDC, is unique in that it focuses on the operational aspects of managing and protecting an existing network infrastructure. The teams are physically co-located in the same building. Each team is given physically identical computer configurations at the start of the competition. Throughout the competition, the teams have to ensure the systems supply the specified services while under attack from a volunteer Red Team. In addition, the teams have to satisfy periodic "injects" that simulate business activities IT staff must deal with in the real world.


```
jasoncallaway@cloudshell:~ (jasoncallaway-202114)$ gsutil du -sh gs://govce-pcaps
78.69 GiB  gs://govce-pcaps
```

```
jasoncallaway@cyber-analytics-3$ tshark -r maccdc2010_00000_20100310205651.pcap | pcap.txt
jasoncallaway@cyber-analytics-3$ cat pcap.txt | wc -l
10000000
```

 netresec  QUERY  ASK QUESTION  SHARE  COPY  SNAPSHOT  DELETE  EXPORT

SCHEMA DETAILS PREVIEW TABLE EXPLORER

 Filter Enter property name or value

<input type="checkbox"/>	Field name	Type	Mode	Collation	Policy Tags 	Description
<input type="checkbox"/>	filename	STRING	NULLABLE			
<input type="checkbox"/>	packet_number	INTEGER	NULLABLE			
<input type="checkbox"/>	source	STRING	NULLABLE			
<input type="checkbox"/>	destination	STRING	NULLABLE			
<input type="checkbox"/>	everything	STRING	NULLABLE			

EDIT SCHEMA

VIEW ROW ACCESS POLICIES


```
netresec x *Unsaved ...ery x + CREATE v
RUN SAVE SHARE SCHEDULE MORE
1 SELECT count(*) FROM `jasoncallaway-202114.govce_pcaps.netresec`
```

Query results

JOB INFORMATION		RESULTS	JSON	EXECUTION DETAILS	EXECUTION GRAPH	PREVIEW
Row	f0_					
1	287300000					

← 287M rows

1 SELECT * FROM 'jasoncallaway-202114.govce_pcaps.netresec' LIMIT 10

Processing location: US

Query results

JOB INFORMATION RESULTS JSON EXECUTION DETAILS EXECUTION GRAPH PREVIEW

Row	filename	packet_number	source	destination	everything
1	maccdc2011_00003_20110311211935.pcap.txt	9726533	192.168.198.58	192.168.23.208	9726533 3310.102957 192.168.198.58 → 192.168.23.208 TCP 64 48786 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=
2	maccdc2011_00003_20110311211935.pcap.txt	9873250	192.168.207.4	192.168.205.188	9873250 3340.164800 192.168.207.4 → 192.168.205.188 DNS 145 Standard query response 0x6a1f No such name 46.50.57.49.in-addr.arpa SOA A.ORSN-SERVERS.NET
3	maccdc2011_00003_20110311211935.pcap.txt	9967013	192.168.25.2	192.168.205.59	9967013 3361.359499 192.168.25.2 → 192.168.205.59 TCP 70 80 → 44938 [ACK] Seq=1 Ack=187 Win=6880 Len=C TSecr=3419669
4	maccdc2011_00003_20110311211935.pcap.txt	9864218	192.168.207.4	192.168.205.188	9864218 3338.179370 192.168.207.4 → 192.168.205.188 DNS 145 Standard query response 0x9b5d No such name 46.50.57.49.in-addr.arpa SOA A.ORSN-SERVERS.NET
5	maccdc2011_00003_20110311211935.pcap.txt	9804240	192.168.198.58	192.168.24.100	9804240 3325.903834 192.168.198.58 → 192.168.24.100 SNMP 86 get-next-request 1.3.6.1.2.1
6	maccdc2011_00003_20110311211935.pcap.txt	9866019	192.168.198.58	192.168.21.189	9866019 3338.562239 192.168.198.58 → 192.168.21.189 SNMP 99 get-next-request 1.3.6.1.2.1
7	maccdc2011_00003_20110311211935.pcap.txt	9715264	192.168.204.73	192.168.21.164	9715264 3307.896958 192.168.204.73 → 192.168.21.164 TCP 64 40596 → 5432 [SYN] Seq=0 Win=1024 Len=0 MS
8	maccdc2011_00010_20110312194033.pcap.txt	9754485	192.168.201.72	192.168.22.138	9754485 1962.179717 192.168.201.72 → 192.168.22.138 HTTP 262 GET /Skins/Phone.php HTTP/1.1
9	maccdc2011_00003_20110311211935.pcap.txt	9944975	192.168.25.201	192.168.205.188	9944975 3356.240079 192.168.25.201 → 192.168.205.188 TCP 64 22 → 50208 [RST, ACK] Seq=1 Ack=1 Win=0 Len
10	maccdc2011_00010_20110312194033.pcap.txt	9914523	192.168.22.138	192.168.201.72	9914523 2004.555537 192.168.22.138 → 192.168.201.72 HTTP 1326 HTTP/1.1 206 Partial Content (text/html)

RUN SAVE ▾ SHARE ▾ SCHEDULE ▾ MORE ▾

```
1 SELECT count(*) FROM `jasoncallaway-202114.govce_pcaps.netresec`  
2 WHERE destination = "217.22.112.60"
```

Processing location: US

Query results

JOB INFORMATION

RESULTS

JSON

EXECUTION DETAILS

EXECUTION GRAPH **PREVIEW**

Row	f0_
1	9414193

```

1 SELECT * FROM `jasoncallaway-202114.govce_pcaps.netresec`
2 WHERE destination = "217.22.112.60"
3 LIMIT 10

```

Processing location: US

Query results

JOB INFORMATION

RESULTS

JSON

EXECUTION DETAILS

EXECUTION GRAPH

PREVIEW

Row	filename	packet_number	source	destination	everything
1	maccdc2010_00016_20100311225328.pcap.txt	6122016	69.178.85.90	217.22.112.60	6122016 343.716082 69.178.85.90 → 217.22.112.60 SSH 262 Server: Encrypted packet (len=192)
2	maccdc2010_00016_20100311225328.pcap.txt	6551921	69.178.85.90	217.22.112.60	6551921 367.618112 69.178.85.90 → 217.22.112.60 SSH 262 Server: Encrypted packet (len=192)
3	maccdc2010_00016_20100311225328.pcap.txt	6203529	69.178.85.90	217.22.112.60	6203529 348.042803 69.178.85.90 → 217.22.112.60 SSH 262 Server: Encrypted packet (len=192)
4	maccdc2010_00016_20100311225328.pcap.txt	6218017	69.178.85.90	217.22.112.60	6218017 348.881526 69.178.85.90 → 217.22.112.60 SSH 262 Server: Encrypted packet (len=192)
5	maccdc2010_00016_20100311225328.pcap.txt	6313126	69.178.85.90	217.22.112.60	6313126 353.985186 69.178.85.90 → 217.22.112.60 SSH 262 Server: Encrypted packet (len=192)
6	maccdc2010_00016_20100311225328.pcap.txt	6094096	69.178.85.90	217.22.112.60	6094096 342.238436 69.178.85.90 → 217.22.112.60 SSH 262 Server: Encrypted packet (len=192)
7	maccdc2010_00016_20100311225328.pcap.txt	6210575	69.178.85.90	217.22.112.60	6210575 348.452584 69.178.85.90 → 217.22.112.60 SSH 262 Server: Encrypted packet (len=192)
8	maccdc2010_00016_20100311225328.pcap.txt	6336737	69.178.85.90	217.22.112.60	6336737 355.339795 69.178.85.90 → 217.22.112.60 SSH 262 Server: Encrypted packet (len=192)
9	maccdc2010_00016_20100311225328.pcap.txt	6341661	69.178.85.90	217.22.112.60	6341661 355.614714 69.178.85.90 → 217.22.112.60 SSH 262 Server: Encrypted packet (len=192)
10	maccdc2010_00016_20100311225328.pcap.txt	6633156	69.178.85.90	217.22.112.60	6633156 372.288730 69.178.85.90 → 217.22.112.60 SSH 262 Server: Encrypted packet (len=192)

RUN SAVE SHARE SCHEDULE MORE

```
1 SELECT distinct(source) FROM `jasoncallaway-202114.govce_pcaps.netresec`
2 WHERE destination = "217.22.112.60"
3 AND everything LIKE "%SSH%"
```

Processing location: US

Query results

JOB INFORMATION RESULTS JSON EXECUTION DETAILS

Row	source
1	69.178.85.254
2	110.209.6.25
3	69.178.85.89
4	69.178.85.253
5	69.178.85.91
6	69.178.85.69
7	69.178.85.1
8	69.178.85.90

RUN SAVE SHARE SCHEDULE MORE

```
1 SELECT distinct(source) FROM `jasoncallaway-202114.govce_pcaps.netresec`
2 WHERE destination = "217.22.112.60"
3 AND everything LIKE "%SSH%"
```

Processing location: US

Query results

JOB INFORMATION RESULTS JSON EXECUTION DETAILS EXECUTION GRAPH PREVIEW

Job ID	jasoncallaway-202114:US.bquxjob_11d1599c_180aa3b0901
User	jasoncallaway@google.com
Location	US
Creation time	May 9, 2022, 3:10:37 PM UTC-4
Start time	May 9, 2022, 3:10:37 PM UTC-4
End time	May 9, 2022, 3:10:40 PM UTC-4
Duration	2 sec
Bytes processed	41.41 GB

```
1 SELECT distinct(filename) FROM `jasoncallaway-202114.govce_pcaps.netresec`
2 WHERE destination = "217.22.112.60"
3 AND everything LIKE "%SSH%"
```

Processing location: US

Query results

JOB INFORMATION RESULTS JSON EXECUTION DETAILS EXECUTION GRAPH PREVIEW

Row	filename
1	maccdc2010_00014_20100311215444.pcap.txt
2	maccdc2010_00013_20100311213530.pcap.txt
3	maccdc2010_00009_20100311203402.pcap.txt
4	maccdc2010_00018_20100311234054.pcap.txt
5	maccdc2010_00011_20100311210419.pcap.txt
6	maccdc2010_00008_20100311202252.pcap.txt
7	maccdc2010_00010_20100311204949.pcap.txt
8	maccdc2010_00007_20100311193557.pcap.txt
9	maccdc2010_00012_20100311211611.pcap.txt
10	maccdc2010_00016_20100311225328.pcap.txt
11	maccdc2010_00017_20100311230249.pcap.txt
12	maccdc2010_00015_20100311221743.pcap.txt



Get these out of GCS and apply filters

Unified Host and Network Dataset

The Unified Host and Network Dataset is a subset of network and computer (host) events collected from the Los Alamos National Laboratory enterprise network over the course of approximately 90 days. The host event logs originated from most enterprise computers running the Microsoft Windows operating system on Los Alamos National Laboratory's (LANL) enterprise network. The network event data originated from many of the internal enterprise routers within the LANL enterprise network.

The data values have been deidentified (anonymized) to protect the security of LANL's operational IT environment. The identities match across both the host and network data allowing the two data elements to be used together for analysis and research. In some cases, including well-known network ports, system-level users names (not associated to people), and system-level hosts, the values were not deidentified. In addition, in some cases hosts were combined where they represented well-known redundant services including the Active Directory servers, LANL's email servers, and LANL's automated vulnerability scanning systems.

For a detailed description of the data, see [citing](#).

The network and host event data are currently available as multiple files each containing one day of events, which can be accessed through the links below, respectively:

[Netflow](#)

[HostEvents](#)

To download all the individual files for the network and host event data respectively:

```
for i in $(seq -w 2 90); do wget -c https://s3-us-gov-west-1.amazonaws.com/unified-host-network-dataset/2017/netflow/netflow_day-$i.bz2; done
for i in $(seq -w 1 90); do wget -c https://s3-us-gov-west-1.amazonaws.com/unified-host-network-dataset/2017/wls/wls_day-$i.bz2; done
```

Network Event Data

The data is provided in CSV format, one record per line. The network events represent bi-directional events where possible. It is in the form of:

Time, Duration, SrcDevice, DstDevice, Protocol, SrcPort, DstPort, SrcPackets, DstPackets, SrcBytes, DstBytes

The following table contains a description of each field:

Field Name	Description
<i>Time</i>	The start time of the event in epoch time format

```
jasoncallaway@cloudshell:~ (jasoncallaway-202114)$ bq query \  
> "SELECT COUNT(*) FROM [jasoncallaway-202114:govce_pcaps.netflow]"  
Waiting on bqjob_r1aaef67106795aeb_000001641dc131f3_1 ... (2s) Current status: DONE
```

```
+-----+  
|    f0    |  
+-----+  
| 803595000 |  
+-----+
```

```
jasoncallaway@cloudshell:~ (jasoncallaway-202114)$ bq query --format=csv \  
> "SELECT * FROM [jasoncallaway-202114:govce_pcaps.netflow] LIMIT 10"
```

```
Waiting on bqjob_r299420595c661a98_000001641dc2f83c_1 ... (0s) Current status: DONE  
time,duration,srcdevice,dstdevice,protocol,protocol_name,srcport,dstport,srcpackets,dstpackets,srcbytes,dstbytes,filen  
ame  
129261,1,Comp030334,Comp867811,6,TCP Transmission Control,Port43346,Port58916,20,35,1991,40692,/data/netflow_day-02  
  
129067,822,Comp553253,Comp681312,6,TCP Transmission Control,Port54217,Port63735,71,75,3700,31972",/data/netflow_day-02  
  
129169,230,Comp571028,EnterpriseAppServer,6,TCP Transmission Control,Port41360,1433,18,18,876,876,/data/netflow_day-02  
  
129176,420,EnterpriseAppServer,EnterpriseAppServer,6,TCP Transmission  
Control,Port70056,1433,39,38,4638,8020,/data/netflow_day-02  
  
129223,1,Comp030334,Comp296766,6,TCP Transmission Control,Port71445,Port67717,20,21,1991,23471,/data/netflow_day-02  
  
129046,0,Comp266360,Comp210831,6,TCP Transmission Control,Port93521,Port00034,33,18,2108,1688,/data/netflow_day-02  
  
129293,817,Comp257204,Comp995183,6,TCP Transmission Control,Port16845,5061,51,62,20865,52716,/data/netflow_day-02  
  
129183,2696,Comp026764,Comp704126,6,TCP Transmission  
Control,Port36886,Port63252,63,49,44717,39264,/data/netflow_day-02  
  
129294,350,Comp044849,EnterpriseAppServer,6,TCP Transmission  
Control,Port74941,1433,26,26,1268,1268,/data/netflow_day-02  
  
129151,830,Comp510558,Comp578709,6,TCP Transmission Control,Port09056,7002,28,17,28288,1941,/data/netflow_day-02
```



```
jasoncallaway@cloudshell:~ (jasoncallaway-202114)$ bq query \  
> "SELECT COUNT(UNIQUE(srcdevice)) FROM [jasoncallaway-202114:govce_pcaps.netflow]"  
Waiting on bqjob_r2c2f96337011f64e_000001641de75e6a_1 ... (0s) Current status: DONE  
+-----+  
| f0_ |  
+-----+  
| 35824 |  
+-----+
```

```
1 SELECT * FROM `jasoncallaway-202114.govce_pcaps.netflow`
2 WHERE dstdevice LIKE "%EnterpriseApp%"
3 LIMIT 10
```

Query results

JOB INFORMATION			RESULTS	JSON	EXECUTION DETAILS	EXECUTION GRAPH	PREVIEW						
Row	time	duration	srcdevice	dstdevice	protocol	protocol_name	srcport	dstport	srcpackets	dstpackets	srcbytes	dstbytes	filename
1	129169	230	Comp571028	EnterpriseAppServer	6	TCP Transmission Control	Port41360	1433					
2	129176	420	EnterpriseAppServer	EnterpriseAppServer	6	TCP Transmission Control	Port70056	1433					
3	129294	350	Comp044849	EnterpriseAppServer	6	TCP Transmission Control	Port74941	1433					
4	129274	400	Comp044849	EnterpriseAppServer	6	TCP Transmission Control	Port92108	1433					
5	129187	440	Comp571028	EnterpriseAppServer	6	TCP Transmission Control	Port43116	1433					
6	129089	820	Comp319139	EnterpriseAppServer	6	TCP Transmission Control	Port11416	Port22425					
7	129126	320	Comp044849	EnterpriseAppServer	6	TCP Transmission Control	Port18560	1433					
8	129060	440	Comp044849	EnterpriseAppServer	6	TCP Transmission Control	Port39979	1433					
9	129236	6	Comp216639	EnterpriseAppServer	6	TCP Transmission Control	Port81953	Port68911					
10	129039	0	EnterpriseAppServer	EnterpriseAppServer	6	TCP Transmission Control	Port66352	1433					

netresec x netflow x *Unsaved ...ery x + CREATE

RUN SAVE SHARE SCHEDULE MORE

```
1 SELECT * FROM `jasoncallaway-202114.govce_pcaps.netflow`
2 WHERE dstdevice LIKE "%EnterpriseApp%"
3 LIMIT 10
```

Query results

JOB INFORMATION RESULTS JSON EXECUTION DETAILS EXECUTION GRAPH PREVIEW

Job ID jasoncallaway-202114.US.bquxjob_55362537_180aa3ec617
User jasoncallaway@google.com
Location US
Creation time May 9, 2022, 3:14:42 PM UTC-4
Start time May 9, 2022, 3:14:42 PM UTC-4
End time May 9, 2022, 3:14:43 PM UTC-4
Duration 0 sec
Bytes processed 898.99 GB
Bytes billed 899 GB
Job priority INTERACTIVE
Use legacy SQL false
Destination table [Temporary table](#)

```
1 SELECT * FROM `jasoncallaway-202114.govce_pcaps.netflow`
2 WHERE srcdevice IN("Comp044849", "Comp571028", "Comp319139")
3 LIMIT 10
```

Processing location: US

Query results

JOB INFORMATION RESULTS JSON EXECUTION DETAILS EXECUTION GRAPH PREVIEW

Row	time	duration	srcdevice	dstdevice	protocol	protocol_name	srcport	dstport	srcpackets	dstpackets	srcbytes	dstbytes	filename
1	743721	340	Comp571028	EnterpriseAppServer	6	TCP Transmission Control	Port10213	1433					
2	743767	400	Comp044849	EnterpriseAppServer	6	TCP Transmission Control	Port30201	1433					
3	743579	230	Comp044849	EnterpriseAppServer	6	TCP Transmission Control	Port81363	1433					
4	743621	420	Comp044849	EnterpriseAppServer	6	TCP Transmission Control	Port18476	1433					
5	743595	240	Comp044849	EnterpriseAppServer	6	TCP Transmission Control	Port99400	1433					
6	743659	430	Comp044849	EnterpriseAppServer	6	TCP Transmission Control	Port92658	1433					
7	743585	250	Comp571028	EnterpriseAppServer	6	TCP Transmission Control	Port68111	1433					
8	743629	361	Comp571028	EnterpriseAppServer	6	TCP Transmission Control	Port60306	1433					
9	743709	440	Comp571028	EnterpriseAppServer	6	TCP Transmission Control	Port74511	1433					
10	743585	350	Comp571028	EnterpriseAppServer	6	TCP Transmission Control	Port25760	1433					

netresec X netflow X *Unsaved ...ery X CREATE

RUN SAVE SHARE SCHEDULE MORE

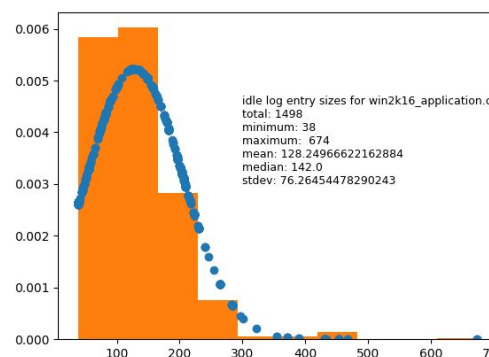
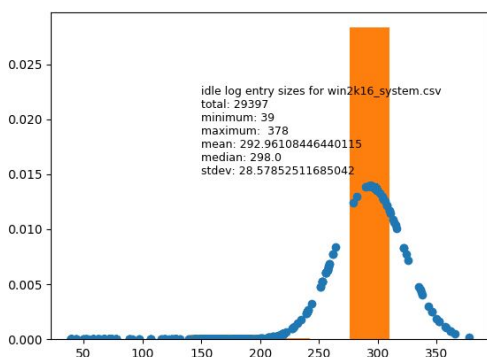
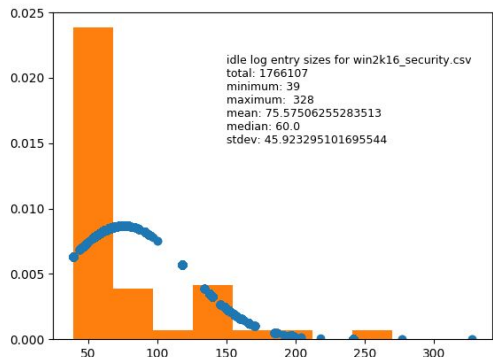
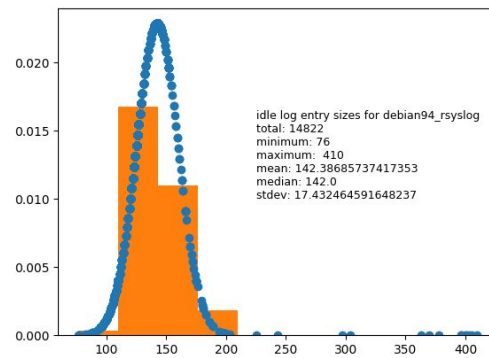
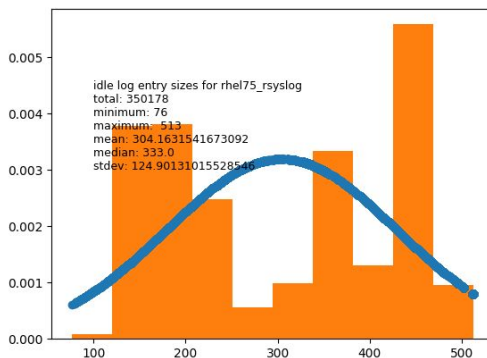
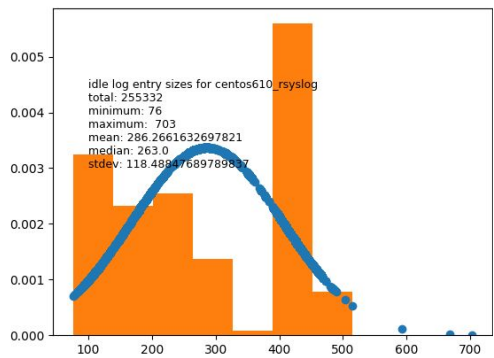
```
1 SELECT * FROM `jasoncallaway-202114.govce_pcaps.netflow`
2 WHERE srcdevice IN("Comp044849", "Comp571028", "Comp319139")
3 LIMIT 10
```

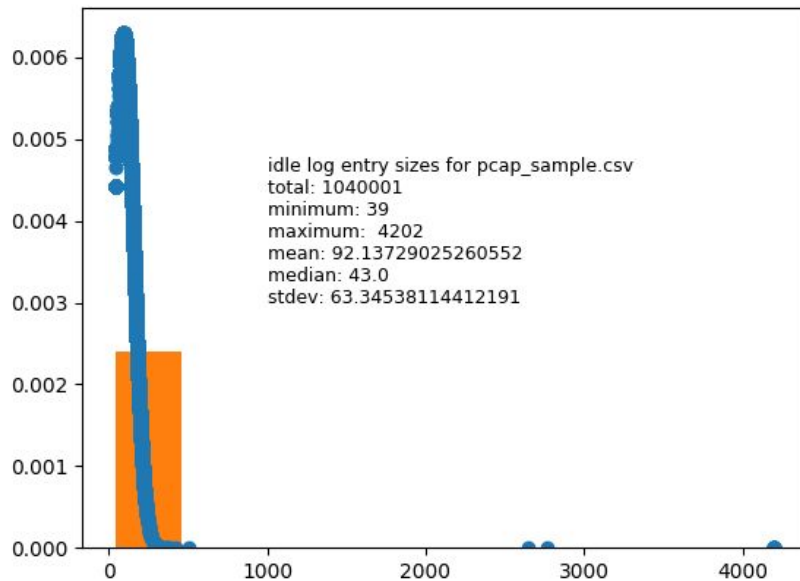
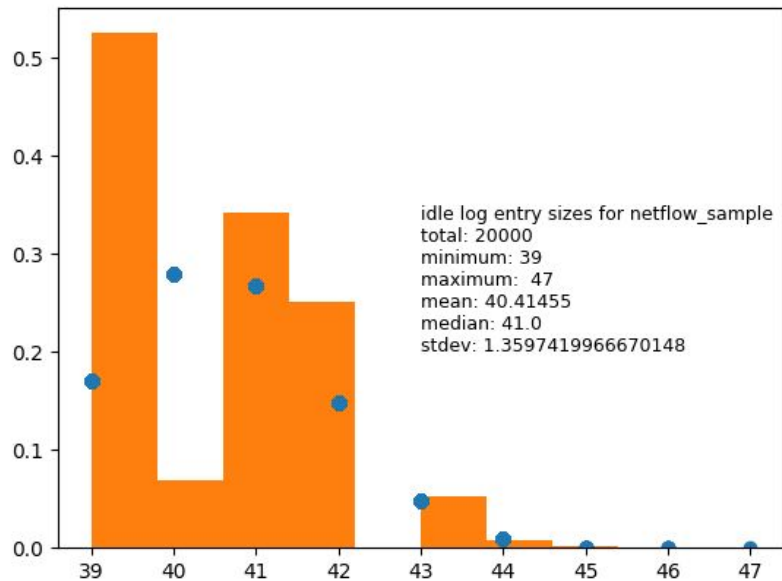
Processing location: US

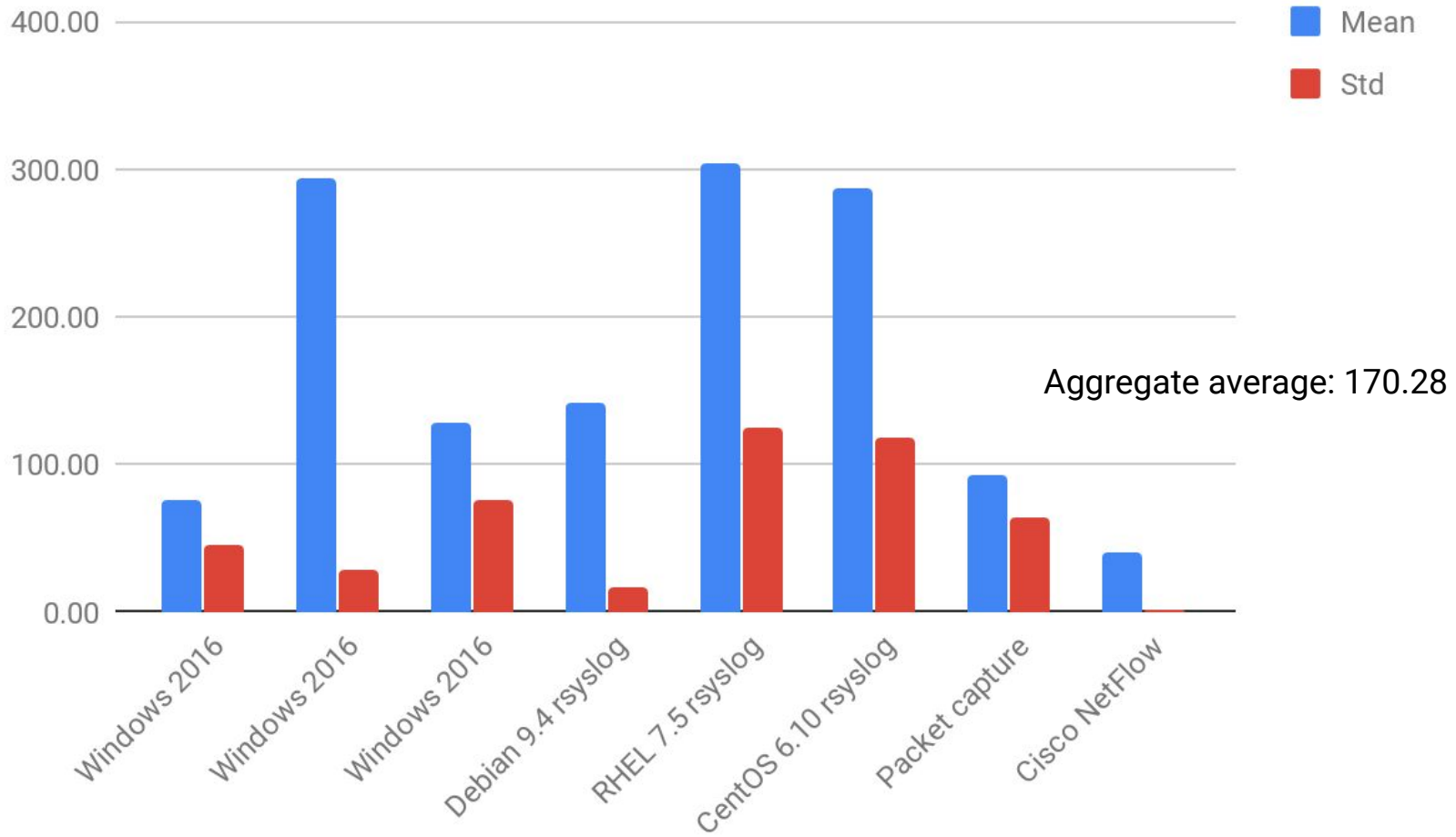
Query results

JOB INFORMATION RESULTS JSON EXECUTION DETAILS EXECUTION GRAPH PREVIEW

Job ID jasoncallaway-202114.US.bqxijob_4c1f5882_180aa406b41
User jasoncallaway@google.com
Location US
Creation time May 9, 2022, 3:16:30 PM UTC-4
Start time May 9, 2022, 3:16:30 PM UTC-4
End time May 9, 2022, 3:16:31 PM UTC-4
Duration 0 sec
Bytes processed 898.99 GB
Bytes billed 899 GB
Job priority INTERACTIVE
Use legacy SQL false
Destination table [Temporary table](#)







Q&A

And thank you!

Scott Frohman, sfrohman@google.com

Jason Callaway, jasoncallaway@google.com