ManageEngine
Log360

Top 5 Critical alerts you need for IT security

Introduction

Analyzing log data and identifying which security events are of concern among thousands of routine events can be a challenge, especially if you aren't sure which events to track. While IT security requirements vary for different enterprises, there are a few key security events that raise major security and compliance concerns for everyone. To help you stay on top of security, we've compiled a list of five critical events your organization should be on the lookout for.

1. Modifications made to confidential data

Securing confidential data is a primary concern for IT administrators. This data includes employee, customer, and business-sensitive data stored in files and databases. Configure your auditing process to alert you about accesses and modifications made to confidential data in files, folders, and databases to ensure only authorized individuals are performing operations. You should also be tracking changes made to data access rights, such as changes made to access control lists (ACLs).

This ensures that you not only periodically review important activity on your files, folders, and databases by scheduling audit reports, but that you'll also receive alerts when there is an event that requires your attention.

2. Repeated server shutdowns and restarts

Critical servers must always be up and running to ensure continuity of business (COB). Hackers often target these servers in an attempt to affect an organization's productivity, which makes tracking security logs generated by your server vital.

On its own, a server shutting down doesn't necessarily mean you are being attacked. But anomalous activity such as a server restarting five times within half an hour tells a more troubling story. Automatically assign this type of activity a ticket and have it sent to a designated server administrator so they can quickly analyze the event and resolve the incident.

3. Login failures and account lockouts

You already know that login activity needs to be tracked to ensure you're meeting compliance regulations. Real-time logon activity auditing can help you detect repeated logon failures which could be associated with an attack. You can also get details on accounts that are being denied access to the server and identify the cause of the lockout.

Privileged account logons are especially important to track, as these accounts are specifically targeted by hackers. It is essential to configure auditing for both successful and failed logons for these accounts so you can analyze the log data with reports and alerts.

4. Security group membership changes in Active Directory

Security groups in Active Directory provide users with access to resources. Changes made to your security groups, whether intentional or not, can create a potential security loophole. In order to secure privileged access, you need real-time alerts about critical changes being made in your Active Directory, such as changes to elevated privileged groups.

Active Directory change auditing is vital for aligning with different data security regulations and keeping internal threats under control. Real-time alerts help avert security threats, but due to the short comings of Event Viewer, you need to leverage a specialized auditing solution to achieve this.

5. Firewall rule changes

Firewalls are a critical log source for SIEM, because they have the power to allow or deny access to network traffic. By analyzing syslog data from firewalls, you can detect rising threats at the network perimeter level. While you may be watching the traffic passing through your firewalls, changes to network configurations are often overlooked. It's important to track firewall rules that are being added, deleted, or modified, as they might inadvertently grant permission to a malicious actor.

Audit logs with a SIEM solution

These are just some of the many common alert events you need to watch out for to stay on top of your organization's security. You also need alerts for malicious web server requests, application crashes, and more. A specialized auditing tool, such as a security information and event management (SIEM) solution, can help you do all of this by centralizing log data from your network infrastructure. It can then alert you about important security events that require your attention. This ensures you'll be able to quickly detect security threats and promptly respond to them.

About the author

Siddharth Sharathkumar is a computer science engineer who works in ManageEngine's product marketing team. He writes IT security articles and technical guides, presenting webinars on key security topics to educate security professionals and help enterprises solve their security challenges as well. Check out his blogs here.