ManageEngine
Log360

WHITEPAPER

Improving incident detection with event correlation

www.manageengine.com/log360

Contents

Improving incident detection with event correlation

Introduction

For years, organizations have invested their efforts in preventing security incidents and network attacks. Today, however, their approach to cybersecurity is much different. Most organizations recognize that the concept of total prevention is simply too idealistic; no organization is completely secure from cyber attacks. Instead, organizations are shifting their focus to incident detection and response as a better method of identifying and containing security incidents. One way to improve incident detection is through event correlation.

This white paper explains the process of event correlation, how you can work correlation into the fabric of your security strategy, and how Log360's correlation module can be leveraged to fit perfectly with your security needs.

What event correlation involves

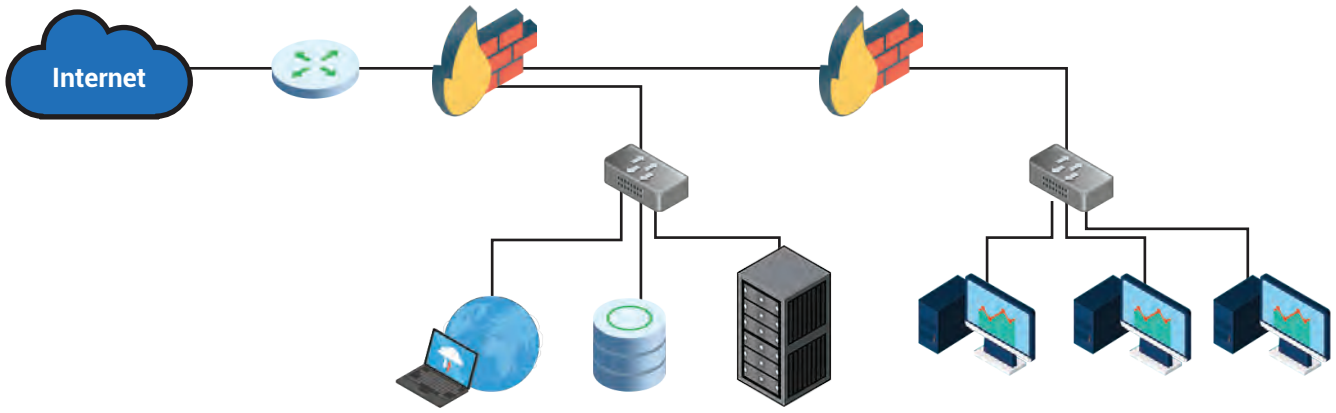


Figure 1. A typical network architecture diagram.

All enterprise networks, whether large or small, include essential components such as routers, firewalls, servers, and applications. Event correlation works with the log information from devices across your network, and discovers attack patterns. This is quite a complex task, as it involves:

- Working with millions of logs that have varied formats.
- Identifying logs related to a single incident based on common factors, such as username or device name.
- Tracking how incidents unfold by checking for the sequence and timing of events.
- Matching these incidents to known attack patterns (or correlation rules) to discover potential attacks.

By doing all this, event correlation is able to solve two of the most pressing problems with incident detection: detection time and accuracy. Here's how:

Detection time: It can often take weeks or even months to detect a threat to network resources. It took an entire two months before the shocking Equifax data breach of September 2017 was discovered, during which the personal data of 143 million consumers was compromised. Event correlation can raise alerts at two points: when the network has been breached, or when the intruder carries out their intended attack. This dramatically reduces the detection time and saves you from spending exorbitant amounts of money in the wake of an attack on your network.

Accuracy: In an attempt to capture all possible attacks, organizations set up alerts for various types of events, resulting in hundreds of alerts per day. This is often counter-productive, as it takes time to investigate all these alerts and identify the valid ones. Event correlation looks for highly specific incidents and checks for several conditions before identifying a potential security incident, thus delivering only the most valid alerts.

Log management solutions typically come equipped with correlation engines that can help you capitalize on the log information that your network generates. Event correlation adds context to network events by qualifying them with related information from other devices, allowing you to conduct precise investigations.

Event correlation in practice

Event correlation is a highly flexible technique which can be used to detect all kinds of attacks, and can be customized to suit your specific business needs. The process of integrating event correlation into your security strategy is depicted below:

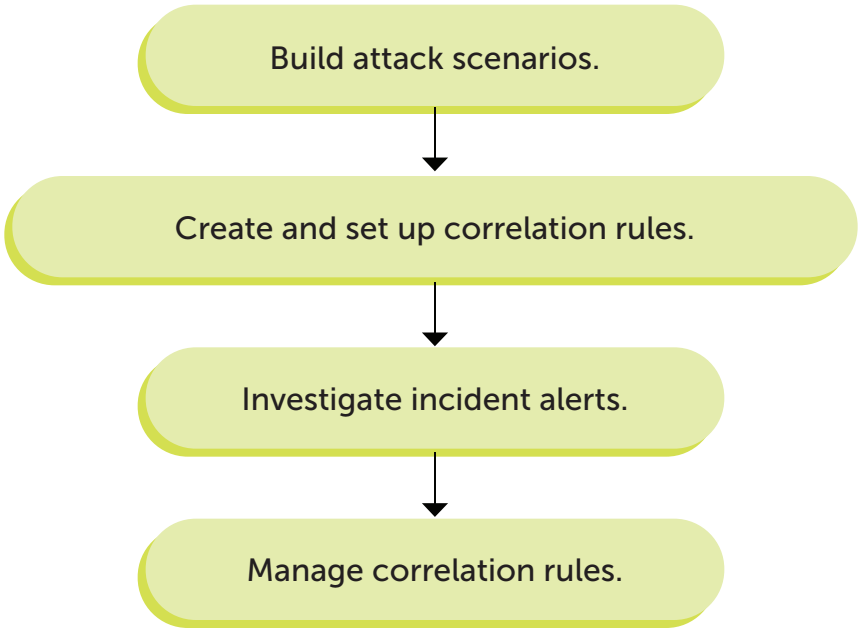


Figure 2. Event correlation in practice.

Build attack scenarios

In this stage, you need to identify all possible attack scenarios which your network is likely to face. To do this, begin by mapping out and prioritizing your network assets. For each type of device (such as database servers or Windows workstations), identify the various ways in which they can be accessed. For instance, do users need physical access to the devices or can they log on remotely? Can they be breached by an external attacker or only by a malicious insider?

Next, determine what types of attacks are possible. For example, in the case of a database server, identify the ways in which your data can be compromised (e.g. an SQL injection attack or an unauthorized backup). List out the steps and types of devices involved in each scenario.

Create and set up correlation rules

For each scenario, sequentially list out the types of logs generated by the various devices involved. If the first step involves brute-force access to a Windows workstation, the logs generated are for failed logons, followed by a successful logon. Determine the threshold limit for each log—or how many times the particular event it describes has to occur—in order to trigger an alert.

Next, determine the time frame for each step. Be sure to mention all applicable conditions. For instance, in the brute-force example, all failed logons as well as the successful one should come from the same user account. This sequence of logs, along with all associated conditions and threshold limits, is a complete description of the attack pattern and is used to form your correlation rule. Feed these rules into the correlation engine of your log management solution, and set up alerts or automated responses as needed.

Investigate incident alerts

Now that your correlation rules are up and running, you will receive real-time alerts each time an attack pattern is detected, so you can quickly conduct a forensic investigation into each detected incident. With the trail of events leading to the incident readily available, it's easy to arrive at the root cause and identify how any given attack occurred. Additionally, you can look into the specific users involved, as well as the devices or data affected to determine your response strategy. Event correlation gives you the advantage of responding quickly, so you can prevent or contain any damage to your network resources.

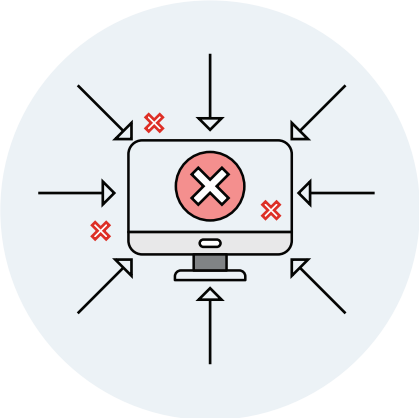
Manage correlation rules

It is important to periodically review the performance of your correlation rules. If your rule definition is too broad, you'll continue to get too many invalid alerts or false positives. On the other hand, if some parameters in your rule are too limiting, your correlation engine might miss a valid security incident.

If you notice any of this happening, simply revisit the rule definition. Add or remove events to make the rule more or less specific, and adjust the parameters (such as the thresholds and time frames) to more suitable values. This way you can continuously improve your correlation rules to ensure your network remains protected at all times.

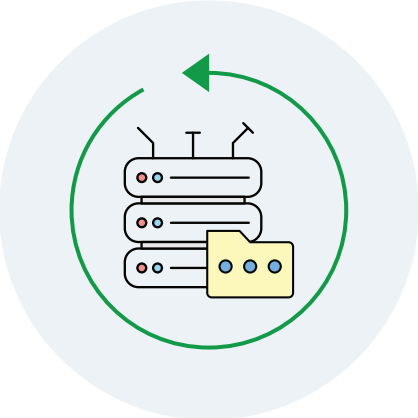
An example of building a correlation rule

Imagine that you are building possible attack scenarios for your database servers, and would like to protect against unauthorized database backups. First, you identify methods in which the attacker could access your database servers. You determine it is possible for a malicious insider to remotely gain access to your database servers, and back up the data to their local machine. Next, you want to check for brute-force access to your database server, followed by a SQL backup event. The events (or logs) in this case are:



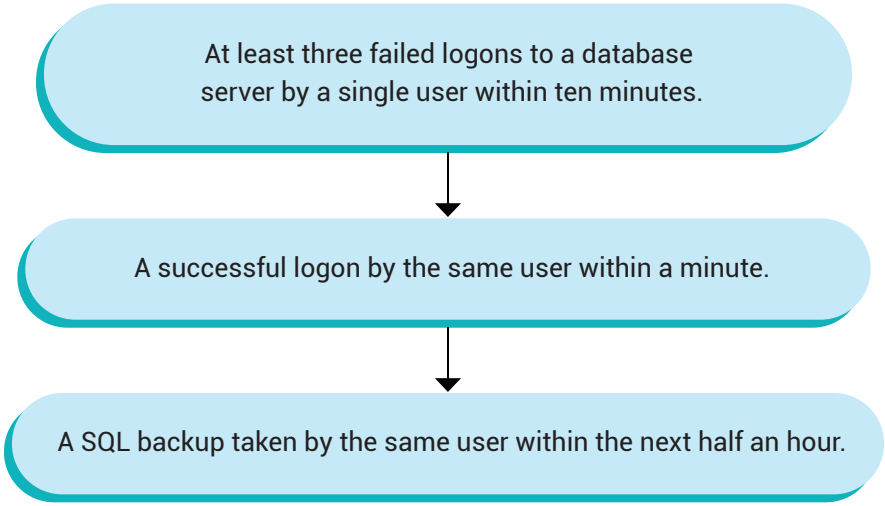
Multiple failed logons.

A successful logon.



A SQL backup.

For the above scenario, use this correlation rule:



With this rule, every time you receive an alert, you can determine that a user has potentially taken an unauthorized backup, and immediately investigate to prevent the user from misusing the data.

Event correlation with Log360

ManageEngine's security information and event management solution, Log360, comes with a powerful correlation engine that detects attack patterns instantly. It identifies the log trail of various incidents as they span out over multiple devices in your network, and alerts you of any suspicious ones. Log360 also gives you access to over 30 predefined attack patterns, which you can use to proactively tackle network threats and stay a step ahead of attackers. Key features include:

- **Correlation dashboard:** Access, customize, and schedule incident reports as needed.
- **Timeline view:** View the sequence of logs that led to each detected event, and drill down to raw log information when needed.
- **Custom rule builder:** Create custom rules, specify time frames, and use advanced filters with an intuitive drag-and-drop interface.
- **Ticket-based incident management:** Manage correlation alerts as tickets, assign them to specific technicians, and track their status using the built-in incident management

ManageEngine
Log360

ManageEngine Log360, an integrated solution that combines ADAudit Plus and EventLog Analyzer into a single console, is the one-stop solution for all log management and network security challenges. This solution offers real-time log collection, analysis, monitoring, correlation and archiving capabilities that help protect confidential data, thwart internal security threats, and combat external attacks. Log360 comes with over 1,200 predefined reports and alert criteria to help enterprises meet their most pressing security, auditing and compliance demands.

The event correlation module is an essential network security feature which helps security administrators detect various types of attacks and investigate their details, and facilitates efficient incident resolution. You can get a clear picture of how event correlation can help your organization through our personal demos.

Understand how correlation can help your organization:

Yes, I want a demo