BALABIT

DATA PROTECTION WITH SYSLOG-NG

As applications log more and more events about users, personal data can increasingly be included in log messages. Here are few examples of logs with potentially sensitive data:

- Internet search logs
- Social media logins
- Geolocation data of mobile subscribers
- Credit card transaction logs

By removing or transforming certain fields within a dataset, data handlers can remove any link between the dataset and any individual. This process, also known as de-identification, allows for data analysis without infringing on an individual's rights. This technique is often used in medical research in which patients' are removed or written over with a unique identification code. If the list of unique IDs and corresponding patients is deleted, then the patients are anonymous.

Identifying Personal Data with syslog-ng

The syslog-ng Pattern Database feature can compare the contents of the received log messages to predefined message patterns. By comparing the messages to the known patterns, syslog-ng is able to identify PII and classify the type of the event described in the log message. The message classes can be customized, and for example can label the messages as user login, web search, a transaction or any other predefined event.

To make the message classification more flexible and robust, the predefined patterns can contain built-in pattern parsers: elements that match on a set of characters. For example, the NUMBER parser matches on any integer or hexadecimal number (for example 1, 123, 894054, 0xFFFF, and so on). Other pattern parsers match on various strings and IP addresses. The PatternDB feature can identify personal data in real-time and scales independently of the number of predefined patterns.

Encrypting Log Data

Encrypting log files reduces the risk that unauthorized personnel can access data. It does not, however, remove log data from the scope of regulations. Should the decryption key be acquired by a malicious actor, then all of the private data can easily be ex-filtrated.

syslog-ng uses the Transport Layer Security (TLS) protocol to encrypt the communication. TLS also allows the mutual authentication of the host and the server using X.509 certificates.

syslog-ng can store log messages securely in encrypted, compressed, and timestamped binary files, so any sensitive data is available only for authorized personnel who have the appropriate encryption key. Timestamps can be requested from external Timestamping Authorities.

Anonymization of log data with syslog-ng

User names or IP addresses (parsed by the PatternDB or some other way) can be anonymized using a hashing function so that a specific log message cannot be tied to a specific user. The tfhash template function offers several types of one-way transformations including md5, md4, sha1, sha256, and sha512.

Pseudonymization of log data with syslog-ng

Anonymization isn't feasible if a security team needs to analyze user activity and respond to suspicious behavior, as a one-way transformation of certain fields will remove any chance to identify the user. A way to avoid this situation is to store the original logs in a secure environment and forward the anonymized logs for analysis by the security team. By assigning a unique ID for each log messages to both sets of logs, the user can be re-identified. syslog-ng provides a unique ID for each log message using the use-uniqid() global option. It is generated from the HOSTID and the RCPTID in the format of HOSTID@RCPTID. It has a fixed length: 16+@+8 characters. This method of pseudonymization offers the benefit of enhanced security for the original logs while retaining the ability of security teams to access the private data only when necessary.

ABOUT BALABIT

Balabit – headquartered in Luxembourg – is a leading provider of contextual security technologies with the mission of preventing data breaches without constraining business. Founded in 2000, Balabit has more than one million users worldwide and serves 23 Fortune 100 companies.

Read more about syslog-ng

Request an evaluation

Request a callback

BALABIT
CONTEXTUAL SECURITY INTELLIGENCE

www.balabit.com