Course 4 resources and citations

Module 1: Detection foundations

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

Essential SecOps skills

- Google Cloud: Google on SecOps
- Google Cloud: Welcome to the Google Cloud Security Community
- YouTube: *Google Cloud SecOps*

AI in SecOps: Red teams

- Google: Why red teams play a central role in helping organizations secure AI systems

Log types: A breakdown

- Google Cloud: Sample audit log entry
- Google Cloud: Samples for Google Workspace Login Audit

Alert and log optimization

- Google Cloud: Alerting overview

- Google Cloud Whitepaper: Google Cloud security foundations guide

Guide to event threat detection

- Google Cloud: Overview of Event Threat Detection
- Google Cloud: Query findings in the Google Cloud console

Determine the difference between normal activity and an incident

- Google Cloud: Configuring Security Command Center
- Google Cloud: Findings – Security
- Google Cloud: IAM & Admin
- Google Cloud: Logs explorer

Citations

SecOps and its components

- Google Cloud. (n.d.). *Cloud Logging*.
- Google Cloud. (n.d.). *Cloud Monitoring*.
- Google Cloud. (n.d.). *Identity and Access Management (IAM)*.
- 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.
- Kent, K., & Souppaya, M. (2006, September). *Guide to computer security log management: Recommendations of the National Institute of Standards and Technology* (Special Publication 800-92). National Institute of Standards and Technology.
- Google Cloud. (2024, January 22). *Overview of Web Security Scanner*.
- Google Cloud. (n.d.). *Security Command Center*.

Essential SecOps skills

- Lange, K., (2023, May 31). What Is SecOps? Security Operations defined. *Splunk Blog*.
- Google Cloud. (2024, January 22). *Vulnerability findings*.

Vulnerability management techniques

- Angafor, G. N., Yevseyeva, I., & He, Y. (2020). Game-based learning: A review of tabletop exercises for cybersecurity incident response training. *SECURITY AND PRIVACY*, *3*(6), e126.
- Joint Task Force. (2012, September). *Guide for conducting risk assessments* (Special Publication 800-30 Revision 1). National Institute of Standards and Technology.
- Murdoch, D. (2016). *Blue team handbook: Incident response edition: A condensed field guide for the cyber security incident responder.* Createspace Independent Publishing.
- National Cyber Security Centre (NCSC), UK. (2016, September 23). *Vulnerability management*.
- Rehberger, J. (2020). *Cybersecurity Attacks – Red Team Strategies*. Packt Publishing Ltd.
- Tenable. (n.d.). *Solutions for vulnerability management*.
- Weidman, G. (2014). *Penetration testing: A hands-on introduction to hackin*g. No Starch Press.

Vulnerability scanning, penetration testing, and tabletop exercises

- Google Cloud. (2024, January 22). *About Patch*.
- Google Cloud. (2024, January 22). *Overview of Web Security Scanner*.
- Google Cloud. (2024, January 22). *Rapid Vulnerability Detection overview*.
- Google Cloud. (2024, January 22). *Vulnerability findings*.

AI in SecOps: Red teams

- Mandiant. (n.d.). *Red team assessment*.
- Venables, P. (2023, July 26). The Prompt: Insights from our AI Red Team's first report (Q&A). *Google Cloud Blog*.

Incident detection basics

- Evans, E. (2020, August 24). *Incident detection and response in Google Cloud Platform (GCP)*. CSNP.
- Google Cloud. (2024, January 22). *Overview of Event Threat Detection*.
- Google Cloud. (2024, January 23). *Alerting overview*.
- Minherz. (2023, October 12). Make actionable alerts using Google Cloud. *Google Cloud - Community*.
- New Relic. (2023, August 7). *Effective alerting in practice* [Whitepaper].

Phases of incident response and management

- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August). *Computer security incident handling guide (Special Publication, 800-61, Revision 2)*. National Institute of Standards and Technology.
- Google Google Cloud. (2022, September). *Data incident response process*.
- Mell, P., & Grance, T. (2011, September). *The NIST definition of cloud computing (Special Publication 800-145)*. National Institute of Standards and Technology.
- Scarfone, K., & Mell, P. (2007, February). *Guide to intrusion detection and prevention systems (IDPS) (Special Publication 800-94)*. National Institute of Standards and Technology.

Incident response plans

- Bejtlich, R. (2013). *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*. No Starch Press.
- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August). *Computer security incident handling guide (Special Publication 800-61, Revision 2)*. National Institute of Standards and Technology.
- European Network and Information Security Agency (ENISA). (2010, December 20). *Good practice guide for incident management*.
- Kral, P. (2012, February 21). *Incident handler's handbook [White paper]*. SANS Institute.
- Verizon. (n.d.). *2023 Verizon Data Breach Investigations Report*. Verizon Business.

More about incident response phases

- Google Cloud. (2022, September). *Data incident response process*.

Intrusion detection systems

- Google Cloud. (n.d.). *Cloud Monitoring*.
- Google Cloud. (n.d.). *Security*.
- Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019, July 17). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity*, *2(1)*.

Signature and anomaly-based detection

- Google Cloud. (n.d.). *Cloud Monitoring*.
- Google Cloud. (n.d.). *Security*.
- Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019, July 17). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity*, *2(1)*.

Logs for analysis and monitoring

- Chuvakin, A. A. (2013). *Logging and Log Management: the Authoritative Guide to Dealing With Syslog, Audit Logs, Events, Alerts and Other It Noise*. Syngress Media Inc.
- Google Cloud. (n.d.). *Chronicle – Suite*.
- Google Cloud. (n.d.). *Cloud Logging*.
- Google Cloud. (2024, January 22). *Reading and writing application logs*.
- Google Cloud. (2024, January 23). Cloud *Audit Logs overview*.
- Kent, K., & Souppaya, M. (2006, September). *Guide to computer security log management (Special Publication 800-92)*. National Institute of Standards and Technology.

Log types: A breakdown

- Cloud Identity Help. (n.d.). *Admin log events*.
- Cloud Identity Help. (n.d.) *User log events*.
- Google Cloud. (2023, June 13). *gcloud logging sinks create*.
- Google Cloud. (2024, January 23). *Cloud Audit Logs overview*.
- Google Cloud. (2024, January 23). *Route logs to supported destinations*.
- Google Cloud. (2024, January 23). *Routing and storage overview*.

Log management: The skills needed for success

- Chuvakin, A. A., Schmidt, K., & Phillips, C. (2012). *Logging and Log Management: The authoritative guide to understanding the concepts surrounding logging and log management*. Syngress Media Inc.
- Kent, K., & Souppaya, M. (2006, September). *Guide to computer security log management (Special Publication 800-92)*. National Institute of Standards and Technology.
- Tracy, M., Jansen, W., Scarfone, K., & Winograd, T. (2007, September). *Guidelines on securing public web servers (Special Publication 800-44 Version 2)*. National Institute of Standards and Technology.

Alerts and notifications

- Alrashdi, I., Alqazzaz, A., Aloufi, E., Alharthi, R., Zohdy, M., & Ming, H. (2019, March 14). *AD-IoT: Anomaly detection of IoT cyberattacks in Smart City using machine learning*. *IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 0305–0310.*
- Alsubhi, K., Al-Shaer, E., & Boutaba, R. (2008, August 26). Alert prioritization in intrusion detection systems. *NOMS 2008 - 2008 IEEE Network Operations and Management Symposium.*
- Spathoulas, G. P., & Katsikas, S. K. (2010). Reducing false positives in intrusion detection systems. *Computers & Security, 29(1), 35–44*.

Alert search techniques

- Alsulami, B., Almalawi, A., & Fahad, A. (2022, June 6). A review on machine learning based approaches of network intrusion detection systems. *International Journal of Current Science Research and Review, 05(06), 2159-2177*.
- Cotroneo, D., Paudice, A., & Pecchia, A. (2019). Empirical analysis and validation of security alerts filtering techniques. *IEEE Transactions on Dependable and Secure Computing, 16(5), 856–870*.
- Maheyzah Md Siraj, Mohd Aizaini Maarof, & Mohd, Z. (2009, January). Intelligent alert clustering model for network intrusion analysis. *International Journal of Advances in Soft Computing and its Applications, 1(1), 33–48*.
- Manganaris, S., Christensen, M., Zerkle, D., & Hermiz, K. (2000). A data mining analysis of RTID alarms. *Computer Networks, 34(4), 571–577*.

Alert and log optimization

- Google Cloud. (2024, January 23). *Alerting overview*.

Guide to event threat detection

- Google Cloud. (2024, January 22). *Overview of Event Threat Detection*.
- Google Cloud. (2024, January 22). *Work with findings in the Google Cloud console*.

Module 2: Detection in practice

Resources

Lockheed Martin's Cyber Kill Chain® in practice

- Lockheed Martin: Cyber Kill Chain

Guide to false positive analysis

- Google Cloud: Best practices for using service accounts

Explore false positives through incident detection

- Google Cloud: Findings – Security

IoCs for threat detection

- Google Cloud: How to hunt the cloud: Lessons and experiences from years of threat hunting
- Google Cloud: Overview of Event Threat Detection
- Google Cloud: Strategic Threat Hunting with SOAR and Threat Intel

Query tools: RegEx and YARA-L

- Google Cloud: Creating a custom regex detector

Citations

Introduction to Lockheed Martin's Cyber Kill Chain®

- Hornetsecurity. (n.d.). *Cyber Kill Chain*.
- Howard, R., & Olsen, R. (2020). Implementing intrusion kill chain strategies. *Cyber Defense Review*.
- Kauhanen, J. [Host] (2021, March 11). *Looking at phishing through the intrusion kill chain (051)* [Audio podcast]. Cyber Security Sauna.

- Lockheed Martin. (n.d.). *Cyber Kill Chain*.
- Spring, J. and Hatleback, E. (2017, January 4). Thinking about intrusion kill chains as mechanisms. *Journal of Cybersecurity, 3(3), 185-197.*

False positive analysis

- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August) *Computer security incident handling guide* (Special Publication 800-61 Revision 2). National Institute of Standards and Technology.
- KirstenS, Wichers, Jkurucar, kingthorin. (n.d.). *Intrusion detection*. OWASP.
- Maqbool, Z., Aggarwal, P., Pammi, V. S. C., & Dutt, V. (2020, January 28). Cyber security: Effects of penalizing defenders in cyber-security games via experimentation and computational modeling. *Frontiers in Psychology*, *11*, 11.
- National Institute of Standards and Technology. (n.d.). *False positive*. Computer Security Resource Center.
- Proofpoint. (2023, February 3). *What is alert fatigue?*
- The Hacker News. (2022, August 9). *The truth about false positives in security*.

Lockheed Martin's Cyber Kill Chain® in practice

- MITRE ATT&CK. (n.d.). *Cloud Matrix*.

Guide to false positive analysis

- Google Cloud. (2024, January 22). *Service accounts overview*.

Introduction to security monitoring

- Exabeam. (n.d.). *What is cloud security monitoring?*
- Google Cloud. (n.d.). *Cloud Logging*.
- Google Cloud. (2024, January 22). *Overview of Event Threat Detection*.
- Sharif, A. (2023, March 14). *What is cloud monitoring?* Crowdstrike.
- Vergadia, P. (2022, July 13). Security monitoring in Google Cloud. *Google Cloud Blog*.

Security monitoring key concepts

- Blumira. (n.d.). *What is cloud security monitoring? A complete guide*.
- Cooney, C. (2022, May 3). Proactive monitoring vs. reactive monitoring. *Coralogix Blog*.
- Exabeam. (n.d.). *What is cloud security monitoring?*
- Google Cloud. (n.d.). *Operations suite*.
- Google Cloud. (2022, July 13). Security monitoring in Google Cloud. *Google Cloud Blog*.
- Lawrence, M. (n.d.). What is proactive monitoring? *Chron*.
- Vinoth, K.P. (2023, September 26). *Why proactive monitoring matters: Benefits and best practices*. Knowledge Hut.

Tools for proactive security monitoring

- Google Cloud. (n.d.). *Security Command Center*.
- Google Cloud. (2020, November 18). *Security talks: Improve your security posture with the security command center* [Video]. YouTube.
- Google Cloud. (2024, January 22). *Overview of Event Threat Detection*.

Indicators of compromise (IoCs)

- Cybersecurity & Infrastructure Security Agency. (n.d.). *Using indicators of compromise (IOC) for incident response* [Powerpoint slides].
- Cybersecurity & Infrastructure Security Agency. (2023, January 26). *Protecting against malicious use of remote monitoring and management software*.
- Evans, E. (2020, August 24). *Incident detection and response in Google Cloud Platform (GCP)*. CSNP.
- FBI. (2022, March 7). *RagnarLocker ransomware indicators of compromise*.
- Google Cloud. (2024, January 24). *Investigating and responding to threats*.
- Gwalani, R. (2021, October 11). Investigate threats surfaced in Google Cloud's Security Command Center using Chronicle. *Medium*.
- Johnson, C., Badger L., Waltermire, D., Snyder, J., & Skorupka, C. (2016, October). *Guide to cyber threat information sharing* (Special Publication 800-150). National Institute of Standards and Technology.
- National Security Agency. (2019, August). *Continuously hunt for network instructions*.

Essentials of threat hunting

- Chang, B. & Correa, R. (2022, August 17). Announcing curated detections in Chronicle SecOps Suite. *Google Cloud Blog*.
- IBM. (n.d.). *What is threat hunting?*
- Kaplan, D. (2022, September 12). Threat hunting. *Chronicle Blog*.
- MITRE ATT&CK. (n.d.). *Frequently asked questions*.
- Trellix. (n.d.). *What is cyber threat hunting?*

IOCs for threat detection

- Daszczyszak, R., Ellis, D., Luke, S., & Whitley, S. (2019, March). *TTP-based hunting*. MITRE.
- Mandiant. (2023). *M-Trends 2023*.
- SANS. (2016, February 16). *The Who, what, where, when, why and how of effective threat hunting* [Whitepaper].
- Secwriter. (2023, June 23). Unleashing the power of threat hunting in the cloud. *CyberDom*.

Aggregations and correlations

- National Institute of Standards and Technology. (n.d.). *Aggregation*. Computer Security Resource Center.
- National Institute of Standards and Technology. (n.d.). *Correlation*. Computer Security Resource Center.

Introduction to query tools

- Google Cloud. (2024, January 22). *Overview of the YARA-L 2.0 language*.
- Google Cloud. (2024, January 23). *Build queries by using the Logging query language*.
- Google Cloud. (2024, January 23). *Logging query language*.

Query tools: RegEx and YARA-L

- Google Cloud. (2024, January 22). *Creating a custom regex detector*.
- Google Cloud. (2024, January 22). *Yara-L best practices*.

Module 3: Incident response management and attack mitigation

Resources

Guide to log queries, exports, and analysis

- Google Cloud: Query syntax

Analyze audit logs using BigQuery

- Google Cloud: Welcome to BigQuery studio!
- Google Cloud: Stream findings to BigQuery for analysis
- Google Cloud: Quotas and limits

Documentation in practice

- Google Cloud: T-Systems Sovereign Cloud Powered by Google Cloud

Incident response partners

- Google Cloud Chronicle: Welcome to Chronicle
- Mandiant: Cyber threat defense solutions
- MITRE ATTt&CK
- Virustotal

Playbooks' role in incident response

- Google Cloud: *Chronicle documentation*
- NIST: NIST Cybersecurity Framework

Citations

The importance of evidence preservation

- Borkar, P. (2023, May 2). *Incident response: 6 steps and teams and tools that make them*

happen. Exabeam.

- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August). *Computer security incident handling guide* (Special Publication 800-61 Revision 2). National Institute for Standards and Technology.
- Connectwise. (n.d.). *Tier 1 vs. tier 2 vs. tier 3 cybersecurity*.
- Google Cloud. (2022, September). *Data incident response process*.

Digital evidence preservation: Techniques and best practices

- Digicert. (n.d.). *What is an electronic timestamp?*
- Guttman, B., White, D. R., & Walraven, T. (2022, September). *Digital evidence preservation* (Interagency Report 8387). National Institute of Standards and Technology.
- Jabeen, S. (2023, December 20). What are the best practices for protecting digital evidence? *Vidizmo*.
- Namer, A. (2021, August 18). How to conduct live network forensics in GCP. *Google Cloud Blog*.
- Palter, J. (2021, April 19). Preserving digital evidence the right way: Your 10-step guide. *Real Time Networks Blog*.
- United Nations Office on Drugs and Crime (UNODC). (2019, March). *Handling of digital evidence*.

How security teams preserve evidence

- Grispos, G., Storer, T., & Glisson, W.B. (2012). Calm before the storm: The challenges of cloud computing in digital forensics. *Interdisciplinary Informatics Faculty Publications, 44*.
- U.S. Department of Education (ED), Office of the Chief Information Officer (OCIO), & Information Assurance Services (IAS). (2021, January 13). *Standard RS.CO: Computer crime incident reporting*. Department of Education.

Incident response in Google Cloud

- Google Cloud. (n.d.). *Chronicle SIEM*.
- Google Cloud. (2022, September). *Data incident response process*.
- Google Cloud. (2024, January 22). *Chronicle SOAR overview*.
- Stubbs, J., Menn, J. & Bing, C. (2019, June 26). *Inside the West's failed fight against China's 'Cloud Hopper' hackers*. Reuters.

Incident response best practices with Chronicle SOAR

- Exabeam. (n.d.). *Incident response automation and security orchestration with SOAR*.
- Google Cloud. (n.d.). *Chronicle documentation*.
- Google Cloud. (2024, January 22). *Cases overview*.
- Google Cloud. (2024, January 22). *Create Entities (Mapping & modeling)*.
- Google Cloud. (2024, January 22). *Getting started with Chronicle SOAR*.
- Google Cloud. (2024, January 22). *What's on the Playbooks screen?*
- Red Hat. (2022, May 11). *What is SOAR?*

Incident identification

- AT&T Cybersecurity. (n.d.). *Security Incidents: Types of attacks and triage options*. Insider's guide to incident response: Expert tips.
- Cybersecurity & Infrastructure Security Agency. (2020, September 24). *Technical approaches to uncovering and remediating malicious activity*.
- Kleitman, S., Law, M. K. H., & Kay, J. (2018, October 26). *It's the deceiver and the receiver: Individual differences in phishing susceptibility and false positives with item profiling*. PLoS One, 13(10). 10.1371/journal.pone.0205089.

Coordination for incident response

- *Google Cloud*. (2022, September). *Data incident response process*.
- Site Reliability Engineering (SRE). (2017). *Example incident state document*. Google.
- Vankirk, S. (2022, September 2). Protect your company with our cyber incident management expert advice. *Cybersecurity Exchange*.

Guide to log queries, exports, and analysis

- Google Cloud. (2024, January 23). *Cloud Audit Logs overview*.
- Google Cloud. (2024, January 23). *Routing and storage overview*.

Documentation fundamentals

- Borkar, P. (2023, May 2). *Incident response: 6 steps and teams and tools that make them happen*. Exabeam.
- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August). *Computer security incident handling guide* (Special Publication 800-61 Revision 2). National Institute for Standards and Technology.
- Connectwise. (n.d.). *Tier 1 vs. tier 2 vs. tier 3 cybersecurity*.
- Google Cloud. (2022, September). *Data incident response process*.

Elements of successful documentation

- California Department of Technology. (n.d.). *Incident response plan example* [Word doc].
- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August). *Computer security incident handling guide* (Special Publication 800-61 Revision 2). National Institute for Standards and Technology.
- Login. Gov handbook. (n.d.). *Incident response guide*. U.S. General Services Administration.
- Google Cloud. (2022, September). *Data incident response process*.
- Office of Inspector General. (2023, January). *P@s$w0rds at the U.S. Department of the Interior: Easily cracked passwords, lack of multifactor authentication, and other failures put critical DOI systems at risk* (2021–ITA–005). U.S. Department of the Interior.

Documentation in practice

- Cloud.gov. (2023, December 11). *Security incident response guide*.
- Google Cloud. (n.d.). *Google Cloud Armor*.
- Google Cloud. (2022, September). *Data incident response process*.

Actionable alert identification

- Davis, J., & Cheung, J. (2020, August 6). Logs-based security alerting in Google Cloud: Detecting attacks in Cloud Identity. *Google Cloud Blog*.
- Evans, E. (2020, August 24). *Incident detection and response in Google Cloud Platform (GCP)*. CSNP.
- GitLab. (2024, January 24). *Incident management*. The GitLab Handbook.
- Google Cloud. (n.d.). *Operations suite*.
- Google Cloud. (2024, January 22). *Overview of Event Threat Detection*.
- Google Cloud. (2024, January 23). *Alerting overview*.
- Google Cloud. (2024, January 23). *Behavior of metric-based alerting policies*.
- Google Cloud. (2024, January 23). *Using Security Health Analytics*.
- Minherz. (2023, October 12). Make actionable alerts using Google Cloud. *Google Cloud - Community*.
- New Relic. (2023, August 7). *Effective alerting in practice* [White paper].

Security orchestration with playbooks

- Chronicle SOAR. (n.d.). *Working with Playbooks*.
- Nyre-Yu, M. (2020). *Identifying expertise gaps in cyber incident response: Cyber defender needs vs. technological development*. (SAND2020-5902C). Sandia National Lab.
- Tankard, C. (2020). Pandemic underpins need for SOAR. *Network Security*, *2020*(5), 20–20.
- Trustradius. (n.d.). *Chronicle SOAR*.

Incident response orchestration vs. automation

- Deacon-Smith, R. & Atamel, M. (2021, April 21). Choosing the right orchestrator in Google Cloud. *Google Cloud Blog*.
- CloudBolt Software. (n.d.). *Comparing cloud automation and orchestration processes*.
- Cyware Labs. (2021, March 5). *What is the difference between security orchestration and security automation?* *Security orchestration and response.*

Playbooks' role in incident response

- Google Cloud. (n.d.). Chronicle documentation – SOAR.
- Google Cloud. (2022) *Top security playbooks 2022-2023* [Whitepaper]. 3rd Edition.
- Nichols, M. (2023, December 7). *What is SOAR and how does it improve threat detection and remediation?* Red Scan.
- Team ZCySec. (n.d.). *9 SOAR playbook examples for SOC processes*. ZCybersecurity.

Module 4: Incident recovery

Resources

System recovery steps and scenarios

- Dark reading: Homepage
- Infosecurity magazine: Homepage
- National Institute of Standards and Technology (NIST): Computer Security Resource Center
- SecurityWeek: Homepage
- *SysAdmin, Audit, Network and Security (SANS) Institute*: Homepage

Guide to backups and VM recovery

- Google Cloud: Backup and DR Service overview

Recover VMs with Google Backup and DR Service

- Google Cloud: Backup and DR Service overview
- Google Cloud: Backup/recovery appliance types
- Google Cloud: Create a production to snapshot policy
- Google Cloud: Supported regions

Disaster recovery planning in Google Cloud: Build a DRP

- DevOps: Cloud disaster recovery best practices
- Google Cloud: Backup and DR Service documentation
- Google Cloud: Disaster recovery planning guide
- Medium: Disaster recovery on Google Cloud for data (Part 1)
- TechTarget: Cloud disaster recovery (cloud DR)

Disaster recovery planning in Google Cloud: Implement a DRP

- DevOps: Cloud disaster recovery best practices
- Google Cloud: Backup and DR Service documentation
- Google Cloud: Disaster recovery planning guide
- Medium: Disaster recovery on Google Cloud for data (Part 1)
- TechTarget: Cloud disaster recovery (cloud DR)

Create and manage effective BCDR plans

- Google Cloud: Cloud Architecture Center
- Google Cloud: Disaster recovery planning guide
- Google Cloud: Site reliability engineering (Sre)

Interview tip: End responses with positive takeaways

- Interview Warmup

Citations

Recovery plans in action

- Alabama Department of Labor. (n.d.). *Unemployment Insurance Program disaster recovery plan* [White Paper].
- Cybersecurity & Infrastructure Security Agency. (n.d.). *Online toolkit: Partnering to safeguard k-12 organizations from cybersecurity threats*.
- Github. (n.d.). *Playbook: Ransomware*.
- Google Cloud. (2023, November 22). *Disaster recovery planning guide*.
- National Cyber Security Center. (n.d.) *NCSC CAF guidance*.
- Parsons, M. (2023, October, 17). *IT DRP : How best to plan your company's recovery from a cyber crisis*. C-Risk.
- Ready (2023, September 7). *IT disaster recovery plan*. U.S. Department of Homeland Security.
- VMware. (n.d.). *What is disaster recovery?*

Information recovery and system restoration

- Alabama Department of Labor. (n.d.). *Unemployment Insurance Program disaster recovery plan* [White Paper].
- Google Cloud. (n.d.). *What is disaster recovery?*
- MSP360. (2021, January 11). Cloud disaster recovery: Planning and approaches. *MSP3360 Blog*.

System recovery steps and scenarios

- Fearn, N. (2023, December 5). How to recover systems in the event of a cyber attack. *Computer Weekly*.
- ISO. (2012). *ISO/IEC 27037:2012: Information technology - Security techniques - Guidelines for identification, collection, acquisition, and preservation of digital evidence*.
- National Institute of Standards and Technology. (n.d.). *Digital evidence*.
- National Institute of Standards and Technology. (2020, September). *Security and privacy controls for information systems and organizations* (Special Publication 800-53, Revision 5).

Business continuity and disaster recovery (BCDR) basics

- AWS. (n.d.). *Business continuity plan (BCP)*.
- Bartock, M., Cichonsk, J., Souppaya, M., Smith, M., Witte, G., & Scarfone, K. (2016, December). *Guide for cybersecurity event recovery* (Special Publication 800-184). National Institute of Standards and Technology.
- Elephant Drive. (n.d.). *Ultimate guide for beginners: Data backup and recovery explained*.
- Google Cloud. (n.d.). *Backup and disaster recovery*.

- Swanson, M. (2010). *Contingency planning guide for federal information systems* (Special Publication 800-34, Revision 1) [PowerPoint Slides]. National Institute of Standards and Technology.
- Vergadia, P. (2019, October 28). Disaster recovery on Google Cloud: An overview. *Google Cloud - Community*.

The role of BCDR tools

- Hanna, T. (n.d.). *The 15 best business continuity software and tools for 2024*. Solutions Review.
- Moore, J., Bigelow, S.J., & Crocetti, P. (n.d.). *What is BCDR? Business continuity and disaster recovery guide*. Techtarget.
- Rao, S. (2020, April, 23). *Disaster recovery and business continuity plan on Google Cloud*. Unified Data Sciences.

BCDR in Google Cloud

- Google Cloud. (n.d.). *Backup and disaster recovery*.
- Google Cloud. (2024, January 22). *Backup plans*.
- Google Cloud. (2024, January 22). *Set up and plan a Backup and DR Service deployment*.
- Google Cloud. (2024, January 24). *Backup and DR Service overview*.

Guide to backups and VM recovery

- Google Cloud. (2024, January 22). Backup plans.
- Google Cloud. (2024, January 22). Define backup policies.

Recovery options and measures of success

- Google Cloud. (n.d.). *Backup and disaster recovery*.
- Google Cloud. (2023, January 16). *Architecting disaster recovery for cloud infrastructure outages*.
- IBM. (2023, September 18). *Business continuity and disaster recovery overview*. IBM Cloud Framework for Financial Services.
- Swanson, M. (2010). *Contingency planning guide for federal information systems* (Special Publication 800-34, Revision 1) [PowerPoint Slides]. National Institute of Standards and Technology.

Components of a disaster recovery plan (DRP)

- Google Cloud. (n.d.). *Backup and disaster recovery*.
- Ready (2023, September 7). *IT disaster recovery plan*. U.S. Department of Homeland Security.
- Swanson, M., Bowen, P., Phillips, A.W., Gallup, D., & Lynes, D. (2010, May). *Contingency planning guide for federal information systems* (Special Publication 800-34 Revision 1). National Institute of Standards and Technology.

Disaster recovery planning in Google Cloud: Build a DRP

- Cybary. (2022, December 15). CISSP study guide: Disaster recovery - hot, cold, and warm sites. *Cybary Blog*.
- Google Cloud. (2023, January 16). *Architecting disaster recovery for cloud infrastructure outages*.
- Google Cloud. (2023, November 22). *Disaster recovery planning guide*.
- Google Cloud. (2024, January 22). Optimize Security Command Center.

- National Institute of Standards and Technology. (n.d.). *Cold site*. Computer Security Resource Center.
- National Institute of Standards and Technology. (n.d.). *Hot site*. Computer Security Resource Center.
- National Institute of Standards and Technology. (n.d.). *Warm site*. Computer Security Resource Center.

Disaster recovery planning in Google Cloud: Implement a DRP

- Cybary. (2022, December 15). CISSP study guide: Disaster recovery - hot, cold, and warm sites. *Cybary Blog*.
- Google Cloud. (2023, January 16). *Architecting disaster recovery for cloud infrastructure outages*.
- Google Cloud. (2023, November 22). *Disaster recovery planning guide*.
- Google Cloud. (2024, January 22). Optimize Security Command Center.
- National Institute of Standards and Technology. (n.d.). *Cold site*. Computer Security Resource Center.
- National Institute of Standards and Technology. (n.d.). *Hot site*. Computer Security Resource Center.
- National Institute of Standards and Technology. (n.d.). *Warm site*. Computer Security Resource Center.

Business continuity and disaster recovery plans

- Ready (2023, September 7). *IT disaster recovery plan*. U.S. Department of Homeland Security.
- Swanson, M., Bowen, P., Phillips, A.W., Gallup, D., & Lynes, D. (2010, May). *Contingency planning guide for federal information systems* (Special Publication 800-34 Revision 1). National Institute of Standards and Technology.
- Google Cloud. (n.d.). *What is disaster recovery?*
- Google Cloud. (2024, January 22). *Business continuity planning and disaster recovery*.
- Grachis, G. (2018, August 16). *Are you prepared for hurricane season? Disaster recovery and business continuity plan best practices*. CSO Online.
- National Institute of Standards and Technology. (n.d.). *Business continuity plan (BCP)*. Computer Security Resource Center.
- Theimer, M. (2021, October 31). Business continuity and disaster recovery in the cloud. *Cloud Security Alliance Blog*.

Create and manage effective BCDR plans

- Ailsa. (2023, February 1). *Ultimate guide: Google Cloud backup and restore*. CBackup.
- Google Cloud. (2023, January 16). *Architecting disaster recovery for cloud infrastructure outages*.
- Google Cloud. (n.d.). *Cloud Build*.
- Google Cloud. (n.d.). *Cloud Monitoring*.
- Google Cloud. (n.d.). *Identity and Access Management (IAM)*.
- Google AdSense Help. (n.d.). *Overview of the Policy center*. Google Cloud.

- Johnson, C. (n.d.) Building resilience: A step-by-step guide to creating a BCDR plan. *Axcient*.
- Marker, A. (2021, October 17). *Business continuity and disaster recovery: Their differences and how they work together*. Smartsheet.
- Sullivan, E. (2018, December). *Essential guide to business continuity and disaster recovery plans*. TechTarget.

Disaster recovery plan stakeholders

- Bartock, M., Cichonsk, J., Souppaya, M., Smith, M., Witte, G., & Scarfone, K. (2016, December). *Guide for cybersecurity event recovery* (Special Publication 800-184).
- Cloudian. (n.d.). *Disaster recovery plan examples and essential elements for your plan*.
- Google Cloud. (2023, November 22). *Disaster recovery planning guide*.
- ITtoolkit. (n.d.). *How to take a team approach to disaster recovery planning*.
- National Institute of Standards and Technology. (2018, April 16). *Framework for improving critical infrastructure cybersecurity*.
- Spring, J.M., Hatleback, E., Householder, A., Manion, A., & Shick, D. (2020, December), *Prioritizing vulnerability response: A stakeholder-specific vulnerability categorization*. Carnegie Mellon University.