Google Cloud

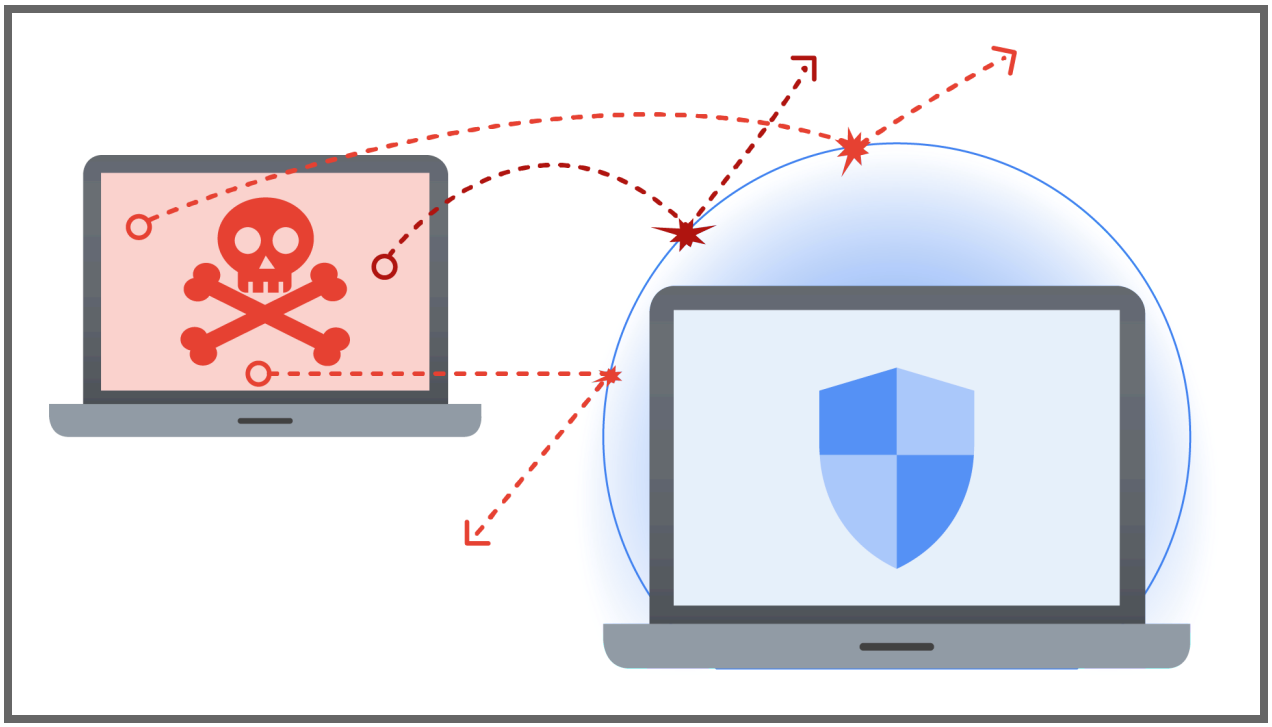
System recovery steps and scenarios

Previously, you learned about ways to keep systems running smoothly as a cloud cybersecurity professional. In this reading, you'll learn how to prepare for the unexpected. Whether it's a cyber attack, natural disaster, or internal error, you'll need to be able to recover quickly and efficiently. How well security operations teams can recover from a security incident can mean the difference between a minor inconvenience and a major catastrophe.

Recall that business continuity (BC) is an organization's ability to maintain their everyday productivity by establishing a risk disaster recovery plan. Cybersecurity administrators use a variety of methods to restore systems to normal operations after a cyberattack or security incident. In this reading, you'll first review a sample set of system restore steps. Then, you'll explore some on-the-job cybersecurity scenarios on effective system recovery solutions. Finally, you'll identify the benefits of evidence preservation and its impact on the success of investigations.

Sample set of system restore steps

As a cybersecurity administrator, there are some common steps you can take to restore systems to normal operations after a security incident.



While the specific steps involved will vary depending on the nature of the incident and the systems affected, here's a sample set you might follow:

1. **Identify the affected asset(s):** This is a critical initial step of recovery. It can involve leveraging Security Command Center (SCC) Premium with its centralized visibility into asset discovery and inventory resources running on Google Cloud.
2. **Eradicate the threat:** This may involve removing malware, patching vulnerabilities, or changing passwords.
3. **Restore data from backups:** If data was lost or corrupted during the incident, it can be restored from backups, if available. First, determine whether to restore from a clean backup or rebuild the system entirely. Second, formulate a well-structured recovery plan, focusing on three core areas: identity management, network segmentation, and endpoint verification.
    - **For identity management:** It's paramount to ensure all accounts have strong passwords. In the event of ongoing incidents, it's advised to reset these passwords daily.
    - **For network segmentation:** Establish three segmented environments: the *Red Network* (compromised environment), the *Green Network* (clean environment), and the *Yellow Network* (a review space for newly turned on systems to detect any indicators of compromise (IOC). This *Yellow,* or staging environment, restricts internet access and inter-network traffic, only allowing exceptions for specific security applications.
    - **For endpoint verification:** If a system is rebuilt, it must utilize a clean golden image certified by the incident response team. If the system is not being rebuilt, then it should be turned on within the *Yellow Network,* equipped with endpoint detection tools to allow the incident response team to ensure no IOC are present.
4. **Test systems to ensure that they are functioning properly:** This may involve running security scans, testing applications, and performing manual checks.

Examples of effective system recovery solutions

Here are some on-the-job cybersecurity scenarios using the Google Cloud Backup and DR Service. Each scenario presents good system recovery solutions like immutable backups, incremental backup, and restoration to different target servers:

Scenario 1: A company's data center is hit by a ransomware attack. The company's backups are stored on an **immutable storage system,** which means that they cannot be encrypted or deleted by the ransomware. The company is able to restore its data from the backups and continue operating without paying the ransom.

Scenario 2: A company's database is accidentally deleted. The company has an **incremental backup system** in place, which means that it only backs up the changes that have been made

to the database since the last full backup. The company is able to restore the database from the incremental backup, minimizing data loss.

Scenario 3: A company's website is hacked and defaced. The company has a **restoration system** in place that allows it to restore its website to a previous state. The company is able to restore the website and resume normal operations within a few hours.

These are just a few examples of how good system recovery solutions can be used to protect businesses from cybersecurity threats. By implementing these solutions, businesses can minimize downtime, data loss, and financial losses in the event of a cyberattack.

Pro tip: Be sure your incident response playbooks include targeted system recovery solutions with realistic and relevant scenarios to your organization.

Once you've restored the systems, you'll need to confirm that everything is functioning properly. Here's how this can be done:

- Monitor system logs and alerts for any suspicious activity.
- Run security scans on all systems.
- Test applications to ensure that they're working properly.
- Perform manual checks to verify that all systems and applications are accessible and functioning as expected.
- Create a chain of custody. A chain of custody is the process of documenting evidence possession and control during an incident lifecycle. This documentation includes how

the security team collects, handles, and stores evidence. Maintaining a chain of custody helps ensure that the evidence is not tampered with.

Benefits of evidence preservation and its impact on the success of investigations

The benefits of evidence preservation include:

- **Improved understanding of the attack:** By preserving digital evidence, investigators can better understand how an attack occurred, what data was compromised, and who was responsible. This information can be used to improve security and prevent future attacks.
- **Increased chances of prosecution:** If digital evidence is properly preserved, it can be used to prosecute the perpetrators of a cyber attack. This can help hold the perpetrators accountable, deter future attacks, and bring justice to the victims.

Failure to preserve evidence in any of these situations can have a significant impact on the success of an investigation. For example, if an organization destroys a system that has been infected with malware, investigators may not be able to identify the malware or determine how it infected the system. This can make it difficult to develop remediation strategies and prevent future infections.

Key takeaways

As a cloud cybersecurity professional, you'll likely respond to security incidents within a team to restore systems to normal operations by identifying the affected asset(s), containing the threat, investigating the incident, eradicating the threat, recovering the systems, and testing the systems. You'll also follow best practices of effective system recovery solutions and evidence preservation—like creating a chain of custody—in a number of cybersecurity situations.

Thorough evidence preservation and documentation can provide valuable insights into the nature of the attack and the perpetrators. It can also have a significant impact on the success of cybersecurity investigations, and mitigate a number of negative consequences. While your goal is to help maintain your organization's data in a secure and safe environment, system recovery is important as a last resource that you'll want to be an expert in!

Resources for more information

Check out these resources to learn more about cybersecurity evidence preservation:

- Dark Reading
- Infosecurity Magazine
- NIST Computer Security Resource Center

- SecurityWeek
- SANS Institute