Google Cloud

Course 3 resources and citations

Module 1: Access control and identity management

Resources

Helpful resources and tips

- Google Docs Editors Help: Google Docs Help Center
- Google Docs Editors Help: Google Sheets Help Center
- Google Docs Editors Help: How to use Google Slides
- QWIKlabs Help: Common problems with labs/lab troubleshooting

Guide to firewall rules

- VPC firewall rules
- View logs by using the Logs Explorer

Citations

Core principles of identity management

- Bhargav-Spantzel, A., Squicciarini, A.C., & Bertino, E. (2007). Trust negotiation in identity management. *IEEE Security and Privacy Magazine, 5(2), 55–63*.
- Choudhary, S., & Singh, N. (2022). Analysis of security-based access control models for cloud computing. *International Journal of Cloud Applications and Computing, 12(1), 1–19*.
- Kandukuri, B. R., Ramakrishna, P. V., & Rakshit, A. (2009). *Cloud security issues*. 2009 IEEE International Conference on Services Computing.

- Le Luo Guan, Lin, J., Luo, B., Jing, J., & Wang, J. (2015). *Protecting private keys against memory disclosure attacks using hardware transactional memory*. IEEE Symposium on Security and Privacy.
- Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and Privacy Challenges in Cloud Computing Environments. *IEEE Security & Privacy, 8(6), 24-31.*
- White, G. L., Mediavilla, F. A. M., & Shah, J. R. (2011). Information privacy. *International Journal of Information Security and Privacy, 5(1), 50–66*.

Uses for identity management measures

- Cloudflare Learning Center. (n.d.). *What is an identity provider (IdP)?* Cloudflare.
- Google Cloud. (2020, February 5). *Enforce uniform MFA to company-owned resources*.
- Google Cloud (2024, January 22). *Access control best practices*.
- Google Cloud. (2024, January 22). *Role-based access control (RBAC) overview*.
- Google Cloud. (2024, January 22). *Role-based access control (RBAC) user guide*.
- Google Cloud. (2023, February 27). *Single sign-on*.
- Google Workspace Admin Help. (n.d.). *Security best practices for administrator accounts*. Google.
- OneLogin. (n.d.). *SAML explained in plain english*.
- Salstonstall, M., & Vergadia, P. (2021, February 8). Security keys and zero trust. *Google Cloud Blog*.

Authentication, authorization and auditing (AAA)

- CISCO. (2023, February 2). Compare TACACS + and RADIUS.
- Google Cloud. (2024, January 22). *Authenticate by using API keys*.

- Lalchandani, N., Jiang, F., Jeong, J.J., Zolotavkin, Y., & Doss, R. (2021, December 21). *Evaluating the current state of application programming interfaces for verifiable credentials*. 2021 18th International Conference on Privacy, Security and Trust (PST).
- Trnka M., Abdelfattah A.S., Shrestha A., Coffey M., & Cerny T. (2022, February 10) Systematic Review of Authentication and Authorization Advancements for the Internet of Things. *Sensors (Basel), 22(4):1361*. doi: 10.3390/s22041361.

Credential handling and service accounts

- Cisco Umbrella. (n.d.). *Cybersecurity threat trends report*.
- Cloudflare. (n.d.). *What is mutual TLS (mTLS)?*
- Google Identity. (2023, November 7). *OAuth 2.0 for client-side web applications*. Google for developers.
- IBM. (2022, December, 13). *OpenID Connect overview*.
- OWASP. (n.d.). *Secrets management cheat sheet*. OWASP Cheat Sheet Series.

Access controls in the cloud

- Amazon Web Services. (n.d.). AWS Identity and Access Management.
- Ferraiolo, D. F., & Kuhn, R. (1992). Role-based access controls. *15th National Computer Security Conference (1992), 554-563*.
- Google Cloud. (n.d.). *Identity and Access Management documentation*.
- Hu, V. C., Kuhn, D. R., & Ferraiolo, D. F. (2015, February). Attribute-based access control. *Computer, 48(2), 85-88*.
- Joint Task Force. (2013, April). *Security and privacy controls for federal information systems and organizations* (Special Publication 800-53, Revision 4). National Institute of Standards and Technology.
- OpenVPN. (n.d.). *What is a VPN?*

- Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *Computer, 29(2), 38-47*.

Cloud access control in action

- Device42. (n.d.). *A guide to cloud asset management*.
- Google Cloud. (n.d.). *VPC service controls*.
- Google Cloud. (2024, January 22). *Access Context Manager overview*.
- Google Cloud. (2024, January 22). *Access control overview*.
- Google Cloud. (2024, January 22). *Compute Engine IAM roles and permissions*.
- Google Cloud. (2024, January 22). *IAM basic and predefined roles reference*.
- Google Cloud. (2024, January 22). *IAM overview*.
- Google Cloud. (2024, January 22). *Introduction to the Organization Policy Service*.
- Google Cloud. (2024, January 22). *Reauthenticating users*.
- Google Cloud. (2024, January 22). *Shared VPC*.
- Google Cloud. (2024, January 22). *Virtual Private Cloud (VPC) overview*.
- Google Cloud. (2024, January 22). *VPC firewall rules*.
- Kulkarni, S., Dixon, F., Nachmany, A., & Erukulla, R. (2023, February 10). *Access control review: Addressing challenges and ensuring compliance in cloud service consumers*. Cloud Security Alliance.
- Mollison, G., & Hohpe, G. (2019, January 10). Identity and authentication, the Google Cloud way. *Google Cloud Blog*.
- National Institute of Standards and Technology. (n.d.). *B.4 Authenticators and verifiers* (Special Publications 800-63B).

- National Security Agency. (2020, January 22). *Mitigating cloud vulnerabilities*.
- OWASP. (2021). *A01:2021 – Broken Access Control*. OWASP Top 10: 2021.

Perimeter protection

- Cloud Security Alliance. (2020). *CSA security guidance for critical areas of focus in cloud computing*.
- Mell, P., & Grance, T. (2011, September). *The NIST definition of cloud computing* (Special Publication 800-145). National Institute of Standards and Technology.
- Meng, G., Liu, Y., Zhang, J., Pokluda, A., & Boutaba, R. (2015, July 22). Collaborative security. *ACM Computing Surveys, 48(1), 1-43*.
- Scarfone, K., & Mell, P. (2007, February). *Guide to intrusion detection and prevention systems (IDPS)* (Special Publication 800-94). National Institute of Standards and Technology.
- Yasar, K., & Letkovich, B. (2018). *Firewall*. TechTarget.

Trust boundaries

- Dotson, C. (2019, April 23). *Practical cloud security*. O'Reilly.
- Google Cloud. (2024, January 22). *Configure firewall rules*.
- Google Cloud. (2024, January 22). *VPC firewall rules*.
- National Institute of Standards and Technology. (n.d.) *Cybersecurity Framework*.
- National Institute of Standards and Technology. (2011). *Chapter 14: Cloud security essentials and architecture*.
- O'Keefe, M. (2019, January 22). Welcome to the service mesh era: Introducing a new Istio blog post series. *Google Cloud Blog*.
- OWASP. (n.d.). *OWASP risk assessment framework*.

- Peacock, T., & Chuvakin, A. (2023, May 22). *How to implement trust boundaries for access control* (122) [Audio podcast]. Cloud Security Podcast.

Guide to firewall rules

- Google Cloud. (2024, January 22). *Firewall Rules Logging*.
- Google Cloud. (2024, January 22). *Virtual Private Cloud (VPC) overview*.
- Google Cloud. (2024, January 22). *VPC Flow Logs*.

Common attack vectors

- Chen, T. M., & Abu-Nimeh, S. (2011, April). Lessons from Stuxnet. *Computer, 44(4), 91-93*.
- Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review, 34(2), 39-53*.
- Scarfone, K., & Mell, P. (2007, February). *Guide to intrusion detection and prevention systems (IDPS)* (Special Publication, pp. 800-94). National Institute of Standards and Technology.
- Stallings, W. (2017). *Network security essentials: Applications and standards (6th ed.)*. Pearson.
- Symantec. (2019, February). *Internet security threat report (ISTR)*. Vol. 24.

Zero trust

- Cybersecurity Action Team. (2022, March). *Applying the NCSC zero trust principles on Google Cloud* [Whitepaper]. Google Cloud.
- Grance, T., & Jansen, W. (2011, December 9). *Guidelines on security and privacy in public cloud computing* (Special Publication 800-144). National Institute of Standards and Technology.
- Palo Alto Networks. (n.d.). *What is a zero trust architecture*.

- Pratt, M. (2023, March 7). *What is zero trust? A model for more effective security*. CSO Online.
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020, August). *Zero trust architecture* (*Special Publication 800-207*). National Institute of Standards and Technology.
- Vigliarolo, B. (2020, May 29). *Zero trust security: A cheat sheet*. TechRepublic.

Zero trust policies and complementary controls

- Crowdstrike. (n.d.) CrowdStrike *Zero Trust*.
- Forrester. (n.d.). Revolutionize your security with Forrester's zero trust model.
- Gartner. (n.d.) *Implementing zero trust security in the public sector*.
- Google Cloud. (n.d.). *What is zero trust?*
- Google Cloud. (2024, January 22). *Create and manage access control lists (ACLs)*.
- Rose, S. , Borchert, O. , Mitchell, S. and Connelly, S. (2020). *Zero trust architecture* (Special Publication 800-207). National Institute of Standards and Technology.
- Wired. (n.d.). *The future of trust starts with "zero"*.

Core principles of identity management

- Bhargav-Spantzel, A., Squicciarini, A. C., & Bertino, E. (2007). Trust negotiation in identity management. *IEEE Security and Privacy Magazine, 5(2), 55-63*.
- Choudhary, S., & Singh, N. (2022). Analysis of security-based access control models for cloud computing. *International Journal of Cloud Applications and Computing, 12(1), 1–19*.
- Kandukuri, B. R., Ramakrishna, P. V., & Rakshit, A. (2009). *Cloud security issues*. 2009 IEEE International Conference on Services Computing.
- Le Luo Guan, Lin, J., Luo, B., Jing, J., & Wang, J. (2015). *Protecting private keys against*

memory disclosure attacks using hardware transactional memory. IEEE Symposium on Security and Privacy.

- Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security and Privacy Magazine, 8(6), 24-31.*
- White, G. L., Mediavilla, F. A. M., & Shah, J. R. (2011). Information privacy. *International Journal of Information Security and Privacy, 5(1), 50–66.*

Module 2: Threat and vulnerability management

Citations

Introduction to threat management

- IBM. (n.d.). *Cybersecurity services*.
- National Cybersecurity Alliance. (n.d.). *CyberSecure My Business*.
- National Institute of Standards and Technology. (2018, April 16). *Framework for improving critical infrastructure cybersecurity*.
- Verizon. (2020). *2020 data breach investigations report*.

Threat and vulnerability management assessments

- Alvarenga, G. (2022, January 11). *What is a cloud security assessment?* Crowdstrike.
- Haber, M.J. (2022, September 16). *How to solve complex cloud security problems with AI*. Cloud Security Alliance.

Asset and resource management

- Center for Internet Security. (n.d.). *CIS Critical Security Control 1: Inventory and control of enterprise assets*.
- Gartner. (n.d.). *IT asset management (ITAM)*. Gartner Glossary.

- National Institute of Standards and Technology. (2018, April 16). *Framework for improving critical infrastructure cybersecurity*.
- SANS Institute. (2023, June 9). *CIS Controls v8*.

Steps for asset management

- Alonso, J., Orue-Echevarria, L., Casola, V., Torre, A.I., Huarte, M., Osaba, E., & Lobo, J.L. (2023, January 12). Understanding the challenges and novel architectural models of multi-cloud native applications – a systematic literature review. *Journal of Cloud Computing, 12(6)*.
- Google Cloud. (n.d.). *Cloud Asset Inventory*.
- Islam, S., Fenz, S., Weippl, E., & Mouratidis, H. (2017, April 22). A risk management framework for cloud migration decision support. *Journal of Risk and Financial Management, 10(2), 10*.
- National Institute of Standards and Technology. (2018, April 16). *Framework for improving critical infrastructure cybersecurity*.

On-the-job asset management applications

- Archer, D. (2023, July 12). The importance of effective asset management in today's cloud environment. *CPO Magazine*.
- Device 42. (n.d.). *A guide to cloud asset management*.
- Google Cloud. (n.d.). *Identity and access management documentation*.
- Google Cloud. (2023, August 4). *Manage your assets*.
- Google Cloud. (2024, January 22). *Introduction to Cloud Asset Inventory*.
- Google Cloud. (2024, January 22). *Review and apply role recommendations for projects, folders, and organizations*.
- Hitachi Vantara. (n.d.). *What is cloud access management (CAM)?*

- IBM Cloud Education. (2022, May 6). What is IT asset management (ITAM)? *IBM Blog*.
- Smart, E. (2023, January 10). *Why asset management is crucial for cyber teams in 2023*. appNovi.
- Rossi, E. (2022, December 21). Introducing cybersecurity asset management. *Qualys Security Blog*.

Vulnerability remediation and posture management

- Almorsy, M., Grundy, J., & Müller, I. (2016, September 5). *An analysis of the cloud computing security problem*. Cornell University.
- Cloud Security Alliance. (2017, July 26). *Security guidance for critical areas of focus in cloud computing v4.0*.
- Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing* (Special Publication 800-145). National Institute of Standards and Technology.
- Zissis, D., & Lekkas, D. (2012, March). Addressing cloud computing security issues. *Future Generation Computer Systems, 28(3), 583-592*.

Vulnerability remediation and posture management in software development

- Cloud Security Alliance. (2017, July 26). *Security guidance for critical areas of focus in cloud computing v4.0*.
- National Institute of Standards and Technology. (2018, April 16). *Framework for improving critical infrastructure cybersecurity*.
- OWASP. (n.d.). *OWASP top ten*.
- Scarfone, K., & Souppaya, M. (2013, July). *Guide to enterprise patch management technologies* (Special Publication 800-40 Revision 3). National Institute of Standards and Technology.
- Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security*. Boston, MA:

Cengage Learning.

- Zalewski, M. (2017). *Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks*. San Francisco, CA: No Starch Press.

Posture management tools and techniques

- Farber, S. (2022, August 2). *Mastering data security posture management: A practical guide to DSPM*. Dig Security.
- Gillis, A.S. (2023, July). *Cloud security posture management (CSPM)*. TechTarget.
- Murphy, T, & Smith, S. (2022, May 6). Know your cloud security acronyms: An overview of CWPP, CSPM, CIEM, and CNAPP. *Orca Security Blog*.
- Puzas, D. (2023, April 17). *What is cloud security posture management (CSPM)?* Crowdstrike.
- Smith, A. (2023, May 3). Top takeaways from the Gartner innovation insight: Data security posture management. *Laminar Security Blog*.
- Snyk. (n.d.). *4 steps of the vulnerability remediation process*.
- Van der Vaart, L. (2021, June 10). 7 steps to improve your cloud security posture management. *VMware Cloud Blog*.

IT automation tools for posture management

- Ansible. (n.d.). *Ansible community documentation*.
- Ansible Galaxy. (n.d.). *Welcome to Galaxy*.
- Fowler, M. (2010, March 1). *Blue green deployment*.
- Humble, J., & Farley, D. (2015). *Continuous delivery: Reliable software releases through build, test, and Deployment Automation*. Addison-Wesley.
- Puppet. (n.d.). *Explore product documentation*.

- Puppet Forge. (n.d.). *Welcome to Puppet Forge*.
- Red Hat. (n.d.). *Red Hat Ansible Automation Platform*.

IT automation tools for security configuration management

- Cybersecurity & Infrastructure Security Agency (n.d.) *Secure by design*.
- Donahue, P.R., & Connolly, E. (2023, April 20). Secure by default: Recommendations from the CISA's newest guide, and how Cloudflare follows these principles to keep you secure. *The Cloudflare Blog*.
- Gillis, A.S. (2023, July). *Cloud security posture management (CSPM)*. TechTarget.
- Moline, J. (2023, June 23). *What is SCM (security configuration management)?* Tripwire.
- National Institute of Standards and Technology. (n.d.) *Security configuration management (SecCM)*. Computer Security Resource Center.
- Souppaya, M. & Scarfone, K. (2022, April). *Guide to enterprise patch management planning: Preventive maintenance for technology* (Special Publication 800-40r4). National Institute of Standards and Technology.

Guide to web application security scanning

- Google Cloud. (2024, January 22). *Setting up custom scans using Web Security Scanner*.
- Hitachi Vantara. (n.d.). *What is cloud access management (CAM)?*

Patching and rehydration

- Antonopoulos, N., Gillam, L., & Springerlink Online Service. (2017). *Cloud Computing : Principles, Systems and Applications. Springer International Publishing.*
- Chapple, M., & Seidl, D. (2021). *CompTIA Security+ SY0-601 Exam Cram (6th ed.).* Pearson IT Certification.

- Hashizume, K., Rosado, D.G., Fernández-Medina, E., & Fernandez, E.B. (2013, February 27). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications, 4(5)*.
- Modi, C., Patel, D., Borisaniya, B., Patel, H., & Rajarajan, M. (2013, January). A survey of intrusion detection techniques in Cloud. *Journal of Network and Computer Applications, 36(1), 42-57*.
- Singh, S., Jeong, Y. S., & Park, J. H. (2016, November). A survey on cloud computing security: Issues, threats, and solutions. *Journal of Network and Computer Applications, 75, 200-222*.
- Zhang, Q., Cheng, L., & Boutaba, R. (2010, April 20). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications, 1, 7-18*.

Compare and contrast: Patching and rehydration

- Balalaie, A., Heydarnoori, A., & Jamshidi, P. (2016). Microservices architecture enables devops: Migration to a cloud-native architecture. *IEEE Software, 33(3), 42-52*.
- Google Cloud. (2023, February 28). *Best practices for operating containers*.
- Leitner, P., Wittern, E., Spillner, J., & Hummer, W. (2019, March). A mixed-method empirical study of Function-as-a-Service software development in industrial practice. *Journal of Systems and Software, 149, 340-359*.

Rehydration keeps systems up-to-date

- Google Cloud. (2023, May 8) *Best practices and reference architectures for VPC design*.
- Google Cloud. (2024, January 26) *Overview of Web Security Scanner*.
- Myres Training. (n.d.). *What is rehydration in AWS*.
- Scappman. (2022, August 5). *Top 5 challenges of patch management*.

Trends in vulnerability and threat management

- Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016, March). Integration of cloud computing and Internet of Things: A survey. *Future Generation Computer Systems, 56, 684-700*.
- Buczak, A. L., & Guven, E. (2016). *A survey of data mining and machine learning methods for cybersecurity intrusion detection*. *IEEE Communications Surveys & Tutorials, 18(2), 1153-1176*.
- Costello, K. & Rimol, N. (2020, October 19). *Gartner identifies the top strategic technology trends for 2021*. Gartner.
- Gai, K., Qiu, M., & Sun, X. (2018, February). A survey on FinTech. *Journal of Network and Computer Applications, 103, 262-273*.
- Hashem, I.A.T., Yaqoob, I., Anuar, N.B., Mokhtar, S., Gani, A., & Khan, S.U. (2015, January). The rise of "big data" on cloud computing: Review and open research issues. *Information Systems, 47, 98-115*.
- Li, Z., Xu, K., Wang, H., Zhao, Y., Wang, X., & Shen, M. (2019, May 30). Machine-learning-based positioning: A survey and future directions. *IEEE Network, 33(3), 96–101*.
- Pan, J. & McElhannon, J. (2018, February). Future edge cloud and edge computing for Internet of Things applications. *IEEE Internet of Things Journal, 5(1), 439-449*.

Trends in security: Artificial Intelligence (AI), machine learning (ML), and Internet of things (IoT)

- Cisco. (n.d.). *What Is Device Security?*
- Corde, C. & Lichtenstein, S. (2023, April 24). Introducing AI-powered investigation in Chronicle Security Operations. *Google Cloud Blog*.
- Google Cloud. (n.d.). *What is artificial intelligence (AI)?*
- IBM. (n.d.). *What is SOAR?*

- Oracle. (n.d.). *What is IoT?*
- Potti, S. (2023, April 24). Supercharging security with generative AI. *Google Cloud Blog*.
- Roeckl, A. (2022, September 23). *What is Internet of Things (IoT) security?* CrowdStrike.
- Segal, E. (2020, March 31). *The impact of AI on cybersecurity*. IEEE Computer Society.

Reports and assessments for threat and vulnerability management

- Assante, M.J. & Lee, R.M. (2015, October 5). *The industrial control system cyber kill chain* [White Paper]. SANS Institute.
- National Institute of Standards and Technology. (2018, April 16). *Framework for improving critical infrastructure cybersecurity*.

Module 3: Resilience and stability in cloud computing

Resources

Guide to automating deployment with Terraform

- HashiCorp: Terraform Language Documentation
- HashiCorp: Google Cloud Platform provider
- GitHub: HCL Native Syntax Specification

Citations

Cloud-native design and architecture principles

- Google Cloud (2023, February 28). *Best practices for operating containers*.
- Google Cloud (2023, November 13) *Manage traffic and load for your workloads in Google Cloud*.
- Google Cloud (2024, January 26) *Managing infrastructure as code with Terraform.*

Cloud Build, and GitOps.

- Grey, T. (2019, June 19). 5 principles for cloud-native architecture – What it is and how to master it. *Google Cloud Blog*.
- Intel (n.d.). *What is cloud automation?*
- Jones, C. (2022, February 1). *What does "Cloud Managed Services" even mean?* Red River.
- Palmore, M.K. & Holmes, W. (2022, April 13) The journey to the cloud mitigates enterprise risk. *Google Cloud Blog*.
- Red Hat (2022, May 11). *What is open source software?*
- Red Hat (2023, December 21). *Stateful vs. stateless*.
- Security Compass (2021, September 16). *How can you identify your internet-facing applications?*

Cloud-native architecture for security

- Google Cloud (2023, August 21). *Shared responsibilities and shared fate on Google Cloud*.
- Hughes. C.(2021, June 20). The shared responsibility model explained and what it means for cloud security. *CSO*.
- Kubernetes (2023, September 7). *Overview of cloud native security*.
- Tasleem, S. & Vijayaraghavulu, P. (2020, October). A multi-level security mechanism for cloud storage system. *International Journal of Innovative Research in Technology, 7(5), 140-148*.

TTL policies and expiration

- Google Cloud. (2024, January 26) *Manage data retention with TTL policies*.
- Google Cloud. (2024, January 26) *Time to live (TTL) overview*.

- Scylla. (n.d.). *Time to live (TTL) value*.

Introduction to ephemerality and immutability

- Aima, A. (2020, February 5). Storage options in Google Cloud Platform - Rundown. *DataDrivenInvestor*.
- Cyral Inc. (n.d.). Immutability for cloud infrastructure (and for turning pets into cattle). *Cyral Inc Blog*.
- Dadgar, A. (2018, November 15) *What is mutable vs. immutable infrastructure?* HashiCorp.
- Google Cloud (2024, January 26). *Create short-lived credentials for a service account*.
- Moore, M. (2022, April 12). *The principle of ephemerality*. Chainguard.
- Peacock, T., & Chuvakin, A. (Host). (2022, May 31). *Cyber defense matrix and does cloud security have to DIE to win?* (67)[Audio podcast episode]. Cloud Security Podcast.
- Posey, B. (2021, June 9). *How immutable object storage can help protect data*. TechTarget.

Automation in cloud security

- HashiCorp (n.d.). *Configuration syntax*.
- Hashicorp (n.d.) *Initialize Terraform configuration*.
- Intel. (n.d.). *What is cloud automation?*
- Rajasekar, P. (2022, August 3). Why automation and scalability are the most important traits of your Kubernetes platform. *Google Cloud Blog*.
- Red Hat. (2022, July 25). *What is cloud automation?*

Infrastructure as code, policy as code, and DevSecOps

- Buchanan, I. (n.d.). *Infrastructure as code - How infrastructure as code manages complex infrastructure*. Atlassian.
- Clegg, T. (2022, March 25). *GUIs, CLI, APIs: Learn basic terms of infrastructure-as-code*. The New Stack.
- IBM (n.d.) *What is IT infrastructure?*
- Karam, T. (2022, January 19). Securing DevOps: The ABCs of security-as-code. *Cloud Security Alliance Blog*.
- Lee, B. (2020, February 21). Using Open Policy Agent (OPA) to develop policy as code for cloud infrastructure. *Cloud Security Alliance Blog*.
- National Institute of Standards and Technology (n.d.) *Application programming interface (API)*. Computer Security Resource Center.
- National Institute of Standards and Technology. (n.d.) *Infrastructure as code*. *Computer Security Resource Center*.
- Paloalto Networks (n.d.). *What is policy-as-code?*
- Red Hat (2022, May 11). *What is infrastructure as code (IaC)?*
- Tech at GSA. (n.d.) *Building a DevSecOps culture - from a technical perspective*.
- Wilson, B. (2023, March 14). *Infrastructure as code vs. configuration management vs. infrastructure provisioning*. DevOps Cube.
- Zhang, X. (2023, April 7). Realize policy-as-code with Pulumi through CrossGuard on Google Cloud. *Google Cloud Blog*.

Automation to improve cloud security efficiency

- Bigelow, S.J. & Montgomery J. (2021, July). *Cloud automation*. TechTarget.
- Ghanizada, I. (2022, December 9). IT prediction: the vast majority of security operations workloads will be automated. *Google Cloud Blog*.
- Ghanizada.I. & Chuvakin, A. (n.d.) *Autonomic security operations: 10x transformation of the Security Operations Center*. Google Cloud.
- Martinez, R., & Shin, P. (2023, January 20). Building an automated serverless deployment pipeline with Cloud Build. *Google Cloud Blog*.
- Shackleford, D. (2021, January 29). *4 steps toward cloud security automation*. TechTarget.

AI and automation in security

- Barret, C., Boyd, B., Burzstein, E., Carlini, N., Chen, B., Choi, J., Chowdhury, A.R., Christodorescu, M., Datta, A., Feizi, S., Fisher, K., Hashimoto, T., Hendrycks, D., Jha, S., Kang, D., Kerschbaum, F., Mitchell, E., Mitchell, J., Ramzan, Z., ... Yang, D. (2023, December 29). *Identifying and mitigating the security risks of generative AI*.
- Boutin, Chad. (2022, March 16). *There's more to AI bias than biased data*. National Institute of Standards and Technology.
- Dhoni, P., & Kumar, R. (2023, August 18). *Synergizing generative AI and cybersecurity: Roles of generative AI entities, companies, agencies, and government in enhancing cybersecurity*. TechRxiv.
- IBM Data and AI team. (2023, October 16). Shedding light on AI bias with real world examples. *IBM Blog*.
- Pothukuchi, A.S., Kota, L.V., & Mallikarjunaradhya, V. (2023, August 8). Impact of generative AI on the software development lifecycle (SDLC). *International Journal of Creative Research Thoughts, 11(8)*.

Infrastructure as code and cloud-native security

- Ferrari, M., & Glissmann, J. (2019, April 5). Want repeatable scale? Adopt infrastructure as code on GCP. *Google Cloud Blog*.
- Google Cloud. (2024, January 26). *Using recommendations for infrastructure as code*.
- Hughes, C. (2021, July 8). *Securing infrastructure as code: Perils and best practices*. CSO.
- OWASP. (n.d.). *Infrastructure as code security cheatsheet*. OWASP Cheat Sheet Series.
- Stevens, A. (2021, November 11). Automating Cloud Security. *Infosecurity Magazine*.
- Zamot, M. (2019, July 1). How to use infrastructure as code. *OpenSource*.

Benefits of policy as code

- Hashimoto, M., & Dadgar, A. (2020, January 6). *How policy as code imbues DevOps with speed & protection*. Hashicorp.
- Paloalto. (n.d.). *What is policy as code?*
- Pathak, A. (2024, January 2). *Policy-as-code: How to understand and implement it in 2024*. Geekflare.
- Sebek, M. (2022, March 31). 7 benefits of policy as code. *Progress Chef Blog*.

Terraform for IaC management

- Chen, M. (2022, June 20) The 3 phases of infrastructure automation. *HashiCorp Blog*.
- Clegg, T. (2023, June 8). Securing your multi-cloud Terraform pipelines with policy-as-code. *Pluralsight Blog*.
- IBM (n.d.). *What is Terraform?*
- Kosaka, G. (2021, April 17). An introduction to secure infrastructure as code (IaC) using Terraform. *SUSE Blog*.

- Morris, K. (2021, January 19). *Infrastructure as Code, 2nd Edition*. O'Reilly.
- Oracle. (2022, May 10). *What is Infrastructure as Code (IaC)?* Developer Resource Center.
- Red Hat (2022, May 11). *What is infrastructure as code (IaC)?*
- Ruddy, K. (2020, June 29). *Managing policy as code with Terraform and Sentinel*. Hashicorp.
- Terraform (n.d.) *Policies API*. Hashicorp.
- Terraform (n.d.) *Policy enforcement*. Hashicorp.
- Terraform (n.d.). *State*. Hashicorp.
- Terraform (n.d.). *The core Terraform workflow*. Hashicorp.
- Szymanski, S. (2023, October 12). What are Terraform modules and how to use them: Tutorial. *Spacelift Blog*.

Terraform and cloud security automation

- Google Cloud. (2023, December 20). Enterprise foundations blueprint.
- Google Cloud. (2024, January 26). *Best practices for using Terraform*.
- Martinez, R. (2021, November 29) Getting started with the security foundations blueprint automation repo. *Google Cloud Blog*.
- Matharu, Y. & Coulter, T. (2022, December 16). *Introduction to policy as code with automation*. Red Hat.
- Terraform (n.d.) *Policies and policy sets*. Hashicorp.
- Terraform (n.d.) *Policy enforcement*. Hashicorp.
- Terraform (n.d.) *Running Terraform in automation*. Hashicorp.

- Terraform (n.d.) *Terraform cloud security model*. Hashicorp.
- Terraform (n.d.) *What is Terraform?* Hashicorp.

Guide to automating deployment with Terraform

- Isla, D. (2018, October 31). *GoogleCloudPlatform/terraform-google-examples*. Github.
- Terraform. (n.d.). *What is Terraform?* HashiCorp.

Containers vs. virtual machines

- Google Cloud (n.d.) *What are containers?*
- Google Cloud (n.d.). *What is a virtual machine?*
- Intel (n.d.) *Containers and the cloud: An easier way to deploy workloads*.
- VMware (n.d.). *What is a hypervisor?*

A brief guide to containers

- Google Cloud (n.d.). *Containers vs VMs*.
- Google Cloud (n.d.) *What are containers?*
- Google Cloud (2024, January 26). *Deploy an app in a container image to a GKE cluster*.

Containers' importance in cloud

- Dhaduk, H. (2022, May 26). 14 containerization use cases: Hit a home run with containers. *Simform Blog*.
- Google Cloud (n.d.). *Containers vs VMs*.
- Google Cloud (n.d.) *What are containers?*
- Google Cloud (n.d.). *What is microservices architecture?*

Container benefits and considerations

- Awan, A. (2019, August 5). Security concerns around rapid container growth. *The New Stack*.
- Despoudis, T. (2019, June 14). How to lock down the kernel to secure the container. *The New Stack*.
- Docker (n.d.). *About storage drivers*.
- Docker (n.d.). *Multi container apps*.
- Docker (n.d.). *Docker manifest*.
- Flockport (n.d.). *Understanding layers and containers*.
- Google Cloud (2023, February 28). *Best practices for building containers*.
- Google Cloud (n.d.) *What are containers?*
- Kumar, A. (2023, October 19). *Multi container pods in Kubernetes*. K21 Academy.
- National Institute of Standards and Technology (n.d.) *Container runtime*. Computer Security Resource Center.
- Nvidia docs hub. (n.d.). *Preparing to use Docker containers*.
- Red Hat (2022, May 11). *What is a Linux container?*
- Rice, L. (2020. May 12). *Container Security: Chapter 1*. O'Reilly.
- Sanche, D. (2018, January 2). Kubernetes 101: Pods, nodes, containers, and clusters. *Google Cloud – Community*.
- The Hacker News. (2022, May 23). *Yes, containers are terrific, but watch the security risks*.
- Ubuntu Manuals. (2019). *Focal (1): Containers storage*.

- Velayudhan, N. (2021, September 1). What are container runtimes? *Opensource*.
- [x]cube LABS (2023, February 23). *The advantages and disadvantages of containers*.

Techniques to secure containers

- Google Cloud. (2023, February 28). *Best practices for building containers*.
- Kaczorowski, M. (2018, March 29). Exploring container security: An overview. *Google Cloud Blog*.
- Google Cloud (n.d.) *What are containers?*
- Google Cloud (n.d.). *What is Kubernetes?*
- IBM (n.d.). *What are containers?*
- National Institute of Standards and Technology. (n.d.) *Role-based access control (RBAC)*. Computer Security Resource Center.
- Paloalto. (n.d.). *What is container security?*
- Red Hat (2021, September 10). *A layered approach to container and kubernetes security* [Whitepaper].
- Red Hat (2023, April 6). *Understanding containers*.
- Souppaya, M., Morello, J., & Scarfone, K. (2017, September). *Application container security guide* (Special Publication 800-190). National Institute of Standards and Technology.
- VMware (2022). *10 things you must do to secure containers now*.
- VMWare (n.d.). *What is Kubernetes security?*
- Wright, L. (n.d.). Examples of managed services. *Core Blog*.

Container drift

- Fruhlinger, J. (2022, July 19). What is an SBOM? Software bill of materials explained. *CSO Online*.
- Lehmann, T. & Rosenblatt, S. (2022, June 23). How SLSA and SBOM can help healthcare's cybersecurity resiliency. *Google Cloud Blog*.
- Howe, R. (2023, March 22). Container drift: Where age isn't just a number. *Security Intelligence*.
- Kellermann, M. (n.d.). *The Dirty Pipe vulnerability*. M4All.
- Korren, T. (2020, March 19). Blocking attacks in runtime with drift prevention. *Aquqasec Blog*.
- Losh, C. (2021, August 26). *Detect container drift in your Kubernetes deployments*. Trend Micro.
- Nwankwo, E. (2022, October 4). Drift Detection. *Palo Alto live Community Blog*.
- Pelletier, J. (2021, May 18). Configuration drift in Kubernetes - What it is and why it matters. *Fairwinds Blog*.
- Sysdig. (n.d.). *Managing container security with container scanning and more*.
- The Linux Foundation. (2021, June 15). *What is an SBOM?*
- Toulas, B. (2022, November 24). Docker Hub repositories hide over 1,650 malicious containers. *Bleeping Computer*.

Security in containers

- Donston-Miller, D. (2021, August 24). Containers vs. virtual machines: Why you don't always have to choose. *Red Hat*.
- Google Cloud (n.d.). *Containers vs. VMs*.
- Guo, J. (2017, August 9). Demystifying container vs. VM-based security: Security in plaintext. *Google Cloud Blog*.
- Iradier, Á. (2021, October 14). Container security best practices: Comprehensive guide. *Sysdig Blog*.
- Kaczorowski, M. (2018, March 29). Exploring container security: An overview. *Google Cloud Blog*.
- Kubernetes. (2023, August 24). *Using RBAC authorization*.
- Kubernetes. (2023, November 3). *User namespaces*.
- Lidder, U. (2023, July 19). Enhancing cloud security: Four vital practices for Kubernetes security. *Cloud Security Alliance Blog*.
- Sheps, A. (2023). What is container security? *Cloud Native Wiki*.
- Security Guidance Working Group. (2021, August 19). Five recommendations for securing cloud containers. *Cloud Security Alliance Blog*.
- The Google Cloud content marketing team. (2021, May 23). Cloud computing 101: Frequently asked questions. *Google Cloud Blog*.
- OWASP (n.d.). *OWASP DevSecOps Guideline – v–0.2*.
- Scanlon, T. & Laughlin, R. (2020, April 6). 7 quick steps to using containers securely. *SEI Blog, Carnegie Mellon University*.

Serverless functions and security

- Cloudflare (n.d.). *Serverless computing vs. containers – How to choose*.
- Hamerman, O. (2023, February 9). Containers and serverless – Rivals or cohorts? *InfoQ*.
- Jacques, N. (2021, March 16). A guide to serverless functions and how to deploy them. *SitePoint*.
- Khani, A. (2021, March 11). Multi-cloud security best practices for serverless functions. *VMware Blog, Broadcom*.
- Mayaan, G.D. (2022, January 3). The basics of serverless user authentication. *Cloud Native Now*.
- Red Hat (2022, May 11). *What is serverless?*
- Watts, S. (2023, July 10). The serverless functions beginner's guide. *Splunk Blog*.

Container orchestration

- Beda, J. (2015, January 22). What makes a container cluster? *Google Cloud Platform Blog, Google*.
- Gilbert, C. (2019, September 4). 5 Kubernetes RBAC mistakes you must avoid. *Red Hat Blog*.
- Google Cloud. (n.d.) *What is container orchestration?*
- IBM (n.d.) *What is container orchestration?*
- Magnezi, K. (2020, July 15). GKE best practices: Designing and building highly available clusters. *Google Cloud Blog*.
- McCune, R. (n.d.). Container orchestration is key. What your security team needs to know. *Tech Beacon*.
- Opentext (n.d.). *What is policy orchestration?*

- Red Hat (2021, June 22). *What is Kubernetes role-based access control (RBAC)?*
- Red Hat (2022, May 10). *What is container orchestration?*
- Red Hat (2022, October 10). *What is high availability and disaster recovery for containers?*
- Sysdig. (n.d.). *Designing a secure container orchestration and containerized architecture strategy*.
- Tolety, K. (2022, April 22). *Building Kubernetes high availability clusters: Easy guide 101*. Hevodata.
- Velimirovic, A. (2021, December 9). Orchestration vs. automation: Overlapping, but different IT concepts. *phoenixNAP Blog*.
- VMware (n.d.). *What are Kubernetes pods?*
- VMware (n.d.). *What is container orchestration?* Broadcom.
- VMware (n.d.). *What is Kubernetes Security?* Broadcom.

Module 4: Data protection and privacy

Citations

Introduction to the three states of data

- Cloudflare (n.d.). *What happens in a TLS handshake? | SSL handshake*.
- Confidential Computing Consortium (n.d.). *About the Confidential Computing Consortium*.
- Fitzgibbons, L. (2019, February). *Data in use*. TechTarget.
- Google Cloud (n.d.) *Confidential VM documentation*.
- Google Cloud (2022, September). *Default encryption at rest*.

- Google Cloud (2022, September). *Encryption in transit* [Whitepaper].
- IBM (n.d.) *What is confidential computing?*
- Inpher (n.d.) *What is fully homomorphic encryption?*
- Rjaibi, W. (2022, April 18). The next frontier for data security: Protecting data in use. *Security Intelligence*.
- SSL Support Team. (2023, June 12). Private and public keys. *SSL*.

Data encryption

- Google Cloud. (n.d.) *What is encryption?*
- Google Cloud (2022, September) *Encryption in transit* [Whitepaper].
- Kong, J.H., Ang, L.M., & Seng, K.P. (2015, March). A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments. *Journal of Network and Computer Applications, 49, 15-50*.
- Mouha, N. (2021, July). *Review of the advanced encryption standard* (Internal report 8319). National Institute of Standards and Technology.
- National Institute of Standards and Security. (2023, February 6). *Elliptic curve cryptography*. Computer Security Resource center.
- Rimkienė, R. (2023, November 15). What is AES encryption and how does it work? *Cyber News*.
- Tyson, M. (2022, February 24). Understand the RSA encryption algorithm. *Infoworld*.

Data encryption at rest, in transit, and in use

- Alfatec (2022, June 27). *What is a centralized key management system?*
- Cloudflare (n.d.). *What is a cryptographic key?*
- Google Cloud (2022, September) *Default encryption at rest*.

- Google Cloud (2023, August 15). *Client-side encryption with Tink and Cloud KMS*.
- Google Cloud (2024, January 26). *Setting up access control*.
- National Institute of Standards and Technology. (2023, May 9). *Advanced Encryption Standard (AES)* (NIST FIPS; 197).
- Velimirovic, A. (2021. November 4). Data encryption at rest explained. *phoenixNAP Blog*.

Asymmetric versus symmetric encryption

- Adee, R. & Mouraditis, H. (2022, February). A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. *Sensors, 22(3), 1109*.
- Arampatzis, A. (2023, July 25). When should you use symmetric vs asymmetric encryption? *Venafi Blog*.
- Google Cloud. (n.d.). *What is encryption and how does it work?*
- Google Cloud. (2022, September). *Default encryption at rest*.
- Google Cloud. (2022, September). *Encryption in transit* [Whitepaper].
- National Institute of Standards and Technology. (2023, May 9). *Advanced Encryption Standard (AES)* (NIST FIPS; 197).

Data classification and tagging

- Buckbee, M. (2023, May 26). What is data classification? Guidelines and process. *Varonis Blog*.
- Google Cloud. (2024, January 26). *Tags and tag templates*.

Protection of personally identifiable information (PII)

- Google Cloud (2024, January 26) *Classification, redaction, and de-identification*.
- National Institute of Standards and Technology. (n.d.) *Data loss*. Computer Security Resource Center.

Cryptographic keys for data protection

- Cloudflare. (n.d.). *How does public cryptography work?*
- Cloudflare. (n.d.). *What is a cryptographic key?*
- Cloud Security Alliance. (n.d.). *Cloud key management*.
- Google Cloud. (n.d.). *Cloud key management*.
- Google Cloud. (n.d.). *What is encryption?*
- Google Cloud. (2024, January 26). *Destroy and restore key versions*.
- Google Cloud. (2024, January 26). *Key rotation | Cloud KMS documentation*.
- National Institute of Standards and Technology. (n.d.). *Domain parameter*. Computer Security Resource Center.
- National Institute of Standards and Technology. (n.d.) *Key*. Computer Security Resource Center.

Data governance for security and data quality

- Collibra. (2023, October 18). *The 6 data quality dimensions with examples*.
- Google Cloud. (n.d.) *What is data governance?*
- Herzberg, B. (2021, November 11). The datamasters: Data owners vs. data stewards vs. data custodians. *Satori Blog*.
- Montvilas, T. (2022, January 7). How to approach data governance to avoid poor data quality. *Forbes*.

- Oracle (n.d.). *What is data management?*
- OvalEdge Team. (2022, September 8). Data governance and data quality: Working together. *OvalEdge Blog*.
- Sarfin, R.L. (2021, May 12). Data quality dimensions: How do you measure up? *Precisely Blog*.

Data sovereignty and data governance

- Chia, A. (2023, July 11). Data sovereignty vs. data residency: Uncovering the differences. *Splunk Blog*.
- Cloudflare (n.d.). *What is data localization?*
- Cloudian (n.d.). What is *data sovereignty? Challenges and considerations*.
- Google Cloud (2024, January 26). *Data residency overview*.

Data sovereignty challenges and strategies

- Bertucci, D. (2022, April 5). Data sovereignty: Everything you need to know. *Auvik Blog*.
- Chia, A. (2023, July 11). Data sovereignty vs data residency: Uncovering the differences. *Splunk Blogs*.
- Mohanty, P.R. (2023, August 24). Data sovereignty in the AI age: Gupshup's innovative approach. *Gupshup Blog*.
- Spanning Cloud Apps. (n.d.). Data sovereignty: Definition, requirements and how to ensure it. *Spanning Blog*.
- Tan, A. (2023, May 1). Tackling the challenges of data sovereignty in a multi-cloud world. *Computer Weekly, Tech Target*.
- Karlstad, W. (2022, April 19). Why sovereign cloud is a hot topic – 5 tips, and the background. *CIO*.

Data discovery to support data governance

- Chuvakin, A. & Ellis, S. (2020, October 20). Improving security, compliance, and governance with cloud-based DLP data discovery. *Google Cloud Blog*.
- Imperva. (n.d.). *Data discovery*.

Data retention policies

- Druva (n.d.). *Data retention policy definition*.
- Eliaçık, E. (2022, March 30). Everything you need to know about data retention policy. *Dataconomy*.
- Google Cloud. (2024, January 26). *Data deletion on Google Cloud*.
- Marker, A. (2019, July 17). The essentials of data retention: Policies, plans, and templates. *Smartsheet*.
- Onna. (2020, October). The best data retention policy template to get you started. *Onna Blog*.
- Proofpoint (n.d.). *What is a data retention policy?*
- Qureshi, A. (n.d.). Data retention policy 101: Best practices, examples & more [with template]. *Intradyn Blog*.

Plan for business continuity

- Google Cloud. (n.d.). *What is encryption?*
- Google Cloud. (2023, November 22). *Disaster recovery planning guide*.
- Google Cloud. (2024, January 29). *Business continuity planning and disaster recovery*.
- Theimer, M. (2021, October 31). Business continuity and disaster recovery in the cloud. *Cloud Security Alliance Blog*.

Create a business continuity plan

- Cisco (n.d.). *What is business continuity?*
- Posey, B. (2022, May 31). Business continuity in the cloud: Benefits and planning tips. *TechTarget*.
- Sathyanarayanan, K. (2023, June 6). Disaster recovery and business continuity preparedness for cloud-based startups. *ISACA Now Blog*.
- Theimer, M. (2021, October 31). Business continuity and disaster recovery in the cloud. *Cloud Security Alliance Blog*.

Business continuity scenario

- Glickman, H. (2021, March 10). Architecting for failure and the future of resilience: How to ensure you're prepared for risks now and five years down the line. *Forbes*.
- Google Cloud (2023, January 16). *Architecting disaster recovery for cloud infrastructure outages*.
- Google Cloud (2023, November 22). *Disaster recovery planning guide*.
- Marker, A. (2020, November 11). The beginner's guide to business continuity management in the cloud. *Smartsheet*.
- Roddie-Fonseca, M. (2023, July 5). Ransomware in the cloud. *SANS Blog*.
- Theimer, M. (2021, October 31). Business continuity and disaster recovery in the cloud. *Cloud Security Alliance Blog*.
- Torres, G. (2022, March 5). *The key components of a business continuity plan*. *Zerto Blog*.