ManageEngine
EventLog Analyzer

Automating incident response with workflows

in EventLog Analyzer

www.eventloganalyzer.com

Introduction

According to the 2018 Ponemon Cost of Data Breach Study, it takes 69 days on average to contain a breach. It's alarming to consider that, even after a data breach is identified, it typically takes over two months to contain its effects. Where are organizations going wrong?

To put it simply, many organizations lack proper incident response planning. A comprehensive incident response plan clearly defines the people, processes, and technology involved in responding to a breach, so organizations can avoid confusion and resolve incidents quicker.

Technology plays a crucial role in optimizing the incident resolution cycle. Of the various tools and techniques you can use, automated incident workflows are the most useful. Each time a potential incident is detected, these workflows automatically execute a series of common remedial measures based on the type of incident, lightening the workload for your security team.

This solution brief highlights the benefits of using incident workflows and explains how you can set up automated workflows for incident alerts in EventLog Analyzer.

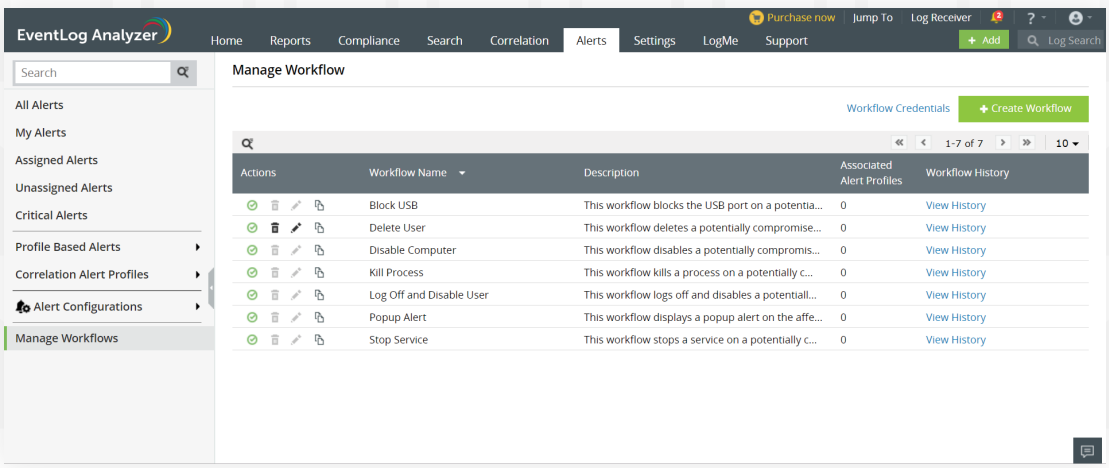
Benefits of automated incident workflows

- **Contain more damage.** In the digital world, a few seconds is all an attacker needs to cause a lot of problems. Automated responses go a long way in containing potential damage to your network.

- **Reduced alert fatigue.** A typical organization can receive hundreds of incident alerts every day. Automated workflows decrease or eliminate the time you spend responding to each alert, thereby reducing alert fatigue.

- **Optimal use of security personnel.** Since security personnel don't have to manually execute mundane repetitive actions in response to incident alerts, they'll be free to invest their time in more complex incidents or security problems that require their attention; or they may have time to focus on projects that move your business forward, rather than just keeping it on track.

Using incident workflows in EventLog Analyzer



EventLog Analyzer enables you to create and manage incident workflows and automate common incident response steps. Highlights include:

- **Workflow builder:** Use a flexible drag-and-drop interface to build your own workflows from scratch. Choose from a variety of actions you'd like to include, provide the necessary details, and arrange them in the desired order.

- **Built-in workflows:** Utilize predefined workflow templates included in the product.

- **Workflow management:** View all created workflows, enable or disable them, and view the number of associated alert profiles for each workflow.
- **Workflow tracking:** Display the history of each workflow, view the status of all its occurrences, and track details of each action within the workflow.
- **Automatic incident assignment:** Assign incidents automatically to relevant personnel who can track and handle the incidents during workflow execution and after.

Examples of EventLog Analyzer's incident workflows

Protect data from malicious insiders

While organizations set up several checks against external attackers, they tend to neglect the threat posed by malicious insiders. Employees have easy access to sensitive data. For example, they can physically access a critical server and extract files on a removable device.

To mitigate this, you can set up an alert to notify you when a USB device is plugged in to this server during non-work hours. However, an alert alone may not suffice; you may not be able to manually prevent the theft of data, as it takes just a few minutes to copy files.

Fortunately, EventLog Analyzer provides a built-in workflow that can block the USB port on a device and notify you of the status. With this workflow in place, employees won't be able to take confidential information, and you can investigate the incident at your convenience.

Disable compromised systems in your network

When an incident occurs, the first step of the investigation is to review your device logs, as all network activity leaves a log trail. Sometimes, attackers gain entry to a network by compromising a legitimate user account. They may then delete logs from the machines they breach to escape detection or hide their continued presence in the network

Thankfully, you can set up alerts to identify when security logs are cleared from a machine. In these cases, it may be too late to undo any damage already done, but you can prevent any further malicious activity. EventLog Analyzer provides a built-in workflow to log off and disable the compromised user account, effectively cutting off the attacker from your network..

Conclusion

When you draft your incident response plan, you should identify how to thwart the various types of incidents that occur, and then develop the appropriate responses to these incidents in the form of automated workflows. Automated responses provide several business benefits, including saving costs and optimizing personnel time, all while keeping your network secure from attacks.