Official Google Cloud Certified Professional Cloud Security Engineer Exam Guide

Become an expert and get Google Cloud certified with this practitioner's guide

Ankush Chowdhary and Prashant Kulkarni

BIRMINGHAM—MUMBAI

Table of Contents

6

Google Cloud Identity and Access Management 91

7

Virtual Private Cloud 135

10

Cloud Data Loss Prevention 259

11

Secret Manager 301

12

Cloud Logging 317

13

Image Hardening and CI/CD Security 341

15

Container Security 397

Preface

Organizations are increasingly adopting cloud migration for several reasons, including scalability, cost-efficiency, and agility. Cloud platforms offer the ability to scale resources on demand, reduce infrastructure costs, and quickly adapt to changing business needs. As a result, businesses are seeking to leverage the benefits of cloud computing, leading to rising demand for cloud security. Cloud security plays a crucial role in cloud computing, and so cloud service providers such as Google Cloud invest heavily in security measures such as encryption, access controls, threat detection, and incident response. By migrating to the cloud, organizations can leverage the expertise and infrastructure of cloud providers to enhance their overall security posture, protecting against data breaches, unauthorized access, and other cyber threats. As a result, there is growing demand for skilled professionals who can ensure the security of these cloud environments.

Data breaches and security incidents have become a major concern for businesses. The role of a Google Cloud security engineer involves implementing robust security measures, designing secure architectures, and managing access controls to safeguard data from unauthorized access, breaches, and other security threats. The Google Professional Cloud Security Engineer Certification acts as a testament to your proficiency in securing cloud environments and demonstrates your commitment to professional development. It enhances your credibility and opens up new career opportunities in the field of cloud security.

This book will introduce you to a range of essential topics. It will provide an understanding of cloud security fundamentals and the shared responsibility model. The book will go in-depth into the security features and services offered by Google Cloud, such as IAM, network security, container security, and Security Command Center. It will also address secure cloud architecture and design, data protection and encryption, security operations compliance and governance, and best practices. Additionally, the book has two full mock exams to aid in exam preparation. By covering these topics thoroughly, the book prepares you to excel in the certification exam and thrive as a cloud security practitioner using Google Cloud.

By the end of this book, you will have gained the knowledge and skills required to pass the Google Professional Cloud Security Engineer Certification exam and implement architectural best practices and strategies in your day-to-day work.

Who this book is for

This book is for IT professionals, cybersecurity specialists, system administrators, and any technology enthusiasts aspiring to strengthen their understanding of Google Cloud security and elevate their career trajectory. We delve deep into the core elements needed to successfully attain the Google Cloud Professional Security Engineer certification—a credential that stands as a testament to your proficiency in leveraging Google Cloud technologies to design, develop, and manage a robust, secure infrastructure. As businesses increasingly migrate their operations to the cloud, the demand for certified professionals in this field has skyrocketed. Earning this certification not only validates your expertise but also makes you part of an elite group of GCP Security Engineers, opening doors to opportunities that can significantly advance your career. Whether you're seeking to gain a competitive edge in the job market, earn higher pay, or contribute at a higher level to your current organization, this book will guide you every step of the way on your journey to becoming a certified Google Cloud Professional Security Engineer.

What this book covers

Chapter 1, *About the Google Professional Cloud Security Engineer Exam*, focuses on the Google Professional Cloud Security Engineer Certification and provides guidance on how to register for the exam. This chapter also covers the outline of the exam.

Chapter 2, *Google Cloud Security Concepts*, covers how Google secures its cloud infrastructure. You will learn how shared security responsibility is applied to the different Google Cloud services, the defense-in-depth model that Google deploys in securing its infrastructure at various layers, and how the isolation and security of data are achieved. Other areas covered include threat and vulnerability management, security monitoring, and data residency.

Chapter 3, *Trust and Compliance*, looks at two essential aspects of cloud architecture. The first part of the chapter focuses how Google builds security and privacy and provides customers with full transparency. Data security is all about control, and you will learn about how Google Cloud empowers its consumers to own, control, and protect their data. The second part of the chapter covers the different compliance standards and programs that Google Cloud is compliant with and how you can gain access to compliance reports. It also gives an introduction to some advanced topics that will be discussed later in the book when covering continuous monitoring and continuous compliance.

Chapter 4, *Resource Management*, covers Google Cloud Resource Manager and how resources are organized. It also covers of IAM policies, organizational policy controls, Cloud Asset Inventory, and firewall rules that can be applied and inherited via the resource hierarchy.

Chapter 5, *Understanding Google Cloud Identity*, introduces Google Cloud Identity. You will learn how to design and build your authentication strategy on Google Cloud using Cloud Identity. The topics include user lifecycle management, device security, cloud directory, account security, app management, identity federation, and single sign-on.

Chapter 6, *Google Cloud Identity and Access Management*, takes a deep dive into Google Cloud Identity and Access Management. It covers IAM roles, permissions and conditions, service accounts, how to manage service account keys, and IAM policy intelligence, along with best practices and design considerations.

Chapter 7, *Virtual Private Cloud*, covers network security concepts within Google Cloud. You will look at what a VPC is and the different types of VPC models, as well as how to do micro-segmentation using subnets, custom routing, and firewall rules. Furthermore, you will also look at DNSSEC in Google Cloud and different types of load balancers.

Chapter 8, *Advanced Network Security*, teaches you how to secure your content by using the advanced network security features that are available on Google Cloud. This chapter also covers Identity-Aware Proxy, Private Google Access, VPC Service Controls, DDoS, and the web application firewall.

Chapter 9, *Google Cloud Key Management Service*, lays the foundation for understanding the key hierarchy in Google Cloud **Key Management Service** (**KMS**) and how envelope encryption works. In this chapter, you will look at different types of encryption keys, their purpose, and how Google does encryption and key management, including coverage of the underlying cryptographic operation. The chapter also covers concepts such as bringing your own key to the cloud.

Chapter 10, *Cloud Data Loss Prevention*, guides you on how to use Google Cloud **Data Loss Prevention** (**DLP**) to secure sensitive data. It covers techniques used to scan for sensitive data by creating scan jobs and also how to enforce DLP rules to redact sensitive data using techniques such as masking, redaction, and tokenization.

Chapter 11, *Secret Manager*, guides you on how to use Google Cloud Secret Manager to create secrets that are used during runtime by your applications.

Chapter 12, *Cloud Logging*, covers how Cloud Logging works on Google Cloud. You will look at the different log types and key components for logging and learn how to build a centralized logging system for continuous monitoring.

Chapter 13, *Image Hardening and CI/CD Security*, teaches you how to harden compute images for both virtual machines and containers. It covers how to manage, secure, patch, and harden images, and how to build image management pipelines. Furthermore, you will look at building security scanning of the CI/CD pipeline. Finally, this chapter covers some Google Cloud Compute Engine security capabilities such as Shielded VMs and confidential computing.

Chapter 14, *Security Command Center*, explores the capabilities offered by Security Command Center and teaches you how to configure and use Security Command Center's capabilities to detect threats, vulnerabilities, and misconfigurations. You will also look at how Security Command Center can be used to build automated incident response and ingest its findings with third-party security information and event management tools such as Splunk.

Chapter 15, *Container Security*, covers how to design, develop, and deploy containers securely on Google Cloud. The topics covered include various aspects of container security, such as image hardening, isolation, implementing a security policy, scanning containers, and Binary Authorization. It also covers various security features of **Google Kubernetes Engine** (**GKE**) and some best practices.

Mock Exam 1 is a full-length exam covering all certification areas. Pay attention to the language of the questions.

Mock Exam 2 is another full-length exam covering all certification areas. This exam should increase your confidence in passing the exam.

To get the most out of this book

To get the most out of a certification book like this, follow these strategies:

- **Set clear goals**: Define your objectives and what you aim to achieve by studying the certification book. Identify the specific areas you want to strengthen your knowledge in and the skills you want to acquire.
- **Plan and allocate time**: Create a study schedule that fits your routine and allows for consistent learning. Allocate dedicated time each day or week to focus on the book's content. Consistency is key to retaining information effectively.
- **Active reading**: Approach the book with an active mindset. Take notes, highlight important concepts, and jot down questions for further exploration. Engage with the material actively to enhance comprehension and retention.
- **Hands-on practice**: Supplement your reading with practical exercises and hands-on labs whenever possible. Apply the concepts and techniques described in the book to real-world scenarios. This will solidify your understanding and help you develop practical skills.
- **Review and reinforce**: Regularly review the topics covered in the book to reinforce your knowledge. Make use of review questions or quizzes provided in the book or seek additional practice exams to test your understanding and identify areas that require further study.
- **Seek additional resources**: While the certification book serves as a comprehensive guide, supplement your learning with additional resources such as official documentation, online tutorials, video courses, and practice exams. Use these resources to gain different perspectives and reinforce your understanding.
- **Join study groups or communities**: Engage with others pursuing the same certification. Join online study groups or communities where you can discuss concepts, share insights, and clarify doubts. Collaborating with peers can enhance your learning experience.
- **Track your progress**: Keep track of your progress by setting milestones or checkpoints throughout your study journey. Celebrate achievements along the way, and identify areas that require more attention to ensure a well-rounded understanding.

- **Practice time management**: Efficiently manage your time during the exam preparation phase. Allocate sufficient time for reviewing and practicing sample questions or mock exams to simulate the actual exam environment and improve your test-taking skills.
- **Stay motivated**: Maintain a positive mindset and stay motivated throughout your certification journey. Remember your goals and the benefits that achieving the certification can bring. Reward yourself for milestones reached and stay committed to the process.

By implementing these strategies, you can maximize your learning experience with the certification book, deepen your knowledge, and increase your chances of success in the certification exam.

Conventions used

Code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles are shown as follows: "The lifecycle state is displayed as `ACTIVE` or `DELETE_REQUESTED`."

Words that you see on the screen, for example, in menus or dialog boxes, also appear in the text like this: "Navigate to **Billing** from the console menu on the left."

A block of code is set as follows:

```
 {
  "creationTime": "2020-01-07T21:59:43.314Z",
  "displayName": "my-organization",
  "lifecycleState": "ACTIVE",
  "name": "organizations/34739118321",
  "owner": {
    "directoryCustomerId": "C012ba234"
  }
}
```

When we wish to draw your attention to a particular part of a code block, the relevant lines or items are set in bold:

```
{
  "type": "service_account",
  "project_id": "project-id",
  "private_key_id": "key-id",
  "private_key": "-----BEGIN PRIVATE KEY-----\private-key\n-----END
PRIVATE KEY-----\n",
  "client_email": " prod-service-account@project-id.iam.
gserviceaccount.com ",
  "client_id": "client-id",
  "auth_uri": "https://accounts.google.com/o/oauth2/auth",
  "token_uri": "https://accounts.google.com/o/oauth2/token",
```

```
  "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/
v1/certs",
  "client_x509_cert_url": "https://www.googleapis.com/robot/v1/
metadata/x509/service-account-email"
}
```

Any command-line input or output is written as follows:

```
git secrets --add 'private_key'
git secrets --add 'private_key_id'
```

New terms and important words are shown like this: "The aim of this book is to help cloud security professionals pass the **Google Cloud Platform** (**GCP**) Professional Cloud Security Engineer exam."

> **Tips or important notes**
> Appear like this.

If you are using the digital version of this book, we advise you to type the code yourself. Doing so will help you avoid any potential errors related to the copying and pasting of code.

Get in touch

Feedback from our readers is always welcome.

General feedback: If you have any questions about this book, please mention the book title in the subject of your message and email us at `customercare@packtpub.com`.

Errata: Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you have found a mistake in this book, we would be grateful if you could report this to us. Please visit `www.packtpub.com/support/errata` and complete the form.

Piracy: If you come across any illegal copies of our works in any form on the Internet, we would be grateful if you could provide us with the location address or website name. Please contact us at `copyright@packt.com` with a link to the material.

If you are interested in becoming an author: If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, please visit `authors.packtpub.com`.

1

About the GCP Professional Cloud Security Engineer Exam

The rate of migration to the cloud is growing exponentially. The cloud is something of a *Masai Mara* right now, and we don't expect that this will slow down. New projects are often now born in the cloud and end up staying there.

> **Note**
>
> The Masai Mara is an iconic African savanna landscape characterized by an annual wildebeest and zebra migration of over 1.5 million animals.

This growing trend has created new opportunities, specifically for cloud security. There is now soaring demand for cloud security professionals. It is not news to those in the field of cybersecurity that cloud security skills are not only in demand but scarce. Cybersecurity professionals with cloud security skills are now very sought after. Security used to be the number one obstacle to organizations moving to the cloud. Now, security is the top reason that organizations want to move to the cloud. This only increases the demand for cloud security professionals.

> **Note**
>
> For more details see *13 Cloud Computing Risks & Challenges Businesses Are Facing In These Days* by *Bernardita Calzon*, published on June 6, 2022 on the datapine website (`https://packt.link/xlnX6`).

The aim of this book is to help cloud security professionals to pass the **Google Cloud Platform** (**GCP**) Professional Cloud Security Engineer exam. The topics covered in this book not only include exam-specific content but also extend to some optional GCP cloud security topics.

This chapter covers why you should take this exam, how to register, and what to expect in the exam.

In this chapter, we will cover the following topics:

- The benefits of being a certified cloud security engineer
- How to register for the exam
- What to expect and some helpful tips

Benefits of being certified

As per Burning Glass, a leading labor market analytics firm, there is 115% projected growth for cloud security in the next five years. Not only are cloud security skills in demand, but it's also a very lucrative field. For Google Cloud security skills more specifically, there is 113% growth expected. This makes having GCP cloud security knowledge a must for cybersecurity professionals. What's more, earning the Professional Cloud Security Engineer certification will be a resounding endorsement of their skills.

Gaining a new skill or certification always helps boost your profile and increase your chances of being hired. The Google Cloud Professional Security Engineer certification validates a person's proficiency in designing, developing, and managing a secure infrastructure that leverages Google Cloud Platform technologies. This globally recognized certification can offer various benefits, including the following:

- **Increased employability**: This certification is recognized by many employers globally. It proves your skill set and makes you a desirable candidate for roles that involve Google Cloud security.
- **Higher earning potential**: On average, certified Google Cloud professionals have a higher salary compared to non-certified professionals in similar roles.
- **Skill validation**: The certification validates your knowledge and skills in Google Cloud Platform security. This can boost your confidence and credibility when dealing with projects or discussing solutions with clients or colleagues.
- **Professional development**: The preparation process for the certification exam can significantly enhance your current understanding of Google Cloud Platform security features and best practices. This knowledge is critical for those who want to excel in the cloud security domain.
- **Keep up-to-date**: The field of cloud technology is constantly evolving. The process of getting certified requires you to study and understand the latest Google Cloud security services, tools, and best practices.
- **Expand your professional network**: When you become certified, you can join groups and communities of other certified professionals. This provides opportunities to network, learn, and share experiences.
- **Company benefits**: If you're a part of a company that's a Google Cloud partner, your certification can contribute to your company's partner level, which can offer additional benefits, resources, and recognition for the company.

Overall, being a certified Google Cloud Professional Security Engineer is a valuable credential that can open significant career opportunities and benefits in the rapidly growing field of cloud computing.

Whether you're looking to get certified or just acquire new skills, the aim of this book is to help you understand GCP's cloud security capabilities.

Registering for the exam

The GCP Professional Cloud Security Engineer exam is two hours long and consists of multiple-choice questions. The exam can be taken at a testing center, or you can choose to have an online-proctored exam from a remote location. The cost of the exam is USD$200 plus tax and is only available in English. You can register for the exam by following these steps:

1. Navigate to the GCP Professional Cloud Security Engineer landing page at `https://packt.link/PZx8D`, where you can find more detailed information about the exam.

   You will find many useful resources here, such as an exam guide, sample questions, training options, and links to community learning and the certification hub.

2. Select the option to book the exam by clicking on **Register**, which will take you to the Webassessor Google Cloud certification landing page at `https://packt.link/2FmkY`. You will need to create an account with Webassessor in order to book your exam.

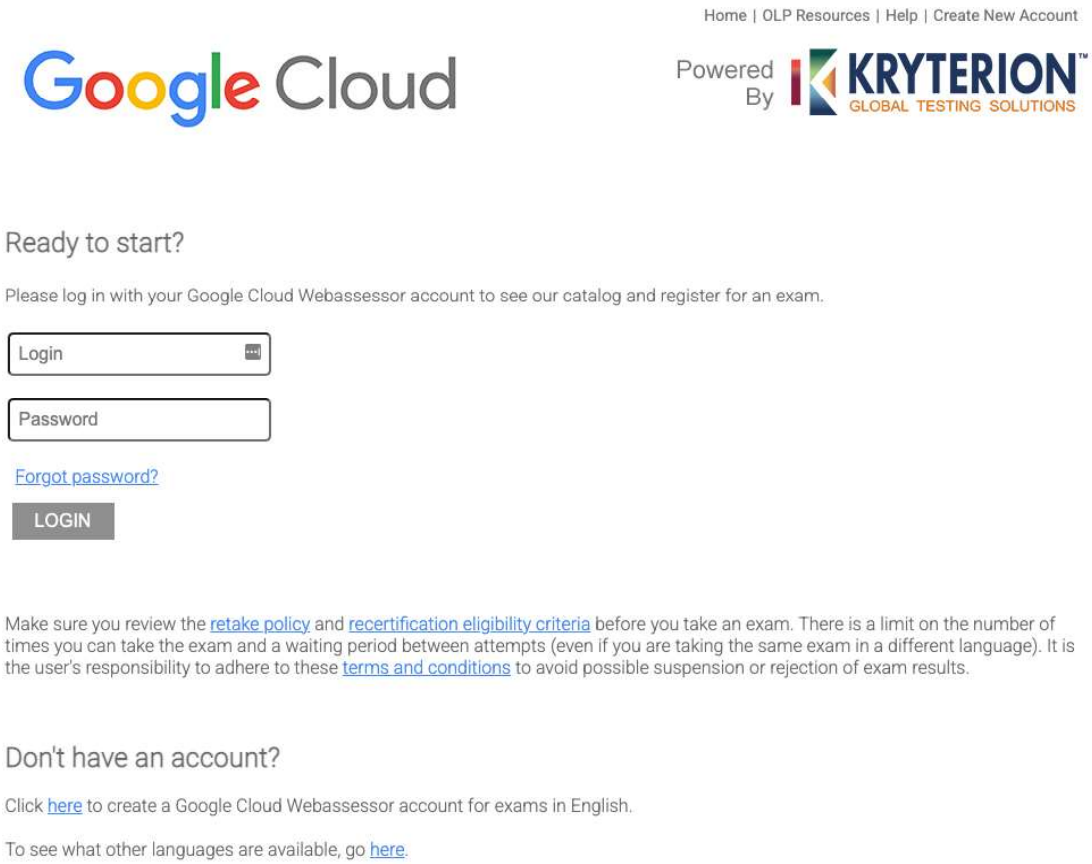

Figure 1.1 – Logging in to Webassessor

3. Once you have created an account and logged in, you will need to select the exam you would like to register for. Here you will also be able to select whether you would like to sit the exam at a testing center or via the online-proctored method.

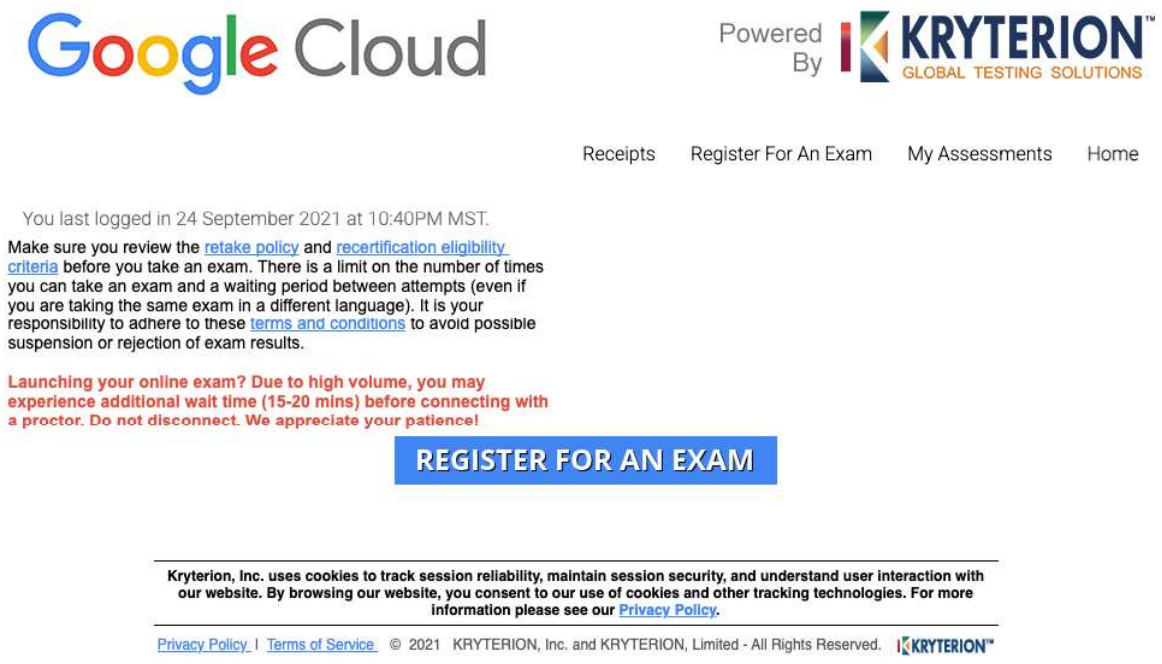

Figure 1.2 – Registration page

4. Note that for every exam, there is a + sign. By expanding that, you will be able to choose between the options of testing center and online-proctored.

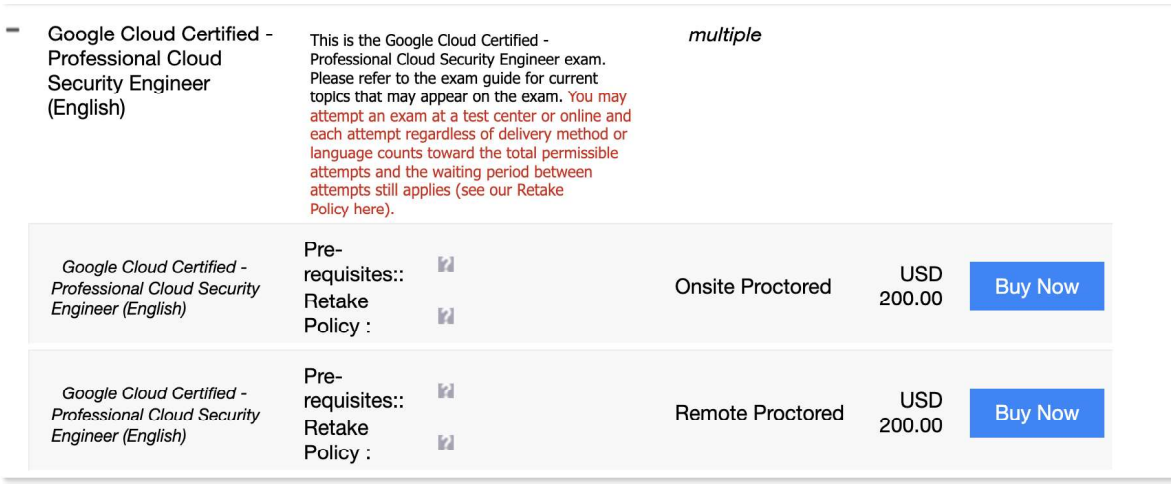

Figure 1.3 – Exam selection

5. Next, you will be allowed to select a testing center.

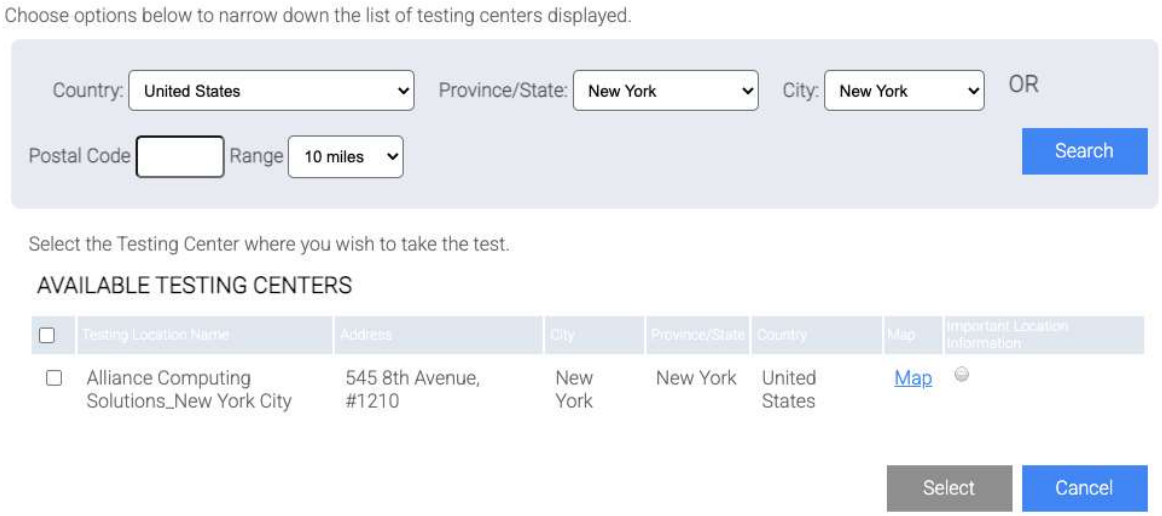

Figure 1.4 – Select a testing center

6. Next, you will need to select a date and time when you wish to sit the exam at your preferred center.

Figure 1.5 – Book a date and time for the exam

7. Proceed to checkout and complete the transaction by either paying the fees or using a voucher, if you have one.

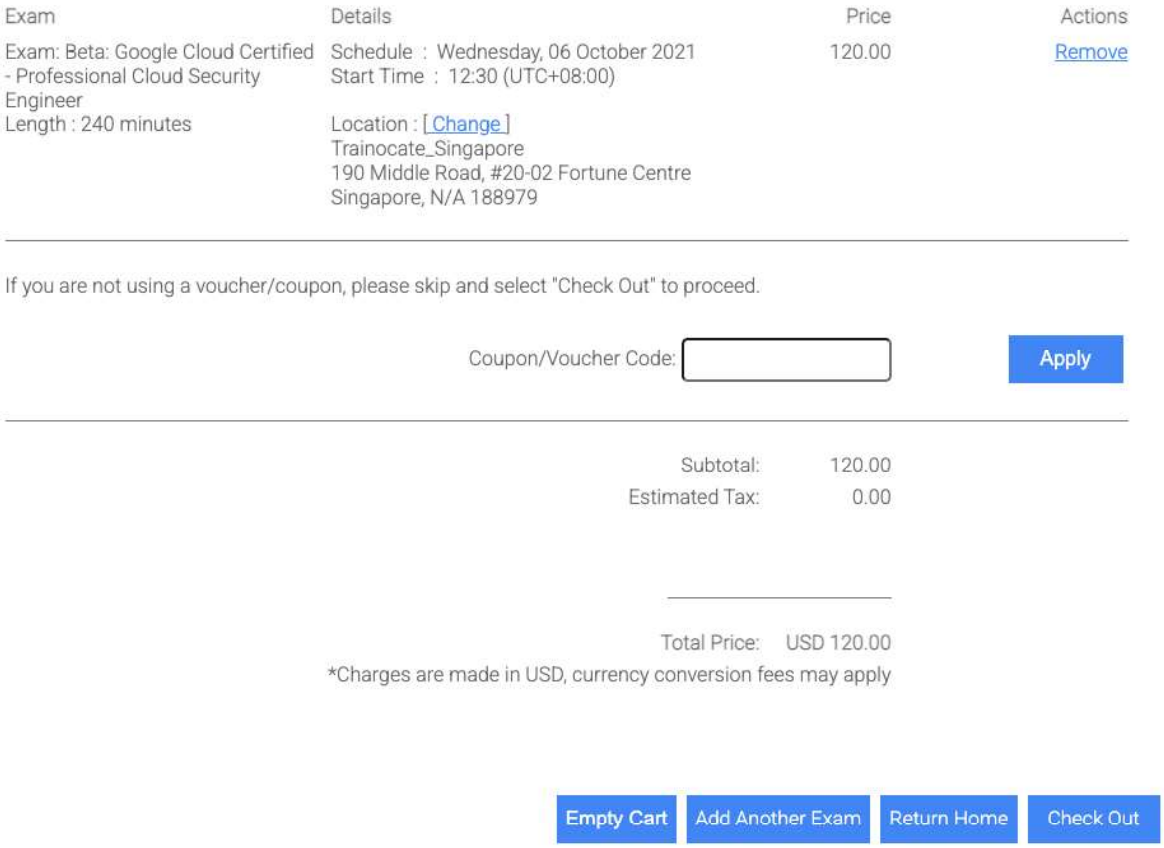

Figure 1.6 – Review and pay

Once you have completed the process, you have the option to make changes to either the center or the date/time. Please refer to the instructions in the confirmation email on how to reschedule without incurring cancellation charges.

Each center has specific requirements as to the identification you need to provide. All this information will be included in the email. Do pay attention to the requirements as you will not be allowed to sit the exam, whether online-proctored or on-site, if you do not have the proper identification.

Some useful tips on how to prepare

Cloud security exams are different from those for other security certifications. They require both depth and breadth of knowledge in multiple security domains. Most vendor security certifications focus on the product, but the GCP Professional Cloud Security Engineer exam focuses on domains such as identity and access management, data protection, network security, logging and monitoring, and security operations. It is important for those attempting the exam to have a sound understanding of the foundational security concepts. This book assumes that you already have basic knowledge of these concepts; if you don't, it's highly encouraged that you gain that knowledge before attempting the exam.

Every individual has a different way to prepare and study, but it's advised that you follow the structure laid out in this book and build knowledge in the areas covered. If you are familiar with GCP security, you can skip chapters and/or read them in any order. For those who are new to GCP, it is highly recommended that you follow the sequence of chapters.

The GCP certification page (`https://packt.link/WlaJJ`) for the Professional Cloud Security Engineer exam contains some helpful details on the exam syllabus, an exam guide, and sample questions. Do take the time to read those as they offer insights. The content of this book is based on the exam blueprint.

The exam questions are multiple-choice and based on real-world scenarios. The test is based on your knowledge of GCP security products and technology. The topics and options can range from cloud security best practices and security configuration to product-specific security controls and how you would meet compliance objectives. The exam is geared toward what cloud security engineers experience day to day while performing their roles.

This book will help you prepare for the range of questions in the exam, and each chapter has a section to test your knowledge. Nothing compares to having hands-on experience; therefore, it is highly encouraged that you create a free GCP account if you don't already have one and spend some time playing around with GCP's security products. Google Cloud Skills Boost has a great collection of GCP security labs, and that collection is recommended for you to get some hands-on experience. In each chapter, there are links to whitepapers and relevant Google Cloud Skills Boost for you to complete. Please note that Google Cloud Skills Boost is a paid service; you can either buy a subscription or pay for each lab.

Another useful resource is courses offered by Google Cloud Skills Boost. In the *Further reading* section of each chapter, you will find links to Google's official courses that are offered through Google Cloud Skills Boost. For those who are new to GCP or familiar with another cloud provider, it is highly recommended that you do some introductory GCP courses from Google Cloud Skills Boost. They will help you build a sound understanding of how GCP is different and what capabilities are offered.

Finally, some key things to remember for the exam. Many of you will already know this, but remember to read the questions very carefully. Most questions have a scenario to paint a picture, but the actual question that is asked is usually in the last line. For example, a question may describe how developers in an organization are building an application that stores sensitive data and how developers and end users access it. It is important to focus on aspects such as who the user is (*the developer*), how they access the application (*by identity and access control*), and what needs to be protected (*the sensitive data*). Extracting such information will help you identify the solution that addresses all those areas.

Always use the option of marking the question for later if you are not sure. Sometimes, the next question is asked in a way that answers the previous question. In that case, you can mark both questions to come back to later and then revisit them before you hit submit. Do keep some time at the end to revisit the questions. Often, when you do 60+ questions, you tend to overlook certain things. Giving yourself an opportunity to check your answers will help.

Summary

In this chapter, we looked at how the GCP Professional Cloud Security Engineer certification is distinguished from others by the kinds of security domains it concerns. We also covered the benefits of getting certified and how to register for the exam.

The next chapter will cover aspects of Google Cloud security at the infrastructure level to help you understand how Google secures its cloud footprint and the various compliance programs and standards it is compliant with.

Further reading

Refer to the following links for further information and reading:

- Google Cloud Certification: `https://packt.link/9hV9a`
- Professional Cloud Security Engineer: `https://packt.link/knxFi`
- Google Cloud Skills Boost: `https://packt.link/gyaJD`

2

Google Cloud Security Concepts

In this chapter, we will cover Google Cloud's security and compliance fundamentals. We will take a look at how Google Cloud secures its cloud infrastructure using strategies such as defense in depth and zero trust. On the compliance side, we will look at different compliance standards and frameworks that Google Cloud is compliant with. Google has a unique approach to shared security responsibility and recently adopted the *shared fate* concept. We will look at these ideas to get a better understanding of Google's responsibility and the customer's responsibility when it comes to security.

After that, we will look at the key pillars of security that Google applies to build a trusted infrastructure that doesn't rely on a single technology but has multiple stacks. We will get a better understanding of each of those stacks and how and where they are applied. Finally, we will briefly cover aspects such as threat and vulnerability management from a Google infrastructure perspective.

The key topics in the chapter include the following:

- Overview of Google Cloud security
- Shared security responsibility
- Addressing compliance with Google Cloud
- The key pillars of security by design
- Threat and vulnerability management

Overview of Google Cloud security

The concepts in this chapter don't appear in the exam and are not part of the exam blueprint. As a Google Cloud security professional who will be responsible for securing enterprise workloads and making them compliant, it's important that you gain a sound understanding of how Google secures its infrastructure. As a security practitioner myself, I have seen many customers who like to understand

aspects such as how the underlying infrastructure is secured, how the hypervisor is secured, how Google achieves multi-tenancy, and which compliance objectives are and are not met. To be able to advise your customers or internal teams, it's essential to know about these topics.

Google Cloud provides a very comprehensive set of security documentation on these topics and it's highly recommended that you take the time to read them. This chapter is a summary of some of the key topics that you must know. There are links at the end of this chapter for you to refer to these documents.

Google has the mission to build the most trusted cloud. In order to achieve this, Google has implemented multiple layers of security to protect its infrastructure, the data, and its users. Let's further understand how Google Cloud doesn't rely on single technologies to make it secure, but rather builds progressive layers of security that deliver true defense in depth.

Google, from the beginning, built its infrastructure to be multi-tenant, and the hardware is Google built, managed, hardened, and operated. All identities, whether they are users or services, are cryptographically authenticated, and only authorized application binaries are allowed to run. Google applies zero-trust principles whereby there is no trust between services, and multiple mechanisms are applied to establish trust. As a Google Cloud user, you have the option to use the Google-operated, -owned, and -managed end-to-end private encrypted network. Google enforces **Transport Layer Security** (**TLS**) for its externally exposed **Application Programming Interfaces** (**APIs**) across its network, and any data stored on Google Cloud is encrypted by default. This makes things much simpler for organizations as it removes the overhead of managing encryption infrastructure and the lifecycle management of the encryption keys. You can find more on encryption and key management in *Chapter 9*, *Google Cloud Key Management Service*. The scale of Google's network allows it to absorb the largest of DDoS attacks; protection from volumetric attacks (Layers 3 and 4) is applied by default. Last and most importantly, Google operates 24x7 security operations to detect threats and respond to security incidents.

In order to further strengthen its security posture, Google has end-to-end provenance. Google servers are custom-built for the sole purpose of running Google services and don't include unnecessary components such as video cards that can introduce vulnerabilities. The same applies to software, including the **operating system** (**OS**), which is a stripped-down, hardened version of Linux. Google has also built Titan, a custom security chip that offers first-nanosecond boot integrity and allows for both server and peripherals to establish a hardware root of trust. Titan uses cryptographic signatures to validate low-level components such as the BIOS, bootloader, kernel, and base OS image during each boot or update cycle. Titan is embedded across Google's hardware infrastructure, servers, storage arrays, and even Pixelbooks and the latest Pixel phones. Google has developed its own network hardware and software to enhance performance and security, resulting in custom data center designs that incorporate various layers of physical and logical protection. Moreover, by maintaining end-to-end control over its hardware stack, Google minimizes the risk of third-party vendors interfering. In the event of a vulnerability, Google's security teams can promptly create and deploy a solution without relying on external parties.

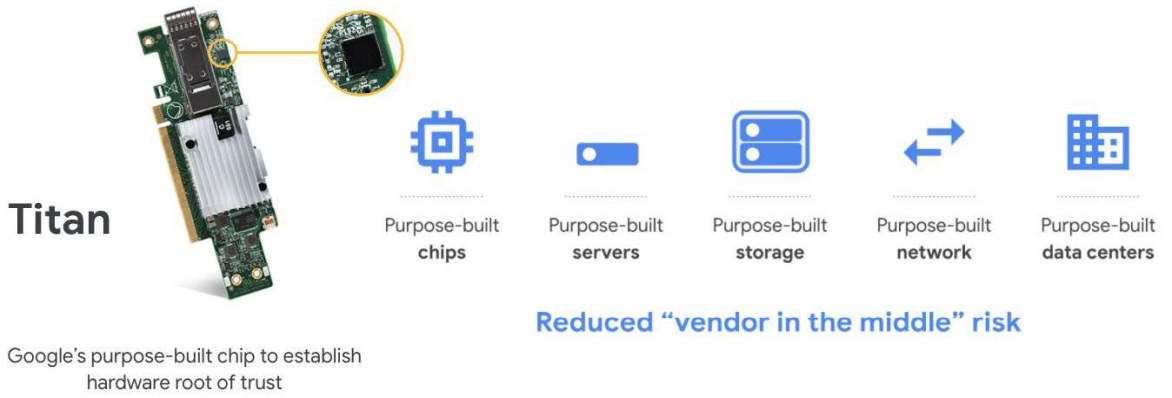

Figure 2.1 – End-to-end provenance and attestation

Data privacy is an important aspect for many customers using the cloud. A key Google Cloud differentiator is how Google Cloud has built-in privacy controls to earn customer trust. One of those services is **Access Transparency**; this service allows customers to gain visibility if and when Google engineers try to access a customer environment. A typical use case would be when a customer contacts Google Cloud support and an engineer is assigned to work to resolve the case and requires access to customer cloud components. In this case, Google can provide full transparency logs to the customer. All these cloud privacy commitments are backed by contractual agreements and commitments, including third-party independent assessments.

The data privacy commitments include the fact that as a customer you own and control your data; Google does not access your data or move it to another location. As a customer, you are responsible for securing and controlling access to your data. Furthermore, Google does not sell or use your data for advertising. There is no backdoor access to Google services for government or law enforcement. As covered earlier, Google encrypts all communications across physical boundaries and encrypts data at rest automatically without customer intervention, adding a further layer of security by default. Lastly, a unique and key differentiation of Google Cloud is how transparent Google is in sharing the logs of any activity that may have led to a Google engineer accessing customer data. This is done by a service that Google offers called Access Transparency. We will cover more on this in the coming chapters.

Shared security responsibility

Google offers a range of services on its cloud platform, including traditional **Infrastructure as a Service** (**IaaS**) services such as Google Compute Engine, **Platform as a Service** (**PaaS**) services such as managed databases, and also **Software as a Service** (**SaaS**). Besides these, Google Cloud offers a rich set of security products and services that customers can use to secure their workloads on Google Cloud. Broadly, when we talk about security on the cloud, we divide it into two parts: security *of* the cloud and security *in* the cloud. These are standard industry terms, where security *of* the cloud refers to what the cloud service provider is responsible for and security *in* the cloud is about the customer

having the responsibility to use security products and services offered natively in the cloud or third-party products. As shown in *Figure 2.2*, the boundaries of responsibility between the customer and the cloud provider change based on the services selected. If the customer is using IaaS to host their workload, then the customer is responsible for protecting the virtual infrastructure, data, users, and monitoring. The responsibility shifts based on the type of service being used.

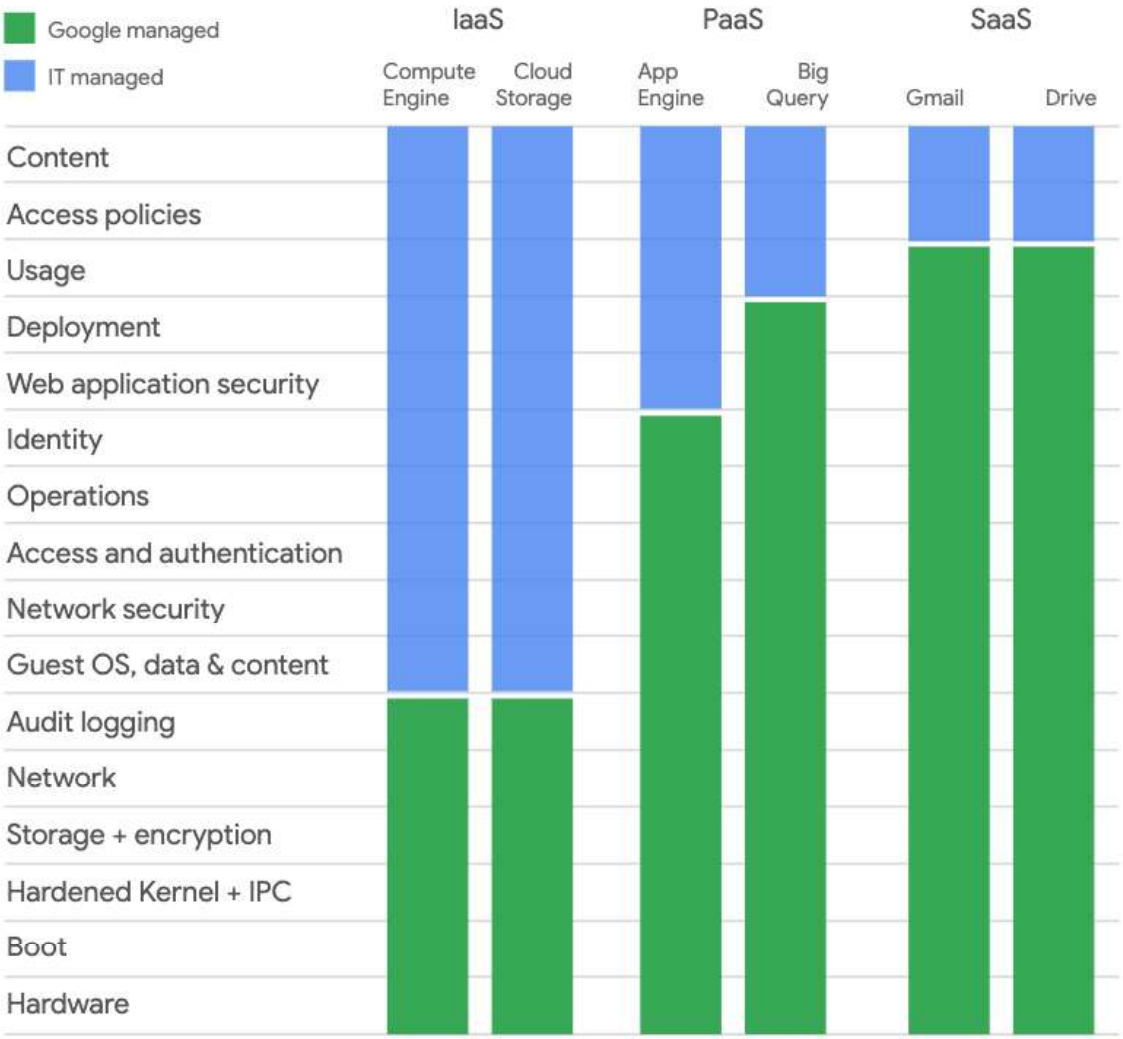

Figure 2.2 – Google Cloud's shared security responsibility (IaaS)

Google has more recently adopted a *shared fate* rather than *shared responsibility* mindset. The premise of this is to operate using a shared fate model for risk management in conjunction with customers. Google believes that it's their responsibility to be active partners as their customers deploy securely on Google Cloud, not to be delineators of where Google's responsibility ends. Google is committed to standing with customers from day one, helping them implement best practices for safely migrating to and operating in a trusted cloud. This is a big step, with Google extending help to customers using

Google Cloud and providing assurance that they will help customers not only when they are adopting the cloud but also if and when there are security incidents that require collaboration between Google and the customer. There is a great whitepaper on how Google responds to incidents and how the responsibility model works; do check out the link in the *Further reading* section for more details.

Addressing compliance on Google Cloud

Google is committed to building trust with customers through certifications and compliance across Google Cloud. A full list of compliance badges can be found here: `https://packt.link/abHuN`. As part of Google's compliance commitments, all of Google's products undergo various third-party independent assessments against compliance controls in order to achieve certifications for standards such as PCI-DSS, ISO, SOC 2, and so on. A full list of all compliance certifications and their relevant reports can be found on the Google Cloud website.

As a customer who is looking to adopt Google Cloud, compliance is key. In order to be compliant, Google implements hundreds of security controls to meet those compliance objectives. As a customer, when you move to Google Cloud, whether you host a single virtual machine or hundreds, you end up inheriting all of these security controls. This not only makes your security posture better but also takes the cost and complexity out of your project scope, making things much simpler from a compliance perspective.

Similar to security being a shared responsibility, compliance is also shared. Google is compliant with a number of international and local standards and privacy guidelines, such as the **Personal Data Protection Act** (**PDPA**), for various countries. Let's take a look at PCI-DSS as an example of how shared responsibility for compliance works. As a customer, if you have the requirement to be PCI-DSS compliant, you can use Google Cloud to run your compliant workloads, by consuming Google Cloud services that are PCI compliant. A list of PCI compliance services can be found here: `https://packt.link/nZhGL`. From an infrastructure perspective, Google Cloud is compliant with PCI-DSS. Your responsibility as a customer includes securing and making your applications and services compliant. These applications and services are not part of Google's core infrastructure, so they fall under the customer's set of responsibilities. It should not be assumed that just because Google Cloud is compliant with PCI-DSS, you will automatically be compliant; although you do inherit compliance-specific controls, they are limited to Google infrastructure.

The next section will further explain how Google's security and compliance controls are built into its cloud infrastructure.

Security by design

Google's approach to security by design is to ensure that multiple technology stacks are deployed to secure the infrastructure, identities, services, and users. *Figure 2.3* highlights the different layers of security that are built into the Google Cloud infrastructure.

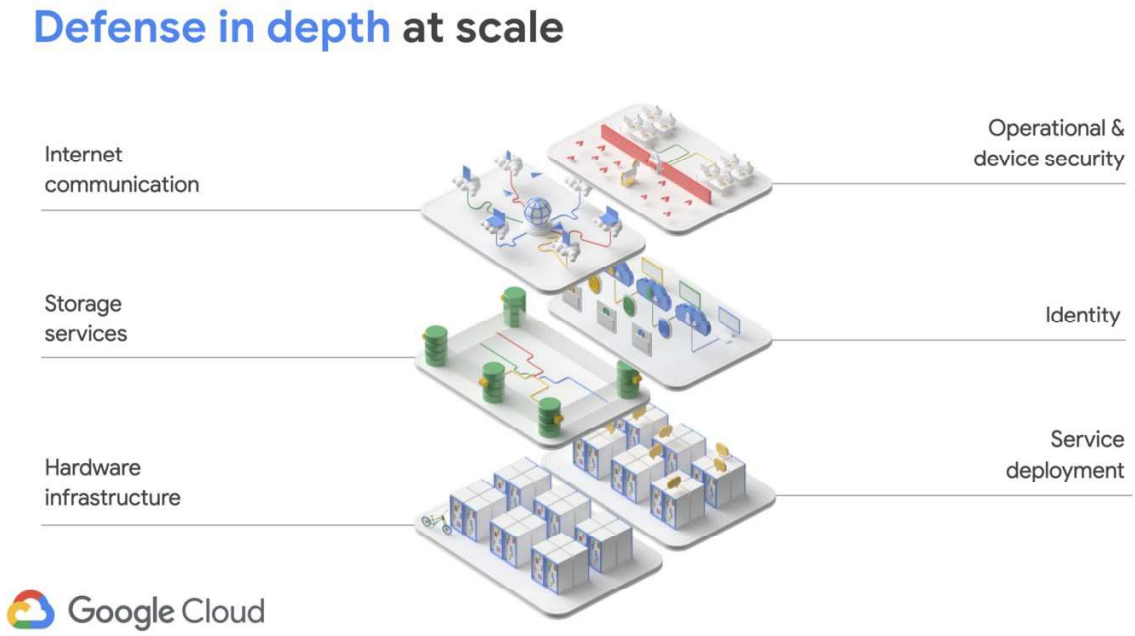

Figure 2.3 – Google defense in depth

In this section, we will cover the key concepts, from operational security to physical security, that Google uses to deliver true defense in depth and at scale.

Operational security

Google's operational security covers aspects such as how Google deploys software services, secures devices and credentials, addresses insider threats, and manages intrusion detection. Let's look at each of these concepts briefly.

In order to securely deploy software services, Google has a secure central control and conducts two-way reviews. Furthermore, Google also provides libraries that prevent developers from introducing certain vulnerabilities such as XSS attacks in web applications. In addition to using automated tools for source code static analysis and identifying bugs, manual security testing is also conducted. These manual tests are run by experts covering areas such as web security, cryptography, and operating systems.

Google also runs a Vulnerability Rewards Program where they pay anyone who discovers and discloses bugs in Google's infrastructure or applications.

Google implements robust security measures to protect employee devices and credentials. In fact, Google leverages a service accessible to all cloud users to safeguard its own devices and user credentials. Through BeyondCorp Enterprise, Google ensures that appropriate users have timely access to designated applications. This approach involves continuous monitoring of devices and users, regular patching and updates, enforcement of strong authentication measures, and utilization of **two-factor authentication** (**2FA**) at Google. Additionally, application-level access controls restrict access to internal applications solely for authorized users accessing the service from managed devices and from network addresses or geolocations that align with the established policy.

To address insider risk, all privileged user access is actively monitored. To further limit employee access, any privileged action that can be safely performed using automation is done so. All users who have access to end-user data have their activity logged and monitored by the security team for access patterns and to investigate anomalies. More details on how Google Cloud does this can be found here: `https://packt.link/PuBbM`.

Google uses very sophisticated intrusion detection techniques, where all data processing pipelines integrate with both host- and network-level signals. These signals are combined with detection rules and machine learning to identify potential threats that are monitored and actioned by security operation teams around the clock. Google also conducts an active Red Team exercise to improve security and its overall effectiveness.

Network security

We have already covered how Google owns, operates, and manages its own global private network, which is fully encrypted and has TLS enforced. This not only delivers lower latency but improves security. Once customers' traffic is on Google's network, it no longer transits the public internet, making it less likely to be attacked, intercepted, or manipulated in transit. Besides this, Google also secures its **Google Front Ends** (**GFEs**). When a service wants to make itself available on the internet, it can register itself with the GFE. The GFE performs a number of functions, such as ensuring that the correct certificates are used for terminating TLS and applying best practices such as perfect forward secrecy. GFEs also provide protection against DDoS attacks. Google has multi-tier and multi-layer protection for DDoS to ensure that the services behind GFEs are protected from such volumetric attacks. Besides GFEs, there are multiple layers of hardware- and software-based load balancers that are both network- and application-aware. All these security controls, together with Google's global-scale infrastructure, ensure that the largest of the DDoS attacks can be absorbed and mitigated.

Besides these network-based security controls, Google further enforces user authentication before it allows any access to its network. The user authentication goes beyond a simple username and password and also intelligently challenges users for additional information based on risk factors. These risk factors include information about the device the user is logging in from, such as the IP address and geographical location of the device. Once past these controls, the user is then prompted for a second factor before access is granted.

Data security

Google ensures that data in motion and data at rest are both secured. We've already covered how Google enforces TLS for all data in motion and encryption by default for data at rest. In addition to the default encryption of data at rest, as a Google Cloud user, you also get the option to select a variety of different options for how you can encrypt data. Recall the previous section on data privacy and Google's commitment to establishing itself as a trusted cloud provider; you as a Google Cloud customer have full control and ownership over your data, meaning you can choose to use the default encryption or use Cloud Key Management Service, which can perform the entire key lifecycle management. Alternatively, you can use Cloud Key Management Service and import your own key material, or you can go the **Bring Your Own Key** (**BYOK**) route or use multi-tenant Cloud HSM, which provides FIPS 140-2 Level 3 protection for your keys. If you operate in a highly regulated environment and need to retain full control of the keys and the infrastructure, you do have the option to use a Google-partner-provided external HSM that is integrated with an external key management service and is accessed via Google's Cloud Key Management Service. More on this in *Chapter 9*, *Google Cloud Key Management Service*.

The challenge with data security is that the data has to remain secure throughout its lifecycle. Whether the data is being created, shared, stored, analyzed, archived, or deleted, it has to be secure. This brings us to how Google manages the data deletion side of things. A key concern from customers is that when you stop using a service that you've used to store sensitive data, even when you have deleted the data, how can you be sure that the data will be wiped from physical media as well? Let's take a quick look at the controls and compliance side of data deletion. When you want to delete data on Google Cloud, it's not immediately deleted but is marked as *scheduled for deletion*; so, if you have accidentally deleted your data, you have the option to recover it. After the data is scheduled for deletion, it is deleted in accordance with service-specific policies.

Google details the entire data handling and data governance as part of their whitepaper called *Trusting your Data with Google Cloud Platform*; a link to this resource can be found in the *Further reading* section of this chapter. We will be covering the data management side of things in more detail in the next chapter on trust and compliance on Google Cloud.

Services and identity

For human-to-system interaction or for calls between systems (such as inter-service access), Google applies cryptographic authentication and authorization at the application layer before any access is granted. Although there are network-perimeter-based controls and network segmentation and firewall rules, Google does not rely solely on that and applies zero-trust principles. Each service that's running also has an associated service account, including the cryptographic credentials that are used for authenticating and authorizing when a remote procedure call is initiated to access other services. Besides this, there are a number of techniques used, such as isolating and sandboxing in order to protect services that might be running on the same machine. Some of the techniques used are language- and kernel-based sandboxing, hardware virtualization, and Linux user separation.

Besides the techniques discussed here, Google's infrastructure also provides strong privacy and integrity for the data that traverses its networks. All protocols for applications such as HTTP are encapsulated inside the remote procedure call infrastructure. To provide greater control, every service owner has the ability to configure the crypto-based protection level required for remote procedure calls; for example, service owners can enable integrity-level protection for data that is of low sensitivity inside data centers. As part of Google's encryption capability, all data is automatically encrypted, including the data that goes between the **wide area network** (**WAN**) and data centers. There is no additional configuration required to enable this and it is configured as default.

Physical and hardware security

In this section, we will look at how Google provides the physical security of its facilities, hardware design, and provenance, and finally, we will look at boot-level security. Together, all these components cater to what we call low-level security controls for Google Cloud.

All Google data centers that cater to Google Cloud services are designed and built as per Google's stringent physical and access controls. Through the *security by design* principle, Google also implements redundant security layers for physical security.

Google employs a range of controls to ensure secure access to its data centers, limiting it only to those who require it to do the job. In terms of physical security, Google has implemented multiple layers of protection across its global data center facilities. These measures include the use of **Closed-Circuit Television** (**CCTV**), vehicle barricades, biometric identification systems, access restrictions for authorized personnel, thorough background checks for employees with facility access, as well as the deployment of laser-based intrusion detection and metal detectors.

At some sites, Google operates some of its servers inside a third-party data center. In those situations, Google ensures that all additional physical security controls mandated by Google are deployed on top of what the data center already has in place. These physical security controls also form part of many compliance programs. Therefore, it's important for Google, in order to stay compliant, to adhere to consistent physical security controls for each of its facilities.

Google has a complex infrastructure consisting of thousands of servers and plenty of network equipment in each of its data centers. Google custom-designs its equipment, which includes the server infrastructure and the network equipment.

In order to eliminate supply chain risks, Google has a process in place to vet every component vendor and audit and validate the security of the components. As covered in earlier sections on end-to-end provenance, all of Google's server and network infrastructure components have a hardware security chip built in; these custom chips are designed by Google. With the deployment of these chips, security is further enhanced and Google is able to not only securely identify the hardware but also authenticate approved devices.

Secure boot stack controls are becoming increasingly common, and more and more customers are expecting their cloud service providers to have them in place. Google is leading the space in securing the boot stack and machine identity. A secure boot chain is built into servers to ensure that the right software is running. In order to ensure this, Google applies techniques such as cryptographic signatures in its low-level components, including the kernel, BIOS, bootloader, and base operating system. Every time the server boots or updates, these signatures are validated. In order to establish a hardware root of trust, every server in the Google data center has an identity bound to the root of trust and the software. When using an API, the same authentication credentials are used for all calls made in order to manage the underlying systems and perform administrative tasks. To manage a large fleet of servers and to ensure they are updated and patched in a timely manner, Google has created automation systems to detect and diagnose both hardware- and software-related issues where, if required, machines are removed from the respective service.

Threat and vulnerability management

The reason for covering threat and vulnerability management at this point is that the components that form this domain, such as vulnerabilities, malware protection, incident response, and security monitoring, are key for customers adopting the cloud. Questions relating to how a cloud service provider manages threats and vulnerabilities are some of the top concerns of customers. Therefore, as security practitioners and engineers, it's important to understand and be able to articulate how Google Cloud provides capabilities to manage threats and vulnerabilities.

As part of its vulnerability management program, to keep its infrastructure secure from cyber threats, Google has technological controls, techniques, and processes to address a multitude of attack vectors. Google actively scans for security-related threats and has manual and automated penetration testing, security assurance programs, and a very mature software security system that includes automated source code scanning and manual reviews. The aim is to ensure that if and when a security vulnerability is identified, it is proactively managed, contained, and controlled. Each identified vulnerability is assigned a priority based on its severity, and the respective team and owners are assigned to mitigate and fix the vulnerability.

Similar to vulnerability management, malware protection controls are built into the Google Cloud infrastructure. Malware attacks can lead to a variety of risks, such as account compromise, data theft, and unauthorized access to the network. Malware continues to increase both in variety and in number. Therefore, it is important for any organization to build strong controls and processes to address malware. Google has higher stakes when it comes to protecting its infrastructure as it has thousands of customers who use its cloud infrastructure to run their business-critical workloads. Hence, Google has built a strategy to manage malware infection, and it applies both automated and manual tools to detect malware. Google has automated scanners that look for websites that host malware and flag them in its search for potential malicious websites used for malware and phishing. The Google Safe Browsing solution scans billions of URLs every day in order to find unsafe websites and then flag them to warn users. This technology is also built into Chrome browsers to warn users of potentially malicious websites. Besides Google Safe Browsing, another of Google's products is VirusTotal, which is a repository for viruses, Trojans, backdoors, worms, and other malicious software. Many adversaries modify their virus signatures to avoid detection by anti-virus tools; therefore, Google uses multiple anti-virus engines in products such as Google Drive and Gmail to effectively identify malware that may be missed by a single engine.

Google has built an effective and robust security monitoring program. Google security monitoring tools gather a variety of information, such as telemetry from its internal network, user actions such as those taken by employees who may have privileged access, and external vulnerabilities, to further enrich the data.

At different points in Google networks, technologies are implemented to monitor and flag anomalous behavior using a variety of techniques, such as detecting the presence of traffic that might indicate botnet connections. Google uses a combination of proprietary and open source technologies for its security monitoring. Google's Threat Analysis Group and its security research arm, Project Zero, work by identifying security threats and making organizations aware of them, such as by placing alerts on public data repositories. Furthermore, like any other security analytics and intelligence unit, Google scans multiple security-related reports on the internet, including blogs, wikis, and mailing lists. For unknown threats, Google conducts automated analysis of the network, and further investigation is conducted to understand how it operates and whether a flag is a false positive or not.

We've already covered aspects of incident response and how Google effectively manages security incidents. Google's incident management response process is aligned with NIST (NIST SP 800-61). Not only is this a rigorous and tested process, but aligning with NIST also helps Google in its compliance program. The incident management process covers the entire lifecycle from detecting and responding to containing, resolving, and then applying the learnings from the incident.

This might be helpful to many customers using Google Cloud, as there are many organizations that adopt the NIST model for handling incidents, meaning the entire end-to-end process is further streamlined for them. Google's security incident response team is available 24x7 to address incidents. For an incident that may have impacted a customer, Google responds to the customer and/or its partners based on the nature of the incident and then helps and supports the customer throughout the process to ensure the incident is resolved. The entire end-to-end process for how Google manages its incident response process is documented and the whitepaper is available and highly recommended for further reading. The following diagram is from that whitepaper. It illustrates the workflow of how Google responds to security incidents and manages the lifecycle.

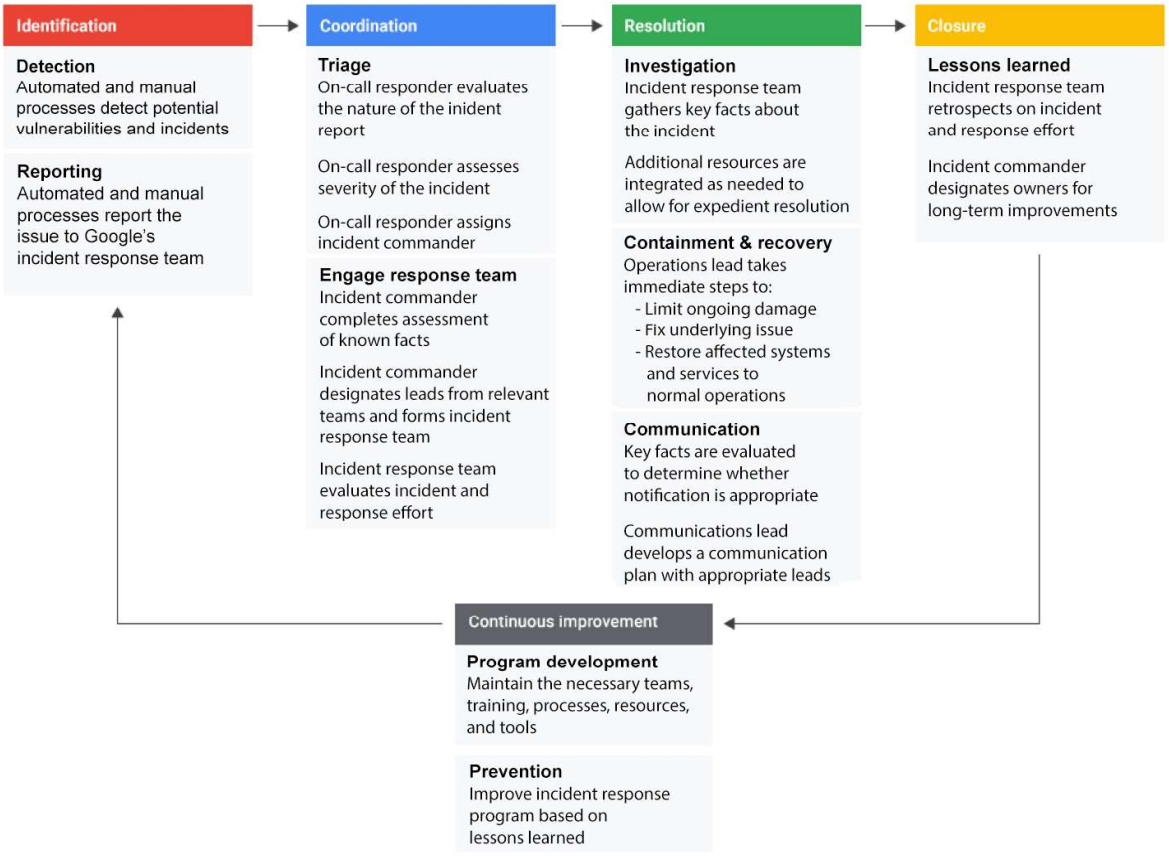

Figure 2.4 – Google Incident response workflow

The incident response process can be complex, and it's important that as a customer you understand what responsibilities fall under your scope. Google will help guide and support as required, but the final responsibility does sit with the user, who is the owner of the system, to take action and remediate.

Summary

In this chapter, we gave an overview of Google Cloud's core security infrastructure. We looked at how Google secures and makes its infrastructure compliant, and we covered what the shared security responsibility model and shared fate on Google Cloud are. Next, we looked at some *security by design* building blocks, covering operational security, data security, service and identity, and low-level security controls, such as physical security and boot stack security. Finally, we learned about threat and vulnerability management and how Google Cloud runs its malware protection, vulnerability management, security monitoring, and incident response.

In the next chapter, we will look at trust and compliance, which is an extension of the core security and compliance infrastructure of Google Cloud.

Further reading

For more information on Google Cloud security, read the following whitepapers:

- Google security whitepaper: `https://packt.link/uQ9Oq`
- Google Infrastructure Security Design Overview: `https://packt.link/Bf8JM`
- Trusting your data with Google Cloud: `https://packt.link/4hV6r`
- Data incident response process: `https://packt.link/zKPNf`
- Encryption in transit: `https://packt.link/PPPxJ`