Recognizing an Incident

Reading

40m

Status Incomplete

Introduction

Before a security team can respond to an incident, it’s critical to determine if it’s an incident at all. To achieve this, you will need to consider all of the events on the network or system that may indicate a potential attack. These events are called **incident candidates**. The Cyber Security team needs to have strategies to determine whether incident candidates are actual attacks. This reading explores some of the strategies that can help you with this process.

Identifying an Incident

> **Reflect before you read**
>
> Before you begin the reading, make a list of as many events you can think of that might indicate that your organization is experiencing a security incident.
>
> *Adjust, organize, or add to your list as you read. You can store your complete notes in your PKM.*

Author and security expert Donald Pipkin has defined three broad kinds of event indicators: possible, probable, and definite. These broad categories can help a company to swiftly make decisions on incident classification when occurrences are analysed, activating the IR plan as soon as possible and ensuring that the correct processes are followed.

Possible Indicators of an Incident

According to Pipkin's criteria, there are four distinct sorts of signals that might indicate genuine occurrences are taking place:

- **Presence of unfamiliar files** - files that are either at an illogical place, such as in personal folders, or are not held by a valid user.
- **Presence or execution of unknown programs or processes** – unfamiliar programs running, or processes executing, on office machines or network servers.
- **Unusual consumption of computing resources** - a sudden and dramatic increase or decrease in the amount of memory or storage space. You can keep tabs on CPU and memory use in many modern operating systems, as well as your computer's hard disc space. File additions and deletions are recorded in server logs.
- **Unusual system crashes** - Computer failures are not a guaranteed indicator of an incident - you’ve undoubtedly seen the "Program Not Responding," "General Protection Fault," and "Windows Blue Screen or White Screen of Death" error messages

before. However, if a computer system is unusually prone to crashes, hangs, reboots, or freezes, it may be an incident candidate.

Probable Indicators of an Incident

Pipkin goes on to name four categories of unfavourable occurrences that may serve as precursors to real incidents:

- **Activities at unexpected times** - An incident candidate is present if there is an unexpected burst of activity in network traffic, especially during off hours when less activity is expected. Another example of unexpected activity is if systems are accessing associated devices such as mounted discs or USB media while the end user is not actively utilising them.
- **Presence of unexpected new accounts** - New accounts that haven't yet been accessed are a potential target for attack. It's much more likely to be a real event if the new account was created when the user was not signed in and had root or other elevated access.
- **Reported attacks** - A system user reporting a possible attack strongly suggests the existence of an event. There’s a high likelihood that an attack has really happened, though you will also need to take into account the level of technical expertise of the reporter.
- **Notification from an IDPS** - A properly configured IDPS will alert you when an event is likely occurring. However, even when properly set up, IDPSs sometimes report false positives, or false alarms. The administrator must then decide whether the alert is legitimate or the result of a regular action taken by a user or another administrator.

Definite Indicators of an Incident

Pipkin outlines five distinct types of negative incidents that provide unambiguous evidence that an occurrence has taken place or has already happened. The relevant IR strategy must be implemented quickly in such circumstances.

- **Use of dormant accounts** - Default accounts, deactivated accounts, and test accounts are commonly kept on network servers. An incident is very likely to have taken place if any of these accounts start making use of system resources, requesting servers, or doing any other action.
- **Changes to logs** - Systems administrators may check for tampering by comparing offline system logs with their online counterparts during the course of a normal incident scan. If the logs indicate changes, and the systems administrator is unable to definitively establish a legitimate reason for the changes, an incident has happened.
- **Presence of hacker tools** - Scanning internal systems and networks using system vulnerability and network assessment tools to see what an outside hacker may see is a common practice for network administrators. Many companies have implemented strict policies that make installing software without the CISO's approval a serious infraction.
- **Notifications by partner or peer** - Your company has had an incident if a third party claims being attacked by your computer systems or being the target of an attack.
- **Notification by hacker** - Some hackers enjoy taunting their victims. Some common ways they might do this are defacing your organization’s web pages, or making an extortion request for money in exchange for your customers’ credit card files.

Incidents vs. Non-Events

A key stage of the IR plan will be to evaluate incident candidates to distinguish between true **incidents** (or adverse events with the potential to become true incidents) and **non-events**, also known as false positive incident candidates. This is crucial, since the great majority of incident candidates that any given company receives will turn out to be false positives.

> ⚠ False positives are often thought to be intrinsic to incident candidate-gathering systems, even the most well tailored ones. While this is true, you want to keep the number of false positive events below a tolerable threshold through continuous enhancement of your collection methods.

The connection between a false-positive event candidate and background noise is a challenge for many businesses. Events that are wrongly reported as incident candidates are noise, and should trigger a feedback process to improve the system so that legitimate activities are not flagged as events.

Did you know?

Many high-profile hacks, such the 2013 Target breach, occur because symptoms of an ongoing intrusion are ignored as false positives.

Common Reasons for False Positives:

- **Configuration errors**: When the sensitivity of an intrusion detection system is set too high, or improperly configured, it might generate false positive alarms that are not actually intrusions.
- **Lack of correlation**: Some security systems and technologies just generate warnings without taking anything else into account. When taken in the context of additional facts, an alarm may turn out to be a false positive.
- **Human error**: False positives may also result from human mistake. Clicking a link in a phishing email may cause a false alarm since the user thought they were going to a legitimate website.
- **Interference with other systems**: Sometimes the false positive can be the result of interference between the security systems themselves. An alarm may go out if a security system prevents an essential programme from running.
- **Outdated or legacy systems**: Outdated or legacy systems can generate false positives if they are unable to detect new types of threats or attacks.
- **False assumptions**: False assumptions or basing incident response decisions on incomplete or incorrect information can lead to false positives. To reduce the number of false positives and improve incident response, organizations should implement incident response strategies that include multiple layers of defense, correlation and analysis of data, incident response procedures, incident response teams and regular testing and training. Additionally, it's important to regularly review and update incident response procedures, tools and technologies to ensure they are relevant and effective.

A Word about False Negatives

False negatives are rarely publicised, but they also need attention. A false negative incident is when a security system or tool fails to detect an actual incident.

Some examples of false negatives include:

- an intrusion detection system (IDS) failing to notice malicious traffic because it has been encrypted by the attacker.
- a phishing email that is not detected by the email filtering system, and results in the end user revealing sensitive information.

False negatives result in a delay in response and, in some cases, can lead to a total compromise of the organization's security. Regular testing and review of the security systems and robust incident response procedures can help to detect and respond to false negatives.

Incident Detection Strategies

In this section, you will explore the various ways you can implement incident detection strategies in your organization - from regular security checks to employee training to artificial intelligence.

General Detection Strategies

- Watch the network and systems, including files and directories, for unexpected behavior
- Investigate unauthorized hardware attached to your organization’s network
- Inspect physical resources for signs of unauthorized access
- Review reports about suspicious and unexpected behavior
- Set up an incident centre where potential incidents may be submitted at the first sign of trouble

Operational Processes and Supportive Tools

Detection of incidents requires ensuring that processes and services are established to monitor for abnormal or suspicious activity, identifying potential indicators of compromise, and analyzing system and event data to identify patterns that may indicate an incident. Some operational strategies for detection are:

- **Process monitoring**: This can include monitoring for new or unexpected processes, changes in the behavior of existing processes, or the presence of known malicious processes.
- **Service monitoring**: This can include monitoring for new or unexpected services, changes in the behavior of existing services, or the presence of known malicious services.
- **Event log analysis**: This involves analyzing system and event logs to identify patterns that may indicate an incident. This can include monitoring for unusual error messages, failed login attempts, or unusual network traffic.
- **Network traffic analysis**: This involves monitoring network traffic for unusual patterns or anomalies, such as unusual traffic volume, changes in traffic patterns, or the presence of known malicious traffic.
- **File integrity monitoring**: This can include monitoring for new or unexpected files, changes to file properties, or the presence of known malicious files.
- **Behavioral analysis**: This can include identifying patterns of behavior that may indicate an incident, such as unusual user activity, changes in system performance, or the presence of known malicious activity.
- **Correlation and alerting**: This involves correlating data from multiple sources to identify patterns or anomalies that may indicate an incident.

Automation and AI

In recent years, advances in machine learning and artificial intelligence (AI) have allowed for a more refined capacity to recognise occurrences from a large dataset of recorded events. Analyzing, identifying, correlating, and troubleshooting events manually to find actionable occurrences is a time-consuming and error-prone process. Response teams may benefit from faster and more precise responses thanks to the ability to automate, personalise, and integrate incident detection and management processes with the help of cutting-edge technologies and methods based on machine learning and artificial intelligence. An example of this is security information and event management (SIEM), a solution that can help businesses identify and react to problems more quickly and efficiently.

The Human Factor

As always, never underestimate the importance of people. Often, an organization’s employees will be the first to notice when something isn't quite right. While, staff in the Computer Security Incident Response Team (CSIRT) and/or the Security Operations Center (SOC) are trained to respond rapidly to investigate unusual activity and assess whether an incident is taking place, the security education, training, and awareness (SETA) program across the whole company will be crucial to your organization's ability to recognise and respond quickly to threats.

The readiness of your staff plays a significant role in whether or not an intrusion or other event is detected. Employees that have received proper training and are paying attention will be able to notice unusual occurrences and raise alarms with the CSIRT or SOC.

Conclusion

An organization's response to an attack can make or break the outcome. Successful incident containment and resolution is far more likely if the organization's reaction is swift and well-thought-out than if it is sluggish or ineffective. Ensuring that incident identification strategies are robust and appropriate is the first step to an effective response. The next step is to determine response and escalation.

✓ Mark Completed

← Previous
Group Share and Feedback

Next
Playbooks and Escalation →

How well did this activity help you to understand the content?

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

W06D2

Tue Jul 30

Lectures (1)

Work (8)

6 hrs

- Report on Company Types and Stakeholders
- Group Share and Feedback
- Recognizing an Incident
- Playbooks and Escalation
- Cover Letters
- The Incident Escalation Process
- Incident Escalation Research
- IR Quiz

W06D2 Schedule »