Documentation in practice

As you've been learning, documentation is critical to cloud security. In this reading, you'll review the fundamentals of quality documentation practices and learn more about how a cloud security team creates and uses documentation. Then to reinforce these concepts, you'll review a real-world example of a security team successfully applying the documentation they created and used during an incident response.

Please note, the following reading should not be considered legal advice. If there is an investigation in a workplace situation, reach out to your organization's legal council.

Overview of documentation

Documentation provides a clear description of incidents and actions that a security team experienced and offers insight into what happened. It also provides a roadmap for what should be done to address the situation, should it re-occur. Well-documented incidents serve as teaching tools for future events that enable cloud security teams to improve processes, playbooks, and security posture to adapt to increasing threats.

Security operations teams record evidence in several types of documentation, including:

- Incident reports
- Evidence logs
- Action plans
- Playbooks
- Logbooks

Individual elements of documentation

Although documentation can include different details, there are specific, universal elements in each type of documentation that help security operations teams respond to incidents.

These elements are:

- Incident summaries
- Timelines
- Technical findings
- Actions taken
- Lessons learned
- Recommendations for improvement

Using these documentation elements, cloud security professionals can create comprehensive and impactful documentation for their security operations incident investigations. This allows them to understand what happened, and how to proceed in the future.

Best practices for documentation

Documentation is a critical aspect of proper incident management and investigation. It improves communication, informs security decisions, and supports the continuous improvement of an organization. To have impact, documentation must be accurate, clear, consistent, and timely.

Documentation is also essential for preserving evidence for legal investigations. Additionally, preservation of evidence is critical when the incident documentation includes sensitive information like system vulnerabilities, recent security breaches, and users with elevated privileges.

Because of the importance and often sensitive nature of documentation, it's essential that it be clear, comprehensive, and easy to understand. You can ensure proper documentation procedures by following these best practices:

- **Provide actionable information**. Use clear, concise, and objective language and focus on the facts and evidence rather than speculating. Writing objectively and using unbiased information ensures the documentation is as accurate as possible.
- **Maintain a consistent format and structure across all documents**. This ensures the documents are easy for all team members to understand.
- **Encourage collaboration and communication during incident response**. Use consistent language, set clear expectations, and communicate in secure spaces.
- **Store information in a secure location**. The documents should be kept in a safe place, but where they can be accessed quickly. This ensures the integrity of the documentation.

Example of successful documentation

In the following scenario, you'll explore an example of a fictional software organization as its cloud security team identifies, responds to, and successfully documents a cybersecurity incident.

The organization

The software organization was founded three years ago and specializes in cloud-based file storage. They employ a small cloud security team that monitors the health and security of their cloud environment, responds to incidents, and creates documentation. The organization is

beginning to expand and plans to hire more members of each department soon, so proper documentation practices are critical to define the organization's security procedures.

The incident

One day, a member of the organization's cloud security team is monitoring network logs when they notice that there's an unusually high amount of traffic on the website. The team member investigates and, based on the evidence available, determines that the increase in traffic is not due to legitimate users. They suspect that a malicious actor is attempting to execute a distributed denial-of-service (DDoS) attack to flood the site with traffic, and make it inaccessible to users. The team member follows the documentation protocol and quickly escalates the incident to a supervisor who examines the logs and confirms that the site is experiencing a DDoS attack. The full security team gathers to review their documentation, form a plan, and act on their plan quickly. They check the network's filtering settings and make updates to block traffic from the malicious source. They also install additional firewalls to block traffic from the malicious source. One team member refers to their documentation that details the recommendation to add a DDoS protection service to better protect against this type of attack in the future. Shortly after their response plan goes into effect, site traffic returns to normal. The team continues to monitor traffic closely over the next few weeks, but there is no indication of abnormal traffic levels.

Type of documentation

Based on the nature of the incident, the organization's cloud security team decides to create an incident report. They make sure to document the incident throughout the response process. They also update their playbook so they have guidance if a similar incident occurs in the future. This allows them to store a record of what happened with as much detail and clarity as possible. It can also be accessed at any time by anyone with the proper authorization.

Steps taken

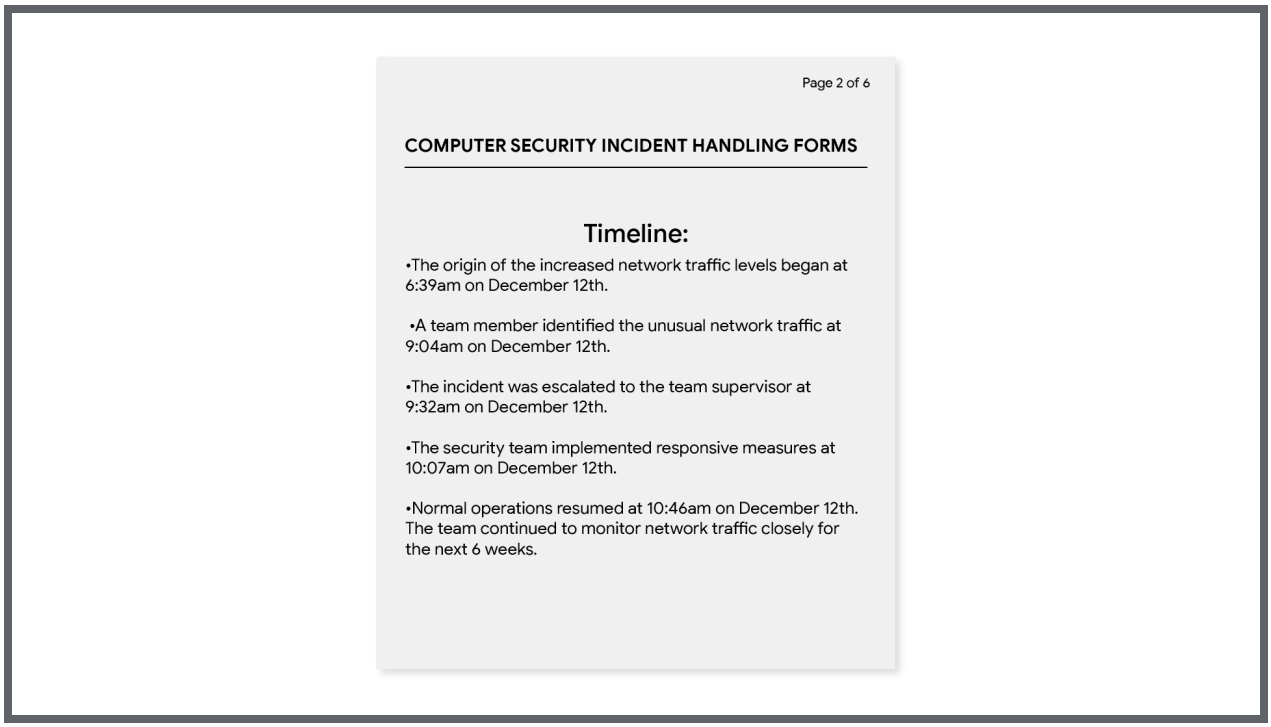
During the incident response process, the security team carefully documents each step of the process and notes any relevant details in an incident report. The following is a high-level summary of their approach to document the incident.

Incident summary

First, the team creates an incident summary. The incident summary includes a brief overview of the incident, including information about how the incident occurred, its severity, and any other relevant context.

Timeline

Second, the team establishes a timeline of events. After the summary section in the incident report, the team creates a section that outlines a clear, chronological sequence of events.



Page 2 of 6

COMPUTER SECURITY INCIDENT HANDLING FORMS

Timeline:

•The origin of the increased network traffic levels began at 6:39am on December 12th.

•A team member identified the unusual network traffic at 9:04am on December 12th.

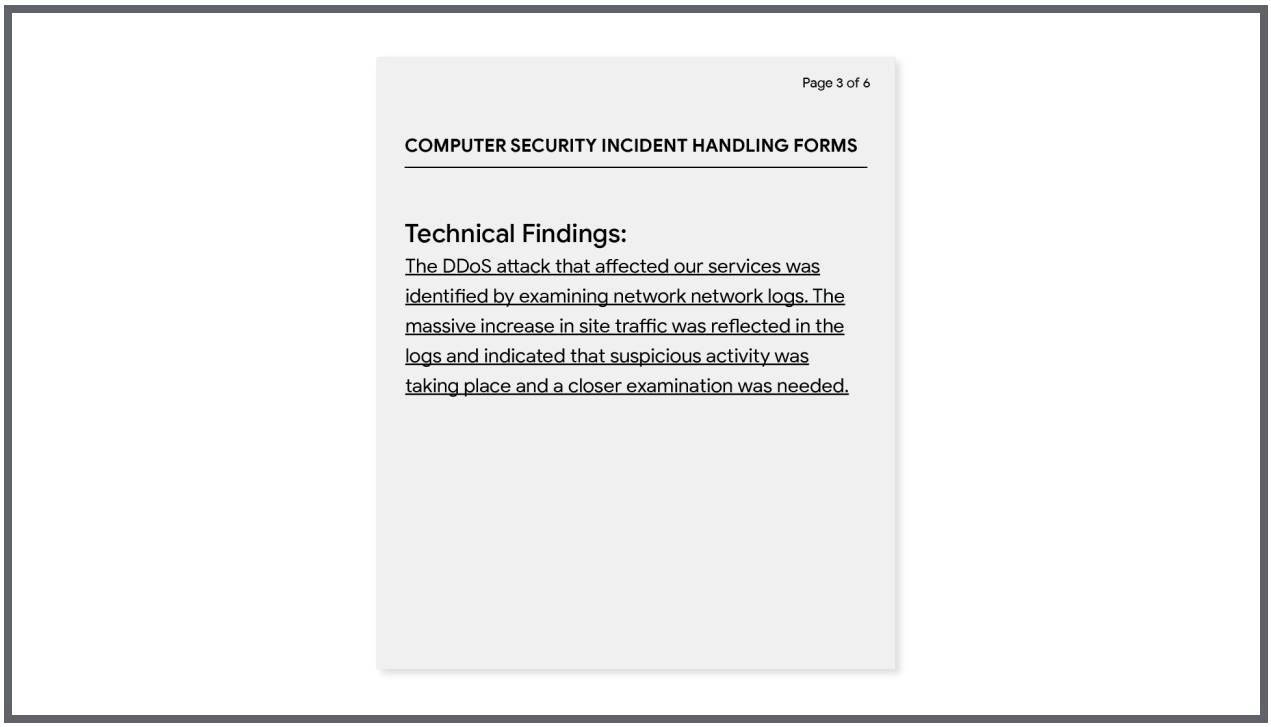
•The incident was escalated to the team supervisor at 9:32am on December 12th.

•The security team implemented responsive measures at 10:07am on December 12th.

•Normal operations resumed at 10:46am on December 12th. The team continued to monitor network traffic closely for the next 6 weeks.

Technical findings

Third, the team records their technical findings. After the timeline section in the incident report, the team adds a section with details about the evidence that prompted the incident response process. This detailed information provides context and understanding about why the incident occurred.



Actions taken

Fourth, the team describes the actions they took. After the timeline and technical findings sections, the team describes their actions and why they were taken. This is an opportunity for the team to document what they did to mitigate the damage caused by the incident.

Page 4 of 6

COMPUTER SECURITY INCIDENT HANDLING FORMS

Actions Taken:

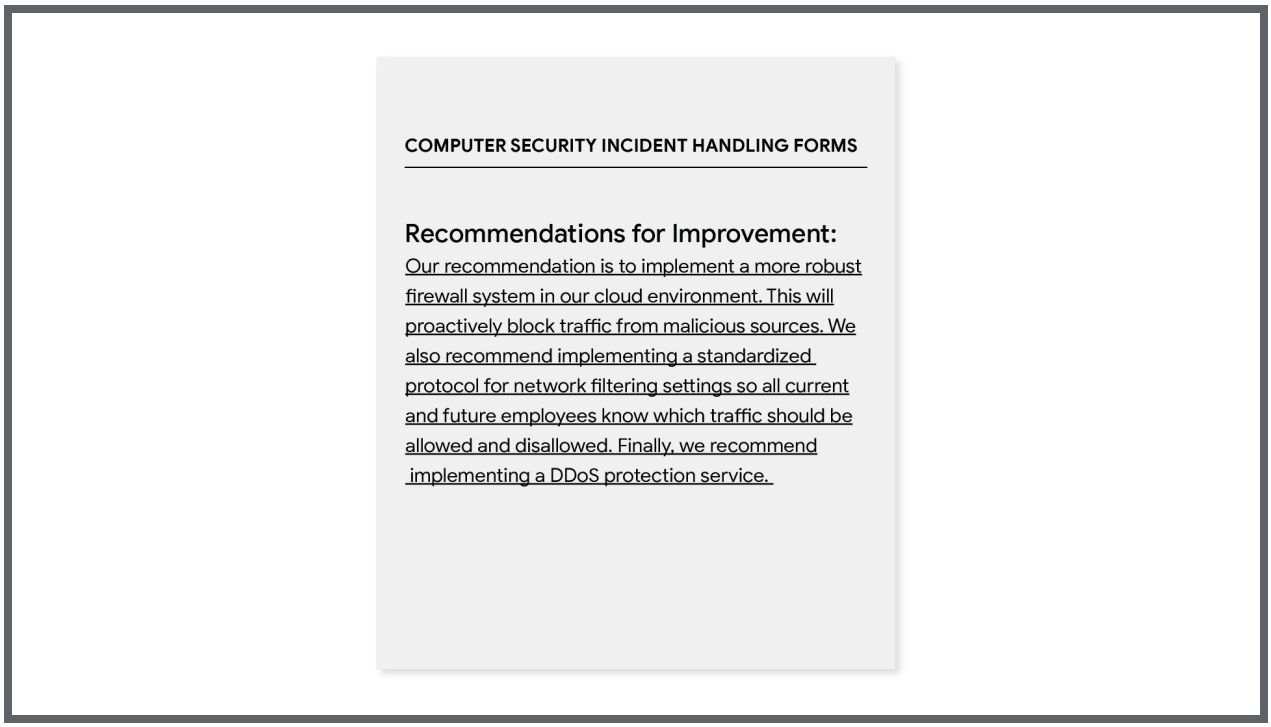
The team took action immediately once the team supervisor confirmed that a DDoS attack had taken place. They adjusted the network's filtering settings to block traffic from the malicious source, identified the IP ranges that were determined to be the source of the attack, and installed additional firewalls to prevent traffic from the malicious source. The team used the IP addresses they identified when implementing the new firewall rules. The team also implemented a DDoS protection service to better protect against this type of attack in the future.

Lessons learned

Fifth, the team lists any lessons they learned. Incident documentation typically ends with lessons learned from the security incident, and what should be done so it doesn't happen again. To document lessons learned, the team reviews the incident to understand and record what went well, and what caused the incident.

Recommendations for improvement

Finally, the team includes any recommendations for improvement. Based on their review, the team suggests actions to take that will lead to future improvements. They also update the company's playbook based on what they learned.



Key takeaways

In this reading you explored documentation, and how it can be applied in the cloud security workplace. You learned about the essentials of documentation, why it's important, and best practices to strengthen its effectiveness. You also explored an example of documentation in a workplace scenario and how a security team would respond to and document an incident successfully.

Resources for more information

- Learn more about sovereignty and Google in T-Systems Sovereign Cloud and Google Cloud