ManageEngine
EventLog Analyzer

Detecting attacks with real-time log correlation

Network security attack handbook

Introduction

Network attacks are constantly changing and unpredictable. While traditional brute force attacks are still used to crack account passwords, ransomware attacks—designed to spread across your network and encrypt your data—are becoming ever more diverse. Other threats come from attackers who create backdoor accounts for themselves to perform harmful activities, or attempt to breach your web servers by raising malicious requests.

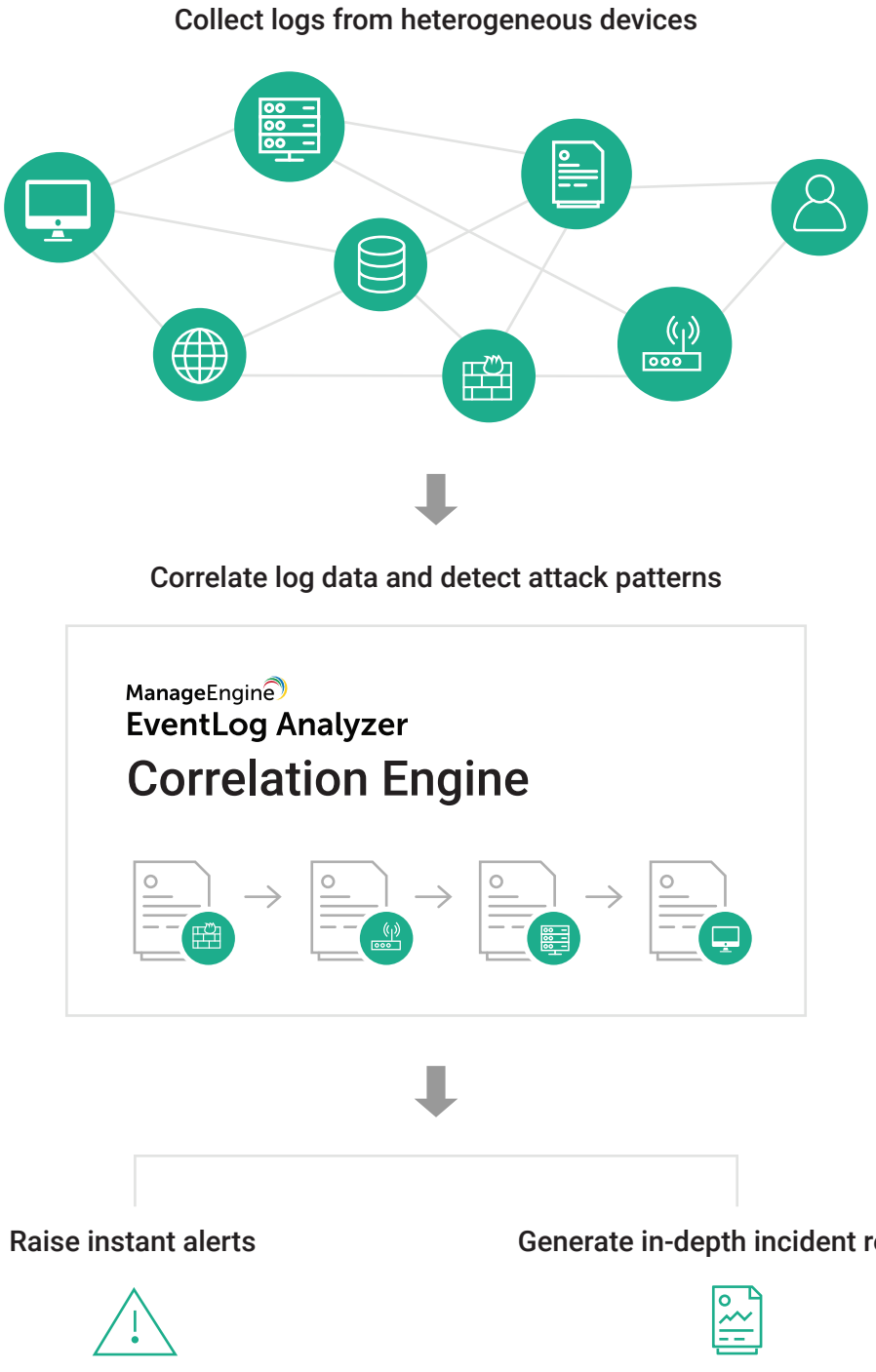
It is difficult to keep track of the variety of attacks, but breaking them down into a few concrete steps gives you common patterns of activity to look out for. Correlation is the perfect method to look for these patterns in your log data.

Detecting complex attacks by correlating log data

EventLog Analyzer's correlation engine is capable of correlating logs from sources across your network to instantly discover attack patterns that occur across disparate log sources. The solution's correlation module sends out real-time email or SMS notifications as soon as an attack is detected, raises a ticket in your help desk console for new incidents to ensure accountability, and provides in-depth incident reports that aggregate all the associated events so as to speed up remediation measures.

EventLog Analyzer currently provides 25 predefined attack rules, and it also gives you the flexibility to create or update attack definitions to suit your business environment and minimize false positives.

Correlation architecture



Correlation use cases: Network security attacks

Detecting malicious URL requests

Hackers send continuous malicious requests targeting web server application vulnerabilities, trying to exploit them and intrude your network. While the occasional malicious request may be sent randomly, detecting targeted attacks is crucial. One of the ways to detect such concentrated intrusion would be analyzing your web server logs and event logs for a series of malicious URL requests that are all from the same source within a limited time frame.

How EventLog Analyzer detects malicious URL requests: EventLog Analyzer centrally stores and analyzes your web server logs, such as IIS and Apache server logs. It then looks through that log data to detect HTTP requests with any malicious data in the URL parameter. By default, if five such malicious requests are made within two minutes, all from the same source IP address, EventLog Analyzer raises an alert and creates a report with the details of the malicious requests. If this threshold generates too many false positives or misses genuine attacks, you can always customize it to suit your network.

Detecting brute force attacks

Brute force attacks are one of the most basic but effective methods used to hack accounts on a network. In a typical brute force attack, an intruder tries to gain access to a device in your network by entering various logon credentials until one succeeds. Sophisticated brute force attacks implement automated techniques to try out different password combinations in quick succession. This trial-and-error method can prove deadly if unchecked.

How EventLog Analyzer detects brute force attacks: EventLog Analyzer scans logon events of critical servers and workstations with high priority. By default, the solution's correlation engine identifies when a single device experiences ten failed logons within ten minutes, followed by a successful logon within the next minute. If it detects such an attack, it raises an alert and creates an incident report with details about the breached device and logon events.

Detecting anomalous user account creation

Attackers often operate by first gaining access to a privileged user account, creating a temporary backdoor account for themselves, using that account to secretly access some critical resource on your network, and finally they delete this account and leave without a trace. Backdoor accounts are serious threats as they might be used for anything from data theft to privilege abuse. While the ways hackers gain initial entry to your network and the types of malicious activity they can perform vary, you can check for backdoor accounts by looking for anomalous user account creation.

How EventLog Analyzer detects backdoor accounts: EventLog Analyzer monitors privileged user activity throughout devices on your network. Its correlation engine discovers anomalies in privileged user activity by identifying any user accounts that were both created and deleted within one hour. Legitimate accounts are created or deleted in a planned manner, so a random account being created and deleted in a short time frame is definitely suspicious. EventLog Analyzer raises an alert in real time once it detects an anomalous user account, generating an incident report that includes details about the anomalous account and the privileged account used to create it.

Detecting possible ransomware activity

Ransomware is a type of malware that takes control of your critical data by encrypting it. Once ransomware infects a device on your network, it quickly starts encrypting all your files and has built-in mechanisms to spread horizontally and impact more vulnerable systems. As important as it is to take preventive measures, having a system in place to detect ransomware as quickly as possible and stop the malware from spreading is equally important. Once all your data has been encrypted, the attacker demands a ransom be paid before releasing your data. Ransomware attacks are evolving every day, which can be troubling for corporations since data is among their most valuable assets.

How EventLog Analyzer detects possible ransomware activity: EventLog Analyzer audits file operations on all Windows systems. A ransomware attack typically progresses with a newly started process modifying several files on a network device, all in an effort to encrypt the files, so EventLog Analyzer's correlation engine looks for processes that are modifying files within five minutes of being started. If a process modifies at least fifteen files within the next half hour, EventLog Analyzer raises an alert and creates an incident report that identifies the rogue process and the affected files.

Detecting possible worm activity

Several malware programs tend to take over your networks by making use of some vulnerability and proliferating from system to system. Operating systems and applications always have vulnerabilities. Some of these may be unknown and not have a patch available, while some are known and yet left widely unpatched by organizations. Hackers take advantage of these vulnerabilities and design a worm to exploit them and infect your network. In these cases, you may not be able to prevent the malware from entering your systems, but you can check for telltale signs of possible worm activity, and keep a check on its spread.

How EventLog Analyzer detects possible worm activity: EventLog Analyzer aggregates system events from all your Windows devices. Worms spread fast, hence checking for an unauthorized service being installed in quick succession on various devices across your network helps detect worm activity. EventLog Analyzer's correlation engine does this by detecting a single service which is installed on at least five devices on your network within fifteen minutes. The solution instantly alerts you and generates an in-depth report on the malicious program and infected systems so you can take quick corrective action and prevent the worm from infecting other devices on your network.