Rules replayed across twelve months of logs

LINDBERGH FORMATION — 16 rue de Maillé, 91310 Montlhéry, France · Companies register (RCS) Evry 817 946 114

Document issued on 09/11/2026

47 rules measured, 4 tightened · fictional document

Fictional document — demonstration example

This document is produced by the Blue Lemon Agent website to illustrate what an AI agent hands to its users. The companies, matters, amounts and people in it are invented. It has no legal, accounting or commercial value.

Fictional document, produced for demonstration. **A detection rule is the written condition that makes an alert appear.** Each of the 47 rules was replayed across **twelve months of archived logs**: alerts produced, share confirmed after investigation, and what it let through.

What the twelve-month measurement shows

Finding	Value	Reading
Rules producing 44 % of alerts	**3 of 47**	**0 confirmations in twelve months**
Rules producing 61 % of confirmations	**9 of 47**	**Fewer than 5 alerts a month each — your best rules, which the triage puts back on top**
Real incidents of the year	**3**	**All raised, all placed among the top 3 signals of their week**

The four tightened rules, costed over twelve months

Rule	Alerts before	Alerts after	Confirmations kept
Failed authentications	**84**	**19**	**3 of 3**
Out-of-hours connections	310	**41**	**2 of 2**
Share access	240	**58**	**1 of 1**
Application errors	186	**12**	No confirmation to keep
Total	**820**	**130**	**6 of 6**

The reasoning rests on no intuition: every proposed rule is written in the form of the existing ones, run across twelve months of real logs, and presented with the alerts it produces, the share confirmed and the incidents it still raises. **The choice is made on figures.**

> **Each rule is signed and withdrawn separately**, without touching the other forty-six. A rule brought into force in the evening can be withdrawn the next morning, and the count of alerts set aside stays viewable at all times.

Rules retained for going live: _____

> **Request a demo with your own documents**
> This document is a fictitious example. To see the agent work on your own documents, request a demo from its page.
> https://bluelemonagent.ai/en/entreprises/cas-usage/agent-de-cybersecurite-analyse-de-logs

Scope of this document: the service operated by Blue Lemon Agent. For an agent deployed at your premises, the applicable location is that of the architecture set out in the quotation and verified before commissioning; local execution is announced only for the configuration explicitly described and accepted in the quotation; the applicable isolation depends on the deployment mode set out in the quotation, no dedicated isolation being presumed; the encryption mechanisms in transit and at rest, their components and key management are those documented for the architecture chosen; roles and permissions are configured and accepted for the identities and systems actually connected; the events logged, their content, their retention period and who may access them are defined for the deployment chosen.

LINDBERGH FORMATION — Blue Lemon Agent — Companies register (RCS) Évry 817 946 114 —
Legal notice (in French): bluelemonagent.ai/mentions-legales