SIEM

Situation:
We are increasingly asked by customers whether we can also arrange Security Information & Event (SIEM) connections. In the current situation, links are created manually with external tools by executing scripts.

Before the integration of SIEM connections can take place, we need to know which functions need to be arranged.

Research questions:
Prioritize the functions, according to MoSCoW methodology, for a SIEM seen from a cyber security function.

Can a SIEM solution offer added value within your company? And why?

Supporting information:
SIEM stands for Security Information & Event Management and combines information from all possible Security and Monitoring applications in your network and ensures that you get an overview as if it were just one application.

Available functions of the current SIEM toolings on the market, after research are:
- Detect threats from within (monitoring)
- Monitoring and Alerting
- Monitoring and analyzing log data
- Dashboard overview
- File manager
- Behavioral analysis
- Integration with third parties
- Central management and storage of logs
- Real time control
- Timeline for Visual Examination
- Report generation
- Anti-spam
- Antivirus
- Auditing
- Documentation and training
- Index search data

The MoSCoW method uses a prioritization technique involving a single criteria class. Per function, a priority can be given with 4 ratings available, namely Must, Should, Could and Would.

Priority	Description
Must (have this)	Realization of this function must at least be reflected in the SIEM coupling. These are the most important requirements that must be returned in order for the product to be usable.
Should (have this if at all possible)	Realization of this function is urgently needed, but the product can still be used without it.
Could (have this if it does not affect anything else)	It is desirable that the link satisfies this function, but if it cannot be realized then it has no negative effect on the realization of the requirements that are reflected in the “Must and Should have” categories. These requirements will only be addressed if there is enough time and budget.
Would (like to have this in the future, but won’t realise it now)	These requirements will not be included in the realization within this project, but could be interesting in the future.