advenica

Secure log collection with Splunk

Do you use Splunk for log collection? Do you want to separate the log collection systems from the monitored systems? By placing a data diode between Splunk Forwarder and Splunk HEC (HTTP Event Collector), it is ensured that this communication is strictly one-way and thus prevents the central log collection from affecting the monitored systems.

Challenge

Secure log collection

Splunk is a data platform for all data needs, built for customers who have a growing need for data access, powerful analysis and automation. Today, Splunk has many users and is used in many different industries. Splunk is often used as a platform for centralised collection and analysis of log events. The systems that are monitored, i.e., create the log events, are often sensitive in themselves, or contain sensitive information.

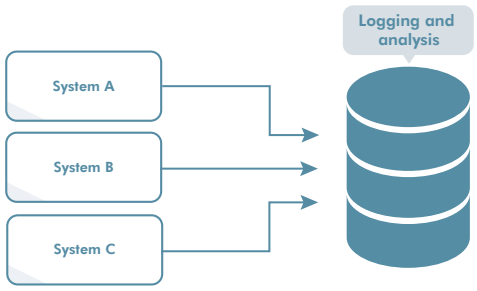

Figure 1. Secure log collection with Splunk.

Several security challenges arise when these systems are connected to a log collection system:

1. The systems are interconnected via the log collection system, which means that an incident or attack on one of the systems can spread to the other systems via the joint log collection.
2. A threat actor who succeeds in establishing themselves in the log collection system can then in the next step attack the monitored systems.

3. The system for log collection and analysis becomes a target for threat actors, risks leaking information, and exposes the monitored systems to risks in the form of intrusion and malware.

If you want a subcontractor, or maybe just another department responsible for collecting, storing, and analysing the logs in the form of a SOC (Security Operations Center), it becomes extra clear that you need to protect your systems against intrusion via the log collection.

Thus, central log collection and analysis, which is a very important part of a secure infrastructure, risks exposing the systems to new potential attacks and incidents.

Solution

One-way information flow

When using Splunk for collecting logs, the logs are usually first sent with the Syslog protocol to a Splunk Forwarder that forwards them via HTTP to a Splunk HEC Indexer (HTTP Event Collector) where the logs are stored.

To separate the monitored systems from the log management systems, a data diode is placed between the Splunk Forwarder and the Splunk HEC Indexes (see Figure 2). In this way, you are guaranteed that no incidents in the log zone can spread to the monitored systems, and at the same time the log collection can continue unhindered.

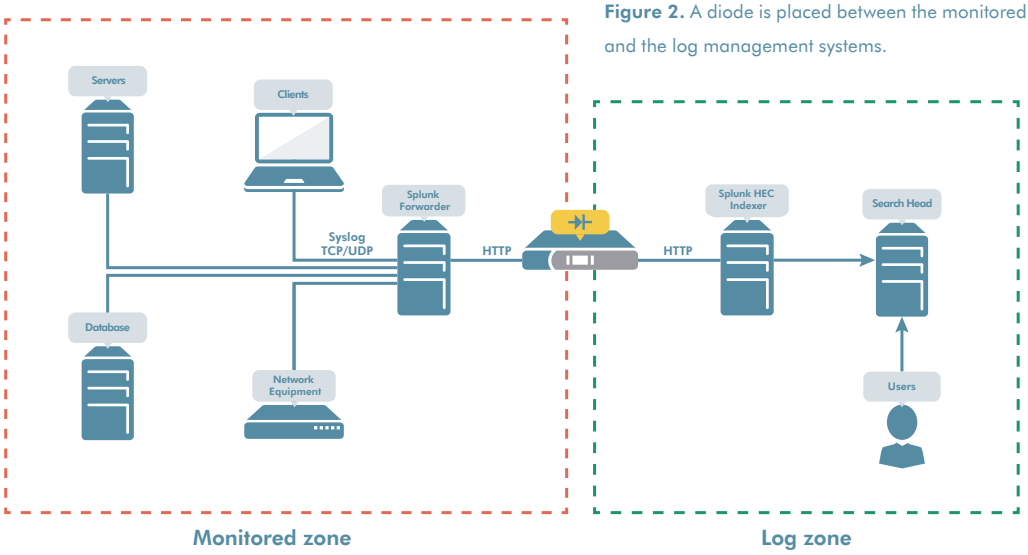

Figure 2. A diode is placed between the monitored systems and the log management systems.

The security is based on the data diode that ensures a one-way traffic flow from Splunk Forwarder to Splunk HEC Indexes.

The fact that network traffic is only allowed to flow from the monitored zone to the log zone also means that Splunk HEC Indexer cannot signal back to Splunk Forwarder if an error has occurred or if Splunk Forwarder temporarily needs to reduce the amount or frequency of logs sent to avoid risking overloading the data diode or Splunk HEC Indexer. The data diode compensates for this by limiting the traffic flow to a configurable threshold value which if it is exceeded results in the data diode sending an HTTP 429 "Too Many Requests" back to Splunk Forwarder, which then reduces the amount of logs sent to the data diode.

The data diode will otherwise respond with HTTP 200 OK back to Splunk Forwarder to indicate that the transfer went well, and then forward the HTTP message to Splunk HEC Indexer.

Should there be a problem in the communication between the data diode and the Splunk HEC Indexer, the data diode will try again a configurable number of times before the message is discarded. An internal log event is

created that tells you that there are problems with the communication.

Advantages

A secure logging zone that fulfils security demands

The data diode ensures that the transmission is one-way and contributes to an environment that meets very high security requirements. The solution eliminates the risk of a threat actor attacking the monitored systems from the log zone. You can also feel secure in outsourcing the operation and responsibility of the log zone to a subcontractor without the latter having access to the monitored systems.

advenica

Advenica provides expertise and world-class high assurance cybersecurity solutions for critical data in motion up to Top Secret classification. We enable countries, authorities and companies to raise information security and digitalise responsibly. Founded in 1993, we are EU approved to the highest level of security. Our unique products are designed, developed and manufactured in Sweden.

Read about us at advenica.com

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED