Best practices for effective documentation

Documentation is any form of recorded content that is used for a specific purpose, and it is essential in the field of security. Security teams use documentation to support investigations, complete tasks, and communicate findings. This reading explores the benefits of documentation and provides you with a list of common practices to help you create effective documentation in your security career.

Documentation benefits

You've already learned about many types of security documentation, including playbooks, final reports, and more. As you've also learned, effective documentation has three benefits:

1. Transparency
2. Standardization
3. Clarity

Transparency

In security, transparency is critical for demonstrating compliance with regulations and internal processes, meeting insurance requirements, and for legal proceedings. **Chain of custody** is the process of documenting evidence possession and control during an incident lifecycle. Chain of custody is an example of how documentation produces transparency and an audit trail.

Standardization

Standardization through repeatable processes and procedures supports continuous improvement efforts, helps with knowledge transfer, and facilitates the onboarding of new team members. **Standards** are references that inform how to set policies.

You have learned how NIST provides various security frameworks that are used to improve security measures. Likewise, organizations set up their own standards to meet their business needs. An example of documentation that establishes standardization is an **incident response plan**, which is a document that outlines the procedures to take in each step of incident response. Incident response plans standardize an organization's response process by outlining procedures in advance of an incident. By documenting an organization's incident response plan, you create a standard that people follow, maintaining consistency with repeatable processes and procedures.

Clarity

Ideally, all documentation provides clarity to its audience. Clear documentation helps people quickly access the information they need so they can take necessary action. Security analysts are required to document the reasoning behind any action they take so that it's clear to their team why an alert was escalated or closed.

Best practices

As a security professional, you'll need to apply documentation best practices in your career. Here are some general guidelines to remember:

Know your audience

Before you start creating documentation, consider your audience and their needs. For instance, an incident summary written for a security operations center (SOC) manager will be written differently than one that's drafted for a chief executive officer (CEO). The SOC manager can understand technical security language but a CEO might not. Tailor your document to meet your audience's needs.

Be concise

You might be tasked with creating long documentation, such as a report. But when documentation is too long, people can be discouraged from using it. To ensure that your documentation is useful, establish the purpose immediately. This helps people quickly identify the objective of the document. For example, executive summaries outline the major facts of an incident at the beginning of a final report. This summary should be brief so that it can be easily skimmed to identify the key findings.

Update regularly

In security, new vulnerabilities are discovered and exploited constantly. Documentation must be regularly reviewed and updated to keep up with the evolving threat landscape. For example, after an incident has been resolved, a comprehensive review of the incident can identify gaps in processes and procedures that require changes and updates. By regularly updating documentation, security teams stay well informed and incident response plans stay updated.

Key takeaways

Effective documentation produces benefits for everyone in an organization. Knowing how to create documentation is an essential skill to have as a security analyst. As you continue in your journey to become a security professional, be sure to consider these practices for creating effective documentation.

Mark as completed