ManageEngine
Log360

USE CASE

Identifying and protecting patient health information with Log360

www.manageengine.com/log-management

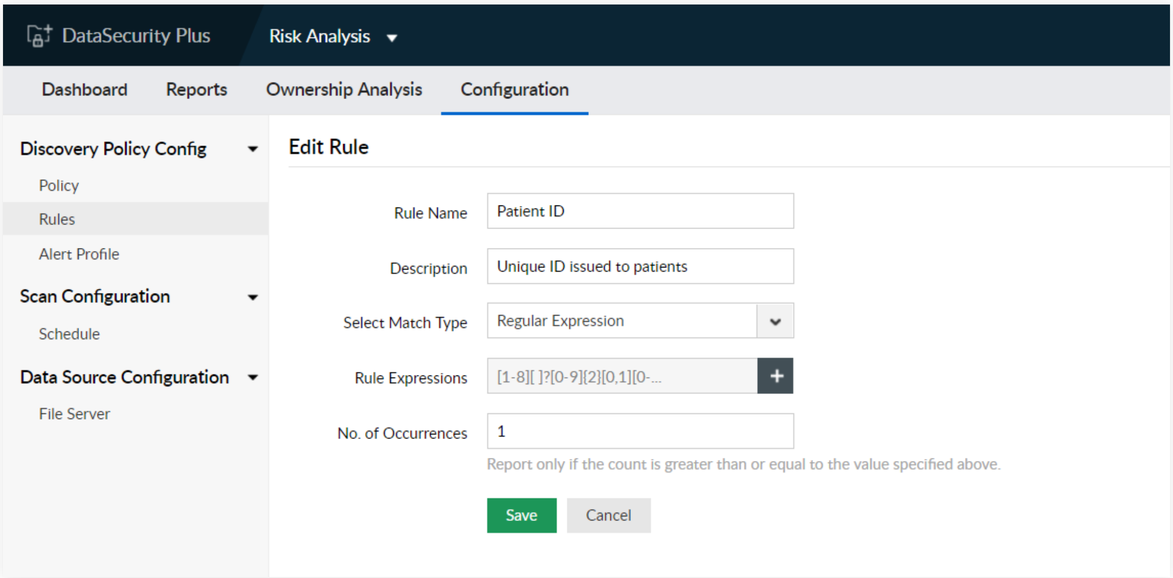
Identifying and protecting patient health information with Log360

Identifying and protecting sensitive patient information is perhaps the most critical task for a security admin in the healthcare sector. A data breach for a health care provider would be devastating for the patients due to the highly sensitive and private nature of the data involved.

With the increased adoption of telemedicine, the digital collection and processing of such highly sensitive medical information is only bound to increase. For hackers looking to steal sensitive healthcare data, the attack surface only widens in scope. How do you identify and protect this data while ensuring that it is readily available for everyday operations?

How Log360 can help

Using Log360 to identify sensitive patient information



Edit Rule

Rule Name: Patient ID

Description: Unique ID issued to patients

Select Match Type: Regular Expression

Rule Expressions: [1-8][ ]?[0-9]{2}[0,1][0-...

No. of Occurrences: 1

Report only if the count is greater than or equal to the value specified above.

Log360 has a range of predefined rules to discover sensitive data like patient information, which can be customized based on your requirements. The rules include PII such as age, address, payment information, and so on. In case the PII you want to scan for is not predefined, all you have to do is to set the parameters, and create your own rule, and Log360 will start looking for the information right away.

Preempting attacks using machine learning

Log360's machine learning (ML) algorithms can also help you preempt attack scenarios like data theft by constantly analyzing the behavior of all users and entities in a network. Any deviation from the baseline in terms of time, pattern, or count will be registered as an anomaly, and a risk score will be added.

Users with a high risk score will be added to a watch list and their actions will be closely monitored by the system. This insight can give you the edge you need to stay a step ahead of potential threats inside and outside your perimeter. This is how Log360 can help you in both the identification and protection of sensitive patient information.

ManageEngine Log360

About Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

$ Get Quote

⤓ Download