Behavioural detection — three rules proposed

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

Document issued on 09/11/2026

90-day baselines · 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. **The baseline is the habitual behaviour of an account, a machine or a time slot**, measured here over **90 rolling days**. It is computed per account and per machine: a company-wide average would show nothing.

Two behaviours no rule described

Behaviour	90-day baseline	Observation	Why no rule saw it
Service account authenticated from a workstation	**4,100 authentications, always from 2 servers**	**1 authentication from an office workstation**	**No rule states where a service account may come from**

Behaviour	90-day baseline	Observation	Why no rule saw it
Export volume of an account	**4 to 11 MB an evening**	**214 MB in 25 minutes**	**The existing fixed threshold sat well above**

The three drafted rules, measured over twelve months

Rule proposed	Firings over 12 months	Confirmed after investigation	Load on analysts
A service account authenticates from a machine absent from its list	**6**	**4**	1 every two months
An account exceeds ten times its usual export volume	**11**	**3**	1 a month
An authentication succeeds after more than 50 failures in the same window	**4**	**2**	1 a quarter
Total	**21 a year**	**9**	**Fewer than one a fortnight**

A proposed rule is only worth the measurement that comes with it. Each of the three is presented with what it produces, what it confirms and the load it imposes — so the decision to bring it into force takes minutes rather than a committee.

> **Behavioural detection complements written rules, it does not replace them.** Both mechanisms work in parallel on the same logs, and a signal from either arrives with its timestamped event chain.

Behavioural rules retained and scope: _____

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

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