ManageEngine
Log360

USE CASE

Using Log360 to discover sensitive data in the network

www.manageengine.com/log-management

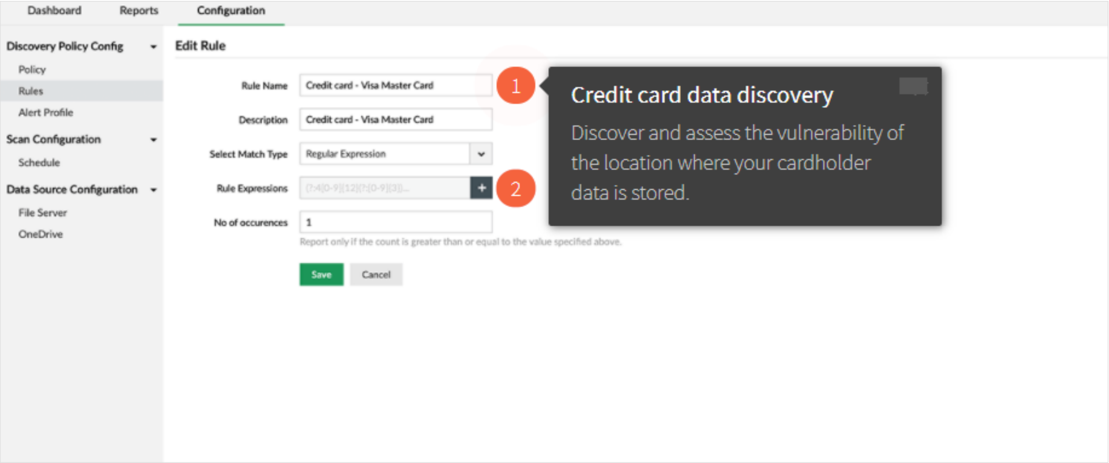
Using Log360 to discover sensitive data in the network

Do you know where all of your organization's sensitive data is stored? Are you certain that no copies of it exist in any legacy system or file server? How frequently do you audit your systems to ensure that copies of data do not exist outside secure systems?

If you're a healthcare or insurance provider, then you have to collect and store large volumes of highly sensitive information for everyday business operations. In cases like these, it is inevitable that copies of data sometimes get scattered through multiple systems in the network. Manually checking all your systems and drives to discover instances of sensitive data is a herculean task that will take essential resources away from other critical operations. But what if you had a solution that could constantly scan your systems to discover and secure all instances of sensitive data?

How Log360 can help

Discovering sensitive information in the network



Edit Rule

Rule Name: Credit card - Visa Master Card

Description: Credit card - Visa Master Card

Select Match Type: Regular Expression

Rule Expressions: (?:4[0-9]{12}(?:[0-9]{3})...

No of occurences: 1

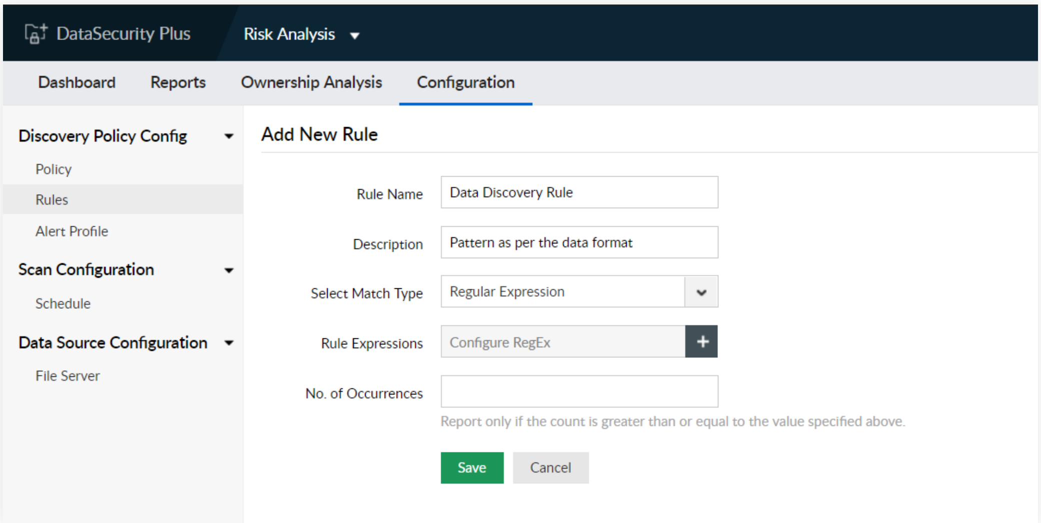
Report only if the count is greater than or equal to the value specified above.

Credit card data discovery

Discover and assess the vulnerability of the location where your cardholder data is stored.

Log360 can scan your systems for sensitive personal data or personally identifiable information (PII) stored in any device across your network. It helps you track credit card details, names, ages, locations, online identifiers, Social Security numbers, and other highly sensitive information. Once the data is located, you can then closely track all activity in the folders containing this sensitive data, and get alerts in case of unauthorized access.

Log360's data scanner uses specific keywords, numerical structures, or a combination of both to discover data like credit card numbers, Social Security numbers, and more. Log 360 has a range of predefined rules to discover PII, which can be customized based on your requirements. 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.



Add New Rule

Rule Name: Data Discovery Rule

Description: Pattern as per the data format

Select Match Type: Regular Expression

Rule Expressions: Configure RegEx

No. of Occurrences:

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

Protecting confidential data using threat detection and mitigation componentsLog360 can also protect your sensitive data from insider threats and unauthorized privilege escalation. The solution's machine learning (ML) algorithms constantly analyze the regular patterns of users and entities to detect any deviation from the baseline.

For instance, if a user copies many files or accesses information they have never accessed before, this will be logged as a pattern anomaly. For each anomaly, a certain risk score will be added. Users with high risk scores will be automatically placed on a watch list, and an alert will be sent to the security admin. Log360 not only helps with automatic discovery of sensitive data, but also helps you in protecting it from malicious actors.

Gartner's Peer Insights Voice of the Customer 2023 is out!

ManageEngine named a Customers' Choice for SIEM

Check out why

Latest Gartner Magic Quadrant for SIEM is out!

ManageEngine recognized in Gartner's Magic Quadrant for Security Information and Event Management, 2020.

Get the report

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