Building better data protection with SIEM

David Howell, ManageEngine

In today’s data-rich enterprises, information is currency. This makes the requirement to protect it against external security threats more acute than ever. Already, the exponential increase in sophisticated data breaches seen in recent years has prompted IT and security administrators to move from simply being aware of the most up-to-date security solutions to proactively building their own internal security policies. Increasingly, they are also deploying security information and event management (SIEM) tools to help mitigate threats.

Proactive security

Following recent large-scale attacks, Gartner has forecast that business security is about to become much more proactive. By 2018, it predicts that 60% of large enterprises will have formal plans to address aggressive cyber-security business disruption attacks – up from none today. Instead of blocking and detecting attacks, this is likely to mean that, increasingly, businesses will devote more attention to actively detecting and responding to security threats.

Rather than the current approach of collecting and analyzing logs from critical log sources in a central location, the only way that security administrators can hope to foresee, prevent or react immediately to a security breach is to adopt a different mindset – and begin to think like a hacker.

This change of approach requires distinct skills and capabilities. In particular, security admins need to be able to predict a suspicious event, treat it as a potential data threat and defuse it before it causes any damage.

Attack patterns

The Pareto principle that, for many events, roughly 80% of the effects come from 20% of the causes is evident from common global attacking patterns used to steal data. According to Verizon, as few as nine attack patterns have given rise to as many as 80% of the security breaches in recent years.

For these reasons, it makes sense to understand how common attack patterns unfold. In turn, this can provide insight into how a data breach may occur in an organization’s network, as well as highlighting any potential security loopholes.

Figure 1: Breaches and incidents in 2013 broken down into nine major attack patterns. Source: Verizon Data Breach Investigation Report 2013.
Before choosing their attacking techniques, hackers will typically explore the business type as well as the nature of the data they want to breach. Once they have carried out this evaluation, they will attempt to invade the network infrastructure.

Rather than allowing the attack to progress, security administrators should look to contain the incident at this stage. One of the biggest challenges, however, is that administrators rarely have detailed visibility of security incidents that could indicate network intrusion. Likewise, hackers often carry out slow intrusions of the network over time that makes it virtually impossible for security administrators to correlate events. In turn, they can easily be missed.

For these reasons, a real-time detection system with a powerful correlation engine can provide an essential defence mechanism. By capturing events and analyzing them as soon as they happen on the network, a truly real-time SIEM engine will improve the speed of discovery by analyzing and correlating incidents, giving security administrators more time to cope with the unfolding incident, contain it and neutralize the damage.

About the author
David Howell is the European director of ManageEngine (www.manageengine.com) and has been with the company for over 14 years. He was part of the team that created the worldwide channel for ManageEngine and established the European operation. Howell is a highly experienced sales and marketing specialist with extensive knowledge in industries such as IT, telecommunications and electronics.

References